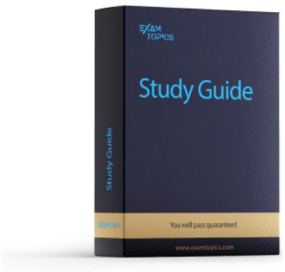
- Expert Verified, Online, **Free**.

**Prepare for your SC-100 exam with additional products**




**Study Guide**

436 PDF Pages

**$19.99**

**Buy Now**

**Video Course**

168 Lectures

**$19.99**

**Buy Now**

Custom View Settings

**Topic 1 - Question Set 1**

Question #1 *Topic 1*

Your company has a Microsoft 365 ES subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment.
You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
☞ Identify unused personal data and empower users to make smart data handling decisions.
☞ Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
☞ Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?

A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

**Correct Answer:** *C*
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:
Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.
Incorrect:
Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the day for uninterrupted, individual work.
Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export content that's responsive to your organization's internal and external investigations.
Reference:
https://docs.microsoft.com/en-us/privacy/priva/risk-management

*Community vote distribution*
C (100%)

**mung** Highly Voted 11 months, 1 week ago
I can't still believe that I have never seen such thing while going thru the official SC-100 study material provided by Microsoft.

I do have Az-500 and Az-104 so i know there are so many missing content in the mslearn, but.. this is the newest cert.. common microsoft.. and they want us to pass without using the Dump.
upvoted 15 times

**Ramye** 1 day, 6 hours ago
Priva is fairly new
upvoted 1 times

**zellck** Most Recent 7 months, 4 weeks ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/privacy/priva/risk-management
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environme and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:
- Detect overexposed personal data so that users can secure it.
- Spot and limit transfers of personal data across departments or regional borders.
- Help users identify and reduce the amount of unused personal data that you store.
upvoted 1 times

**zellck** 7 months, 4 weeks ago
https://learn.microsoft.com/en-us/privacy/priva/risk-management-notifications
Sending notifications to users can be an important component in helping your organization meet its privacy goals. The notifications are designed to:
- Bring immediate awareness to users when their actions could expose personal data to privacy risks.

- Provide remediation methods directly within the emails, so that users can take swift action to protect data at risk.
- Direct users to your organization's privacy guidelines and best practices.

Informing users of potential issues in the moment, and empowering them to remediate issues and refresh their skills, can be powerful tools f building sound data handling practices across your organization.

upvoted 1 times

**zellck** 7 months, 4 weeks ago

https://learn.microsoft.com/en-us/privacy/priva/risk-management-policy-data-minimization
Data minimization policies focus on the age of your content and how long it has been since it was last modified. Monitoring for personal dat that's still being retained in older, unused content can help you better manage your stored data and reduce risks.

Privacy Risk Management allows you to create policies to monitor data that hasn't been modified within a timeframe that you select. When a policy match is detected, you can send users email notifications with remediation options include marking items for deletion, notifying conte owners, or tagging items for further review.

upvoted 1 times

**fchahin** 9 months, 2 weeks ago

Correct answer is C

upvoted 1 times

**AJ2021** 10 months, 2 weeks ago

**Selected Answer: C**

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environme and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:

Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.

https://learn.microsoft.com/en-us/privacy/priva/risk-management

upvoted 4 times

**AJ2021** 10 months ago

Was in the Exam today

upvoted 2 times

**Einstein2** 10 months, 2 weeks ago

Microsoft Priva is the correct answer

upvoted 1 times

**rmafnc** 11 months, 2 weeks ago

Microsoft Viva Insights is a solution that can enhance privacy management in a Microsoft 365 environment. Viva Insights provides employees wi insights and guidance on how they are using collaboration tools, such as Microsoft Teams, to handle personal data. This can help employees ma smart data handling decisions and minimize privacy risks. Viva Insights can also provide notifications and guidance when personal data is sent ir Teams, helping to ensure compliance with privacy regulations. Additionally, Viva Insights can provide recommendations for mitigating privacy ri further enhancing privacy management within the working environment.

upvoted 1 times

**God2029** 11 months, 2 weeks ago

Require (Enterprise Mobility + Security E3, Office E3, or Microsoft 365 E3 or E5 license) to purchase any compliance and data governance solutic

Difference between Priva and Purview

Key features of Microsoft Priva Privacy Risk Management is to Assess your organization's privacy posture.
how much personal data exists in the environment, where it's located, how it moves, and the privacy risks detected.

Microsoft Purview automates data discovery by providing data scanning and classification for assets across your data estate.
Metadata and descriptions of discovered data assets are integrated into a holistic map of your data estate.

upvoted 1 times

**TJ001** 1 year ago

Correct Answer

upvoted 1 times

**Arya1925** 1 year ago

correct answer

upvoted 1 times

**Sec_Arch_Chn** 1 year, 1 month ago

**Selected Answer: C**

Priva is for Privacy handling & mgmt

upvoted 1 times

**Just2a** 1 year, 1 month ago

C is the corect answer

upvoted 1 times

**gaudium** 1 year, 2 months ago

Selected Answer: C

c is correct

upvoted 1 times

**SAMSH** 1 year, 3 months ago

was in 20Sep2020 exam

upvoted 2 times

**JakeCallham** 1 year, 3 months ago

stop placing this under every question, your dates are wrong as well

upvoted 9 times

**TheMCT** 1 year, 4 months ago

Selected Answer: C

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environme and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:

Detect overexposed personal data so that users can secure it.
Spot and limit transfers of personal data across departments or regional borders.
Help users identify and reduce the amount of unused personal data that you store.

upvoted 4 times

**Emmuyah** 1 year, 4 months ago

C is correct

upvoted 2 times

**tester18128075** 1 year, 4 months ago

c is correct

upvoted 1 times

**tester18128075** 1 year, 4 months ago

c and d is correct, fileshare needs onprem AD.

upvoted 1 times

**tester18128075** 1 year, 4 months ago

please ignore, not relevant

upvoted 1 times

Question #2 *Topic 1*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort.
What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Event Hubs

C. Azure Functions apps

D. Azure Logics Apps

**Correct Answer:** *D*
The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.
Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.
Incorrect:
Not C: Using Azure Functions apps would require more effort.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

*Community vote distribution*
D (100%)

**zellck** Highly Voted 7 months, 4 weeks ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launch a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

This feature can trigger consumption logic apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs. You'll also learn how to create logic apps using Azure Logic Apps.
upvoted 5 times

**fchahin** Most Recent 9 months, 2 weeks ago
S is the correct answer
upvoted 1 times

**AJ2021** 10 months, 2 weeks ago
Selected Answer: D
Workflow automation feature of Microsoft Defender for Cloud can trigger consumption Logic Apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs. To do this you would create a Logic App using Azure Logic Apps.
upvoted 2 times

**awssecuritynewbie** 10 months, 3 weeks ago
It says logics app ... i know what it means but come one Microsoft
upvoted 1 times

**TJ001** 1 year ago
Workflow Automation/Playbook (both in Sentinel and Defender for Cloud) requires Logic App
Answer D
upvoted 1 times

**Aerocertif** 1 year, 1 month ago

D is correct
upvoted 1 times

**Just2a** 1 year, 1 month ago
D is correct
upvoted 1 times

**simonseztech** 1 year, 4 months ago
Selected Answer: D
Correct
upvoted 3 times

**tester18128075** 1 year, 4 months ago
d - logic apps
upvoted 3 times

**InformationOverload** 1 year, 4 months ago
Selected Answer: D
Correct.
upvoted 1 times

**HardcodedCloud** 1 year, 4 months ago
Correct. Logic app is required for Workflow automation creation
upvoted 3 times

**prabhjot** 1 year, 4 months ago
yes logic app
upvoted 2 times

**PlumpyTumbler** 1 year, 4 months ago
Selected Answer: D
Yes. Logic Apps.
upvoted 3 times

Question #3 *Topic 1*

Your company is moving a big data solution to Azure.
The company plans to use the following storage workloads:
⇨ Azure Storage blob containers
⇨ Azure Data Lake Storage Gen2

Azure Storage file shares -
▪
⇨ Azure Disk Storage
Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Storage file shares

B. Azure Disk Storage

C. Azure Storage blob containers

D. Azure Data Lake Storage Gen2

**Correct Answer:** *CD*
C: Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.
You can scope access to Azure blob resources at the following levels, beginning with the narrowest scope:
* An individual container. At this scope, a role assignment applies to all of the blobs in the container, as well as container properties and metadata.
* The storage account.
* The resource group.
* The subscription.
* A management group.
D: You can securely access data in an Azure Data Lake Storage Gen2 (ADLS Gen2) account using OAuth 2.0 with an Azure Active Directory (Azure AD) application service principal for authentication. Using a service principal for authentication provides two options for accessing data in your storage account:
A mount point to a specific file or path

Direct access to data -
Incorrect:
Not A: To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS and then set the required domain properties on the storage account. To register your storage account with AD DS, create an account representing it in your AD DS.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

*Community vote distribution*
CD (78%) AD (22%)

**WRITER00347** Highly Voted 8 months, 3 weeks ago
The two storage workloads that support authentication by using Azure Active Directory (Azure AD) are:

A. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Explanation:
Azure Storage file shares and Azure Data Lake Storage Gen2 both support authentication using Azure AD. Azure Disk Storage and Azure Storage

blob containers do not currently support Azure AD authentication.
upvoted 6 times

**Murtuza** Most Recent 1 week, 3 days ago

Selected Answer: CD
C and D are the correct choice
upvoted 1 times

**deposros** 9 months, 1 week ago
i think c and d should be assumed to be correct
upvoted 3 times

**syedaquib77** 9 months, 1 week ago

Selected Answer: CD
Azure Files supports identity-based authentication for Windows file shares over SMB using three methods.
On-premises AD DS authentication:
Azure AD DS authentication:
Azure AD Kerberos for hybrid identities:

Which means the answer C & D is correct.
upvoted 3 times

**fchahin** 9 months, 2 weeks ago
C and D is the correct answer, I agree
upvoted 1 times

**loverboz** 9 months, 3 weeks ago

Selected Answer: AD
he two storage workloads that support authentication by using Azure Active Directory (Azure AD) in the given scenario are:

A. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Both Azure Storage file shares and Azure Data Lake Storage Gen2 support authentication through Azure AD. Azure Storage blob containers and Azure Disk Storage do not natively support authentication through Azure AD. However, Azure Disk Storage can be integrated with Azure AD usi Managed Service Identity (MSI) to authenticate to other Azure services that support Azure AD.

Therefore, the correct answers are Azure Storage file shares and Azure Data Lake Storage Gen2.
upvoted 3 times

**OCHT** 10 months, 1 week ago

Selected Answer: AD
To summarize, the correct answers to the original question are A) Azure Storage file shares and D) Azure Data Lake Storage Gen2. Both Azure Storage file shares and Azure Data Lake Storage Gen2 support authentication using Azure Active Directory (Azure AD).

Azure Storage blob containers also support authentication using Azure AD, as pointed out in one of your previous messages. Therefore, the cor answers could be A) Azure Storage file shares and C) Azure Storage blob containers, or A) Azure Storage file shares and D) Azure Data Lake Stor Gen2.

The statement "To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS" is incorre

To enable Azure Active Directory Domain Services (AD DS) authentication over SMB for Azure file shares, you need to create an AD DS domain, then join your Azure file shares to the AD DS domain. After you have completed these steps, you can use Azure AD DS to manage and authentic users and groups for access to the Azure file shares.
upvoted 2 times

**Holii** 6 months, 2 weeks ago
Azure AD DS =/= Azure AD.
It's impossible to sync a computer account directly to an Azure AD identity (without the placement of an AD DS or Azure AD DS to recognize the machine). Therefore, Azure Storage file shares cannot be authenticated strictly through Azure AD.
upvoted 3 times

**AJ2021** 10 months, 2 weeks ago

Selected Answer: CD
Correct
upvoted 1 times

**TJ001** 1 year ago
C and D correct
Files support Azure AD Domain Services and not Azure AD
upvoted 2 times

**techtest848** 1 year, 2 months ago
Can someone please explain to me why A is not a correct answer in this case??

upvoted 2 times

**techtest848** 1 year, 2 months ago

Found out why - https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview
Agree with Answer C & D

upvoted 4 times

**tester18128075** 1 year, 4 months ago

c and d are correct

upvoted 3 times

**HardcodedCloud** 1 year, 4 months ago

Selected Answer: CD

Correct

upvoted 2 times

**yf** 1 year, 4 months ago

Selected Answer: CD

correct

upvoted 2 times

**d3an** 1 year, 4 months ago

Selected Answer: CD

Correct answer

upvoted 2 times

**BillyB2022** 1 year, 4 months ago

Selected Answer: CD

C and d

upvoted 4 times

**prabhjot** 1 year, 4 months ago

correct ans

upvoted 2 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: CD

Well done.

upvoted 3 times

Question #4 *Topic 1*

HOTSPOT -

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII).

The company plans to use Microsoft Information Protection for the PII data store in Azure.

You need to recommend a solution to discover PII data at risk in the Azure resources.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

**Correct Answer:**

**Answer Area**

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Box 1: Azure Purview -

Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data.

Microsoft Purview allows you to:

Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.

Enable data curators to manage and secure your data estate.

Empower data consumers to find valuable, trustworthy data.

Box 2: Microsoft Defender for Cloud
Microsoft Purview provides rich insights into the sensitivity of your data. This makes it valuable to security teams using Microsoft Defender for Cloud to manage the organization's security posture and protect against threats to their workloads. Data resources remain a popular target for malicious actors, making it crucial for security teams to identify, prioritize, and secure sensitive data resources across their cloud environments. The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.
References:
https://docs.microsoft.com/en-us/azure/purview/overview
https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

**tester18128075** Highly Voted 1 year, 4 months ago
Purview and Defender for cloud
upvoted 15 times

**ServerBrain** Highly Voted 5 months ago
The answer is correct, but it's the first time I know about Azure Purview, I thought it should be Microsoft Purview,
upvoted 5 times

**zellck** Most Recent 7 months, 4 weeks ago
1. Azure Purview
2. Microsoft Defender for Cloud

https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide
Defender for Cloud collects, analyzes, and integrates log data from your Azure, hybrid, and multicloud resources, the network, and connected partner solutions, such as firewalls and endpoint agents. Defender for Cloud uses the log data to detect real threats and reduce false positives. A list of prioritized security alerts is shown in Defender for Cloud along with the information you need to quickly investigate the problem and the steps to take to remediate an attack.
upvoted 2 times

**Gurulee** 9 months ago
Purview and Defender for Cloud; "The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.

Classifications and labels applied to data resources in Microsoft Purview are ingested into Microsoft Defender for Cloud, which provides valuable context for protecting resources. Microsoft Defender for Cloud uses the resource classifications and labels to identify potential attack paths and security risks related to sensitive data. The resources in the Defender for Cloud's Inventory and Alerts pages are also enriched with the classifications and labels discovered by Microsoft Purview, so your security teams can filter and focus to prioritize protecting your most sensitive assets."
upvoted 1 times

**AJ2021** 10 months, 2 weeks ago
Correct:
Azure Purview
Defender for Cloud

Note the new name change as of April 2022:
Microsoft Purview—a comprehensive set of solutions from Microsoft to help you govern, protect, and manage your entire data estate. By bringing together the former Azure Purview and the former Microsoft 365 Compliance portfolio under one brand and over time, a more unified platform Microsoft Purview can help you understand and govern the data across your estate, safeguard that data wherever it lives, and improve your risk and compliance posture in a much simpler way than traditional solutions on the market today.
upvoted 3 times

**janesb** 1 year ago
as per my knowledge, it should be Purview and for alerting it should be Azure Monitor, Because Purview is integrated with Azure Monitor for Alerting.
upvoted 4 times

**TJ001** 1 year ago
correct answers , Microsoft Purview is the new name for Azure Purview
https://learn.microsoft.com/en-us/azure/defender-for-cloud/information-protection
upvoted 2 times

**Just2a** 1 year, 1 month ago
There is nothing called Azure Purview. Correct name if Microsoft Purview and MDC is correct
upvoted 2 times

**techtest848** 1 year, 1 month ago
Azure Purview and Defender for Cloud are the correct answers.

https://learn.microsoft.com/en-us/azure/purview/register-scan-azure-multiple-sources
https://learn.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

upvoted 2 times

**Xyz_40** 1 year, 2 months ago

File policy integration with MIP in Microsoft Defender for Cloud App for sensitivity labels. In this case alerts are created when match is encounte
The alert is also found in the MDCA
Ans: Azure/Microsoft Purview & Microsoft Defender for Cloud Apps

upvoted 1 times

**[Removed]** 1 year, 4 months ago

Seems like the answer is correct: Prioritize security actions by data sensitivity, https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection. As to Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure resources as well): https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azuresql

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

on second box I would select - cloud apps

upvoted 1 times

**cast0r** 1 year, 2 months ago

MS Defender for Cloud Apps is a CASB - so I dont see a "triage" action relevance

upvoted 2 times

**[Removed]** 1 year, 4 months ago

I do understand why you could suggest Defender for Cloud Apps. But as far as I can tell, there is no explicit integration with Azure (in M365 i works very well). https://docs.microsoft.com/en-us/defender-cloud-apps/azip-integration

upvoted 3 times

**prabhjot** 1 year, 4 months ago

Azure Preview is changed to Microsoft Purview ( the ans is Correct)

upvoted 4 times

Question #5 *Topic 1*

You have a Microsoft 365 E5 subscription and an Azure subscription.
You are designing a Microsoft deployment.
You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.
What should you recommend using in Microsoft Sentinel?

A. notebooks

B. playbooks

C. workbooks

D. threat intelligence

**Correct Answer:** *C*
After you connected your data sources to Microsoft Sentinel, you get instant visualization and analysis of data so that you can know what's happening across all your connected data sources. Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/get-visibility

*Community vote distribution*
C (100%)

**JG56** 1 month, 2 weeks ago
in Exam Nov 2023
upvoted 1 times

**zellck** 7 months, 4 weeks ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data
Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoptior Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsof Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to creat custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.
upvoted 3 times

**Gurulee** 9 months ago
Microsoft Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that built in to provide you with analytics for your logs and queries.
upvoted 1 times

**AJ2021** 10 months, 2 weeks ago
Selected Answer: C
Correct
upvoted 2 times

**adamsca** 10 months, 4 weeks ago
Selected Answer: C
Correct
upvoted 1 times

**TheMCT** 1 year, 4 months ago
Selected Answer: C
Correct
upvoted 3 times

**Emmuyah** 1 year, 4 months ago
Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal.

WorkBook is the correct Answer
upvoted 3 times

**tester18128075** 1 year, 4 months ago
workbooks
upvoted 1 times

**BillyB2022** 1 year, 4 months ago
**Selected Answer: C**
Workbooks

https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview
upvoted 4 times

**prabhjot** 1 year, 4 months ago
work book is correct (as it has dash board too)
upvoted 4 times

Question #6 *Topic 1*

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity.
You are informed about incidents that relate to compromised identities.
You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered.
Which Defender for Identity feature should you include in the recommendation?

A. sensitivity labels

B. custom user tags

C. standalone sensors

D. honeytoken entity tags

**Correct Answer:** *D*
Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.
Incorrect:

Not B: custom user tags -
After you apply system tags or custom tags to users, you can use those tags as filters in alerts, reports, and investigation.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-identity/entity-tags

*Community vote distribution*
D (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: D
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity
upvoted 10 times

**prabhjot** Highly Voted 1 year, 4 months ago
Ans is correct as The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicio actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive
upvoted 8 times

**JG56** Most Recent 1 month, 2 weeks ago
Selected answer: D, In exam Nov 23,
upvoted 1 times

**ltu2022** 7 months ago
was on exam 15/06/23
upvoted 2 times

**edurakhan** 7 months, 3 weeks ago
Was on exam 5/25/2023
upvoted 1 times

**zellck** 7 months, 4 weeks ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/defender-for-identity/entity-tags#honeytoken-tags
Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.
upvoted 1 times

**zellck** 7 months, 3 weeks ago
Gotten this in May 2023 exam.
upvoted 1 times

**AJ2021** 10 months, 2 weeks ago
Selected Answer: D

In MDI you can set three types of Defender for Identity entity tags: Sensitive tags, Honeytoken tags, and Exchange server tags.
For this question, D is correct: Honeytoken tags

upvoted 1 times

**tester18128075** 1 year, 4 months ago

honeytoken key

upvoted 2 times

**BillyB2022** 1 year, 4 months ago

Selected Answer: D

D. honeytoken entity tags

upvoted 2 times

Question #7 *Topic 1*

Your company is moving all on-premises workloads to Azure and Microsoft 365.
You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:
☞ Minimizes manual intervention by security operation analysts
☞ Supports triaging alerts within Microsoft Teams channels
What should you include in the strategy?

A. KQL

B. playbooks

C. data connectors

D. workbooks

**Correct Answer:** *B*
Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.
A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.
Incorrect:
Not A: Kusto Query Language is a powerful tool to explore your data and discover patterns, identify anomalies and outliers, create statistical modeling, and more.
The query uses schema entities that are organized in a hierarchy similar to SQL's: databases, tables, and columns.
Not D: Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive experiences.
Workbooks allow users to visualize the active alerts related to their resources.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

*Community vote distribution*
B (89%) 11%

**prabhjot** Highly Voted 1 year, 4 months ago
sentinel soar= playbook (logic app), so correct ans
upvoted 13 times

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC
upvoted 7 times

**JG56** Most Recent 1 month, 2 weeks ago
Selected answer: B, In exam Nov 23,
upvoted 2 times

**zellck** 7 months, 4 weeks ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents#what-are-automation-rules-and-playbooks
Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automa and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.
upvoted 1 times

**Gurulee** 9 months ago

Selected Answer: B

"Minimizes manual intervention", this requires Playbooks

upvoted 2 times

**fchahin** 9 months, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 3 times

**OCHT** 9 months, 3 weeks ago

Selected Answer: C

Data connecter

upvoted 1 times

**AJ2021** 10 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents

Playbooks are collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident. A playbook can help automa and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps. Each playbook is created for the specific subscription to which it belongs, but the Playbooks display shows you the playbooks available across any selected subscriptions.

upvoted 2 times

**adamsca** 10 months, 4 weeks ago

Selected Answer: C

Correct

upvoted 1 times

**Learing** 1 year, 2 months ago

Selected Answer: B

correct

upvoted 2 times

**tester18128075** 1 year, 4 months ago

playbooks

upvoted 3 times

**TJ001** 1 year, 4 months ago

correct answer

upvoted 2 times

Question #8 *Topic 1*

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.
All resources are backed up multiple times a day by using Azure Backup.
You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Enable soft delete for backups.

B. Require PINs for critical operations.

C. Encrypt backups by using customer-managed keys (CMKs).

D. Perform offline backups to Azure Data Box.

E. Use Azure Monitor notifications when backup configurations change.

**Correct Answer:** *BE*
Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication.
As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.
Your backups need to be protected from sophisticated bot and malware attacks. Permanent loss of data can have significant cost and time implications to your business. To help protect against this, Azure Backup guards against malicious attacks through deeper security, faster notifications, and extended recoverability.
For deeper security, only users with valid Azure credentials will receive a security PIN generated by the Azure portal to allow them to backup data. If a critical backup operation is authorized, such as ג€delete backup data,ג€ a notification is immediately sent so you can engage and minimize the impact to your business. If a hacker does delete backup data, Azure Backup will store the deleted backup data for up to 14 days after deletion.
E: Key benefits of Azure Monitor alerts include:
Monitor alerts at-scale via Backup center: In addition to enabling you to manage the alerts from Azure Monitor dashboard, Azure Backup also provides an alert management experience tailored to backups via Backup center. This allows you to filter alerts by backup specific properties, such as workload type, vault location, and so on, and a way to get quick visibility into the active backup security alerts that need attention.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware https://www.microsoft.com/security/blog/2017/01/05/azure-backup-protects-against-ransomware/ https://docs.microsoft.com/en-us/azure/backup/move-to-azure-monitor-alerts

*Community vote distribution*
AB (74%) 11% Other

**malone0001** Highly Voted 1 year, 4 months ago
Selected Answer: AB
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
upvoted 24 times

**ChaBum** 10 months, 1 week ago
B E
https://learn.microsoft.com/en-us/azure/backup/security-overview
upvoted 2 times

**simonseztech** Highly Voted 1 year, 4 months ago
Selected Answer: AB
Keyword are CONTROLS and ENSURE. So A & B both are the answer. https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-pla to-protect-against-ransomware
upvoted 17 times

**JG56** Most Recent 1 month, 2 weeks ago
Selected answer: A,B, In exam Nov 23.

upvoted 4 times

**TomasValtor** 1 month, 3 weeks ago

Answer: BD

Check this link (slide 20). https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F7%2F5%2F1%2F751682ca-5aae-405b-afa0-e4832138e436%2FRansomwareRecommendations.pptx&wdOrigin=BROWSELINK

upvoted 1 times

**itmaster** 3 months, 3 weeks ago

A, C, and E are best practices for ransomware attack:
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq
The right answer is A, soft delete, and C, enabling CMK, to be able to restore after successful attack. If the attack deletes the data, enabled soft delete will restore it. If the attack encrypts the data, the backups that are encrypted by CMK cannot be tampered with and can be decrypted and restored.

upvoted 3 times

**sbnpj** 5 months ago

Selected Answer: BE

Actually given answer is correct,
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

upvoted 1 times

**gujjudesi420** 6 months ago

Options B (Require PINs for critical operations), D (Perform offline backups to Azure Data Box), and E (Use Azure Monitor notifications when backup configurations change) are not directly related to ensuring the availability and restore capabilities of Azure Backup in the event of a ransomware attack.

Therefore, the recommended controls to include in the strategy for protecting against ransomware attacks and ensuring the usability of Azure Backup for resource restoration are:
A. Enable soft delete for backups
C. Encrypt backups by using customer-managed keys (CMKs)

upvoted 5 times

**Holii** 6 months, 2 weeks ago

A & B are the right answers.

upvoted 1 times

**Holii** 6 months, 2 weeks ago

A is a valid answer choice

B is a valid answer choice- MFA or security PIN is a recommendation for permitting an online backup be modified or erased

C is "not" a valid answer choice- it's not needed since PMKs will be used to encrypt backups by default. CMK would add an extra layer of encryption (using your own keys)

D is "not" a valid answer choice- Azure Backups should be stored in offline or off-site storage- and Azure Data Box would be the recommended tooling. However, this is more of a 'perk' and doesn't help with the restoration. Assuming you have an online data store, by going offline you're not necessarily adding anything but a more robust/faster backup transition.

E is a not a valid answer choice- I don't understand what having notifications turned on would do in the case of preventing a ransomware attack other than provide you knowledge that someone backed up your system.

upvoted 1 times

**Itu2022** 7 months ago

was on exam 15/06/23

upvoted 1 times

**JpTheCloudGuy** 5 months, 3 weeks ago

What were your choices?

upvoted 1 times

**BeefStroganoff** 7 months ago

The question says " to restore the resources in the event of a successful ransomware attack".
Which makes me think that:
B - won't make a difference, attack alreade happened
C - encrypted backups are re-encrypted by ransomware, helps with leakage prevention
E - too late for that
Which leaves only 2 options:
A - can be useful to restor what attackers deleted
D - This is a "Plan B" if "A" does not work
Which means the answers are A D
Opinions?

upvoted 2 times

**Holii** 6 months, 2 weeks ago

It's not a post-attack question, it's premeditative.
A&B.

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: AB

AB is the answer.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature-cloud
Concerns about security issues, like malware, ransomware, and intrusion, are increasing. These security issues can be costly, in terms of both mo and data. To guard against such attacks, Azure Backup now provides security features to help protect backup data even after deletion.

One such feature is soft delete. With soft delete, even if a malicious actor deletes a backup (or backup data is accidentally deleted), the backup d is retained for 14 additional days, allowing the recovery of that backup item with no data loss. The additional 14 days of retention for backup da in the "soft delete" state don't incur any cost to you.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature#authentication-to-perform-critical-operations

upvoted 2 times

**bmulvIT** 7 months, 4 weeks ago

Selected Answer: AB

Question in the exam today 19/05/2023
Got 90%

upvoted 4 times

**JpTheCloudGuy** 5 months, 3 weeks ago

What were your choices?

upvoted 1 times

**Maniact165** 8 months ago

Selected Answer: AE

AE according to https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq thoughts?

upvoted 2 times

**Holii** 6 months, 2 weeks ago

I'd agree that Azure Monitor is needed to obtain insight, but it does little to nothing to prevent an actual ransomware attack from hitting you backups once it's inside.
This would fall more in-line with Multi-User Access/PIM controls being set, in this case being MFA or a PIN for critical role operations.

upvoted 1 times

**exampasser06** 8 months, 3 weeks ago

Selected Answer: AC

A. Enable soft delete for backups and C. Encrypt backups by using customer-managed keys (CMKs) should be included in the recommendation.

upvoted 1 times

**Gurulee** 9 months ago

Selected Answer: AB

Soft delete and PIN; See step #4, #5 documented here: https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature#prevent attacks

upvoted 2 times

**loverboz** 9 months, 3 weeks ago

Selected Answer: AC

To ensure that Azure Backup can be used to restore resources in the event of a successful ransomware attack, the two controls that should be enabled are:

A. Enable soft delete for backups: This feature ensures that backups are retained even if an attacker tries to delete them. The backups can be recovered from the soft-deleted state within the retention period.
C. Encrypt backups by using customer-managed keys (CMKs): This feature ensures that backups are encrypted with keys that are under the cont of the customer, making it difficult for attackers to access and read the data.

Therefore, the correct answers are A and C.

Note: B, D, and E are not relevant controls for protecting against ransomware attacks in Azure Backup.

upvoted 1 times

**shahnawazkhot** 9 months, 2 weeks ago

The controls are needed on the backup solution - that's the key here.. In case, the primary data gets encrypted as a result of the successful ransomware attack then the backup should be in the secured state to fulfill the need. I think BE options are correct here!

upvoted 1 times

**PrettyFlyWifi** 9 months, 4 weeks ago

**Selected Answer: AE**

This is a horrible question. Check out the FAQ link below, it lists the exact items. Only problem is, it lists 3 of the available options as "best practi as per https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#what-are-the-best-practices-to-configure-and-protect-azure-backups-against-security-and-ransomware-threats

I'd say it was A and E, as they are both listed, plus I'm not leaning towards the CMK answer, as it quotes "By default, backup data at rest is encrypted using platform-managed keys (PMK). For vaulted backups, you can choose to use customer-managed keys (CMK) to own and manag the encryption keys yourself. ", so CMK is added on top.

upvoted 4 times

Question #9 *Topic 1*

HOTSPOT -

You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:

- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

You need to recommend an access security architecture for App1.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| | |
|---|---|
| To enable Azure AD authentication for App1, use: | Azure AD application<br>Azure AD Application Proxy<br>Azure Application Gateway<br>A managed identity in Azure AD<br>Microsoft Defender for App |
| To implement access requests for App1, use: | An access package in Identity Governance<br>An access policy in Microsoft Defender for Cloud Apps<br>An access review in Identity Governance<br>Azure AD Conditional Access App Control<br>An OAuth app policy in Microsoft Defender for Cloud Apps |

**Correct Answer:**

**Answer Area**

| | |
|---|---|
| To enable Azure AD authentication for App1, use: | Azure AD application<br>Azure AD Application Proxy<br>Azure Application Gateway<br>**A managed identity in Azure AD**<br>Microsoft Defender for App |
| To implement access requests for App1, use: | An access package in Identity Governance<br>An access policy in Microsoft Defender for Cloud Apps<br>**An access review in Identity Governance**<br>Azure AD Conditional Access App Control<br>An OAuth app policy in Microsoft Defender for Cloud Apps |

Box 1: A managed identity in Azure AD

Use a managed identity. You use Azure AD as the identity provider.

Box 2: An access review in Identity Governance

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

**Jasper666** Highly Voted 1 year, 4 months ago

I would go for:
a) Azure AD application (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)
b) An access package in identity governance (https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create)

upvoted 95 times

**dudus999** 5 months ago

exactly 100%

upvoted 1 times

**JohnBentass** 1 year ago
Agreed with this one, answer is A, A
upvoted 4 times

**sunilkms** 1 year ago
The requirement is pretty clear: "Enable Azure AD authentication for App1" hence A
upvoted 4 times

**Curious76** 1 year, 3 months ago
AGREE with this one
upvoted 1 times

**BillyB2022** Highly Voted 1 year, 4 months ago
Answer is incorrect

Box 1 is the Azure AD Application

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

Box 2 is Access Package in Identity Governance

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create
upvoted 22 times

**JG56** Most Recent 1 month, 2 weeks ago
Selected answer: Azure AD application REGISTRATION and Access package in Identity governance, In exam Nov 23
upvoted 4 times

**TomasValtor** 1 month, 3 weeks ago
a) Azure AD application (https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)
b) An access package in identity governance (https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create)
upvoted 1 times

**smanzana** 2 months, 3 weeks ago
Box1: Azure AD application
Box2: An access review in Identity Governance
upvoted 2 times

**cyber_sa** 3 months, 1 week ago
got this in exam 6oct23. passed with 896 marks. I answered
AZURE AD APP REGISTRATION
AN ACCESS PACKAGE IN IDENTITY GOVERNANCE
upvoted 6 times

**slobav** 3 months, 3 weeks ago
Box1: Azure AD application
Box2: An access review in Identity Governance
You can find explanation here:
https://www.youtube.com/playlist?list=PLQ2ktTy9rklhzzkSEZvDZT4QSIVUQZD-Y
upvoted 2 times

**sbnpj** 5 months, 2 weeks ago
Agree ans is AA
upvoted 2 times

**ChrisBues** 6 months, 1 week ago
Azure AD Application and Access Package in Identity Governance are the correct answers.
upvoted 2 times

**zellck** 7 months, 4 weeks ago
1. Azure AD application
2. Access package in Identity Governance

https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-aad

https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview#what-are-access-packages-and-what resources-can-i-manage-with-them
Entitlement management introduces the concept of an access package. An access package is a bundle of all the resources with the access a user needs to work on a project or perform their task. Access packages are used to govern access for your internal employees, and also users outside your organization.
upvoted 2 times

**bmulvIT** 7 months, 4 weeks ago

Question in the exam today 19/05/2023
A was "Azure AD application registration"
Got 90%

upvoted 7 times

**Gurulee** 9 months ago

Box one is self explanatory with AAD App, and box two is Access Package in Identity Governance. The giveaway was "Users will request access to App1 through the My Apps portal"
https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-scenarios#access-package-manager-allow-employees-in-your-organization-to-request-access-to-resources

upvoted 2 times

**loverboz** 9 months, 3 weeks ago

To enable Azure AD authentication for App1, use Azure AD application
To implement access requests for App1, use an access package in identity governance

To enable Azure AD authentication for App1 and provide access security, the recommended solution is to use an Azure AD application. You shou create an Azure AD application, configure the necessary permissions, and assign users and groups to the application.

An access package in identity governance should be used to implement access requests for App1. Identity Governance provides access package that allow users to request access to specific applications, groups, or roles. The request is routed to the appropriate approver, who can either approve or reject the request. Access packages can be created, managed, and assigned in the Azure portal, and can be customized to include specific access policies and permissions. This provides a streamlined and secure way to manage access to App1, ensuring that only authorized users can access sensitive data or resources.

upvoted 3 times

**PeteNZ** 10 months, 2 weeks ago

If you really delve deep, its a sneaky question. As it states your app is running in the Azure App Service, and if you read about it, you can configu AAD as the identity provider here inside the resource group: https://learn.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service-as-user

So you don't need to touch 'Azure AD application' settings at all. The app gets registered by default when following the steps above.

upvoted 2 times

**nieprotetkniteeetr** 12 months ago

Azure AD Application https://learn.microsoft.com/en-us/azure/active-directory/develop/authentication-flows-app-scenarios
An access package in Identity Governance https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-acce package-create#requests

upvoted 1 times

**awssecuritynewbie** 1 year ago

I would agree with A)

BUt for the second option, the question to be lacking good answering because in the real lie you would just permit the group under the "groups for the publish apps and add it in there but i would go with B as that is the only sensible option available.

upvoted 1 times

**TJ001** 1 year ago

A,A is correct

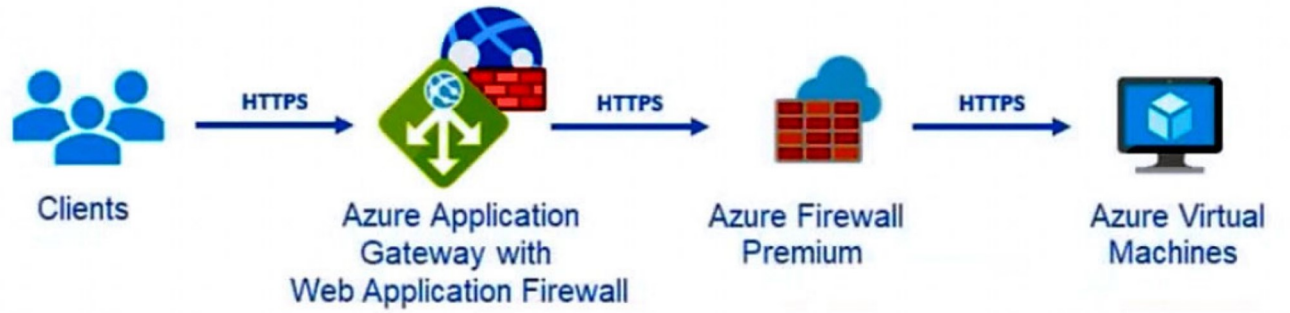
upvoted 2 times

Question #10 *Topic 1*

HOTSPOT -

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel.

The company is designing an application that will have the architecture shown in the following exhibit.




You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements:

- Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
- Use Defender for Cloud to review alerts from the virtual machines.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

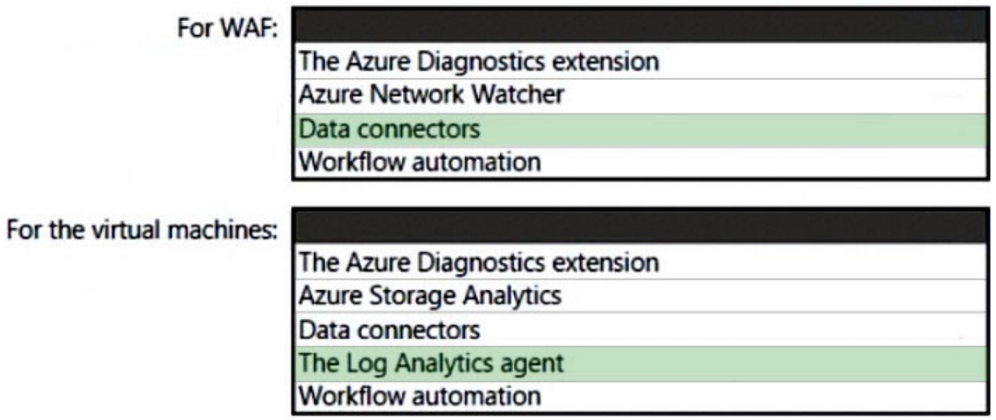
Hot Area:

**Answer Area**

| | |
|---|---|
| For WAF: | The Azure Diagnostics extension<br>Azure Network Watcher<br>Data connectors<br>Workflow automation |
| For the virtual machines: | The Azure Diagnostics extension<br>Azure Storage Analytics<br>Data connectors<br>The Log Analytics agent<br>Workflow automation |

**Correct Answer:**

**Answer Area**




Box 1: Data connectors -
Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel.
Launch a WAF workbook (see step 7 below)
The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource.
To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:
1. Select Diagnostic settings.
2. Select + Add diagnostic setting.
3. In the Diagnostic setting page (details skipped)
4. On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.
5. Select an already active workspace or create a new workspace.
6. On the left side panel under Configuration select Data Connectors.
7. Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.
8. Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven't done so previously.
9. Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent -
Use the Log Analytics agent to integrate with Microsoft Defender for cloud.

## Windows agents

| | Azure Monitor agent | Diagnostics extension (WAD) | Log Analytics agent |
|---|---|---|---|
| Environments supported | Azure<br>Other cloud (Azure Arc)<br>On-premises (Azure Arc)<br>Windows Client OS (preview) | Azure | Azure<br>Other cloud<br>On-premises |
| Agent requirements | None | None | None |
| Data collected | Event Logs<br>Performance<br>File based logs (preview) | Event Logs<br>ETW events<br>Performance<br>File based logs<br>IIS logs<br>.NET app logs<br>Crash dumps<br>Agent diagnostics logs | Event Logs<br>Performance<br>File based logs<br>IIS logs<br>Insights and solutions<br>Other services |
| Data sent to | Azure Monitor Logs<br>Azure Monitor Metrics[1] | Azure Storage<br>Azure Monitor Metrics<br>Event Hub | Azure Monitor Logs |
| Services and features supported | Log Analytics<br>Metrics explorer<br>Microsoft Sentinel (view scope) | Metrics explorer | VM insights<br>Log Analytics<br>Azure Automation<br>Microsoft Defender for Cloud<br>Microsoft Sentinel |

The Log Analytics agent is required for solutions, VM insights, and other services such as Microsoft Defender for Cloud.
Note: The Log Analytics agent in Azure Monitor can also be used to collect monitoring data from the guest operating system of virtual machines. You may choose to use either or both depending on your requirements.

Azure Log Analytics agent -
Use Defender for Cloud to review alerts from the virtual machines.
The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System
Center Operations Manager and sends collected data to your Log Analytics workspace in Azure Monitor.
Incorrect:
The Azure Diagnostics extension does not integrate with Microsoft Defender for Cloud.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Correct Answer
upvoted 19 times

**prabhjot** Highly Voted 1 year, 4 months ago
For WAF - in Sentinel we have Data Conenctor

For the VM - we have to install the Log analytics agent in teh VM in the cloud or on premises
The ans is correct
upvoted 16 times

**JG56** Most Recent 1 month, 2 weeks ago
in Exam Nov 2023 1. Data Connectors 2. Log analytics agent
upvoted 2 times

**smanzana** 2 months, 3 weeks ago
1. Data connectors
2. Log Analytics agent

upvoted 2 times

**Ario** 6 months, 2 weeks ago

correct answer

upvoted 2 times

**Holii** 6 months, 2 weeks ago

I hate it when questions mention Azure Diagnostics extension...

(As an example) Setup the Diagnostic Settings in Azure AD to stream data to a Log Analytics workspace that hosts Sentinel, you will notice that t
Azure AD connector becomes enabled.
I know this would make more sense to just say 'enable the connector', but it's technically correct as well if you stream it to LA; it works the same
if it was a data connector to Sentinel.

upvoted 2 times

**zellck** 7 months, 4 weeks ago

1. Data connectors
2. Log Analytics agent (but should use Azure Monitor Agent now)

https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/azure-web-application-firewall-waf

https://learn.microsoft.com/en-us/azure/sentinel/ama-migrate

upvoted 3 times

**zellck** 7 months, 4 weeks ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/working-with-log-analytics-agent
https://learn.microsoft.com/en-us/azure/defender-for-cloud/auto-deploy-azure-monitoring-agent

upvoted 1 times

**fchahin** 9 months, 2 weeks ago

I agree with the answers

upvoted 1 times

**TJ001** 1 year ago

Correct Answers
New name for Log Analytics Agent - Azure Monitoring Agent

upvoted 8 times

**EM1234** 9 months ago

No. It is not just a new name. Those are two completely different monitoring agents that in some cases can and need to both be installed. Th
can do similar things though.

upvoted 2 times

**panoz** 1 year, 1 month ago

Nobody will comment that the azure firewall (premium) should be BEFORE the application gateway?

upvoted 1 times

**TJ001** 1 year ago

It depends (premium SKU has application level filtering properties but not WAF).Both pattern works it depends where the public exposure is
agreed in the APP GW or FW. Have seen more patterns to keep the APP GW behind FW; in which case only the private listener of APP GW is
activated and public one even if reachable will just drop any connection requests.

upvoted 2 times

**acert976** 1 year ago

it depends on the requirement, please refer here for reference https://learn.microsoft.com/en-us/azure/architecture/example-scenario/gatew
/firewall-application-gateway#application-gateway-before-firewall

upvoted 1 times

**tester18128075** 1 year, 4 months ago

waf - Data connector
VM - LA Agent

upvoted 7 times

**Alex_Burlachenko** 1 year, 4 months ago

both are correct

upvoted 4 times

Question #11 *Topic 1*

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel.
You plan to integrate Microsoft Sentinel with Splunk.
You need to recommend a solution to send security events from Microsoft Sentinel to Splunk.
What should you include in the recommendation?

A. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

**Correct Answer:** *A*
Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP
Data Collector API.
Reference:
https://splunkbase.splunk.com/app/5312/

*Community vote distribution*
B (88%) 12%

**BPQ** Highly Voted 1 year, 4 months ago
if data need to go to splunk then event hub.
https://www.splunk.com/en_us/blog/platform/splunking-azure-event-hubs.html
upvoted 33 times

**xping85** 5 months, 3 weeks ago
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029
upvoted 2 times

**prabhjot** 1 year, 4 months ago
agree as i donot see any Splunk data connector in Sentinel and also no Azure Http PI connector in Sentinel
upvoted 6 times

**[Removed]** 1 year, 4 months ago
Event Hub is the answer:
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029
upvoted 4 times

**TJ001** 1 year ago
catch is this requires a playbook(workflow automation using Logic App) to send from Sentinel to Event Hub First...MS should have give the clarity in the options
upvoted 2 times

**yaza85** Highly Voted 12 months ago
Selected Answer: B
B. Data connectors are for receiving data not to send data
upvoted 10 times

**nils241** 1 week, 1 day ago
Thats the point .Read the Question

"...send security events FROM Microsoft Sentinel TO Splunk."

So it cant be an data connector
upvoted 1 times

**RickySmith** Most Recent 1 week ago
Selected Answer: B
Azure Event Hubs.
"to send security events from Microsoft Sentinel to Splunk"
https://www.splunk.com/en_us/blog/platform/splunking-azure-event-hubs.html - Event Hubs can process data or telemetry produced from you

Azure environment. They also provide us a scalable method to get your valuable Azure data into Splunk!
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029 - Anoth
option would be to implement a Side-by-Side architecture with Azure Event Hub.
Not a Microsoft Sentinel data connector - Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to inge
security logs 'from' Splunk platform using the Azure HTTP

upvoted 1 times

**TomasValtor** 1 month, 3 weeks ago

Answer B
Preparation : The following tasks describe the necessary preparation and configurations steps.

Onboard Azure Sentinel
Register an application in Azure AD
Create an Azure Event Hub Namespace
Prepare Azure Sentinel to forward Incidents to Event Hub
Configure Splunk to consume Azure Sentinel Incidents from Azure Event Hub
Using Azure Sentinel Incidents in Splunk

upvoted 1 times

**XtraWest** 2 months, 1 week ago

Selected Answer: B

B. Events Hubs | Azure Event Hubs can be used to buffer and route events between Microsoft Sentinel and Splunk. This option provides scalabili
and reliability in handling high volumes of security events.

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Selected Answer: B

I must say that I do think it's strange and unusual for a Microsoft exam to have a scenario where data is going from their own product to a third
party's. It's to my experience always the other way.

Therefor I suspect that it could be a typo saying "from Sentinel to Splunk".
It's more likely to be "to Sentinel from Splunk". I.e. Sentinel Data connectors

If appearing on a test make sure to read carefully...

upvoted 2 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: A

To send security events from Microsoft Sentinel to Splunk, you should use a Microsoft Sentinel data connector. Data connectors in Microsoft
Sentinel are used to export security events and logs to external systems, and Splunk is a supported destination for these connectors.

So, the correct recommendation is:

A. a Microsoft Sentinel data connector

upvoted 3 times

**ServerBrain** 5 months ago

Rule of thumb - always go with most votes!!

upvoted 1 times

**WRITER00347** 5 months, 2 weeks ago

To send security events from Microsoft Sentinel to Splunk, you would typically use Azure Event Hubs as the messaging service that can integrate
with both solutions. Azure Event Hubs can be used to collect and stream event data into various services, and it's suitable for integration with th
party SIEM solutions like Splunk.

So, the correct answer to include in the recommendation would be:

B. Azure Event Hubs.

upvoted 1 times

**MaciekMT** 6 months ago

Selected Answer: B

my 2 cents:
given the options to chose from - I would go for event hub.
I would imagine the best solution in this case would be Microsoft Graph Security API Add-On for Splunk
https://splunkbase.splunk.com/app/4564

upvoted 1 times

**ariania** 7 months, 2 weeks ago

Selected Answer: B

Indeed B

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: B

B is the answer.

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029

upvoted 1 times

**Jay_G** 8 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/export-to-siem#stream-alerts-to-qradar-and-splunk

upvoted 1 times

**Hashamkhan** 9 months ago

There is a distinction between data connectors for receiving ( <a href="https://reminiapk.org/">ai</a>) data and data connectors for sending d

upvoted 1 times

**Jayden111** 9 months ago

The recommended solution to send security events from Microsoft Sentinel to Splunk is to use a Microsoft Sentinel data connector. This is beca Microsoft Sentinel data connectors are designed to send security events to external systems, such as Splunk, in real-time. By using a data connector, you can easily configure the integration and define which events to send to Splunk based on your organization's needs. Azure Event Hubs is not the best option for this scenario because it is used to stream large amounts of data to other services and may not provide the requi security and filtering capabilities for security events. A Microsoft Sentinel workbook is not designed for sending data to external systems, but rat for visualizing and analyzing data within the Microsoft Sentinel environment. Azure Data Factory is a data integration service that allows you to create data pipelines and move data between different systems, but it is not designed for sending security events from Microsoft Sentinel to Splunk.

upvoted 3 times

**shahnawazkhot** 9 months, 2 weeks ago

I think the correct answer is B(Event Hub) and not A(Data connector).

The requirement mentioned in the question is Sentinel to send events to Splunk whereas Microsoft Sentinel Add-On for Splunk allows Azure Lo Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP Data Collector API.

For sentinel to send the events to Splunk - we need to use Event hub. Refer more here on this techcommunity link.

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029

upvoted 1 times

**Sixty** 9 months, 2 weeks ago

The question asks about sending data from Sentinel to Splunk which is Event Hub. The referenced Splunk Addon and a data connector are for importing Splunk data into Sentinel. See add-on description "Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP Data Collector API. "

upvoted 2 times

Question #12 *Topic 1*

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.
The customer discovers that several endpoints are infected with malware.
The customer suspends access attempts from the infected endpoints.
The malware is removed from the endpoints.
Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The client access tokens are refreshed.

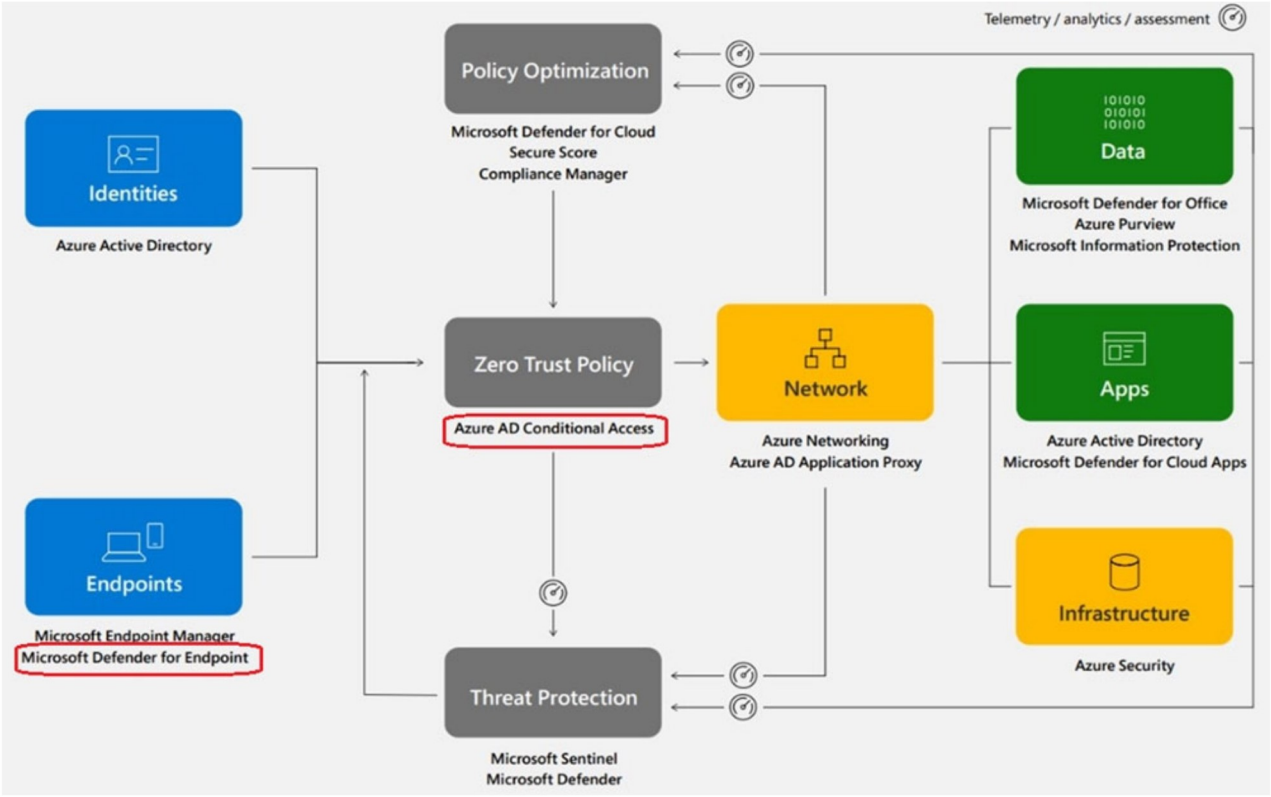
B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. Microsoft Defender for Endpoint reports the endpoints as compliant.

**Correct Answer:** *AC*
A: When a client acquires an access token to access a protected resource, the client also receives a refresh token. The refresh token is used to obtain new access/refresh token pairs when the current access token expires. Refresh tokens are also used to acquire extra access tokens for other resources.

Refresh token expiration -
Refresh tokens can be revoked at any time, because of timeouts and revocations.
C: Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. It uses a combination of endpoint behavioral sensors, cloud security analytics, and threat intelligence.
The interviewees said that ג€by implementing Zero Trust architecture, their organizations improved employee experience (EX) and increased productivity.ג€ They also noted, ג€increased device performance and stability by managing all of their endpoints with Microsoft Endpoint Manager.ג€ This had a bonus effect of reducing the number of agents installed on a user's device, thereby increasing device stability and performance. ג€For some organizations, this can reduce boot times from
30 minutes to less than a minute,ג€ the study states. Moreover, shifting to Zero Trust moved the burden of security away from users. Implementing single sign-on
(SSO), multifactor authentication (MFA), leveraging passwordless authentication, and eliminating VPN clients all further reduced friction and improved user productivity.



Note: Azure AD at the heart of your Zero Trust strategy
Azure AD provides critical functionality for your Zero Trust strategy. It enables strong authentication, a point of integration for device security, and the core of your user-centric policies to guarantee least-privileged access. Azure AD's Conditional Access capabilities are the policy decision point for access to resource
Reference:
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/
https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

*Community vote distribution*
AB (57%) BD (17%) AC (16%) 7%

**Gar23** Highly Voted 1 year, 4 months ago
Selected Answer: AB
AB looks correct to me
upvoted 29 times

**BillyB2022** Highly Voted 1 year, 4 months ago
I don't think this is correct.

Zero Trust its reffering to Conditional Access, so would be

Microsoft Intune reports the endpoints as compliant.
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

and I assume

The client access tokens are refreshed.
upvoted 12 times

**ChaBum** 10 months, 1 week ago
You're assuming endpoints are enrolled in Intune, and assuming is never a good idea in Microsoft exams.
The question says "The customer discovers ..." and "The customer suspends ...", there is nothing about Intune.
upvoted 4 times

**jasscomp** 3 months, 2 weeks ago
Conditional Access reaches out to Intune to check if a device is seen as compliant or not.
Intune will receive the risk score from Defender for Endpoint.
Devices have to be managed by Intune in order for Conditional Access to get the compliance check.
upvoted 3 times

**prabhjot** 1 year, 4 months ago
In Identity to achieve zero trust ( we have to use Conditional access policy stating a condition as that the resource is compliant ) so i guess ar correct ( whereas Intune is for configuring the compliance policy via MDM and MAM)
upvoted 2 times

**prabhjot** 1 year, 4 months ago
A second thought ( why NEW conditional access policy??) so the ans seems wrong and the correct one looks like Microsoft intune reports the endpoints as compliant and The client access token are refreshed
upvoted 10 times

**jgvh** 1 year, 3 months ago
Maybe the Conditional access already in place since he follow zero trust ? so i feel like it should be AB ?
upvoted 3 times

**TJ001** 1 year ago
how the current malware is detected should have been mentioned in the question. only clue given is currently Zero Trust is implement and each access attempt is inspected which means a conditional access policy would have been in place already to detect sign in risk ( from Azure Identity Protection) ..
upvoted 1 times

**ayadmawla** Most Recent 1 week, 2 days ago
Selected Answer: BD
BD - See: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/conditional-access?view=o365-worldwide

Defender needs to say that device is okay
InTune accepts the Defender report
Conditional Access let them in
upvoted 1 times

**ruscomike** 1 month, 2 weeks ago

Selected Answer: BD

not C: verify explicity is made by conditional access. So you already have a policy that requires enpoint is compliant
Not A. With CAE you don't need to wait access token expiration.
So I think it could be B and D:
Conditional Access verifies the compliance with Intune, cannot communicate directly with MDE. So MDE reports the endpoint as compliant. This info goes to intune that reports the endpoint as compliant and CA verify it.

upvoted 2 times

**xping85** 5 months, 3 weeks ago

if the endpoints were infected, then surely there was access to them. Therefore, the costomer must secure access to the endpoints. He can do th with CA Policies and he has to update the existing tokens. AC is the correct answer for me

upvoted 1 times

**MaciekMT** 5 months, 3 weeks ago

I would go for AC. Not B - they don't mention Intune. Not D - as one of pre-requisites for seeing devices in health report is that they need to be onboarded to Microsoft Defender for Endpoint - they don't mention that. Also, according this kb: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-health-microsoft-defender-antivirus-health?view=o365-worldwide, you can only onboard OS: Win, Mac and Linux. the question is not specific about the kind of endpoints - I think we shouldn't exclude mobile devices in this case.

upvoted 1 times

**ChrisBues** 6 months, 1 week ago

Selected Answer: AB

A - Revoking all tokens is a standard security practice.
B - CA looks at Intune for device compliance, which in turn can be influenced by Def Endpoint or other MTM partner connections.

upvoted 3 times

**BlackZeros** 6 months, 1 week ago

Selected Answer: BC

Once the conditional access is setup, the token will refresh. Token will also refresh after 8-12 hours of activity. Tokens are short lived so it cannot the method of verification for long term solution.

upvoted 1 times

**RomanV** 6 months, 2 weeks ago

Selected Answer: BD

For me it's B&D. Why? See what Microsoft says:

"The manual or automated investigation and remediation is completed and the threat is removed. Defender for Endpoint sees that there's no ris on the device and Intune assesses the device to be in a compliant state. Azure AD applies the policy, which allows access to applications."

Source: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/conditional-access?view=o365-worldwide

upvoted 3 times

**Ario** 6 months, 2 weeks ago

Well i see you guys are all wrong :
the correct answer are :
B and D

Option A In the given scenario, the conditions mentioned were focused on verifying the cleanliness and compliance of the endpoints after malw removal. So, while refreshing client access tokens can be beneficial for security, it is not one of the two specific conditions required in this scenar

upvoted 1 times

**Tictactoe** 8 months, 1 week ago

AD right

upvoted 2 times

**Gurulee** 9 months ago

Selected Answer: AB

Best answers are A, B; my decision is based on MS guideline: "Next, we can configure device-based Conditional Access policies in Intune to enfo restrictions based on device health and compliance. This will allow us to enforce more granular access decisions and fine-tune the Conditional Access policies based on your organization's risk appetite. For example, we might want to exclude certain device platforms from accessing speci apps."
https://www.microsoft.com/en-us/security/blog/2020/05/26/zero-trust-deployment-guide-for-devices/

upvoted 2 times

**Gurulee** 9 months ago

Furthermore, Intune is the appropriate choice b/c:
"A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications"

upvoted 1 times

**Xax** 9 months, 1 week ago

Before endpoint users can access the corporate applications again, the following two conditions must be met:

Microsoft Intune reports the endpoints as compliant. This means that the endpoints meet the compliance requirements set by the organization.

Microsoft Defender for Endpoint reports the endpoints as compliant. This means that the endpoints have been scanned and no threats have bee detected.

upvoted 2 times

**loverboz** 9 months, 3 weeks ago

**Selected Answer: AD**

Based on the given scenario, the following two conditions must be met before endpoint users can access the corporate applications again:

A. The client access tokens are refreshed: When access is denied due to malware infection, the client access tokens become invalid. The tokens must be refreshed after malware removal to enable access again.

D. Microsoft Defender for Endpoint reports the endpoints as compliant: As the endpoints were infected with malware, they should be scanned b an endpoint protection solution like Microsoft Defender for Endpoint. The security team should ensure that the endpoints are reported as compliant by the endpoint protection solution before allowing access again.

Therefore, options A and D are the correct answers.

upvoted 5 times

**Fal991l** 10 months, 1 week ago

**Selected Answer: BD**

Microsoft Intune is a cloud-based service that provides mobile device management (MDM) and mobile application management (MAM) capabilities, as well as conditional access and compliance policies. Microsoft Intune can help ensure that mobile devices, such as laptops and mobile phones, meet the organization's security and compliance requirements before allowing access to corporate resources.

On the other hand, Microsoft Defender for Endpoint is a unified endpoint protection platform that provides advanced threat protection and endpoint detection and response (EDR) capabilities. It can help detect and respond to threats, as well as prevent future attacks by providing security insights and recommendations.

upvoted 4 times

**Fal991l** 10 months, 1 week ago

While both solutions can help ensure the security and compliance of endpoints, they have different capabilities and focus on different aspect of endpoint security. Microsoft Intune focuses on managing and securing mobile devices, while Microsoft Defender for Endpoint focuses on threat detection and response on endpoints.

Therefore, in this scenario, the customer needs to ensure that both Microsoft Intune and Microsoft Defender for Endpoint report the endpoir as compliant before allowing access to corporate applications again, as they serve complementary roles in endpoint security.

upvoted 1 times

**God2029** 10 months, 3 weeks ago

It is A and B

The device is infected so a new token to be generated as previous token is already exposed. a refresh token can be used to generate a new acce token. So A is correct.

Zero Trust is based on 3 principles:

1. Assume Breach
2. Verify Explicitly
3. Principles of Least Privilege

Azure AD conditional access policy is already in place as it's a mandatory to verify the user explicitly, moreover question confirms this stating tha user explicitly verifies the devices, so we don't need a new one.
What's required here is to connect the device to intune and defender for endpoint and perform a scan for vulnerabilities, this will help to measu the device compliance against the known vulnerabilities if it's fixed.

upvoted 2 times

**SaadKhamis** 10 months, 3 weeks ago

You said "connect the device to intune (Answer A) and defender for endpoint (Answer D) and perform a scan". So why did choose answer A a not D?
Intune requires more setup and configuration than Defender for endpoint.

upvoted 2 times

**Fal991l** 10 months, 4 weeks ago

**Selected Answer: AD**

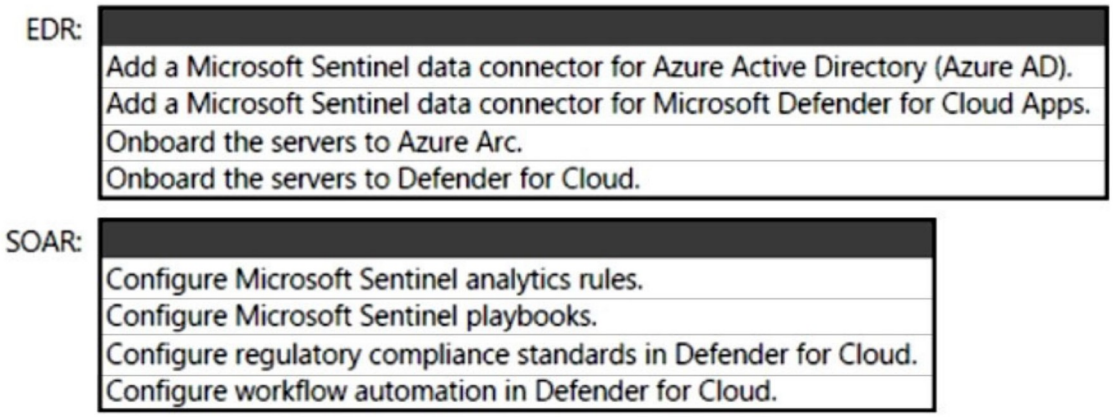
Why AD?

upvoted 1 times

Question #13 *Topic 1*

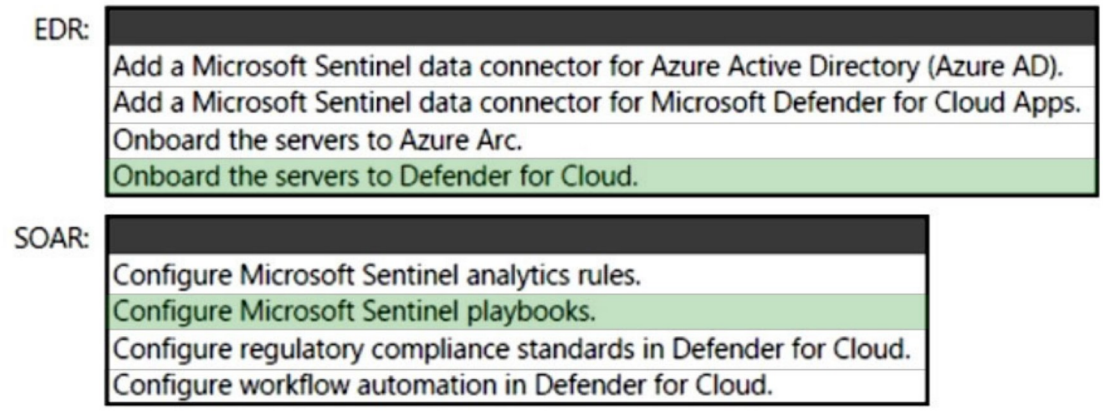
HOTSPOT -
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender,
Defender for Cloud, and Azure.
You plan to deploy Azure virtual machines that will run Windows Server.
You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.
How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

**Answer Area**




**Correct Answer:**

**Answer Area**




Box 1: Onboard the servers to Defender for Cloud.
Extended detection and response (XDR) is a new approach defined by industry analysts that are designed to deliver intelligent, automated, and integrated security across domains to help defenders connect seemingly disparate alerts and get ahead of attackers.
As part of this announcement, we are unifying all XDR technologies under the Microsoft Defender brand. The new Microsoft Defender is the most comprehensive

XDR in the market today and prevents, detects, and responds to threats across identities, endpoints, applications, email, IoT, infrastructure, and cloud platforms.
Box 2: Configure Microsoft Sentinel playbooks.
As a SOAR platform, its primary purposes are to automate any recurring and predictable enrichment, response and remediation tasks that are the responsibility of
Security Operations Centers (SOC/SecOps). Leveraging SOAR frees up time and resources for more in-depth investigation of and hunting for advanced threats.
Automation takes a few different forms in Microsoft Sentinel, from automation rules that centrally manage the automation of incident handling and response to playbooks that run predetermined sequences of actions to provide robust and flexible advanced automation to your threat response tasks.
Reference:
https://www.microsoft.com/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/become-a-microsoft-sentinel-automation-ninja/ba-p/3563377

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
I agree with the answer but the explanation and links are not very good. For SOAR read this https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of Microsoft Defender.
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide
upvoted 24 times

**JG56** Most Recent 1 month, 2 weeks ago
Given answer is correct, in exam Nov 23
upvoted 2 times

**Ario** 6 months, 2 weeks ago
Given answer is correct
upvoted 3 times

**Itu2022** 7 months ago
was on exam 15/06/23
upvoted 1 times

**zellck** 7 months, 4 weeks ago
1. Onboard the servers to Defender for Cloud
2. Configure Microsoft Sentinel playbooks

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers

https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually on-demand on entities (in preview - see below) and alerts, or set to run automatically in response to specific alerts or incidents, when triggered by an automation rule.
upvoted 1 times

**zellck** 7 months, 3 weeks ago
Gotten this in May 2023 exam.
upvoted 3 times

**AJ2021** 10 months, 2 weeks ago
Correct Answers
upvoted 2 times

**crypticdeed** 1 year ago
correct answers provided
upvoted 2 times

**omarrob** 1 year, 2 months ago
answer is correct:
https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

https://learn.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows
upvoted 1 times

**Akintade** 1 year, 3 months ago
Agree to the answer provided.
upvoted 4 times

**SAMSH** 1 year, 3 months ago

was in 20Sep2020 exam

upvoted 3 times

**tester18128075** 1 year, 4 months ago

correct

upvoted 1 times

**HardcodedCloud** 1 year, 4 months ago

Correct. But the acronym for extended detection and response is (XDR) not (EDR) which refers to Endpoint detection and response.

upvoted 3 times

**prabhjot** 1 year, 4 months ago

yes seems to be correct

upvoted 2 times

**Alex_Burlachenko** 1 year, 4 months ago

correct from my side

upvoted 3 times

Question #14 *Topic 1*

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD).
The customer plans to obtain an Azure subscription and provision several Azure resources.
You need to evaluate the customer's security environment.
What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

A. Azure AD Privileged Identity Management (PIM)

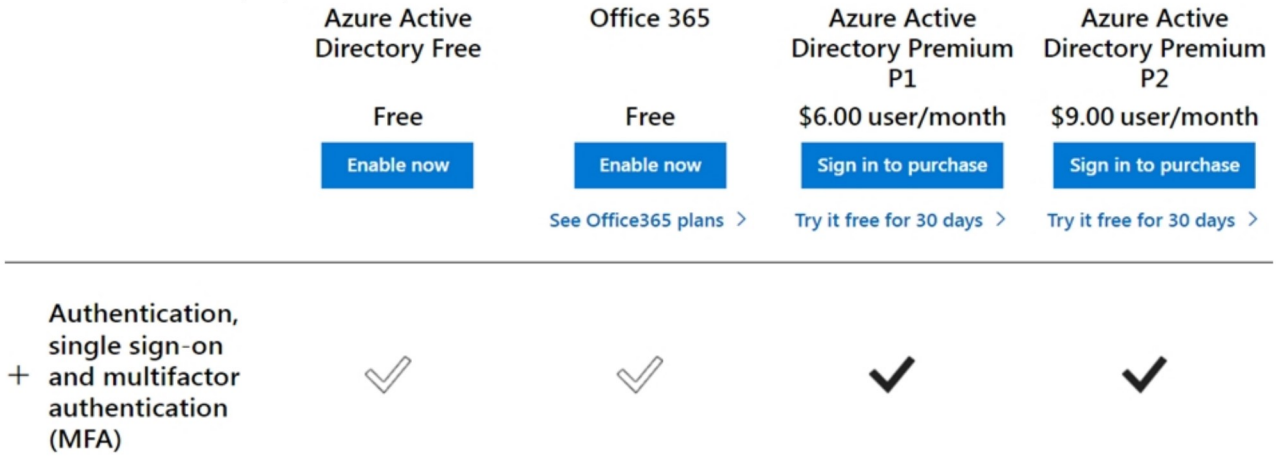
B. role-based authorization

C. resource-based authorization

D. Azure AD Multi-Factor Authentication

**Correct Answer:** *D*

Multifactor authentication (MFA), an important component of the Zero Trust Model, is missing in Azure AD Free edition.




Reference:
https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing

*Community vote distribution*
A (93%) 7%

**d3an** Highly Voted 1 year, 4 months ago
Selected Answer: A
PIM is correct. MFA can be enable on AAD Free using Security Defaults.
upvoted 36 times

**xping85** 5 months, 2 weeks ago
I agree.
The picture in the answer shows the whole package. If we look at the detailed view, we can see that MFA is already available in Azure Free.
https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing
upvoted 3 times

**jasscomp** 3 months, 2 weeks ago
Correct PIM is a P1/P2 feature and also on EMS E5 (not on EMS E3)
upvoted 1 times

**Pereiraman** Highly Voted 1 year, 3 months ago
Selected Answer: A
PIM is the correct.
upvoted 25 times

**Aedefix** Most Recent 1 week, 2 days ago
Selected Answer: A
https://www.microsoft.com/en-ca/security/business/microsoft-entra-pricing?ef_id=_k_fbefaf89b2b81fcf43d9ca1f56389099_k_&OCID=AIDcmm4bo1g8yk_SEM__k_fbefaf89b2b81fcf43d9ca1f56389099_k_&msclkid=fbefaf89b2b81fcf43d9ca1f56389099
upvoted 1 times

**Edgecrusher77** 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

**casualbork** 4 months ago

Selected Answer: A

PIM is correct. It's a P2 Feature

upvoted 2 times

**HappyMahaseth** 4 months, 3 weeks ago

PIM cis the correct one

upvoted 1 times

**Datta2023** 5 months ago

PIM is correct. Check https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing -> Identity Governance -> PIM

upvoted 1 times

**ChrisBues** 6 months, 1 week ago

Selected Answer: A

PIM is correct. MFA is free.

upvoted 1 times

**ehsanhabib** 6 months, 3 weeks ago

PIM is correct answer

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#license-requirements
Using this feature requires Azure AD Premium P2 licenses.

upvoted 1 times

**junji_m** 8 months, 3 weeks ago

IT was confusing for me but here are the links why PIM is correct...

https://learn.microsoft.com/en-us/azure/active-directory/authentication/multi-factor-authentication-faq

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements

upvoted 2 times

**AJ2021** 10 months, 2 weeks ago

Selected Answer: A

PIM is the correct.

upvoted 3 times

**Ram098** 10 months, 2 weeks ago

A
PIM correct.

upvoted 1 times

**God2029** 10 months, 3 weeks ago

Among the Given answers only PIM is the feature comes with Premium P2 license. MFA is a feature available with 365 business basic, don't requ premium license like other options listed except PIM.

upvoted 2 times

**afoui** 10 months, 3 weeks ago

Selected Answer: A

I'll go with PIM because :

Option B (role-based authorization) and Option C (resource-based authorization) are both supported in the Free edition of Azure AD, so they do not require an upgrade to the Premium edition.

Option D (Azure AD Multi-Factor Authentication) is a feature that is available in both the Free and Premium editions of Azure AD, so it does not necessitate an upgrade in this scenario.

upvoted 3 times

**buguinha** 10 months, 4 weeks ago

Selected Answer: D

MFA is correct, if you come from AAD Free you are with default and limited MFA.. After go to P1 https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

upvoted 2 times

**dbhagz** 11 months ago

The questions says M365 and not O365 - P1 is included in M. Therefore answer is PIM

upvoted 1 times

Question #15 *Topic 1*

You are designing the security standards for a new Azure environment.
You need to design a privileged identity strategy based on the Zero Trust model.
Which framework should you follow to create the design?

A. Microsoft Security Development Lifecycle (SDL)

B. Enhanced Security Admin Environment (ESAE)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)

**Correct Answer:** *C*
RaMP initiatives for Zero Trust.
To rapidly adopt Zero Trust in your organization, RaMP offers technical deployment guidance organized in these initiatives.
In particular, meet these deployment objectives to protect your privileged identities with Zero Trust.
1. Deploy secured privileged access to protect administrative user accounts.
2. Deploy Azure AD Privileged Identity Management (PIM) for a time-bound, just-in-time approval process for the use of privileged user accounts.
Note 1: RaMP guidance takes a project management and checklist approach:
* User access and productivity
1. Explicitly validate trust for all access requests

Identities -
Endpoints (devices)

Apps -

Network -
* Data, compliance, and governance
2. Ransomware recovery readiness
3. Data
* Modernize security operations
4. Streamline response
5. Unify visibility
6. Reduce manual effort
Note 2: As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and gives you a set of deployment paths to more quickly implement key layers of protection.
By providing a suggested mapping of key stakeholders, implementers, and their accountabilities, you can more quickly organize an internal project and define the tasks and owners to drive them to conclusion.
By providing a checklist of deployment objectives and implementation steps, you can see the bigger picture of infrastructure requirements and track your progress.
Incorrect:
Not B: Enhanced Security Admin Environment (ESAE)
The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is an approach to provide a secure environment for Windows Server Active Directory (AD) administrators.
Microsoft's recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP) guidance as the default recommended approach for securing privileged users. The ESAE hardened administrative forest pattern (on-prem or cloud-based) is now considered a custom configuration suitable only for exception cases listed below.
What are the valid ESAE use cases?
While not a mainstream recommendation, this architectural pattern is valid in a limited set of scenarios.
In these exception cases, the organization must accept the increased technical complexity and operational costs of the solution. The organization must have a sophisticated security program to measure risk, monitor risk, and apply consistent operational rigor to the usage and maintenance of the ESAE implementation.

Example scenarios include:
Isolated on-premises environments - where cloud services are unavailable such as offline research laboratories, critical infrastructure or utilities, disconnected operational technology (OT) environments such as Supervisory control and data acquisition (SCADA) / Industrial Control Systems (ICS), and public sector customers that are fully reliant on on-premises technology.
Highly regulated environments ג€" industry or government regulation may specifically require an administrative forest configuration.
High level security assurance is mandated - organizations with low risk tolerance that are willing to accept the increased complexity and operational cost of the solution.
Reference:
https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview https://docs.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities https://docs.microsoft.com/en-us/security/compass/esae-retirement

*Community vote distribution*

C (84%) B (16%)

**BillyB2022** Highly Voted 1 year, 4 months ago

Answer is correct.

https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan
This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

upvoted 14 times

**blopfr** 1 year, 2 months ago

agree with the answer but this link provide the zero trust view on it (not the admin access only)
https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 1 times

**casualbork** Most Recent 4 months ago

Selected Answer: C

as pointed out multiple times, C (RaMP) is the correct answer.

upvoted 3 times

**Ario** 6 months, 2 weeks ago

B is correct

upvoted 1 times

**Ario** 6 months, 2 weeks ago

Sorry guys , Answer C is correct based on Microsoft new recommendation :Microsoft's recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP)

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview
As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and gives you a set of deployment paths to more quickly implement key layers of protection.

upvoted 1 times

**OCHT** 10 months, 1 week ago

Selected Answer: B

I think B. RaMP is not a recognized security framework or model

upvoted 3 times

**Gurulee** 9 months ago

Thinking of RaMP and the definition of a framework may help: "a framework is a real or conceptual structure intended to serve as a support guide for the building of something that expands the structure into something useful."

upvoted 1 times

**AJ2021** 10 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 3 times

**MichaelMu** 10 months, 3 weeks ago

C

Rapid Modernization Plan (RaMP) is a framework developed by Microsoft to help organizations quickly implement key layers of protection base on Zero Trust principles. Unlike traditional deployment guidance, RaMP guidance takes a project management and checklist approach to provid set of deployment paths and a checklist of deployment objectives and implementation steps. The framework provides a suggested mapping of stakeholders, implementers, and their accountabilities to help organizations organize internal projects and define tasks and owners to drive ther to completion. RaMP guidance helps organizations see the bigger picture of infrastructure requirements and track progress.

upvoted 2 times

**Sec_Arch_Chn** 1 year, 1 month ago

Selected Answer: C

Rapid Modernization Plan (RaMP) checklist helps you establish a security perimeter for cloud applications and mobile devices that uses identity the control plane and explicitly validates trust for user accounts and devices before allowing access, for both public and private networks - Sour https://learn.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities

upvoted 2 times

**tester18128075** 1 year, 4 months ago

RaMP is correct

upvoted 2 times

**HardcodedCloud** 1 year, 4 months ago

Selected Answer: C

Rapid Modernization Plan (RaMP)

upvoted 3 times

**prabhjot** 1 year, 4 months ago

Rapid Modernization Plan (RaMP) is coorect ans - ( as per MCRA ) RaMP helps to achieve ZERO Trust

upvoted 2 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: C

C, BillyB provides a great link. SDL and OSA are SDLC related. ESAE has been retired and replaced by RAMP.

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

correct

upvoted 1 times

Question #16 *Topic 1*

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All on-premises servers in the perimeter network are prevented from connecting directly to the internet.
The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend solutions to meet the following requirements:
☞ Ensure that the security operations team can access the security logs and the operation logs.
☞ Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two solutions should you include in the recommendation? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a custom collector that uses the Log Analytics agent

B. the Azure Monitor agent

C. resource-based role-based access control (RBAC)

D. Azure Active Directory (Azure AD) Conditional Access policies

**Correct Answer:** *BC*
A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.
Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.
You can connect your data sources to Microsoft Sentinel using custom log formats.
C: Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.
Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel. The different roles give you fine-grained control over what Microsoft Sentinel users can see and do. Azure roles can be assigned in the Microsoft Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel inherits.
Incorrect:
A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.
Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.
You can connect your data sources to Microsoft Sentinel using custom log formats.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview https://docs.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG https://docs.microsoft.com/en-us/azure/sentinel/roles

*Community vote distribution*
BC (77%) AC (23%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
These answer options have been abridged. Other dumps say:
A. Create a custom collector that uses the Log Analytics agent.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Configure Azure Active Directory (Azure AD) Conditional Access policies.
upvoted 17 times

**PlumpyTumbler** 1 year, 4 months ago
Given the expanded answers B and C are the clear best choices.
B - this use case is spelled out in exact detail. This is must be the exact wording that the question was created from https://docs.microsoft.co /en-us/azure/sentinel/best-practices-data#on-premises-windows-log-collection
C - https://docs.microsoft.com/en-us/azure/sentinel/resource-context-rbac#scenarios-for-resource-context-rbac
upvoted 16 times

**JakeCallham** 1 year, 2 months ago
The link for B also states this Servers do not connect to the internet, Use the Log Analytics gateway Configuring a proxy to your agent requires extra firewall rules to allow the Gateway to work.
upvoted 3 times

**Gurulee** 9 months ago

"The Log Analytics gateway supports: Windows computers on which either the Azure Monitor Agent or the legacy Microsoft Monitorir Agent is directly connected to a Log Analytics workspace in Azure Monitor. Both the source and the gateway server must be running tl same agent. You can't stream events from a server running Azure Monitor agent through a server running the gateway with the Log Analytics agent."

upvoted 1 times

**Sorrynotsorry** Highly Voted 1 year, 4 months ago

Selected Answer: BC

I agree with B & C after the expaned version of the answers

upvoted 16 times

**Murtuza** Most Recent 1 week, 3 days ago

Requires splitting operation and security logs Use the Microsoft Monitor Agent or Azure Monitor Agent multi-home functionality

upvoted 1 times

**Azerty1313** 1 month, 1 week ago

Really don't get the point of B. Why?
It all depends on how you read the question.
There is a need for 2 different teams to see the logs. -> RBAC
Second part is only from the perimeter. I read this as the operation people need to be at a certain place before they can read it -> conditional access
So I would go for C & D.

upvoted 1 times

**Azerty1313** 1 month ago

reading it again it will probably be the servers in the perimeter network

upvoted 1 times

**BlackZeros** 6 months, 1 week ago

the actual multiple-choice answers did not make much sense until Plumpy pointed out the full wording.

upvoted 3 times

**Ario** 6 months, 2 weeks ago

A and B

upvoted 1 times

**Ario** 6 months, 2 weeks ago

Was A TYPO A AND C

upvoted 1 times

**imsidrai** 6 months, 2 weeks ago

what is Resource Based Access control??
Its Role based Access control,

upvoted 1 times

**Avanade2023** 7 months, 2 weeks ago

I am sorry, maybe my understand is wrong. why B is the answer like C as a complete solution? the Question condition is "Each correct answer presents a complete solution". I think that Azure Monitor agent is needed of cause, but it is for collecting the log data, doesn't meet the solutior requirements to control access. If the question condition is "Each correct answer presents part of the solution", I will agree with B & C.

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources#custom-logs
For some data sources, you can collect logs as files on Windows or Linux computers using the Log Analytics custom log collection agent.

https://learn.microsoft.com/en-us/azure/sentinel/resource-context-rbac
Typically, users who have access to a Microsoft Sentinel workspace also have access to all the workspace data, including security content. Administrators can use Azure roles to configure access to specific features in Microsoft Sentinel, depending on the access requirements in their team.

upvoted 1 times

**AJ2021** 10 months, 2 weeks ago

Selected Answer: BC

B: Tricky one, no internet on on-premise servers, you need to use the Log Analytics gateway in Azure Monitor.
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/gateway
C: RBAC

upvoted 2 times

**God2029** 10 months, 3 weeks ago

The legacy Log Analytics agent will be deprecated by August 2024, Microsoft recommends to migrate/use Azure Monitor Agent. So if both Log analytics agent and Azure monitor Agents are there in the answer choose the latter.

upvoted 4 times

**rmafnc** 11 months, 2 weeks ago

A. a custom collector that uses the Log Analytics agent
C. resource-based role-based access control (RBAC)

upvoted 2 times

**awssecuritynewbie** 11 months, 2 weeks ago

I agree With the answers, but the explanation is very poor. I would really improve on that.

upvoted 1 times

**hpl1908** 11 months, 2 weeks ago

Selected Answer: AC

A & C is the right answer

upvoted 2 times

**hpl1908** 11 months, 2 weeks ago

To meet the requirements of ensuring that the security operations team can access the security logs and the operation logs, and ensuring tha the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network, you can recommend the following solutions:

A. A custom collector that uses the Log Analytics agent - this will allow you to collect security logs and operation logs from on-premises serv and Microsoft 365, and send the logs to Microsoft Sentinel.

C. Resource-based role-based access control (RBAC) - this will allow you to assign specific access permissions to different teams based on th resources they need to access. For example, you can assign the security operations team access to both the security logs and the operation l and assign the IT operations team access only to the operation logs, including the event logs of the servers in the perimeter network.

upvoted 1 times

**Fal991l** 10 months, 2 weeks ago

That's from ChatGPT.

upvoted 1 times

**Discuss4certi** 11 months, 3 weeks ago

Selected Answer: BC

RBAC is a requirement to set up the permissions, answer B is clarified with the new expanded answers provide by Plumpytumbler on top.

upvoted 2 times

**Rocky83** 1 year ago

Selected Answer: AC

RBAC for sure.
What about the Azure Monitor? This needs internet connection., right?

upvoted 2 times

**JakeCallham** 1 year, 3 months ago

Selected Answer: AC

Answer c Rbac for sure. B makes meldpunt so I'll go for A

upvoted 2 times

**TJ001** 1 year ago

custom collector would need internet as well.

upvoted 1 times

**JakeCallham** 1 year, 3 months ago

Yeah B azure monitor needs public internet access so can't be the correct answer

upvoted 1 times

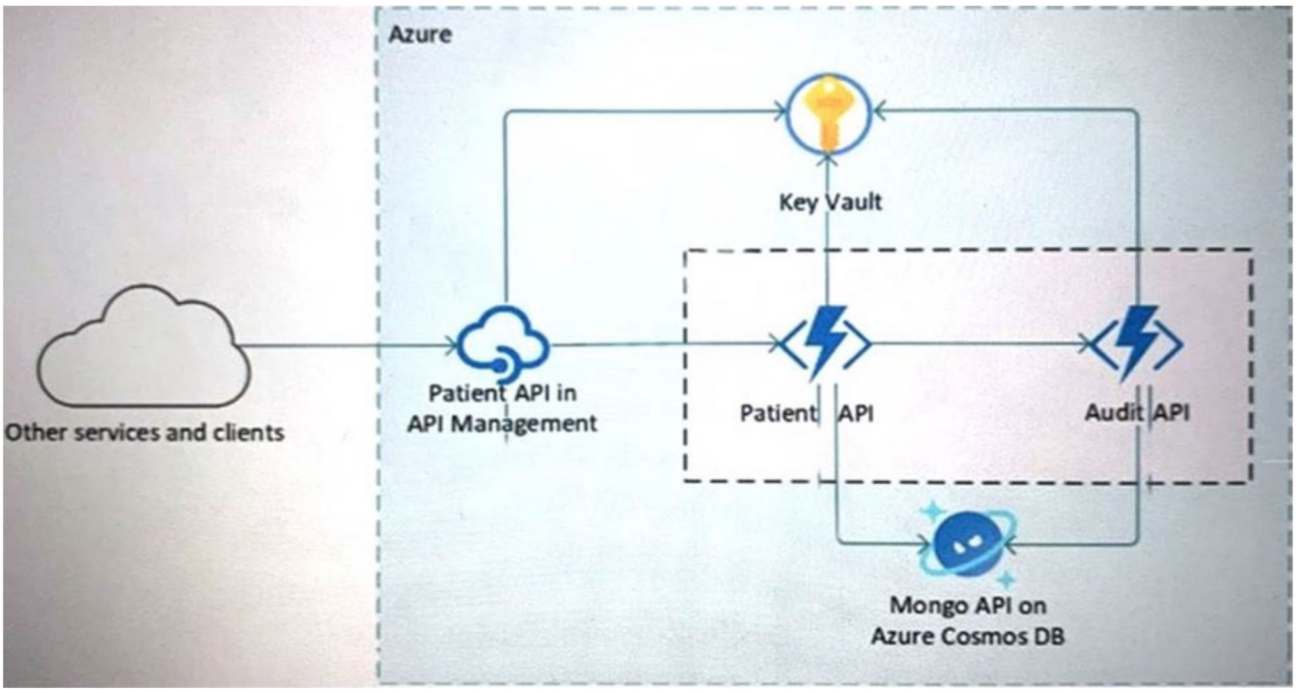
**Bubsator** 1 year, 3 months ago

ou're wrong. It is possible to configure communication with Azure Automation and Azure Monitor by using the Log Analytics gateway wh computers that are directly connected or that are monitored by Operations Manager have no internet access.
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/gateway

upvoted 3 times

Question #17 *Topic 1*

Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.




You need to recommend a solution to isolate the compute components on an Azure virtual network.

What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications

B. an Azure App Service Environment (ASE)

C. Azure service endpoints

D. an Azure Active Directory (Azure AD) application proxy

**Correct Answer:** *B*

The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale. This capability can host your:

Windows web apps -

Linux web apps -

Docker containers -

Mobile apps -

Functions -

App Service environments (ASEs) are appropriate for application workloads that require:

Very high scale.

Isolation and secure network access.

High memory utilization.

Customers can create multiple ASEs within a single Azure region or across multiple Azure regions. This flexibility makes ASEs ideal for horizontally scaling stateless application tiers in support of high requests per second (RPS) workloads.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/environment/intro

*Community vote distribution*

B (92%) 8%

**InformationOverload** Highly Voted 1 year, 4 months ago

Selected Answer: B

Answer is correct.
https://docs.microsoft.com/en-us/azure/app-service/environment/overview

upvoted 8 times

**Murtuza** Most Recent 2 weeks, 1 day ago

The exhibit shows function apps so ASE can support it

upvoted 1 times

**JG56** 1 month, 2 weeks ago

Given answer is correct, in exam Nov 23

upvoted 1 times

**Ario** 6 months, 2 weeks ago

B is correct

upvoted 1 times

**Itu2022** 7 months ago

was on exam 15/06/23

upvoted 2 times

**edurakhan** 7 months, 3 weeks ago

On exam 5/25/2023

upvoted 2 times

**zellck** 7 months, 4 weeks ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/environment/intro#overview
The Azure App Service Environment v2 is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale.

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 1 times

**Cock** 7 months, 3 weeks ago

Thank you Zelleck. I took AZ-500 and SC-100 shortly after you. You helped me a lot. I know you wouldn't see this message, but I really appreciate your effort

upvoted 2 times

**zellck** 7 months, 2 weeks ago

Glad that my comments are useful! =)

upvoted 2 times

**OCHT** 10 months, 1 week ago

Selected Answer: C

Azure service endpoints provide secure and direct connections to Azure services over an Azure virtual network. By using service endpoints, traffi between the virtual network and the Azure service does not traverse the public internet, which enhances security and network performance. Ser endpoints can also be used to restrict access to specific Azure services to only specific subnets within a virtual network. Therefore, including Azu service endpoints in the recommendation can help isolate the compute components on an Azure virtual network.

Azure Active Directory (Azure AD) enterprise applications, an Azure App Service Environment (ASE), and an Azure Active Directory (Azure AD) application proxy are all valid solutions for different scenarios, but they do not address the specific requirement of isolating compute componer on an Azure virtual network.

upvoted 1 times

**init2winit** 9 months, 2 weeks ago

In the above exhibit; it references APIs not hosts, so not endpoints so App Service Environment is the correct answer

upvoted 1 times

**KrisDeb** 11 months, 1 week ago

App Service Environment v2 will be retired on 31 August 2024. There's a new version of App Service Environment that is easier to use and runs c more powerful infrastructure.
https://learn.microsoft.com/en-us/azure/app-service/environment/overview

upvoted 2 times

**itbrpl** 10 months, 4 weeks ago

who cares about that. we are in 2023

upvoted 2 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

only an idiot would start building on outdated components

upvoted 2 times

**Sec_Arch_Chn** 1 year, 1 month ago

Correct Answer. App Service environments are appropriate for application workloads that require 'Isolation and secure network access.'
Source: https://docs.microsoft.com/en-us/azure/app-service/environment/intro

upvoted 2 times

**tester18128075** 1 year, 4 months ago

ASE is correct, webapps on this are hosted in your VNET in a dedicated subnet.

upvoted 4 times

**TheMCT** 1 year, 4 months ago

**Selected Answer: B**

https://docs.microsoft.com/en-us/archive/msdn-magazine/2017/april/azure-the-new-azure-app-service-environment

The Azure App Service Environment (ASE) is a Premium feature offering of the Azure App Service. It gives a single-tenant instance of the Azure A
Service that runs right in your own Azure virtual network (VNet), providing network isolation and improved scaling capabilities.

upvoted 3 times

**prabhjot** 1 year, 4 months ago

App Service environments (ASEs) are appropriate for application workloads that require:
Very high scale,Isolation and secure network access,High memory utilization.This capability can host your:
Windows web apps,Linux web apps
Docker containers,Mobile apps
Functions

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

correct, agree

upvoted 2 times

Question #18 *Topic 1*

HOTSPOT

-

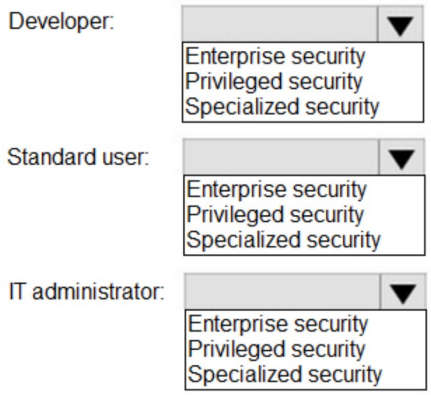
You are planning the security levels for a security access strategy.

You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security level should you configure for each job role? To answer, select the appropriate options in the answer area.

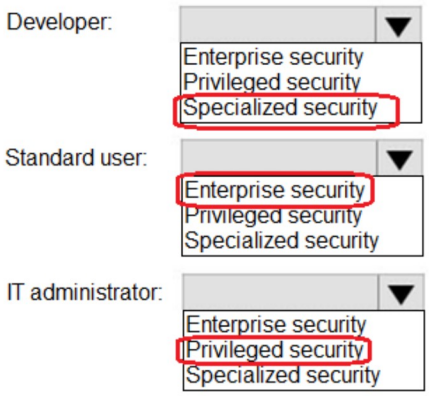
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer Area**

**Correct Answer:**




**Jacquesvz** Highly Voted 1 year ago

Correct Answer: reference = https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra (check page 59 of the MCRA powerpoint deck)

upvoted 15 times

**TomasValtor** 1 month, 3 weeks ago

check page 60 of the MCRA powerpoint deck

upvoted 1 times

**TomasValtor** 1 month, 3 weeks ago

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

upvoted 1 times

**zellck** Most Recent 7 months, 4 weeks ago

1. Specialised security

2. Enterprise security
3. Privileged security

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#specialized
Specialized security provides increased security controls for roles with an elevated business impact (if compromised by an attacker or malicious insider).
Specialized roles typically include:
- Developers of business critical systems.

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#enterprise
Enterprise security is suitable for all enterprise users and productivity scenarios. In the progression of the rapid modernization plan, enterprise al serves as the starting point for specialized and privileged access as they progressively build on the security controls in enterprise security.

upvoted 2 times

**zellck** 7 months, 4 weeks ago

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels#privileged
Privileged security is the highest level of security designed for roles that could easily cause a major incident and potential material damage to the organization in the hands of an attacker or malicious insider. This level typically includes technical roles with administrative permissions o most or all enterprise systems (and sometimes includes a select few business critical roles)

upvoted 1 times

**[Removed]** 9 months, 2 weeks ago

This mentioned above reference architecture is really a hardcore.

upvoted 1 times

**God2029** 10 months, 3 weeks ago

An Easy pick, based on the insider threat logic

upvoted 1 times

Question #19 *Topic 1*

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment.

You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

**Correct Answer:** *ACE*

*Community vote distribution*

ACE (85%) BCE (15%)

**Stubentiger** Highly Voted 1 year ago

Selected Answer: ACE

answers ok.
https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 11 times

**Naqsh27** Most Recent 1 week, 2 days ago

Selected Answer: BCE

As of the Dec 2023 Slides it should be
Secure Identities and Access
Modern SecOps
Infrastructure and Development Security

upvoted 1 times

**Ramye** 5 days, 21 hours ago

Based on the given answers, answer B is not a Zero Trust principle but answer A is.

upvoted 1 times

**TomasValtor** 1 month, 3 weeks ago

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

upvoted 1 times

**TomasValtor** 1 month, 3 weeks ago

check page 22 of the MCRA powerpoint deck

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: ACE

ACE is the answer.

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview#ramp-initiatives-for-zero-trust
Top priority
- User access and productivity
- Data, compliance, and governance
- Modernize security operations

upvoted 2 times

**alifrancos** 9 months ago

Selected Answer: ACE

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview
User access and productivity
Data, compliance, and governance

Modernize security operations

As needed:
OT and Industrial IoT
Datacenter & DevOps Security

upvoted 3 times

**alifrancos** 9 months ago

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

upvoted 1 times

**MichaelMu** 9 months, 1 week ago

To rapidly adopt Zero Trust in your organization, RaMP(Rapid Modernization Plan) offers technical development guidance organized in these initiatives.
The top priority initiatives are
1. User access and productivity
2 Data, compliance and governance
3 Modernize security operations.

As needed initiatives are
1. OT and industrial IoT
2 Datacenter and DevOps Security

upvoted 1 times

**Fal991l** 10 months, 1 week ago

Selected Answer: BCE

ChatGTP: Based on the Zero Trust Rapid Modernization Plan (RaMP), the top three modernization areas to prioritize are:

B. Infrastructure and development, to ensure a secure foundation for the IT environment.
C. User access and productivity, to ensure secure and efficient access to resources for users.
E. Modern security operations, to detect and respond to security incidents and threats in real-time.

Therefore, options B, C, and E are the correct answers.

upvoted 3 times

**technocorgi** 9 months, 1 week ago

while chatGPT also gave me the same answer, https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview lists ACE as th correct answer

upvoted 1 times

**AJ2021** 10 months, 1 week ago

Selected Answer: ACE

Correct, just a slight rewording on E: Modernize security operations

upvoted 2 times

**rmafnc** 11 months, 2 weeks ago

B. infrastructure and development
C. user access and productivity
E. modern security operations

upvoted 3 times

**Discuss4certi** 11 months, 3 weeks ago

Selected Answer: ACE

Correct,
link below lists all three as top priorities:
https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview
in order:
1. user access and productivity: explicitly verify trust for identities, devices, apps and networks
2. data, complaince and governance: ransomware readiness and data policies
3. modern security operations: streamline response, unify visibility, reduce manual effort.

upvoted 3 times

**smosmo** 12 months ago

Selected Answer: ACE

Correct following RAMP

upvoted 2 times

Question #20 *Topic 1*

HOTSPOT
-

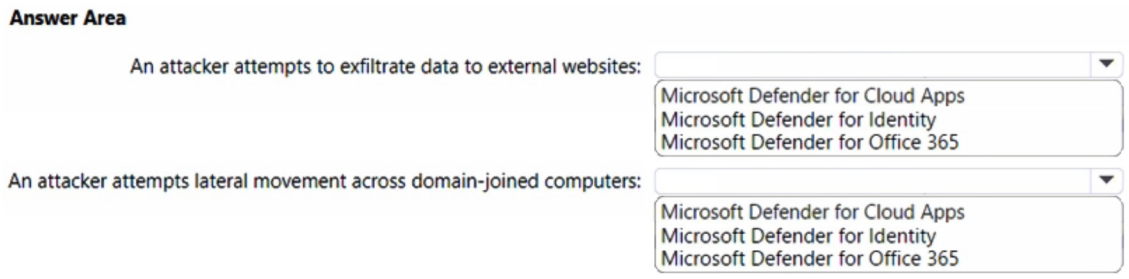
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to protect against the following external threats of an attack chain:

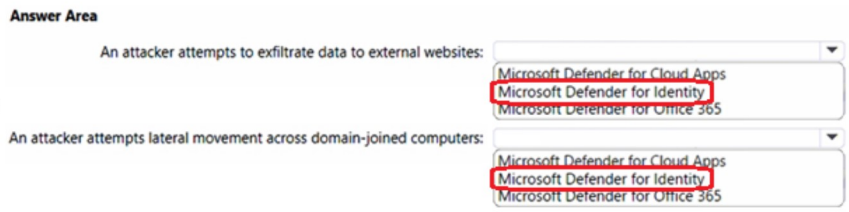
• An attacker attempts to exfiltrate data to external websites.
• An attacker attempts lateral movement across domain-joined computers.

What should you include in the recommendation for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**Sam_Gutterson** Highly Voted 12 months ago
Exfiltration of data - Defender for Cloud Apps
Data across domains - Defender for Identity
Reference: MCRA Slide 15
upvoted 56 times

**cyber_sa** Highly Voted 3 months, 1 week ago
got this in exam 6oct23. passed with 896 marks. I answered
MD FOR CLOUD APPS
MD FOR IDENTITY
upvoted 8 times

**Murtuza** Most Recent 1 week, 3 days ago
Actions that would compromise the security of customer data must be detected and prevented. For example, employees may be using an unapproved cloud application for storing sensitive corporate data or downloading a vast number of sensitive files for exfiltration. These actions be prevented by Microsoft Defender for Cloud Apps.
upvoted 1 times

**UberTech_1888** 6 months ago
the keyword is "Attacker" = "Identity"
upvoted 1 times

**zellck** 7 months, 4 weeks ago
1. Microsoft Defender for Cloud Apps
2. Microsoft Defender for Identity

https://learn.microsoft.com/en-us/defender-for-identity/what-is
Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious

insider actions directed at your organization.

upvoted 3 times

**Fal991l** 10 months, 1 week ago

An attacker attempts to exfiltrate data to external websites:
Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers:
Microsoft Defender for Identity

upvoted 3 times

**Fal991l** 10 months, 1 week ago

To protect against an attacker attempting to exfiltrate data to external websites, the best solution would be to use Microsoft Defender for Of 365, which can help detect and prevent data exfiltration attempts. It provides data loss prevention (DLP) policies that can identify and protec sensitive information, and advanced threat protection (ATP) that can detect and block suspicious activities.

To protect against an attacker attempting lateral movement across domain-joined computers, the best solution would be to use Microsoft Defender for Identity. It provides continuous monitoring of user activities, behavior analytics, and machine learning-based detection capabili to identify and block suspicious activities. It can also help identify and remediate weak passwords, and enforce multi-factor authentication (M policies to prevent unauthorized access. Microsoft Defender for Identity can also integrate with other security solutions, such as Azure Sentin to provide a comprehensive security solution.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

While Microsoft Defender for Cloud Apps can help protect against data exfiltration attempts, it is primarily focused on protecting against threats to cloud applications, such as Microsoft 365, Dynamics 365, and more. It can monitor user activity, detect suspicious behavior, and help enforce policies to prevent data exfiltration.

However, if an attacker is attempting to exfiltrate data from a device or a network that is not connected to a cloud application, Microsoft Defender for Cloud Apps may not be effective. In this case, Microsoft Defender for Office 365, which provides advanced threat protection and data loss prevention policies, would be a better solution.

So, for protecting against an attacker attempting to exfiltrate data to external websites, the best solution would be to use Microsoft Defer for Office 365, which is specifically designed for this purpose.

upvoted 1 times

**Holii** 6 months, 2 weeks ago

Defender for O365 is designed for SharePoint, Exchange and phishing/spam attempts for data transferred via email. It is not designed handle data being exfiltrated to websites.

Also, I am not even sure if Microsoft Defender for O365 can do DLP anymore, I believe that functionality has been shifted to Microsoft Purview.

MDCA is designed for data exfiltration/tracking for websites, and CAN still perform DLP through its action portal (it has separate functionality from Purview) on a variety of policy-types.

upvoted 2 times

**OCHT** 10 months, 1 week ago

For Box 1:
The recommendation should be MS Defender for Cloud Apps as it can protect the cloud application and its data from unauthorized access, and has the capability to detect and prevent data exfiltration attempts.

For Box 2:
The recommendation should be MS Defender for Identity, as it can protect against lateral movement by detecting and blocking suspicious activities across domain-joined computers. It can also identify and remediate misconfigurations and vulnerabilities in the identity infrastructure t attackers could exploit to move laterally.

upvoted 6 times

**AJ2021** 10 months, 1 week ago

First answer incorrect.
Should be:
MDCA
MDI

upvoted 1 times

**Gurulee** 11 months, 1 week ago

"Employees may be using an unapproved cloud application for storing sensitive corporate data or downloading a vast number of sensitive files exfiltration. These actions can be prevented by Microsoft Defender for Cloud Apps."

upvoted 3 times

**buguinha** 11 months, 1 week ago

Defender Cloud Apps to the first and MDI to the second

upvoted 1 times

**Oknip** 11 months, 1 week ago

Defender for cloud apps for first question: https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls.

Defender for Identity for second question.
upvoted 3 times

**SofiaLorean** 11 months, 2 weeks ago
First one - Defender for Cloud Apps
https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls
upvoted 2 times

**Ajdlfasudfo0** 11 months, 2 weeks ago
Hello, why would it be Defender for Identity for the second. To my understanding Defender for Identity is for on-premise? Thank you!
upvoted 1 times

**Holii** 6 months, 2 weeks ago
They're domain-joined, pretty much domained computers.
MDI will pick these up and any traffic going across them in the course of a lateral attack.
upvoted 1 times

**nieprotetkniteeetr** 12 months ago
MCRA slide 13. Defender for Cloud Apps for eflitration protection.
upvoted 1 times

**Navynine** 1 year ago
1st - Microsoft Defender for Cloud Apps
upvoted 7 times

**smosmo** 1 year ago
For domain joined computers I agree with MDI. For the first box I would prefer MD for Cloud Apps.
https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-proxy
upvoted 5 times

**AMDf** 1 year ago
I would go for Microsoft Defender for Cloud Apps : https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-exfiltration-access-controls
Second seems correct
upvoted 3 times

**Jarro** 1 year ago
Agree with this. defender for cloud apps for first question
upvoted 3 times

Question #21 *Topic 1*

For an Azure deployment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

You need to recommend a best practice for implementing service accounts for Azure API management.

What should you include in the recommendation?

A. application registrations in Azure AD

B. managed identities in Azure

C. Azure service principals with usernames and passwords

D. device registrations in Azure AD

E. Azure service principals with certificate credentials

**Correct Answer:** *B*

*Community vote distribution*

B (70%) A (27%)

**mynk29** Highly Voted 1 year ago

Selected Answer: A

It depends on what is "Service account" in the question. Microsoft benchmark recommends https://learn.microsoft.com/en-us/security/benchma /azure/baselines/api-management-security-baseline to use OAuth 2.0 "Configure your Azure API Management instance to protect your APIs by using the OAuth 2.0 protocol with Azure AD." --> App registration

AND
managed identity for the "to allow your API Management instance to easily and securely access other Azure AD-protected resources, such as Az Key Vault instead of using service principals." --> Managed Identity

Its poorly worded question but I would choose A since key consideration for an API gateway in general is authentication of developers which warrants app registration.

upvoted 12 times

**smosmo** 12 months ago

I still think it is B: https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline in context with SERVICE PRINCIPALS in section IM3

upvoted 9 times

**kalyankrishna1** 2 months, 4 weeks ago

app reg, SPs with certs, managed Identities all eventually end up as service principals anyways and the most secure type of SP is a managed Identity, so B is the correct answer

upvoted 2 times

**Gurulee** 11 months, 1 week ago

Agreed 👍

upvoted 2 times

**maku067** 12 months ago

At the begining I pointed to rather B but now I choose rather A.
https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-aad#manually-enable-azure-ad-application-and-identity provider
Step 6

upvoted 4 times

**Rocko1** Highly Voted 10 months, 1 week ago

Selected Answer: B

managed identities in Azure recommended solution for service accounts

upvoted 10 times

**sherifhamed** Most Recent 3 months, 3 weeks ago

Selected Answer: B

B. Managed identities in Azure: Managed identities provide a way to automatically manage the credentials used by applications and services. Us managed identities is a best practice for securing access to Azure resources without the need for storing and managing credentials. It aligns witl

the principle of least privilege and reduces the risk associated with credential exposure.

upvoted 3 times

**BlackZeros** 6 months, 1 week ago

Selected Answer: B

Option B seems like the most secure option.
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline#im-3-manage-application-identities securely-and-automatically

upvoted 1 times

**Ario** 6 months, 2 weeks ago

Selected Answer: E

Azure service principals with certificate credentials

upvoted 2 times

**Ario** 5 months, 4 weeks ago

B is the correct answer

upvoted 2 times

**zellck** 7 months, 4 weeks ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-use-managed-service-identity
A managed identity generated by Azure Active Directory (Azure AD) allows your API Management instance to easily and securely access other Azure AD-protected resources, such as Azure Key Vault. Azure manages this identity, so you don't have to provision or rotate any secrets.

upvoted 2 times

**Tictactoe** 8 months, 1 week ago

B right

upvoted 1 times

**alifrancos** 9 months ago

Selected Answer: B

it is Managed Identity,
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline
IM-3

upvoted 5 times

**shahnawazkhot** 9 months, 2 weeks ago

I think the answer should be between Service Principal options and managed identity option... And in these options, managed identity option is preferred here considering better security and convenience. Therefore, the correct answer appears to be option "B".

upvoted 1 times

**etblue** 9 months, 3 weeks ago

Refer to https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline IM-3 Manage application identities securely and automatically, selected answer should be B. There is nothing listed in API management security baseline regards to app registration. I do think by using managed identity would meant require earlier app registration as pre-requisite. Hence, answer B is more comprehensive.

upvoted 4 times

**AJ2021** 10 months, 1 week ago

Selected Answer: B

Configuration Guidance: Use a Managed Service Identity generated by Azure Active Directory (Azure AD) to allow your API Management instanc to easily and securely access other Azure AD-protected resources, such as Azure Key Vault instead of using service principals. Managed identity credentials are fully managed, rotated, and protected by the platform, avoiding hard-coded credentials in source code or configuration files.
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline

upvoted 3 times

**Fal991l** 10 months, 2 weeks ago

Selected Answer: B

ChatGPT:The Microsoft Cloud Security Benchmark recommends using managed identities in Azure as a best practice for implementing service accounts for Azure API management. Managed identities are a secure and automated way to provide applications running on Azure services wit an automatically managed identity in Azure Active Directory (Azure AD). By using managed identities, you can avoid storing credentials in your code or configuration files, which reduces the risk of exposing sensitive information.

Therefore, the correct answer is B. Managed identities in Azure.

upvoted 3 times

**PeteNZ** 10 months, 2 weeks ago

B - managed identities because: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-introduction-azure

upvoted 1 times

**PeteNZ** 10 months, 2 weeks ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline

upvoted 2 times

**PeteNZ** 10 months, 2 weeks ago

Managed Identities... See 'IM-3' here: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management

upvoted 1 times

**MichaelMu** 10 months, 3 weeks ago

A

The recommended best practice for implementing service accounts for Azure API management based on the Microsoft Cloud Security Benchma is to use application registrations in Azure AD or managed identities in Azure.

Application registrations provide a way to define a set of permissions for a service account that can be used to authenticate and authorize acces to Azure API Management. They can also be used to configure Azure AD to issue tokens that can be used to access the API management service

Managed identities in Azure provide a way to give Azure services an automatically managed identity in Azure AD. This identity can be used to authenticate and authorize access to Azure resources, including Azure API management.

Using Azure service principals with usernames and passwords or certificate credentials is not recommended as they can be vulnerable to compromise and misuse. Similarly, device registrations in Azure AD are not recommended for implementing service accounts for Azure API management as they are intended for managing devices, not service accounts.

upvoted 1 times

**KrisDeb** 11 months, 1 week ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-3-manage-application-identities-securely-and-automatically

upvoted 2 times

Question #22 *Topic 1*

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators groups on the Windows computers.

You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised.

What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**JG56** 1 month, 2 weeks ago

LAPS is the answer, in exam Nov 23

upvoted 1 times

**Kvoth3** 4 months, 3 weeks ago

What about D.
To provide users with administrative access to the Windows computers only when access is required, you can use Privileged Access Workstations (PAWs). PAWs are dedicated operating systems for sensitive tasks that are protected from Internet attacks and threat vectors. They separate these sensitive tasks and accounts from the daily use workstations and devices, providing strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket 1.

PAWs can be used to minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised. PAWs provide a secure environment for administrative tasks that require elevated privileges. They are designed to protect against advanced persistent threats (APTs) and other sophisticated attacks.

upvoted 4 times

**nExoR** 1 month ago

PAWs are administration workstations. concept from totally different area. the question asks about users having access on their regular workstations - e.g. to install app. not some specialized, isolated workstation

upvoted 1 times

**Ario** 6 months, 2 weeks ago

for those check discussions don't be fool by most rated answers .

upvoted 2 times

**Bondaexam** 1 month, 1 week ago

what should be the final judgement when multiple answers are chosen by multiple people . Dont tell us to go back and look into the documentation, we all know that . What should be the final judgement???

upvoted 1 times

**ltu2022** 7 months ago

was on exam 15/06/23

upvoted 1 times

**edurakhan** 7 months, 3 weeks ago

On exam 5/25/2023

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
Windows Local Administrator Password Solution (Windows LAPS) is a Windows feature that automatically manages and backs up the password local administrator account on your Azure Active Directory-joined or Windows Server Active Directory-joined devices. You also can use Windows LAPS to automatically manage and back up the Directory Services Restore Mode (DSRM) account password on your Windows Server Active Directory domain controllers. An authorized administrator can retrieve the DSRM password and use it.

upvoted 3 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 1 times

**init2winit** 9 months, 1 week ago

Selected Answer: A

Agree with A, as Yarvis pointed out in the link.
For endpoint administrative management, use the local administrative password solution (LAPS).

upvoted 1 times

**Bouncy** 10 months, 2 weeks ago

Selected Answer: A

A, but only because the others don't make sense.
If you ever need to remove admins from PCs in real life, do not use LAPS. Use Microsoft Intune Endpoint Privilege Management instead. It lets you decide precisely for which action users may receive an elevation, whereas LAPS will give users full local admin access until the password changes which can take days or even weeks in reality...

upvoted 3 times

**ARYMBS** 3 months, 2 weeks ago

This does not work on Hybrid AzureAD Joined....

upvoted 1 times

**jasscomp** 3 months, 2 weeks ago

Incorrect - it does work on HAADJ devices - worked for me
https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview#understand-device-join-state-restrictions

upvoted 1 times

**yarvis** 10 months, 3 weeks ago

Selected Answer: A

LAPS - https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

upvoted 2 times

**mynk29** 1 year ago

Selected Answer: A

Granting users access to their PC is not the typical use case for LAPS- admins use it for troubleshooting/as a break glass account.

But PIM is explicitly not meant to do it. see https://www.reddit.com/r/Intune/comments/yqdiyf/azure_ad_joined_device_local_admin_via_pim/

PAW and Identity protection are not relevant so will reluctantly go with A.

upvoted 3 times

**Jacquesvz** 1 year ago

Selected Answer: A

Agree with A, check this link for reason - https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-guide-how-to-configure-microsoft-local/ba-p/2806185

upvoted 4 times

**smosmo** 1 year ago

Selected Answer: A

Agree with A

upvoted 3 times

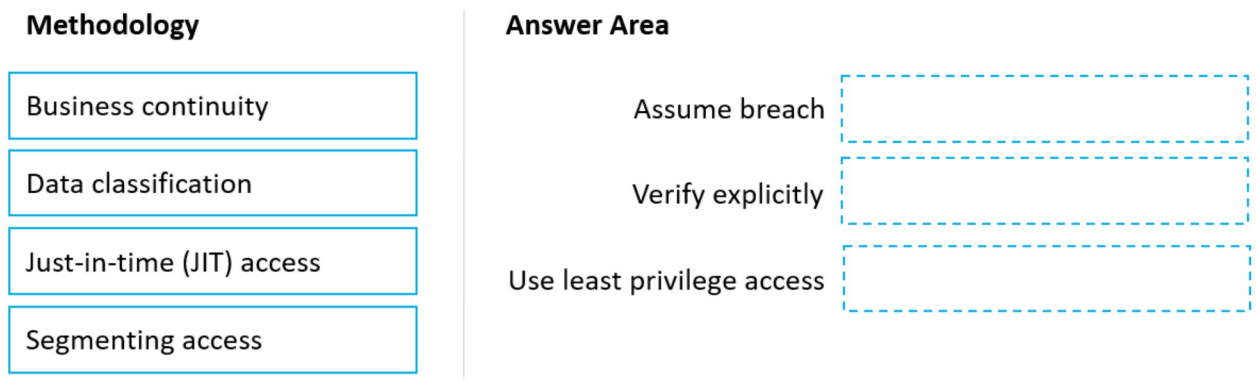
Question #23 *Topic 1*

29 DRAG DROP

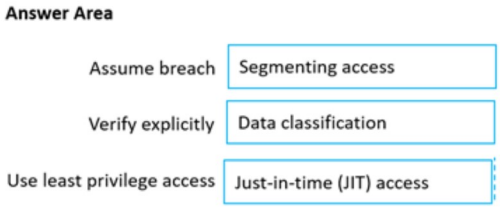
For a Microsoft cloud environment, you need to recommend a security architecture that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security methodologies should you include in the recommendation? To answer, drag the appropriate methodologies to the correct principles. Each methodology may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**zellck** Highly Voted 7 months, 4 weeks ago

1. Segmenting access
2. Data classification
3. JIT access

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust
- Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

- Verify explicitly
Always authenticate and authorize based on all available data points.

- Use least privilege access
Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

upvoted 7 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 1 times

**Ario** Most Recent 6 months, 2 weeks ago

Segmenting access is an important methodology for implementing a least privileged access approach within a Zero Trust architecture

upvoted 1 times

**edurakhan** 7 months, 3 weeks ago

Exam question 5/25/2023

upvoted 3 times

**PrettyFlyWifi** 9 months ago

Slide 20 of the MCRA, answer looks correct!

upvoted 2 times

**God2029** 10 months, 3 weeks ago

Segmentation will contain the breach with the specific instance - This will help to isolate the breach. Enforcing Principle 1 : Assume Breach
Data Classification helps to determine the most sentive data and labeling them, enforcing RBAC based access control on the data will help to enforce the Principle 2 Verify Explicitly.

Finally JIT is providing access based on time period, Enforcing the 3rd in the list, Principles of Least Previlage

upvoted 4 times

**Ceuse** 11 months ago

Answer Looks Good :
https://www.microsoft.com/en-us/security/business/zero-trust

Zero Trust principles
Verify explicitly
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least-privilege access
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data a productivity.

Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

upvoted 2 times

**Jame** 11 months ago

I think Answer is correct.
https://www.microsoft.com/en-us/security/business/zero-trust
Zero Trust principles
Verify explicitly
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
Use least-privilege access
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data a productivity.
Assume breach
Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

upvoted 3 times

Question #24 *Topic 1*

You have legacy operational technology (OT) devices and IoT devices.

You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures (MCRA). The solution must minimize the risk of disrupting business operations.

Which two security methodologies should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. active scanning

B. threat monitoring

C. software patching

D. passive traffic monitoring

**Correct Answer:** *BC*

*Community vote distribution*

BD (78%) BC (22%)

**El_m_o** Highly Voted 10 months, 2 weeks ago

Selected Answer: BD

From MCRA slide 17 (OT): "Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, so they can only be selectively applied (or have a limited security effect). Basic security hygiene for OT starts with network isolation (including good maintenance/**monitoring** of that isolation boundaries), **threat monitoring**, and carefully managing vendor access risk."

upvoted 14 times

**Ajdlfasudfo0** Highly Voted 10 months, 4 weeks ago

Selected Answer: BC

In some legacy environments where modern authentication protocols are unavailable such as operational technology (OT), network controls ma be used exclusively. - Slide 61, MCRA

Slide 17 -
OT - Safety/Integrity/Availability
Hardware Age: 50-100 years (mechanical + electronic overlay)
Warranty length: up to 30-50 years
Protocols: Industry Specific (often bridged to IP networks)
Security Hygiene: Isolation, threat monitoring, managing vendor access risk, (patching rarely)

upvoted 7 times

**Funkydave** Most Recent 3 months, 2 weeks ago

"The solution must minimize the risk of disrupting business operations."

patching is absolutely not non-disruptive

upvoted 2 times

**POOJI123** 5 months, 1 week ago

what is mcra slide mentioned in comments how do i find it

upvoted 1 times

**theplaceholder** 4 months, 3 weeks ago

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

upvoted 1 times

**Ario** 6 months, 2 weeks ago

BD is correct

upvoted 1 times

**zellck** 7 months, 4 weeks ago

Selected Answer: BD

BD is the answer.

OT Security hygiene is different because these systems frequently weren't built with modern threats and protocols in mind (and often rely on 'er

of life' software). Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, s they can only be selectively applied (or have a limited security effect). Basic security hygiene for OT starts with network isolation (including good maintenance/monitoring of that isolation boundaries), threat monitoring, and carefully managing vendor access risk.

upvoted 2 times

**Tictactoe** 8 months, 1 week ago

BD right

upvoted 1 times

**PrettyFlyWifi** 9 months ago

Selected Answer: BD

B and D seem most suitable here, both are mentioned on slide 17 of MCRA.
It doesn't look like C - Software patching is a valid answer. Look at slide 17 of MCRA it states "Many well-established IT security best practices lik software patching aren't practical or fully effective in an OT environment, so they can only be selectively applied (or have a limited security effec so this confirms it isn't practical, so it can't be "best practice".

upvoted 4 times

**edurakhan** 9 months, 1 week ago

Selected Answer: BC

I would go with threat monitoring and patching (rarely, according to MCRA, but there is nothing about passive traffic monitoring)

upvoted 1 times

**GeVanDerBe** 8 months, 2 weeks ago

Read the notes in slide 17 --> Microsoft's approach to threat monitoring is focused on bringing modern security approaches that also deeply respects the constraints and sensitivity of these systems. The approach is based on technology developed by CyberX (recently acquired and integrated into Microsoft).
The solution consists of
Network TAP/SPAN (passive collection) – provides data gathering with passive traffic monitoring to avoid disruption of OT and IIoT operation

upvoted 3 times

**zellck** 7 months, 4 weeks ago

Many well-established IT security best practices like software patching aren't practical or fully effective in an OT environment, so they can onl be selectively applied (or have a limited security effect).

upvoted 2 times

**Fal991l** 10 months, 1 week ago

Selected Answer: BD

ChatGTP: The two security methodologies that should be included in the recommendation for applying Zero Trust principles to OT and IoT devic based on the MCRA while minimizing the risk of disrupting business operations are:

B. Threat monitoring: Continuous monitoring and analysis of network traffic, system logs, and other data sources can help detect and respond t threats and attacks targeting OT and IoT devices. Threat monitoring can help identify indicators of compromise (IoCs) and provide early warning potential security incidents.

D. Passive traffic monitoring: Passive traffic monitoring involves monitoring network traffic without actively sending packets or generating traffic This approach can help minimize the risk of disrupting business operations while still providing visibility into network activity and potential secu incidents. Passive traffic monitoring can also help identify anomalies and suspicious activity that may indicate a security threat.

upvoted 4 times

**Fal991l** 10 months, 1 week ago

Option A, active scanning, and option C, software patching, are not necessarily the best practices for applying Zero Trust principles to OT and IoT devices, as they can potentially disrupt business operations and cause compatibility issues with legacy devices. While software patching c help mitigate vulnerabilities, it should be done in a controlled and tested manner to avoid introducing new issues or downtime.

upvoted 1 times

**AJ2021** 10 months, 1 week ago

Selected Answer: BD

Adapt processes to Operational Technology (OT) - Adjust your tools and processes to the constraints of OT environments as you integrate them These environments prioritize safety and often have older systems which don't have patches available and may crash from an active scan. Focus on approaches like passive network detections for threats and isolation of systems is often the best approach.

https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/3-recommend-for-protecting-from-insider-external-attacks

upvoted 4 times

Question #25 *Topic 1*

You have an on-premises network and a Microsoft 365 subscription.

You are designing a Zero Trust security strategy.

Which two security controls should you include as part of the Zero Trust solution? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. Always allow connections from the on-premises network.

B. Disable passwordless sign-in for sensitive accounts.

C. Block sign-in attempts from unknown locations.

D. Block sign-in attempts from noncompliant devices.

**Correct Answer:** *CD*

*Community vote distribution*

CD (86%) 14%

**JG56** 1 month, 2 weeks ago

C,D is right answer, in exam Nov 23

upvoted 3 times

**BlackZeros** 6 months, 1 week ago

Selected Answer: BC

B seems to be the most obvious answer, since MFA on all Admin accounts is the very basic best practice.
C is most likely the case since company doesnt want to have the access given to anyone outside of onprem network.
D is irrelevant in this case because the devices are part of the onprem network, which is not a big threat since option C will enforce the connecti to be from internal network only.

upvoted 1 times

**jasscomp** 3 months, 2 weeks ago

Zero Trust is about always assuming breach. MFA should ideally be enabled for everyone not just sensitive accounts.

upvoted 1 times

**hw121693** 5 months, 2 weeks ago

According to microsoft passwordless is the best way to protect account, better than MFA

upvoted 3 times

**zellck** 7 months, 4 weeks ago

Selected Answer: CD

CD is the answer.

https://learn.microsoft.com/en-us/security/zero-trust/deploy/identity#v-user-device-location-and-behavior-is-analyzed-in-real-time-to-determi risk-and-deliver-ongoing-protection

upvoted 3 times

**bmulvIT** 8 months ago

Selected Answer: CD

MRCA slide 15 recommmends using passwordless so B is wrong.. "The top priority is to require strong multi-factor authentication (MFA), (and preferably Passwordless authentication). Attackers have easy availability to compromised username/passwords and commonly used passwords, organizations must prioritize moving beyond password-only authentication as their first step. "

upvoted 2 times

**Tictactoe** 8 months, 1 week ago

BC IS CORRECT

upvoted 1 times

**CatoFong** 8 months, 2 weeks ago

Selected Answer: CD

CD makes the most sense to me

upvoted 3 times

**Hanley1999** 8 months, 4 weeks ago

Disable passwordless sign-in - as in go back to passwords? Doesn't sound like ZT to me

upvoted 2 times

**deposros** 9 months ago

still confused, what should be the answer?

upvoted 1 times

**edurakhan** 9 months, 1 week ago

Selected Answer: CD

I don't think A and B make any sense here

upvoted 4 times

**shinda** 9 months, 1 week ago

Selected Answer: BC

C speaks for itself but B is biometric or FIDO2 only. If they include biometric plus a password aka MFA then it would be okay

upvoted 1 times

Question #26 *Topic 1*

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

**Correct Answer:** *B*

*Community vote distribution*

E (100%)

**WRITER00347** Highly Voted 5 months, 2 weeks ago

The primary goal here is to minimize the risk of ransomware encrypting local user files. A feature designed to protect against unauthorized acce to critical system files and user data, particularly from ransomware, is protected folders.
Option E, "protected folders," should be included in the recommendation.

In Windows, the Controlled Folder Access feature protects files in key system folders and user-defined folders by only allowing authorized apps make changes. This can prevent ransomware from encrypting files in those folders.
While some of the other options listed, such as B. Microsoft Defender for Endpoint, may provide broader protection against malware, option E specifically targets the requirement to protect local user files against ransomware encryption. Therefore, the correct answer is:
E. protected folders.

upvoted 14 times

**hovlund** 3 months ago

I Agree!

upvoted 1 times

**jasscomp** 3 months, 2 weeks ago

Well explained - thanks

upvoted 1 times

**sbnpj** Highly Voted 5 months, 2 weeks ago

Selected Answer: E

Protected folders

upvoted 7 times

**JG56** Most Recent 1 month, 2 weeks ago

in exam Nov 23

upvoted 2 times

**Lonlystar** 1 month, 4 weeks ago

How can I help keep my PC secure?
Make sure your PC is up to date with the latest version of Windows and all the latest patches. Learn more about Windows Update.

Be sure Windows Security is turned on to help protect you from viruses and malware (or Windows Defender Security Center in previous versions Windows 10).

In Windows 10 or 11 turn on Controlled Folder Access to protect your important local folders from unauthorized programs like ransomware or other malware.
Link: https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3

upvoted 2 times

**snowfresh** 3 months ago

"Controlled folder access is especially useful in helping to protect your documents and information from ransomware"
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

upvoted 2 times

**rahulnair** 3 months ago

B is correct answer - Controlled folder access works best with Microsoft Defender for Endpoint, which gives you detailed reporting into controlle folder access events and blocks as part of the usual alert investigation scenarios.

upvoted 1 times

**ZZNZ** 4 months, 1 week ago

E is correct

upvoted 1 times

**Socgen1** 5 months, 1 week ago

option E
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide

upvoted 2 times

**Darkren4eveR** 5 months, 1 week ago

D

https://learn.microsoft.com/es-mx/azure/security/fundamentals/data-encryption-best-practices

upvoted 1 times

Question #27 *Topic 1*

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

D. an Azure AD user account that has a password stored in Azure Key Vault

**Correct Answer:** *D*

*Community vote distribution*

A (80%) D (20%)

**WRITER00347** Highly Voted 5 months, 2 weeks ago

In the context of deploying applications using CI/CD pipelines in Azure and following DevSecOps best practices from the Microsoft Cloud Adop Framework for Azure, using managed identities is often recommended. Managed identities provide an identity for applications to use when connecting to resources that support Azure AD authentication, without needing to manage credentials like usernames and passwords.

A managed identity in Azure is automatically managed by Azure and does not require you to provision or rotate secrets. This aligns with the principles of DevSecOps, where security is integrated into the development process, and the management of secrets and credentials is handled securely and automatically.

So, the correct recommendation for this scenario would be:
A. a managed identity in Azure.

upvoted 8 times

**tocane** Most Recent 2 days, 11 hours ago

Selected Answer: D

azure devops cannot connect to azure using managed identities (You need to recommend which types of identities to use for the deployment credentials of the service connection.)

upvoted 1 times

**rahulnair** 3 months ago

A - since D says user account

upvoted 2 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: A

For an Azure DevOps solution that follows DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure, the recommende choice for deployment credentials in a service connection is a managed identity in Azure (Option A).

Here's why this is the recommended choice:

A. Managed identity in Azure: Managed identities provide a secure way to authenticate and authorize services or applications in Azure without t need for explicit credentials such as passwords or secrets. Using a managed identity ensures that your CI/CD pipelines can securely access Azure resources without exposing credentials. It also aligns with best practices for security and eliminates the need to manage and rotate passwords o secrets.

upvoted 3 times

**ZZNZ** 4 months, 1 week ago

A. a managed identity in Azure
https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

upvoted 1 times

**theplaceholder** 4 months, 3 weeks ago

Selected Answer: A

Managed Identities, nobody knows the password, not accessible to anyone except the identity itself.

upvoted 2 times

**celomomo** 4 months, 3 weeks ago

Selected Answer: A

A. A managed identity in Azure

Using a managed identity aligns with DevSecOps best practices, as it provides a secure and automated way to manage credentials for your CI/C pipelines. This approach reduces the risk of exposing sensitive information and follows the principle of least privilege

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: A

A, 100%

upvoted 1 times

**sbnpj** 5 months, 2 weeks ago

Selected Answer: D

I take that Back, Answer D is correct:- an Azure AD user account that has a password stored in Azure Key Vault

upvoted 1 times

**WRITER00347** 5 months, 2 weeks ago

Option D, using an Azure AD user account with a password stored in Azure Key Vault, is not the best choice compared to a managed identity because:

Managed identities are specifically designed for service-to-service communication, unlike individual user accounts.
Managed identities eliminate the need to manage or rotate passwords, providing a more secure and less complex solution.
Option A, using a managed identity, better aligns with DevSecOps best practices by automating identity management, making it the preferre choice for deploying applications through CI/CD pipelines in Azure.

upvoted 3 times

**sbnpj** 5 months, 2 weeks ago

Selected Answer: A

seems like Managed identity is the best answer

upvoted 1 times

Question #28 *Topic 1*

You have an Azure Kubernetes Service (AKS) cluster that hosts Linux nodes.

You need to recommend a solution to ensure that deployed worker nodes have the latest kernel updates. The solution must minimize administrative effort.

What should you recommend?

A. The nodes must restart after the updates are applied.

B. The updates must first be applied to the image used to provision the nodes.

C. The AKS cluster version must be upgraded.

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**sbnpj** 5 months ago

**Selected Answer: B**

agree wtih the answer

upvoted 1 times

**Elvoo** 5 months, 1 week ago

**Selected Answer: B**

Correct

upvoted 1 times

**Victory007** 5 months, 1 week ago

**Selected Answer: B**

Answer is Correct.

upvoted 1 times

Question #29 *Topic 1*

You have the following on-premises servers that run Windows Server:

• Two domain controllers in an Active Directory Domain Services (AD DS) domain
• Two application servers named Server1 and Server2 that run ASP.NET web apps
• A VPN server named Served that authenticates by using RADIUS and AD DS

End users use a VPN to access the web apps over the internet.

You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

What should you include in the recommendation?

A. Publish the web apps by using Azure AD Application Proxy.

B. Configure the VPN to use Azure AD authentication.

C. Configure connectors and rules in Microsoft Defender for Cloud Apps.

D. Configure web protection in Microsoft Defender for Endpoint.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**JG56** 1 month, 2 weeks ago
A , in exam Nov 23
upvoted 1 times

**Myguard** 1 month, 4 weeks ago
Selected Answer: A
Correct Answer
upvoted 1 times

**Victory007** 5 months, 1 week ago
Selected Answer: A
Correct Answer
upvoted 1 times

**WRITER00347** 5 months, 2 weeks ago
The Zero Trust model emphasizes never trusting and always verifying, regardless of whether something is inside or outside the corporate netwo
It minimizes reliance on traditional network security boundaries and instead focuses on identities, endpoints, and resources.In the given scenaric
the main goal is to increase the security of connections to the web apps, aligning with the Zero Trust principles.Option A would align well with
these requirements. Azure AD Application Proxy provides secure remote access to your on-premises applications. It allows users to access their
apps from anywhere without having to connect to the VPN and enables additional security features like Conditional Access and MFA.
This solution minimizes the attack surface by eliminating the need to expose the web applications directly to the internet and follows the Zero T
principles of MCRA, making it the appropriate recommendation.So the correct answer is: A
upvoted 3 times

Question #30 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview, SharePoint Online, and OneDrive for Business.

You need to recommend a ransomware protection solution that meets the following requirements:

- Mitigates attacks that make copies of files, encrypt the copies, and then delete the original files
- Mitigates attacks that encrypt files in place
- Minimizes administrative effort

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use: [ ▼ ]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use: [ ▼ ]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

**Correct Answer:**

**Answer Area**

To mitigate attacks that make copies of flies, encrypt the copies, and then delete the original fifes, use: [ Data loss prevention (DLP) policies ▼ ]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

To mitigate attacks that encrypt files in place, use: [ Versioning ▼ ]
- Data loss prevention (DLP) policies
- The Recycle Bin
- Versioning

**jasscomp** Highly Voted 3 months, 2 weeks ago
Recycle Bin and Versioning after reading : https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#deleting-files-or-email
upvoted 10 times

**sbnpj** Highly Voted 5 months ago
correct answers are Recycle Bin and Versioning
https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#deleting-files-or-ema
upvoted 6 times

**ServerBrain** 4 months, 4 weeks ago
No. what do you do with an encrypted file that is in the Recycle bin???
upvoted 4 times

**LJWBA** 4 months ago
It's the original file that would be deleted, so the file in the recycle bin wouldn't be encrypted. I agree with sbnpj
upvoted 3 times

**smanzana** Most Recent 2 months, 3 weeks ago
1-Recycle Bin
2-Versioning
upvoted 5 times

**sbnpj** 5 months ago

Correct Answers are Recycle Bin and DLP
https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide#deleting-files-or-ema

upvoted 2 times

**DavidSapery** 5 months, 1 week ago

Answers are Recycle Bin and Versioning.

https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

upvoted 4 times

**Victory007** 5 months, 1 week ago

Answer Wrong. 1. Versioning - Versioning allows developers (who use it) to keep tracks of the files. This can help you recover your data if it is encrypted or deleted by an attack. 2. DLP Policies: DLP policies help prevent the unauthorized sharing, transfer, or use of sensitive data. They car help you monitor and protect your data across on-premises systems, cloud-based locations, and endpoint devices.

upvoted 1 times

Question #31 *Topic 1*

You are designing a security operations strategy based on the Zero Trust framework.

You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts.

What should you do?

A. Enable built-in compliance policies in Azure Policy.

B. Enable self-healing in Microsoft 365 Defender.

C. Automate data classification.

D. Create hunting queries in Microsoft 365 Defender.

**Correct Answer:** *A*

*Community vote distribution*

B (100%)

**WRITER00347** Highly Voted 5 months, 2 weeks ago

Among the options provided, B. Enable self-healing in Microsoft 365 Defender is the one that aligns most closely with this goal.

Self-healing capabilities in Microsoft 365 Defender can automatically detect, investigate, and remediate security threats, which would otherwise require manual intervention by SOC analysts. By automating these processes, you can minimize the operational load on Tier 1 analysts and allov them to focus on more complex security issues.

Options A, C, and D are relevant to various aspects of security and compliance but don't specifically target the operational load on Tier 1 SOC analysts in the same way that option B does. Therefore, the correct answer is:
B. Enable self-healing in Microsoft 365 Defender.

upvoted 11 times

**cyber_sa** Highly Voted 3 months, 1 week ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 5 times

**Arockia** Most Recent 1 week, 3 days ago

To minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts while designing a security operations strategy based on the Zero Trust framework, the recommended action is:

B. Enable self-healing in Microsoft 365 Defender: Enabling self-healing capabilities in Microsoft 365 Defender can significantly reduce the operational load on Tier 1 SOC analysts. Self-healing features automate the detection and remediation of common security issues and threats, allowing for faster response times and reducing the need for manual intervention. By automating the remediation process, Tier 1 analysts can fc on more complex and critical security incidents, improving efficiency and productivity.

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: B

To minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts as part of a Zero Trust security operations strate you should recommend enabling self-healing in Microsoft 365 Defender (Option B).

Here's why this recommendation is appropriate:

A. Enable built-in compliance policies in Azure Policy: While compliance policies are essential for maintaining security and compliance, they do r directly address minimizing the operational load on SOC analysts. These policies help in ensuring that resources are compliant with organizatior standards but may require SOC analysts to review and remediate non-compliant resources.

upvoted 3 times

**bronyrafon** 4 months ago

ChatGPT says option C...

upvoted 1 times

**ThePrinceJozef** 4 months, 3 weeks ago

Selected Answer: B

BBBBBBBBBBBB

upvoted 2 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: B

B is the correct answer

upvoted 2 times

**Lippes** 5 months, 1 week ago

Selected Answer: B

Would go for B

upvoted 3 times

**Victory007** 5 months, 1 week ago

Selected Answer: B

https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527.
https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527

upvoted 2 times

Question #32 *Topic 1*

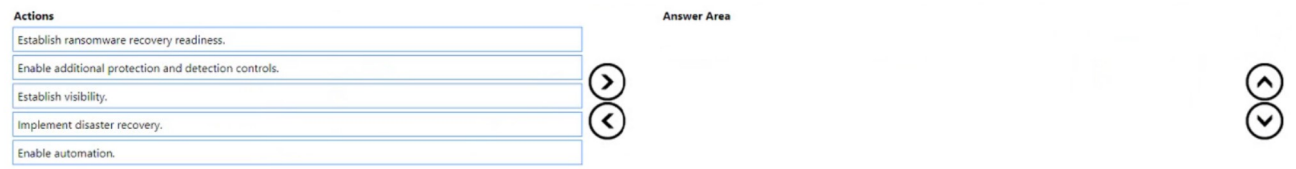
DRAG DROP

-

You are designing a security operations strategy based on the Zero Trust framework.

You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).

Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.




**Correct Answer:**

**hcmonteiro** Highly Voted 3 months ago

The answer is for blind people. But seems correct.

upvoted 7 times

**shanti0091** Most Recent 3 months, 1 week ago

Answer is correct. The focus here is to increase SOC efficiency.

upvoted 2 times

**Topic 2 - Question Set 2**

Question #1 *Topic 2*

You are evaluating an Azure environment for compliance.
You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.
Which effect should you use in Azure Policy?

A. Deny

B. Modify

C. Append

D. Disabled

**Correct Answer:** *D*
This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disable a single assignment instead of disabling all of that policy's assignments.
An alternative to the Disabled effect is enforcementMode, which is set on the policy assignment. When enforcementMode is Disabled, resources are still evaluated.
Incorrect:
Not A: Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
Not B: Modify evaluates before the request gets processed by a Resource Provider during the creation or updating of a resource. The Modify operations are applied to the request content when the if condition of the policy rule is met. Each Modify operation can specify a condition that determines when it's applied.
Operations with conditions that are evaluated to false are skipped.
Not C: Append is used to add additional fields to the requested resource during creation or update.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

*Community vote distribution*
D (82%) A (18%)

**Gar23** Highly Voted 1 year, 4 months ago
Selected Answer: D
It has to be disabled since deny will send the compliance report as non-complaint.
upvoted 25 times

**BlackZeros** 6 months, 1 week ago
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#deny-evaluation
upvoted 2 times

**[Removed]** Highly Voted 1 year ago
The question is misleadingly worded. The question asks which effect can be used to report on compliance without changing anything. The Azur Policy "effect" used to do this is "Audit", which is not one of the provided options. There isn't an "effect" setting in the choices that matches the criteria.

However, "Disabled" and "Enabled" are the two Azure Policy "enforcement" setting options. If an Azure Policy's "enforcement" is set to "Disablec any "effect" set on this Azure Policy will report but will not make changes.
"Disabled" is the best answer available, although technically incorrect because "Disabled" isn't an Azure Policy "effect".
upvoted 16 times

**Joanale** 1 week, 4 days ago
100% correct, please guys report this question if still no see the option "audit".
upvoted 1 times

**Fal991l** 10 months ago
I am on your side
upvoted 2 times

**Arockia** Most Recent 1 week, 3 days ago
"Disabled" effect ensures that the policy is applied for evaluation purposes but does not enforce any specific actions or modifications on the resources themselves. This allows you to gather compliance data and assess the configuration of resources in your Azure environment without impacting their current state.
upvoted 1 times

**UberTech_1888** 6 months ago

Keyword = "Evaluating"

upvoted 1 times

**Ario** 6 months, 2 weeks ago

D is Correct , Using the "Disabled" effect in Azure Policy is particularly useful for scenarios where you want to assess compliance and gather information without making any immediate changes or disruptions to the resources

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#disabled
This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disabl single assignment instead of disabling all of that policy's assignments.

upvoted 1 times

**NinjaSchoolProfessor** 6 months ago

D as you stated is correct. What the question is missing is a reference to the enforcement mode. You can use the enforcement mode Disable (DoNotEnforce) on your policy assignment to prevent the effect from triggering or activity log entries from being created.

This step gives you a chance to evaluate the compliance results of the new policy on existing resources without impacting work flow.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/evaluate-impact#audit-existing-resources

upvoted 1 times

**alifrancos** 9 months ago

Selected Answer: D

the Deny effect, prevent ressources from creation if that not match the policy, but if it match it will be created or modified, i think that'is clear

upvoted 1 times

**Fal991l** 10 months ago

Selected Answer: A

ChatGPT: If you have to choose only one between Disabled and Deny, and the question does not provide any further details or constraints, then the best answer would be Deny.

The Deny effect is a more appropriate and specific choice for evaluating compliance without changing any resources in an Azure environment, a explicitly blocks non-compliant resources from being created or modified while not modifying any existing resources. This can help ensure that environment remains in compliance and does not drift away from the desired state.

upvoted 2 times

**AJ2021** 10 months, 1 week ago

Selected Answer: D

Before looking to manage new or updated resources with your new policy definition, it's best to see how it evaluates a limited subset of existing resources, such as a test resource group. Use the enforcement mode Disabled (DoNotEnforce) on your policy assignment to prevent the effect from triggering or activity log entries from being created.

This step gives you a chance to evaluate the compliance results of the new policy on existing resources without impacting workflow.

https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-polic

upvoted 2 times

**flaluna** 10 months, 3 weeks ago

Selected Answer: D

Disabled, the answer is d

upvoted 1 times

**D3D1997** 11 months, 1 week ago

Selected Answer: D

Perfect explanation by TKDCom

upvoted 1 times

**buguinha** 11 months, 1 week ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/evaluate-impact#audit-existing-resources

upvoted 1 times

**TJ001** 1 year ago

In the absence of other options Disabled .

upvoted 2 times

**Charl** 1 year, 1 month ago

**Selected Answer: D**

Disabled

upvoted 1 times

**afropoet** 1 year, 1 month ago

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects#disabled

upvoted 1 times

**omarrob** 1 year, 2 months ago

D is the correct answer

https://brainscale.com/understanding-azure-policy/

upvoted 1 times

**kukujiao** 1 year, 2 months ago

**Selected Answer: D**

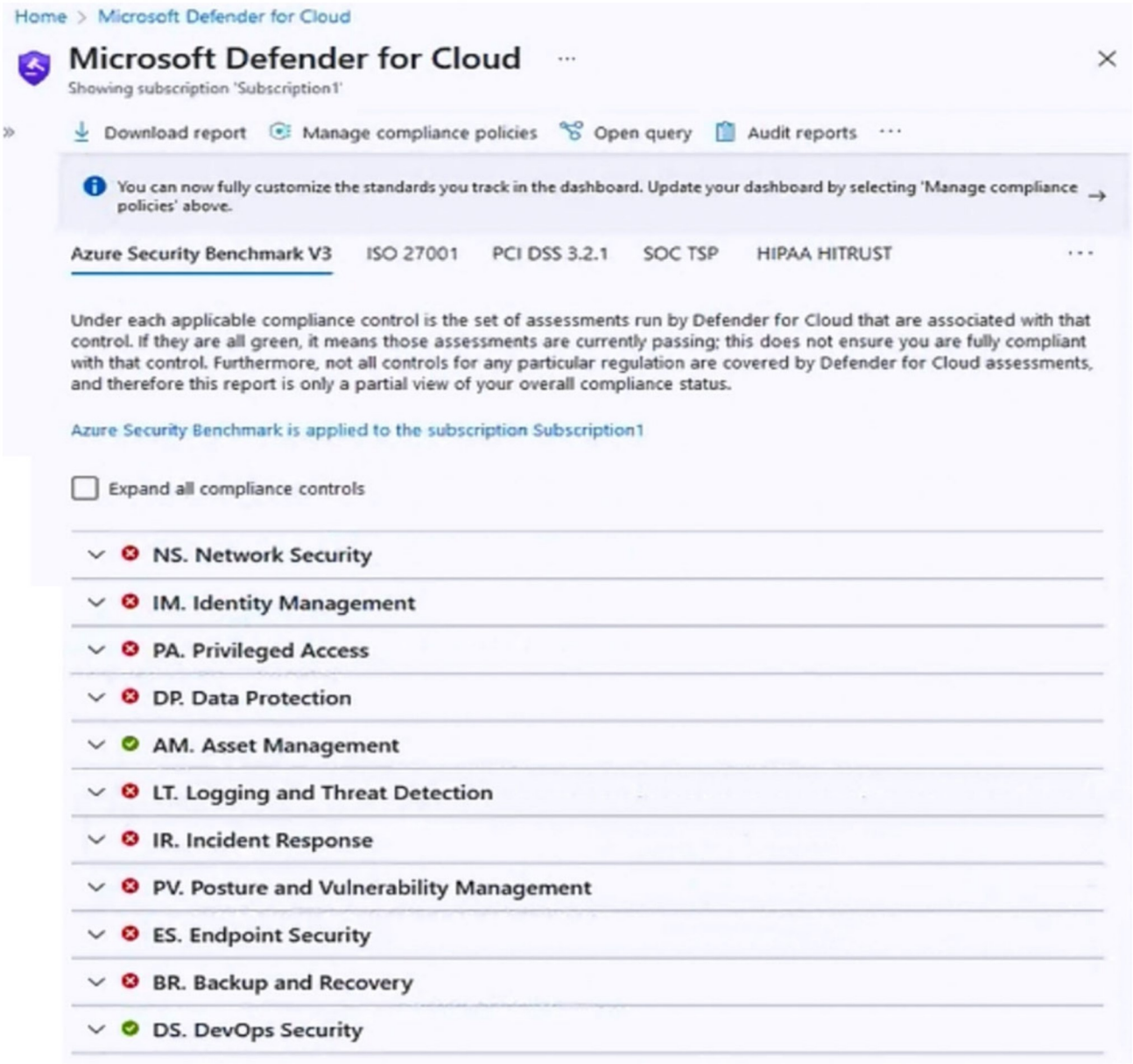
You can't deploy the resource if Deny

upvoted 1 times

Question #2 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.




You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows.

Which compliance control should you evaluate?

A. Asset Management

B. Posture and Vulnerability Management

C. Data Protection

D. Endpoint Security

E. Incident Response

**Correct Answer:** *D*

Microsoft Defender for servers compliance control installed on Windows

Defender for clout "Endpoint Security" azure security benchmark v3

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.

Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.
Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.
Incorrect:
Not A: Asset Management covers controls to ensure security visibility and governance over Azure resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for services and resources (inventory, track, and correct).
Not B: Posture and Vulnerability Management focuses on controls for assessing and improving Azure security posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting, and correction in Azure resources.
Not C: Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key and certificate management in Azure.
Not E: Incident Response covers controls in incident response life cycle - preparation, detection and analysis, containment, and post-incident activities, including using Azure services such as Microsoft Defender for Cloud and Sentinel to automate the incident response process.
Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

*Community vote distribution*

D (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: D

No grey area. Endpoint security is the option that meets the goal.

upvoted 19 times

**tester18128075** Highly Voted 1 year, 4 months ago

D is correct

upvoted 5 times

**Ario** Most Recent 6 months, 2 weeks ago

D is correct

upvoted 1 times

**Itu2022** 7 months ago

was on exam 15/06/23

upvoted 1 times

**edurakhan** 7 months, 3 weeks ago

Exam question 5/23/2023

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 1 times

**D3D1997** 11 months, 2 weeks ago

Selected Answer: D

by definition

upvoted 3 times

**TJ001** 1 year ago

Correct answer

upvoted 2 times

**TJ001** 1 year ago

Defender for Endpoint is available with Defender for Servers Plan1 and 2 .

upvoted 1 times

**prabhjot** 1 year, 4 months ago

correct D is fine

upvoted 5 times

**TheMCT** 1 year, 4 months ago

The given answer D, is correct.

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

great, and yes correct

upvoted 4 times

Question #3 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 subscription and an Azure subscription.

You need to evaluate the existing environment to increase the overall security posture for the following components:

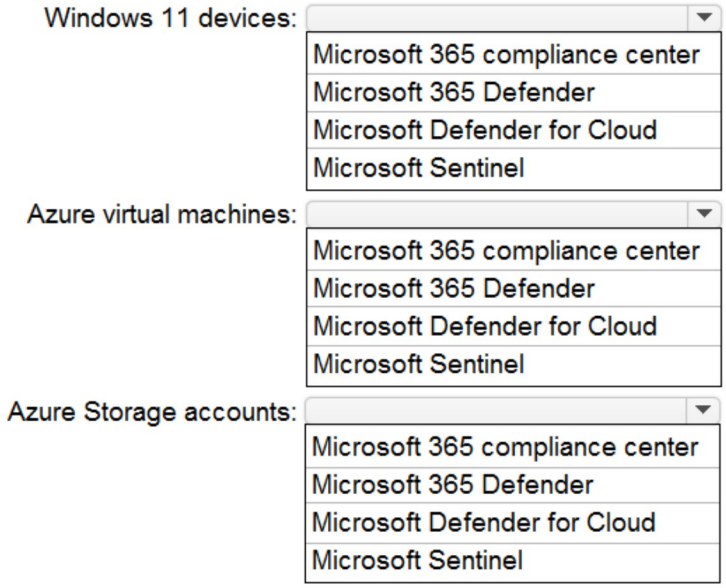
- Windows 11 devices managed by Microsoft Intune
- Azure Storage accounts
- Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

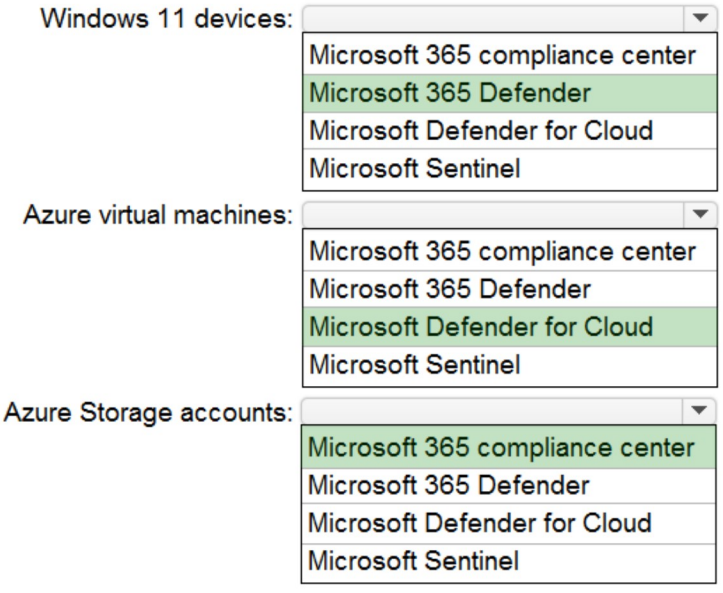
Hot Area:

**Answer Area**




**Correct Answer:**

**Answer Area**




Box 1: Microsoft 365 Defender -

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes
Microsoft Defender for Endpoint.
Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.
Microsoft Defender for Endpoint works with devices that run:

Android -
iOS/iPadOS

Windows 10 -

Windows 11 -
Box 2: Microsoft Defender for Cloud
Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed Instance and Azure Virtual Machines.
Box 3: Microsoft 365 Compliance Center
Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.
Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.
Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender
?
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it).
Selection 2: Microsoft Defender for Cloud.
Selection 3: Microsoft Defender for Cloud.
upvoted 98 times

**Azzzurrre** 1 year ago
Microsoft 365 Defender includes both of those and quite a bit else.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide
"Here's a list of the different Microsoft 365 Defender products and solutions:
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Microsoft Defender Vulnerability Management
Azure Active Directory Identity Protection
Microsoft Data Loss Prevention
App Governance
Microsoft Defender for Cloud"
upvoted 1 times

**bsakabato** 4 months, 1 week ago
The correct wording in the website is :
Here's a list of the different Microsoft 365 Defender products and solutions that Microsoft 365 Defender coordinates with : .....
So Microsoft 365 Defender don't include all theses products, the full list is further down in the documentation and unrelated to the secon and third questions.
upvoted 1 times

**M20200713** 1 year, 3 months ago
agreed x2
upvoted 1 times

**InformationOverload** 1 year, 4 months ago

agreed.
upvoted 3 times

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Defender for cloud on VMs & Storage
Read "Security posture management for storage" in this learning module:
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-security-requirements-for-storag workloads
upvoted 11 times

**Arockia** Most Recent 1 week, 3 days ago
By using Microsoft 365 Defender, you can evaluate the security posture of Windows 11 devices managed by Microsoft Intune. This solution provides advanced threat protection, detection, and response capabilities for endpoints within the Microsoft 365 environment.

For the evaluation of Azure Storage accounts and Azure virtual machines, you should utilize Microsoft Defender for Cloud (formerly known as Azure Defender). It offers comprehensive threat protection and security monitoring for various Azure services, including Azure Storage accounts and Azure virtual machines. This will help you assess their security configurations, detect vulnerabilities, and receive security recommendations.
upvoted 1 times

**Bondaexam** 1 month, 1 week ago
Always look for documentation using the keyword instead of wearing multiple biased hats - Lol - https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction
upvoted 1 times

**Bondaexam** 1 month, 1 week ago
Microsoft Defender for Cloud
upvoted 1 times

**smanzana** 2 months, 3 weeks ago
1. Microsoft 365 Defender
2. Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud
upvoted 3 times

**rahulnair** 3 months ago
Additional context for 3 - Defender for Storage which is part of Defender for cloud
upvoted 1 times

**cyber_sa** 3 months, 1 week ago
got this in exam 6oct23. passed with 896 marks. I answered
1. Microsoft 365 Defender
2. Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud
upvoted 6 times

**ltu2022** 7 months ago
was on exam 15/06/23
upvoted 2 times

**zellck** 8 months ago
1. Microsoft 365 Defender
2. Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud

https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide#microsoft-365-defender-protection
Microsoft 365 Defender services protect:
- Endpoints with Defender for Endpoint - Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detectic automated investigation, and response.
upvoted 1 times

**zellck** 8 months ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers
Microsoft Defender for Servers extends protection to your Windows and Linux machines that run in Azure, Amazon Web Services (AWS), Goc Cloud Platform (GCP), and on-premises. Defender for Servers integrates with Microsoft Defender for Endpoint to provide endpoint detection and response (EDR) and other threat protection features.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction
Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential threats to your storage accounts.
It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption.
upvoted 1 times

**kazaki** 8 months, 1 week ago
Ms 365 defender is post preach defend system so it is not a choice
Section 1 defender for endpoint or compliance center

Section 2 and 3 defender for cloud

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

upvoted 1 times

**Fal991l** 10 months ago

ChatGTP:
Windows 11 Devices: Microsoft 365 Defender
Azure Virtual Machines: Microsoft Sentinel/MS Defender for Cloud
Azure Storage Accounts: Microsoft Defender for Cloud

upvoted 2 times

**AJ2021** 10 months, 1 week ago

Your first two are correct, last one is incorrect.
Should be:
MS 365 Defender
MDC
MDC

upvoted 1 times

**[Removed]** 1 year, 2 months ago

For storage accounts protection it's "Defender for Clouds" hands down. No other choices :)

upvoted 1 times

**SAMSH** 1 year, 3 months ago

was in 20Sep2020 exam

upvoted 1 times

**tester18128075** 1 year, 4 months ago

Windows client - MS 365 Defender
Server and Storage - MS Defender for cloud

upvoted 4 times

**prabhjot** 1 year, 4 months ago

for storage - MS defender for cloud looks the ansn( better will be MS defender for Storage)

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

aaddition - Microsoft Defender for Storage is currently available for Blob storage, Azure Files, and Azure Data Lake Storage Gen2. Account types that support Microsoft Defender for Storage include general-purpose v2, block blob, and Blob storage accounts

upvoted 3 times

Question #4 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

**Correct Answer:** *A*
The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in NIST SP 800-53 Rev. 5.
The following mappings are to the NIST SP 800-53 Rev. 5 controls. Use the navigation on the right to jump directly to a specific compliance domain. Many of the controls are implemented with an Azure Policy initiative definition. To review the complete initiative definition, open Policy in the Azure portal and select the
Definitions page. Then, find and select the NIST SP 800-53 Rev. 5 Regulatory Compliance built-in initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

*Community vote distribution*
A (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: A
The given answer is probably the closest. In real life I'd add a regulatory compliance standard in Defender for Cloud. This question might be see written another way where that is the answer.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-a available-in-defender-for-cloud
upvoted 18 times

**NinjaSchoolProfessor** 6 months ago
A - I agree that I'd probably use Defender for Cloud as the UI is much better, however this service simply doesn't do the work, rather it invok the Azure Policy initiative which is then reported back to Defender for Cloud.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/policy-reference
upvoted 2 times

**ltu2022** Most Recent 7 months ago
was on exam 15/06/23
upvoted 3 times

**zellck** 8 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5
upvoted 1 times

**AJ2021** 10 months, 1 week ago
Selected Answer: A
A is correct
upvoted 2 times

**Nappy123** 11 months, 2 weeks ago
One keyword in the question is "review". Answer A would "assign" the policy initiative - not "review". Given that the company has Defender for Cloud, Answer C would be my choice.
upvoted 3 times

**Toschu** 9 months, 3 weeks ago
I thought the same, but it says for "the current subscription". Assigning an initiative directly to the mentioned subscription might be easier if

there are several.

upvoted 1 times

**TJ001** 1 year ago

Correct Answer.. It is policy initiative assignment .. can be done directly from Policy Blade or Insider Defender for Cloud..end of the day it is an Azure policy .. Correct Answer A

upvoted 1 times

**Zstefanovic** 1 year, 3 months ago

Selected Answer: A

A, built in policy to comply with that regulation

upvoted 1 times

**tester18128075** 1 year, 4 months ago

A is correct

upvoted 2 times

**prabhjot** 1 year, 4 months ago

ans seems correct ( azure policy) as in another option - Defender for Cloud, review the Azure security baseline for audit report. ( review it is mentioned not creating from custom policy )

upvoted 1 times

Question #5 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have an Amazon Web Services (AWS) implementation.
You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc.
Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Containers

B. Microsoft Defender for servers

C. Azure Active Directory (Azure AD) Conditional Access

D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

E. Azure Policy

**Correct Answer:** *ACE*
Environment settings page (in preview) (recommended) - This preview page provides a greatly improved, simpler, onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud's enhanced security features to your AWS resources:
*(A) Microsoft Defender for Containers brings threat detection and advanced defenses to your Amazon EKS clusters. This plan includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control recommendations and more.
* Microsoft Defender for Servers, though it requires Arc.
C: AWS installations can benefit from Conditional Access. Defender for Cloud Apps integrates with Azure AD Conditional Access to enforce additional restrictions, and monitors and protects sessions after sign-in. Defender for Cloud Apps uses user behavior analytics (UBA) and other AWS APIs to monitor sessions and users and to support information protection.
E: Kubernetes data plane hardening.
For a bundle of recommendations to protect the workloads of your Kubernetes containers, install the Azure Policy for Kubernetes. You can also auto deploy this component as explained in enable auto provisioning of agents and extensions.
With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure to enforce the best practices and mandate them for future workloads.
Incorrect:
Not B: To enable the Defender for Servers plan you need Azure Arc for servers installed on your EC2 instances.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-security-solutions

*Community vote distribution*
ACE (47%) ACD (40%) 8%

**zts** Highly Voted 1 year, 4 months ago

Selected Answer: ACE
I would go for ACE. That being said, this link covers Azure Policy Extension in hardening Kubernetes data plane. https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=aws-eks
upvoted 18 times

**[Removed]** 1 year, 4 months ago
Not B (servers require Arc). Not D: PIM is more of the kind nice-to-have.
upvoted 1 times

**Fal991l** 10 months ago
No, Microsoft Defender for servers does not require Azure Arc to extend protection to hybrid cloud workloads, including servers running AWS.

Azure Arc is a separate Azure service that enables you to manage servers, Kubernetes clusters, and applications on-premises, at the edge, and in multi-cloud environments from a single control plane. It provides a centralized management experience and enables you to apply policies, update servers, and deploy applications across your hybrid cloud environment.

However, if you want to use Azure Arc to manage your servers running on AWS, you can do so by using the Azure Arc enabled servers feature. This feature allows you to onboard your AWS instances to Azure Arc and manage them through the Azure portal or Azure APIs. Ir this case, you can also use Microsoft Defender for servers to extend protection to those AWS instances.

upvoted 2 times

**mynk29** 12 months ago

PIM is privilege identity management.. I wouldn't say its nice to have..its a must

upvoted 3 times

**Raven84** 4 weeks, 1 day ago

its only a security feature if you use 4-eyes principle. JIT access is no security feature if u can give roles by urself

upvoted 1 times

**jasscomp** 3 months, 2 weeks ago

Yes, it's a must for protecting identity but not the answer for this requirement.

upvoted 2 times

**Jajee** Highly Voted 11 months, 2 weeks ago

E can not be an answer, because in-order to apply Azure Policy on AWS based resources, you must need to use Azure Arc, which can not be the case based on requirements.

So, ACD can be the possible answers.

upvoted 11 times

**ayadmawla** Most Recent 1 week, 1 day ago

Selected Answer: ACE

ACE seems right as per the following: https://learn.microsoft.com/en-us/defender-cloud-apps/protect-aws

Policy / Sign-in / containers

upvoted 1 times

**Murtuza** 1 week, 2 days ago

Microsoft Entra ID offers several capabilities for direct integration with AWS:

SSO across legacy, traditional, and modern authentication solutions.
MFA, including integration with several third-party solutions from Microsoft Intelligent Security Association (MISA) partners.
Powerful Conditional Access features for strong authentication and strict governance. Microsoft Entra ID uses Conditional Access policies and ris based assessments to authenticate and authorize user access to the AWS Management Console and AWS resources.
Large-scale threat detection and automated response. Microsoft Entra ID processes over 30 billion authentication requests per day, along with trillions of signals about threats worldwide.
Privileged Access Management (PAM) to enable Just-In-Time (JIT) provisioning to specific resources.

upvoted 1 times

**Murtuza** 1 week, 2 days ago

Selected Answer: ACE

A, C, E are correct choices

upvoted 1 times

**Murtuza** 2 weeks ago

E: Kubernetes data plane hardening.
For a bundle of recommendations to protect the workloads of your Kubernetes containers, install the Azure Policy for Kubernetes. You can also auto deploy this component as explained in enable auto provisioning of agents and extensions.
With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure to enforce the best practices and mandate them for future workloads.

upvoted 1 times

**juanpe147** 1 month ago

ACD, Policy requires Axure Policy

upvoted 1 times

**Bondaexam** 1 month, 1 week ago

C. Azure Active Directory (Azure AD) Conditional Access Most VotedMost Voted
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Most Voted
E. Azure Policy Most Voted Both MS Defender for servers and containers need Arc - you could simply google it and it would pull into MS documentation.

upvoted 1 times

**pooppants** 1 month, 3 weeks ago

Selected Answer: ACD

I dont see any references anywhere to using Azure Policy in AWS

upvoted 1 times

**smanzana** 2 months, 3 weeks ago

ACD is OK

upvoted 1 times

**mdijoux25** 4 months, 3 weeks ago

Selected Answer: ACD

ACD because azure policy required Azure A so PIM is a good option

upvoted 1 times

**jasscomp** 3 months, 2 weeks ago

PIM doesn't answer the requirment. PIM protects admin accounts

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

I think ACD is the answer. Azure policy can not work without an agent, and since Azure Arc is not in scope I can only see PIM on this article:
https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-ad-security

upvoted 2 times

**Datta2023** 5 months ago

As per https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-servers-plan, Defender for server is one of the answers.

upvoted 1 times

**Ario** 6 months, 2 weeks ago

ACE are correct

upvoted 1 times

**guchao2000** 7 months ago

ACD
A - Defender for Containers
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-architecture?tabs=defender-for-container-arch-aks

C - AAD Conditional Access
D - AAD PIM
https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-ad-security
Powerful Conditional Access features for strong authentication and strict governance. Azure AD uses Conditional Access policies and risk-based assessments to authenticate and authorize user access to the AWS Management Console and AWS resources.

You can expand PIM to any delegated permission by controlling access to custom groups, such as the ones you created for access to AWS roles.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: ACD

ACD is the answer.

https://learn.microsoft.com/en-us/azure/architecture/guide/aws/aws-azure-security-solutions#workflow
Azure AD provides centralized single sign-on (SSO) and strong authentication through multifactor authentication and the conditional access feature. Azure AD supports AWS role-based identities and authorization for access to AWS resources.

https://learn.microsoft.com/en-us/azure/architecture/guide/aws/aws-azure-security-solutions#defender-for-cloud-for-cspm-and-cwp-platforms
cwpp
Microsoft Defender for Containers brings threat detection and advanced defenses to supported Amazon EKS clusters.

upvoted 2 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-ad-security#advanced-azure-ad-identity-management-with-aws-accounts
Privileged Identity Management (PIM) to provide advanced controls for all delegated roles within Azure and Microsoft 365. For example, inst of an administrator always using the Global Admin role, they have permission to activate the role on demand. This permission deactivates aft a set time limit (one hour, for example). PIM logs all activations and has other controls that can further restrict the activation capabilities. PIM further protects your identity architecture by ensuring extra layers of governance and protection before administrators can make changes.

You can expand PIM to any delegated permission by controlling access to custom groups, such as the ones you created for access to AWS ro

upvoted 1 times

**bmulvIT** 8 months ago

Selected Answer: ACE

Given answers are correct. Arc is listed as prerequisite for Defender for servers:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

upvoted 3 times

Question #6 *Topic 2*

Your company has on-premises network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency for developers.
Which three actions should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.

B. Deploy a Remote Desktop server to an Azure region located in France.

C. Migrate from the Remote Desktop server to Azure Virtual Desktop.

D. Implement Azure Firewall to restrict host pool outbound access.

E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

**Correct Answer:** *CDE*
E: Organizations can use this location for common tasks like:
Requiring multi-factor authentication for users accessing a service when they're off the corporate network.
Blocking access for users accessing a service from specific countries or regions.
The location is determined by the public IP address a client provides to Azure Active Directory or GPS coordinates provided by the Microsoft Authenticator app.
Conditional Access policies by default apply to all IPv4 and IPv6 addresses.
CD: Use Azure Firewall to protect Azure Virtual Desktop deployments.
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
Reference:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

*Community vote distribution*
CDE (86%) 10%

**zellck** Highly Voted 8 months ago
Selected Answer: CDE
CDE is the answer.

https://learn.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop?tabs=azure
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
upvoted 5 times

**zellck** 8 months ago
https://learn.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa
Users can sign into Azure Virtual Desktop from anywhere using different devices and clients. However, there are certain measures you should take to help keep yourself and your users safe. Using Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) with Azure Virtual Desktop prompts users during the sign-in process for another form of identification in addition to their username and password. You can enforce MFA for Azure Virtual Desktop using Conditional Access, and can also configure whether it applies to the web client, mobile apps, desktop clients, or all clients.
upvoted 3 times

**Ario** Most Recent 6 months, 2 weeks ago

ACE are correct answers here
upvoted 1 times

**Holii** 6 months, 2 weeks ago

This question is terrible.
B could work to solve the latency issue...and MFA is explicitly stated as a requirement to migrate their existing firewall, but in the context of Zero Trust > latency I would go with E over B.

CDE.
upvoted 1 times

**Holii** 6 months, 2 weeks ago

is not stated as a requirement to migrate their existing firewall*
upvoted 1 times

**uffman** 8 months, 3 weeks ago

Selected Answer: CDE
Correct.
upvoted 2 times

**Gurulee** 9 months, 1 week ago

Selected Answer: CDE
This is a tricky one... Based on zero trust, minimizing latency, and keeping the existing firewall requirement in place; I'd go with C,D,E
upvoted 2 times

**Holii** 6 months, 2 weeks ago

How exactly does CDE do anything to minimizing latency?
upvoted 1 times

**Fal991l** 10 months ago

Selected Answer: ABE
A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges: This action will restrict access to the on-premises network and the Azure subscription to only specific logical groupings of IP address ranges. This helps ensure that onl authorized traffic is allowed to access the resources.

B. Deploy a Remote Desktop server to an Azure region located in France: This action will help reduce latency for developers by ensuring that the have a closer connection to the Remote Desktop server. This can be achieved by deploying the Remote Desktop server in an Azure region locate in France.

E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations: This action will h ensure that only authorized users are allowed to access the resources. Azure AD Conditional Access can be used to enforce MFA and restrict acc based on named locations. This helps ensure that only authorized users are accessing the resources.
upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

Selected Answer: BCE
AI: To implement a modern security solution based on the Zero Trust model and minimize latency for developers, the following actions should b recommended:

Migrate from the Remote Desktop server to Azure Virtual Desktop: Azure Virtual Desktop is a modern solution that allows users to securely acce their virtual desktops and applications from any device, anywhere. By migrating from the on-premises Remote Desktop server to Azure Virtual Desktop, you can provide secure remote access to the virtual machines hosted in Azure without compromising on security.
upvoted 1 times

**Fal991l** 10 months ago

ChatGPT:
I apologize for the confusion. My previous response was incorrect. The recommended actions for a modern security solution based on the Ze Trust model that minimizes latency for developers and allows access to Azure virtual machines hosted in the Azure subscription by a third-pa development firm from France are:

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Deploy a Remote Desktop server to an Azure region located in France.
E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

I hope this clears up any confusion.
upvoted 1 times

**jasscomp** 3 months, 2 weeks ago

ChatGPT isn't always right and you need to feed it more info to for more contect.

option B isn't a modern 'security' feature
upvoted 1 times

**Fal991l** 10 months, 2 weeks ago

Deploy a Remote Desktop server to an Azure region located in France: To minimize latency for developers, you can deploy a Remote Desktop server in an Azure region located in France. This will ensure that developers can access the resources they need quickly and efficiently.

upvoted 1 times

**Fal991l** 10 months, 2 weeks ago

Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations: Azure AD Conditional Access allows you to control access to resources based on user identity, device health, and location. By configuring Azure AD Conditional Access with MFA and named locations, you can ensure that only authorized users are able to access the resources they need, from trusted locations.

upvoted 1 times

**Fal991l** 10 months, 2 weeks ago

Therefore, the correct answers are C. Migrate from the Remote Desktop server to Azure Virtual Desktop, B. Deploy a Remote Desktop server to an Azure region located in France, and E. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.

upvoted 2 times

**jasscomp** 3 months, 2 weeks ago

Don't use ChatGPT for answers to Microsoft exam questions - I tested it on my renewal exam and it got 50% wrong!

upvoted 1 times

**TJ001** 1 year ago

CDE is perfect

upvoted 4 times

**Bill831231** 1 year, 2 months ago

why there is no option for bastion host?

upvoted 2 times

**mistralst** 1 year, 1 month ago

Because: "by using custom administrative tools installed on the Remote Desktop server."

upvoted 2 times

**PeteNZ** 10 months, 2 weeks ago

The real reason is that they are replacing an RDS environment, so the Azure version of this is AVD. Bastion doesn't support connections to AVD, so it wouldn't be useful in this respect.

upvoted 2 times

**nicknamedude** 1 year, 1 month ago

Bastion for OBM

upvoted 2 times

**JCkD4Ni3L** 1 year, 3 months ago

Selected Answer: CDE

CDE is appropriate

upvoted 2 times

**tester18128075** 1 year, 4 months ago

CDE IS CORRECT

upvoted 3 times

**InformationOverload** 1 year, 4 months ago

Selected Answer: CDE

CDE looks fine to me

upvoted 3 times

**zts** 1 year, 4 months ago

Selected Answer: CDE

same here.

upvoted 2 times

**HardcodedCloud** 1 year, 4 months ago

Selected Answer: CDE

Correct answer

upvoted 2 times

Question #7 *Topic 2*

HOTSPOT -

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation.

You need to recommend a security posture management solution for the following components:

☞ Azure IoT Edge devices

AWS EC2 instances -

▪

Which services should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

For the IoT Edge devices:

- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:

- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

**Correct Answer:**

**Answer Area**

For the IoT Edge devices: Microsoft Defender for IoT

For the AWS EC2 instances: Microsoft Defender for Cloud and Azure Arc

Box 1: Microsoft Defender for IoT

Microsoft Defender for IoT is a unified security solution for identifying IoT and OT devices, vulnerabilities, and threats and managing them through a central interface.

Azure IoT Edge provides powerful capabilities to manage and perform business workflows at the edge. The key part that IoT Edge plays in IoT environments make it particularly attractive for malicious actors.

Defender for IoT azureiotsecurity provides a comprehensive security solution for your IoT Edge devices. Defender for IoT module collects, aggregates and analyzes raw security data from your Operating System and container system into actionable security recommendations and alerts.
Box 2: Microsoft Defender for Cloud and Azure Arc
Microsoft Defender for Cloud provides the following features in the CSPM (Cloud Security Posture Management) category in the multi-cloud scenario for AWS.
Take into account that some of them require Defender plan to be enabled (such as Regulatory Compliance):
* Detection of security misconfigurations
* Single view showing Security Center recommendations and AWS Security Hub findings
* Incorporation of AWS resources into Security Center's secure score calculations
* Regulatory compliance assessments of AWS resources
Security Center uses Azure Arc to deploy the Log Analytics agent to AWS instances.
Incorrect:
AWS EC2 Microsoft Defender for Cloud Apps
Amazon Web Services is an IaaS provider that enables your organization to host and manage their entire workloads in the cloud. Along with the benefits of leveraging infrastructure in the cloud, your organization's most critical assets may be exposed to threats. Exposed assets include storage instances with potentially sensitive information, compute resources that operate some of your most critical applications, ports, and virtual private networks that enable access to your organization.
Connecting AWS to Defender for Cloud Apps helps you secure your assets and detect potential threats by monitoring administrative and sign-in activities, notifying on possible brute force attacks, malicious use of a privileged user account, unusual deletions of VMs, and publicly exposed storage buckets.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/security-edge-architecture https://samilamppu.com/2021/11/04/multi-cloud-security-posture-management-in-microsoft-defender-for-cloud/

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Good answer, bad references
Defender for IoT
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture

EC2 instances need Defender for Cloud by way of Arc
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings
https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations
upvoted 14 times

**zts** 1 year, 4 months ago
We should still be thankful with examtopic researchers for their efforts, and least such examples makes us to validate our review and correct those mistakes :D)
upvoted 13 times

**hb0011** 1 year, 3 months ago
So this means the answer has to be Defender for IoT and Azure Arc only.
upvoted 2 times

**SAMSH** Highly Voted 1 year, 3 months ago
was in 20Sep2020 exam
upvoted 5 times

**AzureJobsTillRetire** 11 months ago
I think he meant that he took the exam on 20 Sept 2022. Thank him for taking the time to verify that this question was in exam. Not many people do that. I was one of those lazy people as well. sorry for those see this comment...
upvoted 4 times

**PeteNZ** 10 months, 2 weeks ago
This exam wasn't even out then. Dude posts this everywhere.
upvoted 1 times

**Pete_4779** 1 year, 3 months ago
Did you get it right? What was your score?
upvoted 1 times

**JakeCallham** 1 year, 3 months ago
Dude stop this nonsense
upvoted 26 times

**ayadmawla** Most Recent 1 week, 1 day ago

AWS accounts should have Azure Arc auto provisioning enabled For full visibility of the security content from Microsoft Defender for servers, EC instances should be connected to Azure Arc. To ensure that all eligible EC2 instances automatically receive Azure Arc, enable auto-provisioning from Defender for Cloud at the AWS account level.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws

upvoted 1 times

**Arockia** 1 week, 2 days ago

For Question 1: Azure IoT Edge devices, the recommended security posture management solution is:

e. Microsoft Defender for IoT: Microsoft Defender for IoT is designed specifically for securing IoT devices and provides advanced threat protecti vulnerability management, and continuous monitoring for IoT environments. It helps protect Azure IoT Edge devices by detecting and respondi to security threats.

For Question 2: AWS EC2 instances, the recommended security posture management solution is:

f. Microsoft Defender for Endpoint only: Microsoft Defender for Endpoint (formerly known as Microsoft Defender ATP) is a comprehensive endp security solution that provides protection against various threats, including malware, advanced attacks, and vulnerabilities. While Azure Arc can used to manage and monitor AWS resources, Microsoft Defender for Endpoint is the appropriate choice for securing the EC2 instances.

upvoted 1 times

**Ramye** 1 week, 3 days ago

Any idea, why Microsoft XDR references don't include Defender for IoT/OT. Below is what I see mostly

The component services that are part of the Microsoft Defender XDR stack are:
Microsoft Defender for Identity
Microsoft Defender for Office 365
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint

upvoted 1 times

**Murtuza** 2 weeks ago

1. Microsoft Defender for IoT
2. Microsoft Defender for Cloud and Azure Arc

upvoted 1 times

**zellck** 8 months ago

1. Microsoft Defender for IoT
2. Microsoft Defender for Cloud and Azure Arc

https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/overview
Microsoft Defender for IoT is a unified security solution built specifically to identify IoT and OT devices, vulnerabilities, and threats. Use Defende for IoT to secure your entire IoT/OT environment, including existing devices that may not have built-in security agents.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings
With cloud workloads commonly spanning multiple cloud platforms, cloud security services must do the same. Microsoft Defender for Cloud protects workloads in Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), GitHub and Azure DevOps (ADO).

To enable the Defender for Servers plan, you'll need:
- Azure Arc for servers installed on your EC2 instances.

upvoted 4 times

**calotta1** 4 months, 3 weeks ago

You are right about Azure Arc, but once the AWS connector is configured on MDC, and auto-provisioning enabled, Azure Arc will install on th EC2 instances.

"We recommend that you use the auto-provisioning process to install Azure Arc on all of your existing and future EC2 instances"

upvoted 1 times

**GeVanDerBe** 8 months, 3 weeks ago

You need to recommend a security posture management solution. with that for AWS EC2 MDC only. https://learn.microsoft.com/en-us/azure /defender-for-cloud/quickstart-onboard-aws?pivots=env-settings. --> Provide an agentless connection.

upvoted 1 times

**GeVanDerBe** 8 months, 3 weeks ago

wrong response. Forget my comment above!

upvoted 1 times

**AJ2021** 10 months, 1 week ago

correct

upvoted 1 times

**tester18128075** 1 year, 4 months ago

correct

upvoted 3 times

**JMuller** 1 year, 4 months ago

correct

upvoted 1 times

**Alex_Burlachenko** 1 year, 4 months ago

correct

upvoted 3 times

Question #8 *Topic 2*

Your company has a hybrid cloud infrastructure.
The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company's on-premises network.
The company's secutity policy prevents the use of personal devices for accessing company data and applications.
You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.
What should you include in the recommendation?

A. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

B. Redesign the VPN infrastructure by adopting a split tunnel configuration.

C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.

D. Migrate the on-premises applications to cloud-based applications.

**Correct Answer:** *A*
You can connect an Azure Virtual Desktop to an on-premises network using a virtual private network (VPN), or use Azure ExpressRoute to extend the on- premises network into the Azure cloud over a private connection.
* Azure AD: Azure Virtual Desktop uses Azure AD for identity and access management. Azure AD integration applies Azure AD security features like conditional access, multi-factor authentication, and the Intelligent Security Graph, and helps maintain app compatibility in domain-joined VMs.
* Azure Virtual Desktop, enable Microsoft Defender for Cloud.
We recommend enabling Microsoft Defender for Cloud's enhanced security features to:
Manage vulnerabilities.
Assess compliance with common frameworks like PCI.
* Microsoft Defender for Cloud Apps, formerly known as Microsoft Cloud App Security, is a comprehensive solution for security and compliance teams enabling users in the organization, local and remote, to safely adopt business applications without compromising productivity.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cloud-apps/ba-p/2835842

*Community vote distribution*
A (100%)

**Ramkid** Highly Voted 1 year ago
it is really nice to see that everyone says the same answer
upvoted 10 times

**zellck** Most Recent 8 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/virtual-desktop/overview

https://learn.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa
Users can sign into Azure Virtual Desktop from anywhere using different devices and clients. However, there are certain measures you should ta to help keep yourself and your users safe. Using Azure Active Directory (Azure AD) Multi-Factor Authentication (MFA) with Azure Virtual Desktop prompts users during the sign-in process for another form of identification in addition to their username and password. You can enforce MFA fc Azure Virtual Desktop using Conditional Access, and can also configure whether it applies to the web client, mobile apps, desktop clients, or all clients.
upvoted 1 times

**zellck** 7 months, 3 weeks ago
Gotten this in May 2023 exam.
upvoted 2 times

**uffman** 8 months, 3 weeks ago
Selected Answer: A
Correct, use AVD.

upvoted 1 times

**Xax** 9 months, 3 weeks ago

I recommend deploying Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access to provide temporary employee with access to company resources. This solution can scale on demand and is secure as it allows you to control access to your applications and d based on conditions such as user location, device compliance, and real-time risk.

This solution also provides a single console for managing devices and applications across all platforms including Windows, Android, iOS, and macOS.

upvoted 1 times

**TJ001** 1 year ago

indeed no brainer

upvoted 2 times

**googler015** 1 year, 1 month ago

No brainer - The answer is A

upvoted 1 times

**IXone** 1 year, 2 months ago

A is correct

upvoted 1 times

**theOldSoldier** 1 year, 3 months ago

I would go with A

upvoted 2 times

**tester18128075** 1 year, 4 months ago

vdi is correct

upvoted 1 times

**InformationOverload** 1 year, 4 months ago

Selected Answer: A

Very logical. Nobrainer.

upvoted 1 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: A

That is the only way.

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

A is correct

upvoted 1 times

Question #9 *Topic 2*

Your company is preparing for cloud adoption.
You are designing security for Azure landing zones.
Which two preventative controls can you implement to increase the secure score? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure Web Application Firewall (WAF)

B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

**Correct Answer:** *BC*
B: Azure identity and access for landing zones, Privileged Identity Management (PIM)
Use Azure AD Privileged Identity Management (PIM) to establish zero-trust and least privilege access. Map your organization's roles to the minimum access levels needed. Azure AD PIM can use Azure native tools, extend current tools and processes, or use both current and native tools as needed.
Azure identity and access for landing zones, Design recommendations include:
* (B) Use Azure AD managed identities for Azure resources to avoid credential-based authentication. Many security breaches of public cloud resources originate with credential theft embedded in code or other text. Enforcing managed identities for programmatic access greatly reduces the risk of credential theft.
* Etc.
C: Improve landing zone security, onboard Microsoft Sentinel
You can enable Microsoft Sentinel, and then set up data connectors to monitor and protect your environment. After you connect your data sources using data connectors, you choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.
Note: Landing zone security best practices
The following list of reference architectures and best practices provides examples of ways to improve landing zone security:
Microsoft Defender for Cloud: Onboard a subscription to Defender for Cloud.
Microsoft Sentinel: Onboard to Microsoft Sentinel to provide a security information event management (SIEM) and security orchestration automated response
(SOAR) solution.
Secure network architecture: Reference architecture for implementing a perimeter network and secure network architecture.
Identity management and access control: Series of best practices for implementing identity and access to secure a landing zone in Azure.
Network security practices: Provides additional best practices for securing the network.
Operational security provides best practices for increasing operational security in Azure.
The Security Baseline discipline: Example of developing a governance-driven security baseline to enforce security requirements.
Incorrect:
Not E: Implementing alerts is not a preventive measure.
Reference:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones
https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

*Community vote distribution*
AD (80%) 9% 4%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: AD
This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secu score. Sentinel & PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

Which leads me to believe that only firewalls fit the bill.

upvoted 41 times

**PeteNZ** 11 months, 1 week ago

Well, disagree. This is about landing zones and if you scroll down here, I'd say PIM would definitely be an answer.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security

upvoted 7 times

**meelaran** 2 weeks, 1 day ago

it does not increase security score

upvoted 1 times

**NinjaSchoolProfessor** 6 months ago

ABCD are correct. All items except "Defender for Cloud alerts" are tools that improve security and are available for use with Azure Landing Zone.

upvoted 1 times

**Ramkid** 10 months, 1 week ago

I agree with you.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones#privileged-identity-management-pim

upvoted 1 times

**mikenyga** 1 year, 4 months ago

Why defender for cloud? Question about landing zone, (CAF) answer correct.
Onboard Microsoft Sentinel.
Azure Identity Management and access control security best practices.
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/landing-zone-security

upvoted 2 times

**alpars** 1 year, 4 months ago

Sentinel does not increase security score and it is used widely for detection and correlation.

upvoted 4 times

**jarihd1** 1 year, 3 months ago

What if - there is no application gateway / traffic manager / CDN etc configured - how you will configure WAF ? CAF needs basic things for t security readiness! Do not confuse people.

upvoted 2 times

**HardcodedCloud** Highly Voted 1 year, 4 months ago

Selected Answer: AD

Preventative controls are WAF & Firewall

upvoted 19 times

**ayadmawla** Most Recent 1 week, 1 day ago

Selected Answer: BC

Answers given are correct and are inline with the Security design component of an Azure landing zone: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security

upvoted 2 times

**Azerty1313** 1 month, 1 week ago

Here you find the list:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/security

The question to answer which ones are preventative? According to me WAF, Firewall & PIM.
Next question which does improve the score? Not sure there.

upvoted 1 times

**rahulnair** 3 months ago

Selected Answer: BC

Improve SS for landing zone explicitly calls out sentinel and PIM. WAF and FW are not classified as basic controls
"Azure native controls. Azure Firewall and Azure Web Application Firewall offer basic security advantages. Advantages are a fully stateful firewall a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration."

upvoted 2 times

**yyYPpp** 3 months ago

Selected Answer: AB

The two preventative controls that can be implemented to increase the secure score in Azure landing zones are:

A. Azure Web Application Firewall (WAF)
B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

while C. Microsoft Sentinel, D. Azure Firewall, and E. Microsoft Defender for Cloud alerts are all valuable tools for enhancing security in Azure, th are not specifically categorized as preventative controls for increasing the secure score.

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

WAF is only required for specific scenario, so many ALZ do not have a requirement for WAF but will PIM is a must for any deployment. AFW is similar, must have on any secure ALZ.

upvoted 1 times

**celomomo** 4 months, 3 weeks ago

Selected Answer: AD

Both Azure WAF and Azure Firewall are preventative controls that enhance the security posture of your Azure environment by protecting agains unauthorized access, threats, and attacks. These controls help in securing your applications and network traffic, contributing to an improved sec score.

upvoted 1 times

**Ario** 6 months, 2 weeks ago

A and D are correct

upvoted 1 times

**rhylos** 6 months, 3 weeks ago

Selected Answer: AD

chatgpt:
A. Azure Web Application Firewall (WAF): Azure WAF helps protect your web applications from common exploits and vulnerabilities by providing centralized protection, monitoring, and logging for your web traffic. It can prevent attacks such as SQL injection, cross-site scripting (XSS), and other malicious activities targeted at web applications.
D. Azure Firewall: Azure Firewall is a managed, cloud-based network security service that provides network traffic filtering and protection for Azu resources. It acts as a preventive control by allowing you to define and enforce network and application-level policies to secure your Azure landi zones. Azure Firewall provides inbound and outbound traffic filtering, application-level inspection, and threat intelligence integration to protect against unauthorized access and threats.

Both Azure WAF and Azure Firewall help increase the secure score by providing essential security controls to protect your Azure landing zones.

upvoted 1 times

**ltu2022** 7 months ago

was on exam 15/06/23

upvoted 1 times

**zellck** 8 months ago

Selected Answer: AD

AD is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
- Restrict unauthorized network access
Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.
Use these recommendations to manage Defender for Cloud's adaptive network hardening settings, ensure you've configured Azure Private Link all relevant PaaS services, enable Azure Firewall on your virtual networks, and more.

- Protect applications against DDoS attacks
Azure's advanced networking security solutions include Azure DDoS Protection, Azure Web Application Firewall, and the Azure Policy Add-on fo Kubernetes. Use these recommendations to ensure your applications are protected with these tools and others.

upvoted 3 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 2 times

**uffman** 8 months, 3 weeks ago

Selected Answer: AD

Key is "Preventative controls".

upvoted 2 times

**shahnawazkhot** 9 months, 2 weeks ago

Firewall and WAF comes under networking whereas the question is about security related preventive controls - which appears to be B&C - PIM Sentinel. Hence, the answer is correct. B&C.

upvoted 1 times

**vitodobra** 9 months, 3 weeks ago

Selected Answer: AD

A. Cortafuegos de aplicaciones web de Azure (WAF) - Proporciona protección avanzada para aplicaciones web, protege las aplicaciones web de ataques comunes como SQL Injection y Cross-site scripting (XSS).

D. Cortafuegos de Azure - Ayuda a proteger los recursos de Azure en la nube de tráfico de red no deseado. Se puede configurar para permitir o

denegar el tráfico de red basado en origen y destino, dirección IP y puerto de origen y destino.

B, C y E también son soluciones de seguridad importantes, pero no son específicas para los controles preventivos en las zonas de aterrizaje de Azure.

upvoted 1 times

**OK2020** 10 months, 2 weeks ago

Talking about preventive, I see the below are most effective tools that would increase teh security score of the landing zone, which is technically identical to securing your Cloud adoption:
1. Azure FW: check traffic, enforce security policies, protect against atacks
2. SENTINEL: provides wholistic security threat detection and response
My answers: CD

upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

**Selected Answer: BD**

The two preventative controls that can be implemented to increase the secure score for Azure landing zones are:

D. Azure Firewall: It provides network-level protection to the resources deployed in Azure. It can be used to enforce network security policies an filtering rules to control access to network resources.

B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM): It is used to manage, control, and monitor access to resources in Az It allows you to grant just-in-time access to the resources that need to be accessed and monitor access to resources to prevent misuse.

upvoted 4 times

**meelaran** 2 weeks, 1 day ago

does PIM increase secure score ..... not

upvoted 1 times

**Fal991l** 10 months ago

Azure AD Privileged Identity Management (PIM) can be considered a preventative control as it helps to reduce the risk of privileged accounts being compromised by implementing just-in-time access, approval workflows, and time-bound access. This reduces the attack surface by reducing the amount of time a privileged account is active and available to be exploited by attackers.

upvoted 1 times

**Fal991l** 10 months, 2 weeks ago

From ChatGPT

upvoted 1 times

Question #10 *Topic 2*

You are designing security for an Azure landing zone.

Your company identifies the following compliance and privacy requirements:

- Encrypt cardholder data by using encryption keys managed by the company.
- Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed keys.

B. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.

C. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM.

D. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.

**Correct Answer:** *CD*

C: Azure Key Vault Managed HSM (Hardware Security Module) is a fully managed, highly available, single-tenant, standards-compliant cloud service that enables you to safeguard cryptographic keys for your cloud applications, using FIPS 140-2 Level 3 validated HSMs.

D: You can generate HSM-protected keys in your on-premise HSM and import them securely into Managed HSM.

Incorrect:

Not A: The company must manage the keys, not Microsoft.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

*Community vote distribution*

BC (67%) CD (32%)

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago

I would like to select B & C

upvoted 28 times

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: CD

Hardware Security Module takes the cake. Want to use your own keys? Great. You can still do that with BYOK.

upvoted 13 times

**mynk29** 11 months, 4 weeks ago

Azure Key Vault Managed HSM. are not hosted on pre. B and C are right answer

upvoted 4 times

**Learing** 1 year, 2 months ago

You can add a local key to an managed HSM, but with customer-provided (not customer-managed) keys they are not stored in any Azure Service

upvoted 3 times

**Arockia** Most Recent 1 week, 2 days ago

Option A is incorrect because it uses Microsoft-managed keys, which does not meet the requirement for the company to manage the encryptio keys for cardholder data.

Option D is incorrect because it uses Azure Key Vault Managed HSM, which is a cloud-based service. The requirement for insurance claim files is use keys hosted on-premises.

upvoted 1 times

**Murtuza** 2 weeks ago

Selected Answer: C

C is definitely one of the answers

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: CD

To meet the compliance and privacy requirements for encrypting cardholder data and insurance claim files, you should consider the following configurations:

✅ C. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM.
✅ D. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

C and D - surely you can't recommend storing cardholder data in a storage account.

upvoted 1 times

**Ramye** 1 week, 3 days ago

Of course you can as long as you can keep it safe, secure and encrypted .

upvoted 1 times

**yoooo9730** 6 months ago

CD
https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

upvoted 1 times

**apyasir** 6 months, 1 week ago

Currently, Azure Blob storage does not support customer-provided keys (BYOK) for encryption. Azure Blob storage utilizes Azure Storage Service Encryption (SSE) to automatically encrypt data at rest.

With SSE, Azure Blob storage encrypts your data using Microsoft-managed keys. These keys are managed and rotated by Azure behind the scer providing a high level of security for your data. You do not have direct control over the encryption keys used by Azure Blob storage.

so answer: C & D

upvoted 1 times

**NinjaSchoolProfessor** 6 months ago

Incorrect, Data in Blob storage and Azure Files is always protected by customer-managed keys when customer-managed keys are configured the storage account.

https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&bc=%2Fazure%2Fstorage%2Fblobs%2Fbreadcrumb%2Ftoc.json#customer-managed-keys-for-queues-and-tables

upvoted 2 times

**zellck** 8 months ago

Selected Answer: BC

BC is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql
Azure SQL transparent data encryption (TDE) with customer-managed key (CMK) enables Bring Your Own Key (BYOK) scenario for data protectic at rest, and allows organizations to implement separation of duties in the management of keys and data. With customer-managed TDE, the customer is responsible for and in a full control of a key lifecycle management (key creation, upload, rotation, deletion), key usage permissions, auditing of operations on keys.

upvoted 2 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-customer-provided-keys
Clients making requests against Azure Blob storage can provide an AES-256 encryption key to encrypt that blob on a write operation. Subsequent requests to read or write to the blob must include the same key. Including the encryption key on the request provides granular control over encryption settings for Blob storage operations. Customer-provided keys can be stored in Azure Key Vault or in another key stor

upvoted 1 times

**Zapman** 8 months ago

AB is correct in my opinion ,Explanation:
A. Storing cardholder data in an Azure SQL database encrypted with Microsoft-managed keys ensures that the data is encrypted. Microsoft-managed keys are suitable for encrypting cardholder data as per compliance requirements.
B. Storing insurance claim data in Azure Blob storage encrypted with customer-provided keys allows for encryption of the data. By using on-premises keys, the company maintains control over the encryption keys and meets the requirement for encrypting insurance claim files.

upvoted 1 times

**Tictactoe** 8 months, 1 week ago

AB is right

upvoted 1 times

**Ramye** 1 week, 3 days ago

A definitely not - requirements is not to use Microsoft keys

upvoted 1 times

**uffman** 8 months, 3 weeks ago

Selected Answer: BC

Key need to be on-prem, customer-provided keys.

upvoted 2 times

**vitodobra** 9 months, 3 weeks ago

Selected Answer: BC

Las opciones B y C cumplen con los requisitos de cumplimiento y privacidad.

La opción B (Almacene los datos de reclamaciones de seguros en Azure Blob Storage cifrados mediante claves proporcionadas por el cliente) cumple con el requisito de cifrar los archivos de reclamos de seguros mediante el uso de claves de cifrado alojadas en las instalaciones del clien

La opción C (Almacenar los datos del titular de la tarjeta en una base de datos de Azure SQL cifrada mediante el uso de claves almacenadas en Azure Key Vault Managed HSM) cumple con el requisito de cifrar los datos del titular de la tarjeta mediante el uso de claves de cifrado administradas por la empresa. Azure Key Vault Managed HSM proporciona una solución segura y gestionada para el almacenamiento de claves.

upvoted 3 times

**Gurulee** 9 months, 1 week ago

English please

upvoted 6 times

**Gurulee** 9 months, 4 weeks ago

Selected Answer: BC

Keys need to be on-prem was the deciding factor for me.

upvoted 4 times

**Ak1009** 10 months ago

Why not A?
Cant we envelope the key?

upvoted 1 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: BC

I will also go with BC. Since keys need to be onprem key vault is not an option obviously.

upvoted 4 times

**CyberG** 10 months, 3 weeks ago

Selected Answer: BC

def BC

upvoted 3 times

Question #11 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You need to enforce ISO 27001:2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically.
What should you use?

A. Azure Policy

B. Azure Blueprints

C. the regulatory compliance dashboard in Defender for Cloud

D. Azure role-based access control (Azure RBAC)

**Correct Answer:** *A*
Control mapping of the ISO 27001 Shared Services blueprint sample
The following mappings are to the ISO 27001:2013 controls. Use the navigation on the right to jump directly to a specific control mapping. Many of the mapped controls are implemented with an Azure Policy initiative.
Open Policy in the Azure portal and select the Definitions page. Then, find and select the [Preview] Audit ISO 27001:2013 controls and deploy specific VM
Extensions to support audit requirements built-in policy initiative.
Note: Security Center can now auto provision the Azure Policy's Guest Configuration extension (in preview)
Azure Policy can audit settings inside a machine, both for machines running in Azure and Arc connected machines. The validation is performed by the Guest
Configuration extension and client.
With this update, you can now set Security Center to automatically provision this extension to all supported machines.
Enforcing a secure configuration, based on a specific recommendation, is offered in two modes:
Using the Deny effect of Azure Policy, you can stop unhealthy resources from being created
Using the Enforce option, you can take advantage of Azure Policy's DeployIfNotExist effect and automatically remediate non-compliant resources upon creation
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive https://docs.microsoft.com/en-us/azure/defender-for-cloud/prevent-misconfigurations

*Community vote distribution*
A (90%) 10%

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Selected Answer: A
Azure policy
upvoted 10 times

**edurakhan** Most Recent 7 months, 3 weeks ago
Exam 5/25/2023
upvoted 1 times

**zellck** 8 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.
upvoted 1 times

**OCHT** 9 months, 2 weeks ago
Selected Answer: B
Blueprint to enforce.
upvoted 1 times

**Gurulee** 9 months, 4 weeks ago

Selected Answer: A

Automatic remediation was the key requirement here for me and it aligns directly with Azure Policy

upvoted 2 times

**KrishnaSK1** 11 months, 2 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal

upvoted 1 times

**Rocky83** 1 year ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/governance/blueprints/samples/iso-27001-2013

upvoted 1 times

**GeVanDerBe** 8 months, 2 weeks ago

In the same link the first explanation refers to Azure Policy --> The ISO 27001 blueprint sample provides governance guardrails using Azure Policy

upvoted 1 times

**TJ001** 1 year ago

blueprint contains policy as a child item , I think key here automatic resolution which happens when deployifnotexists effect is added in the poli so will go with policy to honor the details present in the question

upvoted 3 times

**Sec_Arch_Chn** 1 year, 1 month ago

deployifnotexist to be enabled in Azure Policy. Source: https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal

upvoted 1 times

**techtest848** 1 year, 2 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?tabs=azure-portal

upvoted 1 times

**SelloLed** 1 year, 2 months ago

B
https://azure.microsoft.com/en-us/products/blueprints/#features

upvoted 1 times

**Kamal_SriLanka** 1 year, 3 months ago

B. Azure Blueprints 100% sure

upvoted 2 times

**JCkD4Ni3L** 1 year, 3 months ago

Selected Answer: A

Azure Policy, unfortunatly at the moment of this writting Blueprints are in preview and thus should not be used in production (this will change ir the future as it is a good solution).

upvoted 4 times

**Curious76** 1 year, 3 months ago

I go with B...

upvoted 1 times

**tester18128075** 1 year, 4 months ago

AZURE POLICY

upvoted 2 times

**[Removed]** 1 year, 4 months ago

Why not B? ISO 27001 blueprint sample: https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso-27001-2013.
https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-with-built-in-azure-blueprints/

upvoted 3 times

**hb0011** 1 year, 3 months ago

This is a really good question and good sources. Anyone have a good reason why it would be policy and not blueprints?

upvoted 2 times

**cdizzle** 1 year, 2 months ago

I think both Policy and Blueprints could do the job, but the gottcha is the "automatic remediation" bit of the question. From what I can fin only a Policy will allow you to automate. https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

upvoted 4 times

**Phongsanth** 1 year, 3 months ago

maybe currently, Azure blueprint still in preview which Microsoft is not recommend for customer for production usage

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

yep, correct

upvoted 4 times

Question #12 *Topic 2*

DRAG DROP -

You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

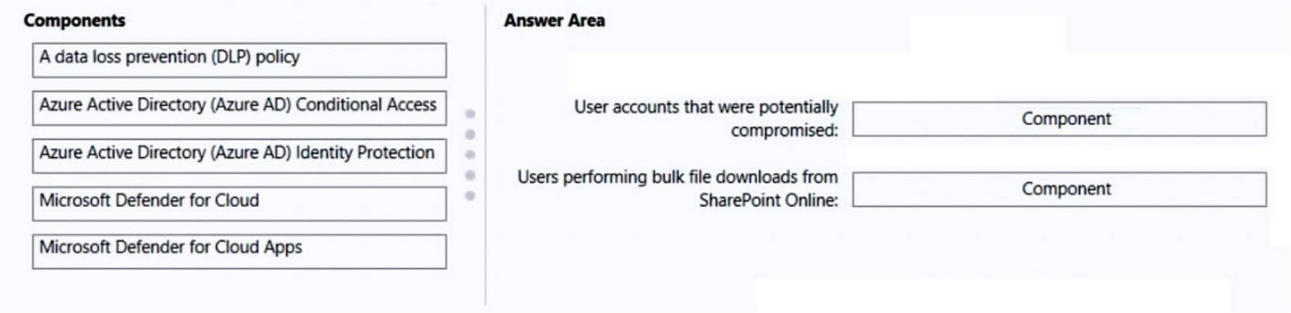
☞ User accounts that were potentially compromised

☞ Users performing bulk file downloads from Microsoft SharePoint Online

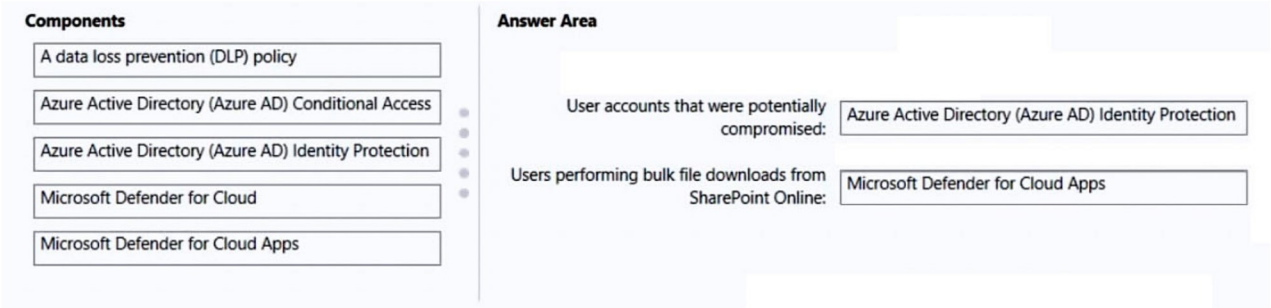
What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:




**Correct Answer:**




Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

Premium sign-in risk detections include:

* Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.

* Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This detection may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.

* Etc.

Incorrect:

Not: Microsoft 365 Defender for Cloud

Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365

Defender portal from Incidents & alerts > incident > Users.

Box 2: Microsoft 365 Defender for App

Defender for Cloud apps detect mass download (data exfiltration) policy

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

**TheMCT** Highly Voted 1 year, 4 months ago

The given answer is correct.

upvoted 15 times

**calotta1** Most Recent 4 months, 3 weeks ago

Has anyone considered DLP as the better solution here since the question is about reporting?
REF: https://www.microsoft.com/en-gb/security/business/security-101/what-is-data-loss-prevention-dlp?ef_id=_k_Cj0KCQjw_5unBhCMARIsACZyzS11Eh7eQSTGLIRjq5TP3xT2cbyWnDkJaHSav13rcKytz0ZwytyaBugaAqq4EALw_wcB_k_&OCID=AIDcmmao55x8o7_SEM__k_Cj0KCQjw_5unBhCMARIsACZyzS11Eh7eQSTGLIRjq5TP3xT2cbyWnDkJaHSav13rcKytz0ZwytyaBugaAqq4EALw_wcB_k_&gclid=Cj0KCQjw_5unBhCMARIsACZyzS11Eh7eQSTGLIRjq5TP3xT2cbyWnDkJaHSav13rcKytz0ZwytyaBugaAqq4EALw_wcB

upvoted 3 times

**Ramye** 4 days, 22 hours ago

DLP is for data loss prevention in terms of sensitive data, i.e., credit card, health info, social security card etc.,

upvoted 1 times

**zellck** 8 months ago

1. Azure AD Identity Protection
2. Microsoft Defender for Cloud Apps

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#nonpremium-user-risk-detectior

https://learn.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration
Detect when a certain user accesses or downloads a massive number of files in a short period of time.

upvoted 4 times

**TJ001** 1 year ago

The given answers are correct as it is for monitoring purpose

upvoted 2 times

**examtopics_100** 1 year ago

Correct

upvoted 3 times

**JCkD4Ni3L** 1 year, 3 months ago

Answers are correct !

upvoted 2 times

**tester18128075** 1 year, 4 months ago

identity protection and cloud

upvoted 2 times

**JMuller** 1 year, 4 months ago

Correct

upvoted 3 times

**prabhjot** 1 year, 4 months ago

yes correct ans

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

right, correct answer

upvoted 4 times

Question #13 *Topic 2*

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.
You receive the following recommendations in Defender for Cloud
- Access to storage accounts with firewall and virtual network configurations should be restricted.
- Storage accounts should restrict network access using virtual network rules.
- Storage account should use a private link connection.
- Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations.
What should you recommend?

A. Azure Policy

B. Azure Network Watcher

C. Azure Storage Analytics

D. Microsoft Sentinel

**Correct Answer:** *A*
An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled. Built in definitions include things like controlling what type of resources can be deployed or enforcing the use of tags on all resources. You can also create your own custom policy definitions.
Note: Azure security baseline for Azure Storage
This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Azure Storage. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Azure Security
Benchmark and the related guidance applicable to Azure Storage.
You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory
Compliance section of the Microsoft Defender for Cloud dashboard.
For example:
* 1.1: Protect Azure resources within virtual networks
Guidance: Configure your storage account's firewall by restricting access to clients from specific public IP address ranges, select virtual networks, or specific
Azure resources. You can also configure Private Endpoints so traffic to the storage service from your enterprise travels exclusively over private networks.
* 1.8: Minimize complexity and administrative overhead of network security rules
Guidance: For resource in Virtual Networks that need access to your Storage account, use Virtual Network Service tags for the configured Virtual Network to define network access controls on network security groups or Azure Firewall. You can use service tags in place of specific IP addresses when creating security rules.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline

*Community vote distribution*
A (100%)

**theOldSoldier** Highly Voted 1 year, 3 months ago
Selected Answer: A
Only answer that meet the given conditions
upvoted 7 times

**roman203** Most Recent 3 months, 1 week ago
Selected Answer: A
Agreed. A is the only answer that meet the given conditions
upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: A

other suggested answers are about alerting..

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 1 times

**TJ001** 1 year ago

Policy however it needs to have the right effect set 'deployifnotexists' to remediate existing workloads..

upvoted 1 times

**tester18128075** 1 year, 4 months ago

Azure policy

upvoted 1 times

**ele123** 1 year, 4 months ago

Selected Answer: A

Azure Policy can "mitigate identified risks"

upvoted 4 times

**JMuller** 1 year, 4 months ago

Selected Answer: A

correct

upvoted 1 times

**HardcodedCloud** 1 year, 4 months ago

Selected Answer: A

Azure Policy for sure.

upvoted 3 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: A

Policy does that.

upvoted 3 times

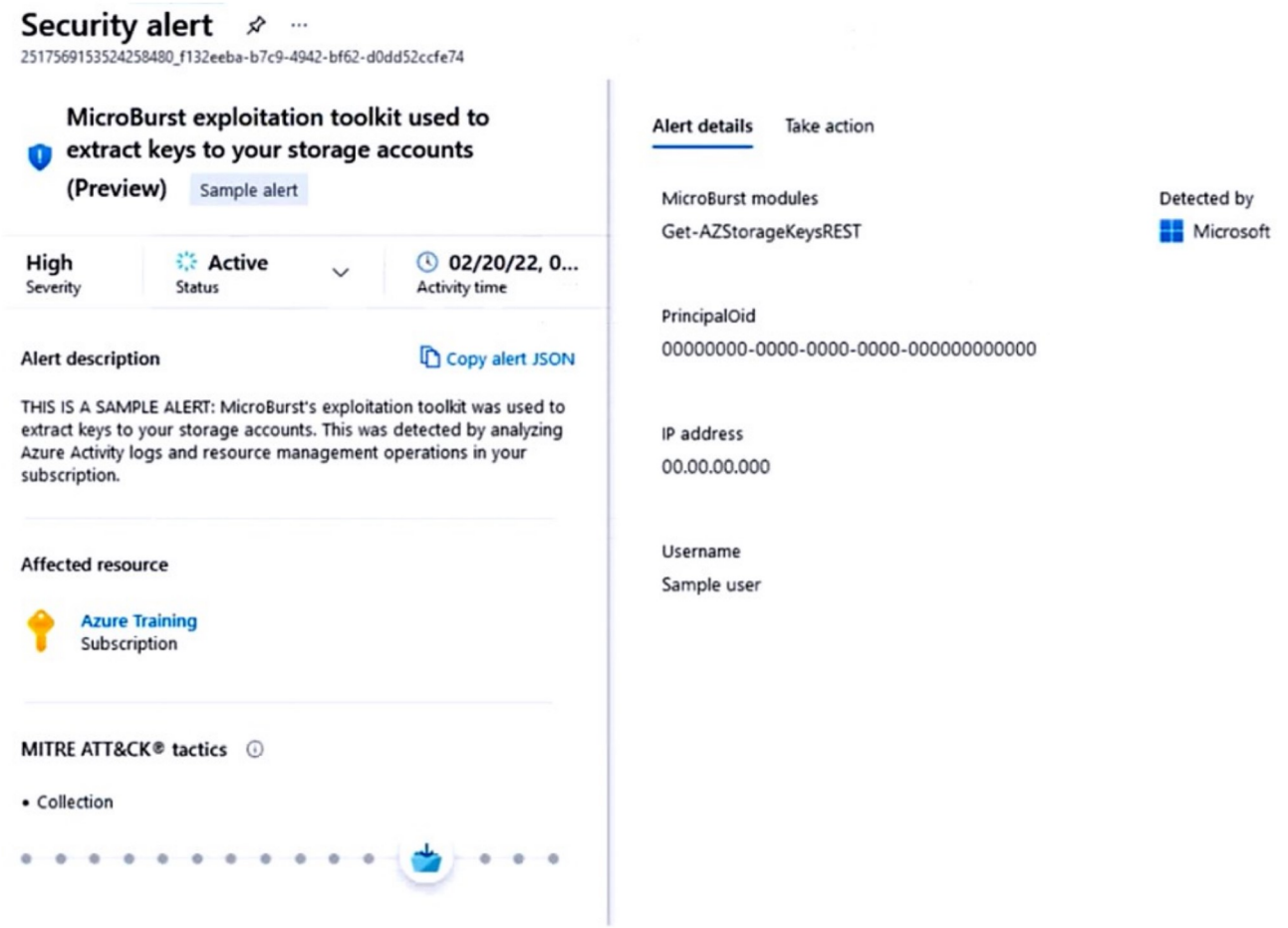
**Alex_Burlachenko** 1 year, 4 months ago

right and correct

upvoted 2 times

Question #14 *Topic 2*

You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)




After remediating the threat, which policy definition should you assign to prevent the threat from reoccurring?

A. Storage account public access should be disallowed

B. Azure Key Vault Managed HSM should have purge protection enabled

C. Storage accounts should prevent shared key access

D. Storage account keys should not be expired

**Correct Answer:** *A*

Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data, but may also present a security risk. It's important to manage anonymous access judiciously and to understand how to evaluate anonymous access to your data. Operational complexity, human error, or malicious attack against data that is publicly accessible can result in costly data breaches. Microsoft recommends that you enable anonymous access only when necessary for your application scenario.

Note: Attackers have been crawling for public containers using tools such as MicroBurst.

Exploiting Anonymous Blob Access

Now, there are thousands of articles explaining how this can be abused and how to search for insecure storage in Azure. One of the easiest way is to use

MicroBurst, provide the storage account name to search for, and it'll check if the containers exists based on a wordlist saved in the Misc/permutations.txt

Reference:

https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent https://hackingthe.cloud/azure/anonymous-blob-access/

*Community vote distribution*

C (79%) A (21%)

**walkaway** Highly Voted 11 months, 3 weeks ago

Selected Answer: C

C is the correct answer. You should read Microburst toolkit - it is an open-source tool. Find Get-AZStorageKeysREST.ps1 it tries to enumerate all storage accounts then the respective storage keys. There is nothing to do with anonymous access here. Even if a storage account allows public acces you can't get the key without being authenticated and authorized.

The preventive control here is to manage Shared Key Authorization.

upvoted 24 times

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago

I would select "Storage accounts should prevent shared key access"

upvoted 16 times

**purek77** 11 months, 4 weeks ago

... by applying read-only lock.

upvoted 1 times

**Arockia** Most Recent 1 week, 2 days ago

MicroBurst leverages the Get-AZStorageKeysREST.ps1 script to brute-force enumerate storage accounts and subsequently attempt to retrieve th keys using REST API calls. Public access isn't directly targeted by this script.
While disallowing public access (option A) is a generally good security practice, it wouldn't specifically prevent the MicroBurst exploitation technique that relies on shared key access. Even with public access blocked, the script could still enumerate accounts and try brute-forcing share keys.
Preventing shared key access (option C) directly addresses the vulnerability exploited by the script. By disabling this access method, storage accounts become protected from unauthorized key retrieval attempts using Get-AZStorageKeysREST.ps1 or similar tools.

upvoted 2 times

**Joe1126** 1 month, 1 week ago

Selected Answer: C

is the right answer

upvoted 1 times

**slobav** 3 months, 3 weeks ago

Selected Answer: A
From the picture above you can see access from IP 0.0.0.0 that means from internet (public access).
SAS token allow limited access to storage.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=portal
Every secure request to an Azure Storage account must be authorized. By default, requests can be authorized with either Azure Active Directory (Azure AD) credentials, or by using the account access key for Shared Key authorization. Of these two types of authorization, Azure AD provides superior security and ease of use over Shared Key, and is recommended by Microsoft. To require clients to use Azure AD to authorize requests, y can disallow requests to the storage account that are authorized with Shared Key.

upvoted 4 times

**valeriafarias** 8 months, 3 weeks ago

The correct is C, see the docs: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference

upvoted 2 times

**etblue** 9 months, 3 weeks ago

My answer would be C.
Note that the question is asking "After remediating the threat, which policy definition should you assign to prevent the threat from reoccurring"
Answer A mitigate the attack by limiting exploit only thru private network links. However, to entirely prevent threat from re-occuring, simply sto using preShare key authorization.

upvoted 3 times

**vins_vins_vins** 10 months, 3 weeks ago

I vote for C.
Azure AD provides superior security and ease of use over Shared Key, and is recommended by Microsoft.

here the link: https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=portal

upvoted 1 times

**KrisDeb** 11 months, 1 week ago

I am torn between A and C, in my opinion it should be both that would make sense. I really don't know what to choose for the exam now - A or

upvoted 1 times

**Azzzurrre** 1 year ago

"... By default, requests can be authorized with either Azure Active Directory credentials, or by using the account access key for Shared Key

authorization. Of these two types of authorization, Azure AD provides superior security and ease of use over Shared Key, and is recommended b Microsoft."
https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Storage/StorageAccountAllowSharedKeyAccess_Audit.jso
upvoted 3 times

**maku067** 12 months ago
I agree. C is correct.
upvoted 2 times

**TJ001** 1 year ago
I would go with C as it is not talking about data but keys..Make a Storage Account Public/Private (if it is related network) is use case based and c be enforced always.. Anonymous access makes sense but that is for the data and the powershell command is trying to extract the access the key and not data
upvoted 4 times

**Aunehwet79** 11 months, 1 week ago
Good point - I am going with C
upvoted 1 times

**johnwick420** 1 year ago
Selected Answer: C
C makes sense in this context, A doesn't mean anything although seems like a trick question
upvoted 2 times

**[Removed]** 1 year ago
Selected Answer: C
C is the only answer that makes sense. Alert was triggered by an authenticated user "Sample user", data was found in Azure Activity Logs and Resource Managment Operations. For this reason I think C is the answer. Alert and question has nothing to do with public or anonymous access
upvoted 3 times

**threshclo** 1 year ago
Selected Answer: C
C is the only answer that makes sense
upvoted 3 times

**dc2k79** 1 year ago
C is the only answer that makes sense.
upvoted 2 times

**SDK91** 1 year, 1 month ago
Selected Answer: C
The question clearly states that the key got compromised, and not data inside the storage account.
upvoted 2 times

Question #15 *Topic 2*

You have 50 Azure subscriptions.
You need to monitor the resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
What are two ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.

B. Assign a policy to each subscription.

C. Assign a policy to a management group.

D. Assign an initiative to each subscription.

E. Assign a blueprint to each subscription.

F. Assign a blueprint to a management group.

**Correct Answer:** *AF*
An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions en masse.
If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions.
Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.
F: Blueprint definition locations
When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have
Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.
A: Create and assign an initiative definition
With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.
Note: The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in ISO 27001:2013.
The Azure Policy control mapping provides details on policy definitions included within this blueprint and how these policy definitions map to the compliance domains and controls in ISO 27001. When assigned to an architecture, resources are evaluated by Azure Policy for non-compliance with assigned policy definitions.
Incorrect:
Not B, D, E: If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.
Reference:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

*Community vote distribution*
AF (80%) AC (17%)

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Selected Answer: AF
Initiative & Blueprint at the management group level
upvoted 18 times

**InformationOverload** Highly Voted 1 year, 4 months ago
Selected Answer: AF
Initiative; A group of related policies joined logically to accomplish a common goal. Better to use initiatives than a single policy in this case. Use on management group level. Answer is correct.
upvoted 7 times

**rahulnair** Most Recent 3 months ago

Selected Answer: AF

Initiative not required as Azure policy already covers ISO. If multiple standards would have been in scope, then inititaives would have made sens

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment - "Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription"

upvoted 1 times

**zellck** 8 months ago

Selected Answer: AF

AF is the answer.

https://learn.microsoft.com/en-us/azure/governance/blueprints/samples/iso-27001-2013
https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

upvoted 1 times

**vitodobra** 9 months, 3 weeks ago

Selected Answer: AC

To minimize the effort required to modify the list of monitored policy definitions for the subscriptions while monitoring resource compliance wit the ISO 27001:2013 standards, you can assign policies to a management group or assign initiatives to a management group. This way, the polici or initiatives will apply to all the subscriptions within that management group, making it easier to manage and update policy definitions across multiple subscriptions at once.

Therefore, the correct answers are:

A. Assign an initiative to a management group.
C. Assign a policy to a management group.

upvoted 2 times

**Toschu** 9 months, 3 weeks ago

A policy doesn't include all the policy definitions needed, which means a big overhead in assigning them all and updating them in the future
They can be all assigned to one blueprint, and the blueprint to the management group.
But it's important to use the initiative because it gets updated by Microsoft if new policy definitions are added! So always use the initiative.

upvoted 1 times

**KrishnaSK1** 11 months, 2 weeks ago

Selected Answer: AF

https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

upvoted 1 times

**sean2022** 1 year ago

why not c?

upvoted 1 times

**Sec_Arch_Chn** 1 year, 1 month ago

Question mentions 'minimize the effort required to modify the list of monitored policy definitions for the subscriptions'.

Initiative - collection of policy definitions that are tailored towards achieving a singular overarching goal
Blueprint - Enables the creation of fully governed environments in a repetitive manner using policies & initiatives.
A -> Ensures compliance of existing resources in the environment
F-> Ensures compliance for any resources getting created in the environment

upvoted 5 times

**IHensch** 1 year, 2 months ago

Selected Answer: AC

You can use Azure Policy or Initiative (a group of policies) to achieve this goal. The Blueprint does not make sense for this question. There are tw possible solutions. In my opinion, they are exactly these.

upvoted 4 times

**dudus999** 5 months ago

I agree blue print not make sense

upvoted 1 times

**Jacquesvz** 12 months ago

I agree with IHensch. the question states: "You need to MONITOR the resource(s) in the subscriptions for compliance" You need to MONITOR not ensure that all new and future deployments are compliant. Policies or Initiatives make sense. To minimize the effort, one would assign it a the Management group level, and not at each subscription. Just my 2 cents worth.

upvoted 1 times

**omarrob** 1 year, 2 months ago

AF are the correct answers

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

upvoted 1 times

**blopfr** 1 year, 2 months ago

Selected Answer: AD

Blueprint can't be assigned to management group can't be F

upvoted 1 times

**EmmanuelDan** 1 year, 2 months ago

yes you can I just finished watching Azure Fridays on Blueprint, and the architects for blueprints mentioned that you can assign blueprints to management groups

upvoted 4 times

**omarrob** 1 year, 2 months ago

You can assign blueprint to managed group

https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

upvoted 2 times

**lHensch** 1 year, 1 month ago

=> "Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription."

upvoted 1 times

**Learing** 1 year, 2 months ago

You can

upvoted 1 times

**tester18128075** 1 year, 4 months ago

A and F

upvoted 2 times

**Alex_Burlachenko** 1 year, 4 months ago

briliant, correct answer

upvoted 5 times

Question #16 *Topic 2*

HOTSPOT -

You open Microsoft Defender for Cloud as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

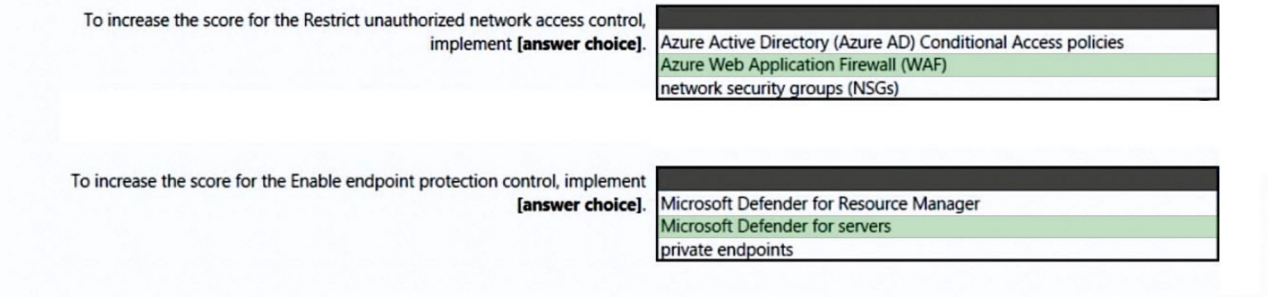
- Azure Active Directory (Azure AD) Conditional Access policies
- Azure Web Application Firewall (WAF)
- network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

- Microsoft Defender for Resource Manager
- Microsoft Defender for servers
- private endpoints

**Correct Answer:**

**Answer Area**




Box 1: Azure Web Application Firewall (WAF)

Restrict unauthorized network access control: 1 resource out of 11 needs to be addresses.

Restrict unauthorized network access - Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.

Use these recommendations to manage Defender for Cloud's adaptive network hardening settings, ensure you've configured Azure Private Link for all relevant

PaaS services, enable Azure Firewall on your virtual networks, and more.

Note: Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway.

Azure WAF protects inbound traffic to the web workloads, and the Azure Firewall inspects inbound traffic for the other applications. The Azure Firewall will cover outbound flows from both workload types.

Incorrect:

Not network security groups (NSGs).

Box 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft

Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

**HardcodedCloud** Highly Voted 1 year, 4 months ago

Selection 1: NSG
Selection 2: Microsoft Defender for servers

upvoted 78 times

**[Removed]** Highly Voted 1 year, 4 months ago

NSGs: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833

upvoted 20 times

**harimurti20** Most Recent 1 month, 1 week ago

NSG:Unautorised Network access can be prevented by NSG
Microsoft Defender for Server

upvoted 2 times

**smanzana** 2 months, 3 weeks ago

Box1: NSG
Box2: Microsoft Defender for servers

upvoted 2 times

**slobav** 3 months, 3 weeks ago

Selection 1: NSG
Selection 2: Microsoft Defender for servers
Explanation: Question 85
https://www.youtube.com/watch?v=_DvisTemjGQ&list=PLQ2ktTy9rklhzzkSEZvDZT4QSIVUQZD-Y&index=6

upvoted 2 times

**calotta1** 4 months, 3 weeks ago

I'd have selected WAF but i can see it is under "Protect applications against DDoS attacks" recommendations. NSG is the right for 1st box and M is correct.

REF: https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls?branch=main#security-controls-and-their-recommendations

upvoted 3 times

**bmulvIT** 7 months, 4 weeks ago

Question in the exam today 19/05/2023

upvoted 6 times

**JpTheCloudGuy** 5 months, 3 weeks ago

What were your selections?

upvoted 1 times

**zellck** 8 months ago

1. NSG
2. Microsoft Defender for servers

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 1 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

NSG + MDfS

upvoted 1 times

**steve_gatsby** 11 months, 1 week ago

WAF is incorrect as it only affects level 7 layer of HTTP protocol

upvoted 3 times

**ad77** 11 months, 4 weeks ago

1. nsg - ref. 4, https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls?branch=main#how-your-secure-scor is-calculated
2.. defender for endpoint ref 2. https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls?branch=main#how-your-secure-score-is-calculated

upvoted 2 times

**ad77** 11 months, 4 weeks ago

2.. defender for server

upvoted 1 times

**nieprotetkniteeetr** 12 months ago

NSG https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/15938

upvoted 2 times

**Rocky83** 1 year ago

NSG and M$ Defender for Servers

upvoted 2 times

**Hullstar** 1 year ago

1 and 2, just checked my live environment and NSG is at the top of the list

upvoted 1 times

**Hullstar** 1 year ago

sorry: 1-NSG, 2:MDS

upvoted 1 times

**purek77** 1 year ago

Quick analysis of https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls tells us that
- Restrict unauthorized network access = Virtual networks should be protected by Azure Firewall

- Enable endpoint protection = Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such [list], [list] shows Defender for Servers and/or Defender for Containers.

Therefore answers are:
- Azure Web Application Firewall (WAF)
- Microsoft Defender for Servers

upvoted 1 times

**purek77** 12 months ago

Well, after rethinking it should be NSG and MDfS

upvoted 1 times

**TJ001** 1 year ago

would go with NSG, WAF is more for DDoS, NSG help to implement JIT as well

upvoted 2 times

**examtopics_100** 1 year ago

1-NSG (https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendatic
2-Defender for Servers

upvoted 2 times

Question #17 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling the VMAccess extension on all virtual machines.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Note:
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

*Community vote distribution*
B (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify network-security-configuration
upvoted 11 times

**[Removed]** 1 year, 4 months ago
Adaptive Network Hardening does not increase the score of the Secure management ports controls (as far as I can tell). Use Microsoft Defen for Cloud Adaptive Network Hardening to recommend NSG hardening rules that further limit ports, protocols and source IPs based on threa intelligence and traffic analysis result.
upvoted 2 times

**Learing** 1 year, 2 months ago
Correct about instructions, but adaptive network hardening is in different category:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
upvoted 1 times

**bmulvIT** Most Recent 7 months, 4 weeks ago
Selected Answer: B
Question in the exam today 19/05/2023
upvoted 2 times

**zellck** 8 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 1 times

**ksksilva2022** 1 year, 1 month ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 1 times

**SAMSH** 1 year, 3 months ago

was in 20Sep2020 exam

upvoted 1 times

**Jasper666** 1 year, 4 months ago

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls, half way under Secure management ports; NSG, JIT, not internet faced. None of those are met so B

upvoted 1 times

**djayawar** 1 year, 4 months ago

Correct

upvoted 2 times

**BillyB2022** 1 year, 4 months ago

**Selected Answer: B**

Correct

upvoted 3 times

Question #18 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling adaptive network hardening.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Note:
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

*Community vote distribution*
B (77%) A (23%)

**yf** Highly Voted 1 year, 4 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls lists "Adaptive network hardening" for "Restrict unauthorized network access" and not for "Secure management ports"

upvoted 31 times

**Jacquesvz** 11 months, 3 weeks ago

Agreed: only 3 controls you can implement for Management Ports =
1.) Internet facing vm's should be protected with NSG's
2.) Management ports should be closed on your vm's
3.) Management ports on VM's should be protected with JIT
Logon to Defender for Cloud and have a look under "General/Recommendations".

upvoted 4 times

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: A

Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify network-security-configuration

upvoted 9 times

**Learing** 1 year, 2 months ago

Correct about instructions, but adaptive network hardening is in different category:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 6 times

**Jacquesvz** 11 months, 3 weeks ago

100%. Adaptive network hardening is to address "Restrict Unauthorized Network Access", and not management ports.

upvoted 2 times

**Murtuza** Most Recent 1 week, 2 days ago

Selected Answer: B

You recommend enabling just-in-time (JIT) VM access on all virtual machines.

upvoted 1 times

**Arjanussie** 1 month, 1 week ago

adaptive network hardening is part of Restrict unauthorized network access NOT part of secure management port - just logon in your tenant an you will see

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 4 times

**Ario** 6 months, 2 weeks ago

this is very tricky question , Adaptive network hardening potentially can improve the security but require additional configuration and JIT is one those , i would vote for B

upvoted 2 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 2 times

**WRITER00347** 8 months, 2 weeks ago

B. No

Enabling adaptive network hardening in Microsoft Defender for Cloud can help improve the security posture of your network by providing recommendations for network security group (NSG) rules. However, it does not directly impact the score of the Secure management ports contr in the Azure Security Benchmark V3 report.

To increase the score for the Secure management ports controls, you should focus on implementing recommendations specific to securing management ports, such as restricting access to management ports, enabling just-in-time VM access, and using Azure Bastion for secure access your virtual machines.

upvoted 1 times

**Ajdlfasudfo0** 10 months, 4 weeks ago

Selected Answer: B

No, https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

"Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with toc like just-in-time VM access and network security groups."

upvoted 1 times

**ad77** 11 months, 4 weeks ago

Selected Answer: B

Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.

upvoted 1 times

**Hullstar** 1 year ago

In my live environment it does not list and Adaptive Network Hardening is not there.

upvoted 2 times

**TJ001** 1 year ago

JIT make sense when we talk about management ports I will stick with B

upvoted 2 times

**examtopics_100** 1 year ago

No: Applicable remediations:
Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control

- Management ports should be closed on your virtual machines

upvoted 4 times

**sunilkms** 1 year ago

**Selected Answer: B**

The answer is clearly B the ask is to gain the potential 8 points which you will only get by doing the recommendation in the Secure managemen ports, whereas adaptive network hardening comes under "Restrict unauthorized network access" and potential max point you can gain is 4.

upvoted 3 times

**hamshoo** 1 year, 1 month ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

upvoted 1 times

**dija123** 1 year, 2 months ago

**Selected Answer: B**

Secure management ports :
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines

upvoted 2 times

**Learing** 1 year, 2 months ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

upvoted 2 times

Question #19 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time
VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

*Community vote distribution*
A (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: A
Keep in mind the instructions "Some question sets might have more than one correct solution" and familiarize yourself with the Azure Security Benchmark V3 report.
Two correct answers are JIT and Adaptive Network Hardening.

JIT: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

Adaptive Network Hardening: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify network-security-configuration
upvoted 12 times

**TJ001** 1 year ago
JIT and NSG make sense under this recommendation category...
upvoted 1 times

**cyber_sa** Most Recent 3 months, 1 week ago

Selected Answer: A
got this in exam 6oct23. passed with 896 marks. I answered A
upvoted 1 times

**zellck** 8 months ago

Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
upvoted 1 times

**TomHoff** 10 months ago

Selected Answer: A

yes, correct

upvoted 1 times

**steve_gatsby** 11 months, 1 week ago

https://learn.microsoft.com/en-us/azure/governance/policy/samples/gov-azure-security-benchmark#avoid-standing-access-for-accounts-and-permissions

upvoted 1 times

**[Removed]** 1 year ago

There are 3 recommendations, at this link. JIT is one of the 3.
https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-secure-management-ports/ba-p/1505770

upvoted 2 times

**SAMSH** 1 year, 3 months ago

was in 20Sep2020 exam

upvoted 1 times

**JMuller** 1 year, 4 months ago

Selected Answer: A

Plumpy is right, there are 2 correct answers in this set. JIT is only ONE of them.

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

yep, correct

upvoted 4 times

Question #20 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend creating private endpoints for the web app and the database layer.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ג€How can we safely deploy internal business applications to Azure App Services?ג€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

*Community vote distribution*
A (89%) 11%

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Selected Answer: A
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.
upvoted 9 times

**Ajdlfasudfo0** 10 months, 4 weeks ago
you need vnet integration in order to send traffic from app service to the cosmos db. Please read it up first.
upvoted 1 times

**JoeMel** Highly Voted 1 year ago
"The solution must follow the Zero Trust model."
Isn't Zero Trust requires mutual authentication ?
The solution proposed is based on trusting the internal network which is not Zero-Trust.

upvoted 7 times

**cybrtrk** Most Recent 1 week, 3 days ago

I think people are getting confused between the old infrastructure and the new.
The question relates to the new infrastructure in Azure, so the solution is WAF.
Private endpoints aren't related to this infrastructure.

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: A

got this in exam 6oct23. passed with 896 marks. I answered A

upvoted 2 times

**bmulvIT** 7 months, 4 weeks ago

Question in the exam today 19/05/2023

upvoted 3 times

**bmulvIT** 8 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint
"Private endpoint is only used for incoming traffic to your app"
NO

upvoted 2 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint
You can use private endpoint for your App Service apps to allow clients located in your private network to securely access the app over Azure Private Link. The private endpoint uses an IP address from your Azure virtual network address space. Network traffic between a client on your private network and the app traverses over the virtual network and a Private Link on the Microsoft backbone network, eliminating exposure from the public Internet.

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

Selected Answer: A

ChatGPT: A. Yes, creating private endpoints for the web app and the database layer is a recommended solution to secure the connection betwee the two layers and meet the Zero Trust model.

Private endpoints allow you to access your Azure PaaS services over a private IP address within your virtual network. By creating private endpoin for both the web app and the MongoDB database, traffic between them can be routed through the private network, making it more secure by preventing access from the public internet.

This approach is recommended because it limits access to only the virtual network where the web app and database are deployed, and it helps t minimize the surface area of potential attacks. By implementing private endpoints, you can ensure that data is transmitted securely between the two layers and reduce the risk of data breaches.

Therefore, creating private endpoints for the web app and the database layer meets the goal of securing the connection between the two layers and follows the Zero Trust model.

upvoted 1 times

**Ajdlfasudfo0** 10 months, 4 weeks ago

I think this is incorrect. Private Endpoint would not be the solution here. The App service does need VNet Integration, not private endpoint in or to reach the cosmos DB via its private address. I think a lot of people just shout yes once they hear private endpoint and don't even understand what it is

upvoted 4 times

**Azzzurrre** 1 year ago

In addition to the private endpoint for the Cosmos DB, the Cosmos DB needs to have its "publicNetworkAccess" flag set to "Disabled" to preven public network access to the Cosmos DB account when it is created, before its private endpoint is created.
Also,
(Just creating the private endpoint could be considered an incomplete solution.)
https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints#blocking-public-network-access-during-account-creation

upvoted 2 times

**GetMonster** 1 year, 3 months ago

Selected Answer: A

The answer is correct.

upvoted 3 times

**tester18128075** 1 year, 4 months ago

Private endpoint is correct. A is the correct answer

upvoted 1 times

**prabhjot** 1 year, 4 months ago

yes seems correct from NETWORK - zero trust principle point of view

upvoted 3 times

**PlumpyTumbler** 1 year, 4 months ago

I think this is right. It's always best to use official Microsoft documentation for answers. Other companies and blogs are not the source of truth.
https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

YES, correct

upvoted 4 times

Question #21 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Key Vault to store credentials.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ɔ€How can we safely deploy internal business applications to Azure App Services?ɔ€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

*Community vote distribution*
B (52%) A (48%)

**Luise** Highly Voted 1 year, 3 months ago
Selected Answer: A
Landing zones are not only networking. Designing a proper authentication flow is also important, and in zero trust, no credentials should be unnattended. Thats why using key vault and managed identities are important thin.gs when designing a zero trust architecture.
My answer is YES
upvoted 17 times

**TJ001** 1 year ago
Should instead disable local authentication for Cosmos DB and use Managed Identity so no Key Vault is needed; would be superior design
upvoted 4 times

**mynk29** 11 months, 4 weeks ago

True. but key vault is better than having nothing

upvoted 1 times

**hw121693** 5 months, 2 weeks ago

What's the use of key vault if we use managed identity?

upvoted 3 times

**hw121693** 5 months, 2 weeks ago

Even better solution is to use managed identity, so no credentials will be required. Even if you use key vault, you still need to grab the secret using managed identity

upvoted 2 times

**AzureJobsTillRetire** 11 months ago

Not sure why you must have key vault. I think key vault is nice to have in this case. Manged identity may be a better solution.

upvoted 3 times

**Avanade2023** 7 months, 1 week ago

You can keep the connection string to Database securely by the Key Vault.

upvoted 1 times

**hw121693** 5 months, 2 weeks ago

Using connection string to connect database has nothing to do with "Securing the connection". "Securing connection" means to secur data in transit to database such as using HTTPS connection to DB.

upvoted 1 times

**MrsSunshine** 1 year ago

You have ro aecure the connection...For this question, it is networking only...

upvoted 1 times

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago

NO is correct answer

upvoted 14 times

**Murtuza** Most Recent 2 weeks ago

Selected Answer: B

Managed identity is the best way to secure connection between Azure services in this case cosmos DB and ASE

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 5 times

**ServerBrain** 4 months, 4 weeks ago

B is the correct answer. The question is about securing the connection not about secure access. Key Vault will give you secure access...

upvoted 1 times

**imsidrai** 6 months, 2 weeks ago

key vault also supports the "use least privilege access " principle, so yes

upvoted 1 times

**PrettyFlyWifi** 7 months, 2 weeks ago

Selected Answer: A

Considering the general overview of Azure Key Vault states a clear "note" on Zero Trust, I'd assume this answer should be "YES". E.g. Data protection, including key management, supports the "use least privilege access" principle.
https://learn.microsoft.com/en-us/azure/key-vault/general/overview
Got to be YES right??

upvoted 2 times

**etblue** 9 months, 3 weeks ago

My suggested answer is B, no.
Question being: Provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model
Zero Trust model guiding principle: Assume breach, Verify explicitly, Use least privilege.
Note that here the main point is about "secure the connection", which tend more towards network controls based "assumed breach prevention' rather than attack on credentials "verify explicitly".
Asking on the opposite side, if we secure the network connectivity between web and DB tier but using credentials that is not stored in Azure vau does it necessarily raise risks? To a certain extend, if the relevant credentials are kept safe, I would think it does not raise a difference if store in vault or not, more importantly there is a secure network connectivity between the web and DB.
Plus the fact this is a continued series question where "private endpoint" seems to be the most "correct" answer. Hope it explains.

upvoted 6 times

**Ram098** 10 months, 2 weeks ago

B CORRECT

upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

Selected Answer: A

ChatGPT: A. Yes, implementing Azure Key Vault to store credentials is a recommended solution to secure the connection between the web app a the MongoDB database, and it meets the goal of following the Zero Trust model.

upvoted 2 times

**awssecuritynewbie** 11 months, 1 week ago

Selected Answer: B

It asks for "secure connection" which is not the same thing as storing the key securely! so it would be B

upvoted 3 times

**Aunehwet79** 11 months ago

Agree with you

upvoted 2 times

**walkaway** 11 months, 3 weeks ago

Selected Answer: B

No for sure. You don't need Key Vault in this case. You can use managed identity.

upvoted 2 times

**ad77** 11 months, 4 weeks ago

Selected Answer: B

My answer is B=NO

upvoted 1 times

**nieprotetkniteeetr** 12 months ago

Selected Answer: B

The answer is no. Is like someone asking you what is the best cheese for pizza and you answer that tomato is best for sause. You are correct but this not the answer for the problem.

upvoted 3 times

**Azzzurrre** 1 year ago

The answer is "B".

System Assigned Managed Identity is the recommended method to access Azure Cosmos DB. Managed Identities do not require or use Key Vau An App Service can use a Managed Identity to connect to Cosmos DB.

This is in addition to using Private Endpoints.

Key Vaults are used if the Azure Cosmos DB is being accessed using an SDK, the API endpoint and either the primary or secondary key. Keys anc Key Vaults are recommended ONLY as a fallback method to connect to Cosmos DB, if the service connecting to Cosmos DB can't use a Manage Identity or certificate based authentication. An App Service can connect to the Cosmos DB using a Managed Identity.
https://learn.microsoft.com/en-us/azure/cosmos-db/store-credentials-key-vault

upvoted 1 times

**TJ001** 1 year ago

I would pick B,
KeyVault is not a must if we are talking about how the WebApp AuthZ with Cosmos DB. The best practice is to Disable Local Authentication (whi case Cosmos DB Keys can be discarded) and use Azure AD based AuthZ (all we need is MI and required permissions)

upvoted 1 times

**dc2k79** 1 year, 1 month ago

B. NO
Microsoft Best Practice for non-user service interaction for Zero Trust is to use Managed Identities.
https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-non-user-applications

upvoted 2 times

Question #22 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Application Gateway with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ɔ€How can we safely deploy internal business applications to Azure App Services?ɔ€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

*Community vote distribution*
B (75%) A (25%)

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Selected Answer: B
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.
upvoted 6 times

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago
correct answer
upvoted 5 times

**Murtuza** Most Recent 1 week, 2 days ago

This is a tricky question MS threw the word client connection to confuse us in picking the WAF component and App Gateway which is irrelevant here

upvoted 1 times

**Victory007** 5 months, 1 week ago

**Selected Answer: A**

Yes, implementing Azure Application Gateway with Azure Web Application Firewall (WAF) can help meet the goal of securing the connection between the web app and the database following the Zero Trust model. Azure Application Gateway is a load balancer that provides application-level routing and load balancing services. It can be configured with the optional addition of Azure Web Application Firewall (WAF), which provid inspection of HTTP requests and prevents malicious attacks at the web layer, such as SQL Injection or Cross-Site Scripting.
https://learn.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway

upvoted 2 times

**tester18128075** 1 year, 4 months ago

Answer is no, App gateway does not provide connectivity between webapp and cosmos DB

upvoted 2 times

**ServerBrain** 4 months, 4 weeks ago

Correct. WAF will give you connectivity between the client and the App.

upvoted 1 times

Question #23 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure Security Benchmark compliance controls in Defender for Cloud

**Correct Answer:** *A*
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
Incorrect:
Not B: App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.
Not C: Cloud Discovery anomaly detection policy reference. A Cloud Discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are considered for each cloud application.
Not D: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy https://docs.microsoft.com/en-us/security/benchmark/azure/overview

*Community vote distribution*
A (96%) 4%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: A
This question is on here twice. Each time it's asked the same way but the answer options are different so look out. In this case A is correct.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute-recommendations
upvoted 13 times

**cybrtrk** Most Recent 1 month, 3 weeks ago
Adaptive application controls don't block.
What am I missing here?
upvoted 2 times

**Intrudire** 2 months, 1 week ago
Selected Answer: A
Answer does not meet the requirements, but it seems to be the closest answer.

"If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes t application."

"No enforcement options are currently available. Adaptive application controls are intended to provide security alerts if any application runs oth than the ones you've defined as safe."
https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
upvoted 3 times

**imsidrai** 6 months, 4 weeks ago

C is the correct answer
https://learn.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-policies

upvoted 2 times

**imsidrai** 6 months, 4 weeks ago

No enforcement options are currently available. Adaptive application controls are intended to provide security alerts if any application runs other than the ones you've defined as safe.

upvoted 1 times

**imsidrai** 6 months, 4 weeks ago

adaptive control wont block/deny , it would only suggest/recommend, so NO for adaptive controls

upvoted 1 times

**imsidrai** 6 months, 3 weeks ago

Please disregard my comments above, The correct answer is B , Microsoft Endpoint manager which is now Intune Admin center has capability to block unauthorized applications and block all other executables, Adaptive control policies would only notify you.

upvoted 1 times

**Intrudire** 2 months, 1 week ago

Intune doesnt seem to support Server.
https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers

upvoted 1 times

**zellck** 8 months ago

Same as Question 19.
https://www.examtopics.com/discussions/microsoft/view/94349-exam-sc-100-topic-4-question-19-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

C is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning tc analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the following instructions.

When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.

upvoted 1 times

**vitodobra** 9 months, 3 weeks ago

Selected Answer: B

La respuesta correcta es B. Debe recomendar políticas de protección de aplicaciones en Microsoft Endpoint Manager. Esta solución permite configurar y administrar las políticas de protección de aplicaciones en todas las máquinas virtuales de forma centralizada. Las políticas de protección de aplicaciones permiten controlar qué aplicaciones pueden ejecutarse o instalarse en las máquinas virtuales. Si una aplicación no autorizada intenta ejecutarse o instalarse, la aplicación se bloqueará automáticamente hasta que un administrador autorice la aplicación. Las políticas de protección de aplicaciones se pueden configurar para permitir aplicaciones específicas, bloquear aplicaciones específicas o permitir los usuarios finales soliciten la instalación de aplicaciones no autorizadas.

upvoted 1 times

**TJ001** 1 year ago

Perfect A

upvoted 1 times

**Sec_Arch_Chn** 1 year, 1 month ago

Selected Answer: A

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machine
Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

upvoted 3 times

**Janusguru** 1 year, 2 months ago

Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

upvoted 1 times

**SAMSH** 1 year, 3 months ago

Correct answer. was in 20Sep2020 exam

upvoted 1 times

**Jasper666** 1 year, 4 months ago

https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls and the feature that does this is "Identify software th banned by your organization but is nevertheless running on your machines"

upvoted 1 times

**tester18128075** 1 year, 4 months ago

A is the correct answer

upvoted 1 times

**Granwizzard** 1 year, 4 months ago

Selected Answer: A

The correct answer is A because you don't have any other option that will block applications from running.
But accordingly, with the latest info, the option to enforce adaptive applications is not available, so it will only alert.https://docs.microsoft.com/e us/azure/defender-for-cloud/adaptive-application-controls#are-there-any-options-to-enforce-the-application-controls

The question is mentioning to block the application from running, and the adaptive application controls don't have this capability available, so t answer shouldn't be correct.

upvoted 3 times

**Janusguru** 1 year, 2 months ago

Adaptive application controls are intended to provide security alerts if any application runs other than the ones you've defined as safe. It doe not block or enforce.

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

A. adaptive application controls - correct

upvoted 4 times

Question #24 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database.
You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.

You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead use solution: You recommend creating private endpoints for the web app and the database layer.
Note:
How to Use Azure Private Endpoints to Restrict Public Access to WebApps.
As an Azure administrator or architect, you are sometimes asked the question: ɔ€How can we safely deploy internal business applications to Azure App Services?ɔ€
These applications characteristically are:
Not accessible from the public internet.
Accessible from within the on-premises corporate network
Accessible via an authorized VPN client from outside the corporate network.
For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private Endpoint is a read-only network interface service associated with the Azure PAAS
Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.
It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources.
They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App, your own / partner owned services, Azure Backups, Event Grids, Azure Service
Bus, or Azure Automations.
Reference:
https://www.varonis.com/blog/securing-access-azure-webapps

*Community vote distribution*
B (91%) 9%

**Learing** Highly Voted 1 year, 2 months ago
Selected Answer: B
Could make sense before web app but nut before DB
upvoted 6 times

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago
correct
upvoted 6 times

**Victory007** Most Recent 5 months, 1 week ago
Selected Answer: A

Yes, implementing Azure Front Door with Azure Web Application Firewall (WAF) can help meet the goal of securing the connection between the web app and the database following the Zero Trust model. Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely available web applications. With the integration of Azure Web Application Firewall (WAF), Azure Front Door can provide centralized protection for your web applications against common exploits and vulnerabilities.

upvoted 1 times

**neoalienson** 7 months, 1 week ago

**Selected Answer: B**

The solution of implementing Azure Front Door with Azure Web Application Firewall (WAF) focuses on securing the web app against external threats and distributed denial-of-service (DDoS) attacks. While this is a valid security measure for protecting your web app, it does not directly address securing the connection between the web app and the database.

upvoted 4 times

**tester18128075** 1 year, 4 months ago

correct

upvoted 2 times

Question #25 *Topic 2*

You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules.
What should you include in the solution?

A. Microsoft Defender for Endpoint

B. Microsoft Endpoint Manager

C. Microsoft Information Protection

D. Microsoft Sentinel

**Correct Answer:** *B*
Microsoft Endpoint Manager includes Microsoft Intune.
Device compliance policies are a key feature when using Intune to protect your organization's resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version.
Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint
Manager includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.
Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co- management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk.
Note: Microsoft Defender for Endpoint Plan 2 protects your Windows and Linux machines whether they're hosted in Azure, hybrid clouds (on-premises), or multicloud.
Microsoft Defender for Endpoint on iOS offers protection against phishing and unsafe network connections from websites, emails, and apps.
Microsoft Defender for Endpoint on Android supports installation on both modes of enrolled devices - the legacy Device Administrator and Android Enterprise modes. Currently, Personally-owned devices with work profile and Corporate-owned fully managed user device enrollments are supported in Android Enterprise.
Reference:
https://docs.microsoft.com/en-us/mem/endpoint-manager-overview https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint

*Community vote distribution*
B (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard
upvoted 7 times

**ltu2022** Most Recent 7 months ago
was on exam 15/06/23
upvoted 4 times

**TomHoff** 10 months ago
Selected Answer: B
yes, Intune MEM
upvoted 1 times

**AJ2021** 10 months, 1 week ago
Selected Answer: B
Correct
upvoted 1 times

**Azzzurrre** 1 year ago
Intune supports the listed device OS -- thus Endpoint Manager.

It's important to note that the explanation given is outdated. Microsoft Defender for Endpoint is not part of Microsoft Endpoint Manager, but integrating Defender for Endpoint with Intune allows Intune (and thus Endpoint Manager) to be the best answer.

upvoted 3 times

**Sec_Arch_Chn** 1 year, 1 month ago

Correct answer. Covers all of the below running devices
Android device administrator
Android (AOSP) (preview)
Android Enterprise
iOS/iPadOS
Linux - Ubuntu Desktop, version 20.04 LTS and 22.04 LTS
macOS
Windows 10 and later
Source: https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

upvoted 2 times

**SAMSH** 1 year, 3 months ago

Correct answer. was in 20Sep2020 exam

upvoted 1 times

**CaracasCCS1** 1 year, 4 months ago

Selected Answer: B

B... you need to create a compliance policy and check MDM devices with it.

upvoted 3 times

**prabhjot** 1 year, 4 months ago

Yes correct ans

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

Selected Answer: B

correct answer

upvoted 3 times

Question #26 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.
You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Note: Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in- time VM access and network security groups.
Recommendations:
- Internet-facing virtual machines should be protected with network security groups
- Management ports of virtual machines should be protected with just-in-time network access control
- Management ports should be closed on your virtual machines
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

*Community vote distribution*
B (100%)

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago
Selected Answer: B
100% correct
upvoted 5 times

**zellck** Most Recent 8 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations
upvoted 1 times

**tester18128075** 1 year, 4 months ago
answer is correct
upvoted 1 times

Question #27 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

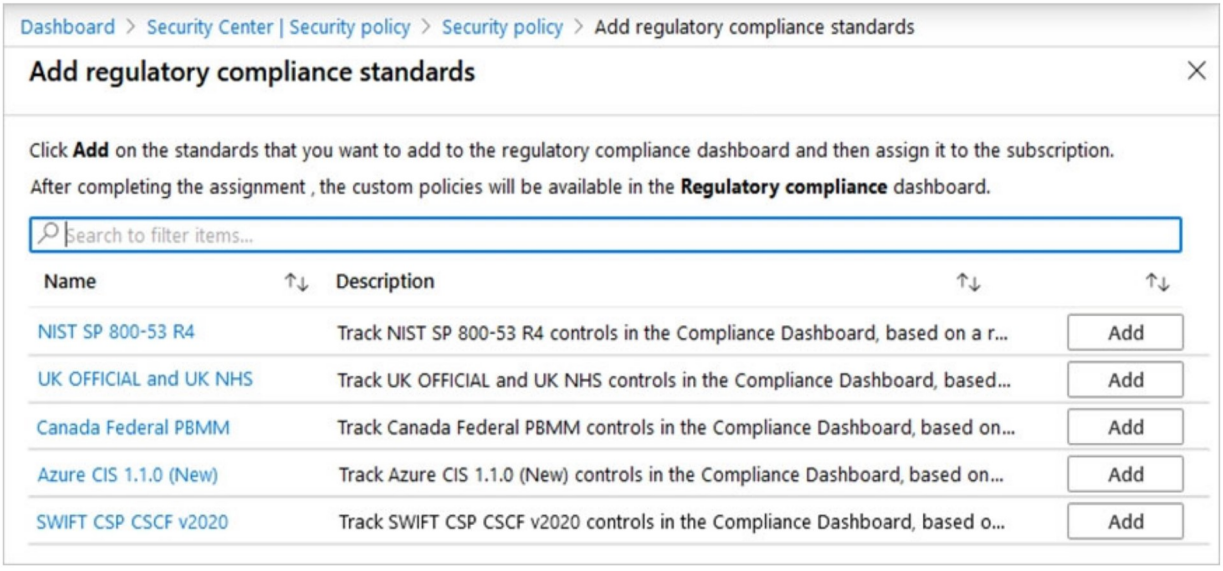
A. From Defender for Cloud, review the secure score recommendations.

B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Defender for Cloud, add a regulatory compliance standard.

**Correct Answer:** *D*
Add a regulatory standard to your dashboard
The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.
Add a standard to your Azure resources
1. From Defender for Cloud's menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.
2. From the top of the page, select Manage compliance policies. The Policy Management page appears.
3. Select the subscription or management group for which you want to manage the regulatory compliance posture.
4. To add the standards relevant to your organization, expand the Industry & regulatory standards section and select Add more standards.
5. From the Add regulatory compliance standards page, you can search for any of the available standards:




6. Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.
7. From Defender for Cloud's menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.
Your new standard appears in your list of Industry & regulatory standards.
Note: Customize the set of standards in your regulatory compliance dashboard.
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

*Community vote distribution*
D (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: D
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-a
available-in-defender-for-cloud

upvoted 13 times

**zellck** Most Recent 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, an benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.

upvoted 1 times

**awssecuritynewbie** 11 months, 1 week ago

Selected Answer: D

The question asks to view .. but NIST is not added by default though... but i guess it is the best option between the given answers.

upvoted 1 times

**Mo22** 11 months, 1 week ago

Selected Answer: D

D. From Defender for Cloud, add a regulatory compliance standard.

The first step in reviewing the Azure subscription for NIST 800-53 compliance is to add the NIST 800-53 regulatory compliance standard in Defender for Cloud. This will allow you to see if your subscription meets the requirements for the NIST 800-53 standard. After adding the standa you can review the compliance status and take appropriate actions to address any issues found.

upvoted 1 times

**tester18128075** 1 year, 4 months ago

D is correct

upvoted 2 times

**prabhjot** 1 year, 4 months ago

this is correct and (add a regulatory compliance standard from MS defender for cloud )

upvoted 3 times

**Alex_Burlachenko** 1 year, 4 months ago

actually exist the same question v.2.0 and answer there would be "From Defender for Cloud, enable Defender for Cloud plans." but that one is correct

upvoted 2 times

Question #28 *Topic 2*

Your company has devices that run either Windows 10, Windows 11, or Windows Server.
You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune

B. Local Group Policy Object (LGPO)

C. Windows Autopilot

D. Policy Analyzer

**Correct Answer:** *D*
Microsoft Security Compliance Toolkit 1.0, Policy Analyzer.
The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:
Highlight when a set of Group Policies has redundant settings or internal inconsistencies.
Highlight the differences between versions or sets of Group Policies.
Compare GPOs against current local policy and local registry settings
Export results to a Microsoft Excel spreadsheet
Policy Analyzer lets you treat a set of GPOs as a single unit. This treatment makes it easy to determine whether particular settings are duplicated across the
GPOs or are set to conflicting values. Policy Analyzer also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.
Note: The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft- recommended security configuration baselines for Windows and other Microsoft products.
The SCT enables administrators to effectively manage their enterprise's Group Policy Objects (GPOs). Using the toolkit, administrators can compare their current
GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active
Directory or individually through local policy.
Security Compliance Toolkit Tools:

Policy Analyzer -
Local Group Policy Object (LGPO)

Set Object Security -

GPO to Policy Rules -
Incorrect:
Not B: Local Group Policy Object (LGPO)
What is the Local Group Policy Object (LGPO) tool?
LGPO.exe is a command-line utility that is designed to help automate management of Local Group Policy. Using local policy gives administrators a simple way to verify the effects of Group Policy settings, and is also useful for managing non-domain-joined systems.
LGPO.exe can import and apply settings from Registry
Policy (Registry.pol) files, security templates, Advanced Auditing backup files, as well as from formatted ز€LGPO textز€ files. It can export local policy to a GPO backup. It can export the contents of a Registry Policy file to the ز€LGPO textز€ format that can then be edited, and can build a Registry Policy file from an LGPO text file.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

*Community vote distribution*
D (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: D

Link referenced is good. Same one I used to study. D is correct.

upvoted 11 times

**WRITER00347** Most Recent 5 months, 1 week ago

The Microsoft Security Compliance Toolkit provides security baselines and allows you to view recommended and current system configurations. When it comes to comparing these baselines to the current device configurations, Policy Analyzer is the appropriate tool.

Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). It can identify whether current policies are complian with the desired baselines, making it suitable for this task.

So the correct answer is:

D. Policy Analyzer

upvoted 1 times

**ltu2022** 7 months ago

was on exam 15/06/23

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10#what-is-the-policy-analyzer-tool
The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:
- Compare GPOs against current local policy and local registry settings

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 1 times

**Mo22** 11 months, 1 week ago

Both the Local Group Policy Object (LGPO) tool and the Policy Analyzer tool support Windows 10, Windows 11, and Windows Server.

The LGPO tool is a Microsoft-supported command line tool that provides the ability to manage local group policies on Windows devices, includi Windows 10, Windows 11, and Windows Server.

The Policy Analyzer tool is a Microsoft-supported graphical tool that provides the ability to compare and analyze different versions of Group Pol Objects (GPOs), including GPOs on Windows 10, Windows 11, and Windows Server.

upvoted 1 times

**cast0r** 1 year, 2 months ago

Selected Answer: D

Given answer is correct, also Intune does not support Server OS

upvoted 2 times

**tester18128075** 1 year, 4 months ago

Policy Analyser is correct

upvoted 1 times

**HardcodedCloud** 1 year, 4 months ago

Selected Answer: D

D is correct

upvoted 3 times

**prabhjot** 1 year, 4 months ago

the SCT also includes the Policy Analyzer and Local
Group Policy Object (LGPO) tools, which also help you manage your GPO settings ( ANS is Policy analyzer)

upvoted 4 times

**Alex_Burlachenko** 1 year, 4 months ago

right, correct

upvoted 4 times

Question #29 *Topic 2*

You have an Azure subscription that is used as an Azure landing zone for an application.

You need to evaluate the security posture of all the workloads in the landing zone.

What should you do first?

A. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.

B. Obtain Azure AD Premium Plan 2 licenses.

C. Add Microsoft Sentinel data connectors.

D. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**hanyahmed** Highly Voted 12 months ago

Selected Answer: D

security posture = MS Defender for Cloud
D is right answer

upvoted 11 times

**zellck** Most Recent 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction#improve-your-security-posture
The security of your cloud and on-premises resources depends on proper configuration and deployment. Defender for Cloud recommendations identify the steps that you can take to secure your environment.

Defender for Cloud includes Foundational CSPM capabilities for free. You can also enable advanced CSPM capabilities by enabling paid Defende plans.

upvoted 2 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: D

understand the current posture of the system. MDfC is correct

upvoted 1 times

**killaK** 11 months, 2 weeks ago

Selected Answer: D

I dont like the wording. 'posture' is always related to recommendations (CSPM) which come free out of the box and dont require enabling any o the paid defender for cloud plans (CWPP), alerts.

upvoted 1 times

**kiko90909** 12 months ago

i think this one is correct one Add Microsoft Sentinel data connectors
correct answer is A

upvoted 1 times

**maku067** 12 months ago

"Add Microsoft Sentinel data connectors" is C but why? Could you explain?

upvoted 1 times

**purek77** 1 year ago

Selected Answer: D

I guess D is the correct answer following below:
https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-secur for-azure-landing-zone

upvoted 4 times

Question #30 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

**Correct Answer:** *A*

*Community vote distribution*

A (70%) B (30%)

**smosmo** Highly Voted 12 months ago

Selected Answer: A

Correct Answer

upvoted 5 times

**Azerty1313** Most Recent 4 weeks, 1 day ago

As enhanced security is already activated, the FIRST thing to do is C in my opinion.

upvoted 2 times

**Ario** 6 months, 2 weeks ago

Selected Answer: B

Azure Policy provides a centralized service for creating, assigning, and managing policies across Azure subscriptions. By assigning a built-in poli definition that aligns with NIST 800-53 compliance, you can evaluate the current state of the subscription against the required controls and iden any non-compliant resources

upvoted 3 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 1 times

**AzureJobsTillRetire** 10 months, 4 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 1 times

Question #31 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**zellck** 8 months ago

Same as Question 30.
https://www.examtopics.com/discussions/microsoft/view/94937-exam-sc-100-topic-2-question-30-discussion

upvoted 2 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 2 times

**03allen** 11 months, 3 weeks ago

I think this question appears 4 times so far in this dump.

upvoted 4 times

**airairo** 11 months ago

for 3rd time. 2 are same. one in a different way.

upvoted 1 times

**fiol82** 12 months ago

looks correct to me!

upvoted 2 times

**smosmo** 12 months ago

I think it is D because you do not need to enable all the Cloud plans to review compliance (not 100% sure)

upvoted 2 times

**nieprotetkniteeetr** 12 months ago

D Correct. https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 2 times

**maku067** 1 year ago

Is it correct?

upvoted 1 times

Question #32 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.

B. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

C. From Defender for Cloud, enable Defender for Cloud plans.

D. From Defender for Cloud, add a regulatory compliance standard.

**Correct Answer:** *D*

*Community vote distribution*

D (75%) C (25%)

**Ario** 6 months, 2 weeks ago

Selected Answer: C

FIRST STEP

upvoted 2 times

**ServerBrain** 4 months, 4 weeks ago

No, don't think like that, else you will think first step is to login to the portal

upvoted 3 times

**zellck** 8 months ago

Same as Question 27.
https://www.examtopics.com/discussions/microsoft/view/78456-exam-sc-100-topic-2-question-27-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, an
benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific
compliance requirements.

upvoted 2 times

**OrangeSG** 12 months ago

Selected Answer: D

Duplicate with question 27

upvoted 3 times

**fiol82** 12 months ago

Selected Answer: D

D is correct according to me!

upvoted 1 times

**maku067** 12 months ago

C or D?

upvoted 1 times

Question #33 *Topic 2*

Your company has an Azure subscription that uses Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Defender for Cloud, review the Azure security baseline for audit report.

C. From Defender for Cloud, add a regulatory compliance standard.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**Ario** 6 months, 2 weeks ago

Selected Answer: C

Adding a regulatory compliance standard allows you to assess the current state of the Azure subscription against specific compliance framework such as NIST 800-53. This step enables you to evaluate the compliance posture and identify any gaps or areas that require attention to meet the compliance requirements.

upvoted 1 times

**zellck** 8 months ago

Same as Question 27.
https://www.examtopics.com/discussions/microsoft/view/78456-exam-sc-100-topic-2-question-27-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.

upvoted 1 times

**Ajdlfasudfo0** 10 months, 4 weeks ago

Selected Answer: C

correct

upvoted 4 times

Question #34 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

C. From Defender for Cloud, review the secure score recommendations.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**zellck** 8 months ago

Same as Question 30.
https://www.examtopics.com/discussions/microsoft/view/94937-exam-sc-100-topic-2-question-30-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 1 times

**awssecuritynewbie** 11 months ago

Correct answer is selected

upvoted 2 times

Question #35 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, enable Defender for Cloud plans.

B. From Azure Policy, assign a built-in initiative that has a scope of the subscription.

C. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

D. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

**Correct Answer:** *B*

*Community vote distribution*

B (67%) D (33%)

**baptista** Highly Voted 10 months, 3 weeks ago

this question is repeated 3 times.

upvoted 11 times

**EmarOliva** Most Recent 5 months, 2 weeks ago

Selected Answer: B

It is repeated. So the answer is B (https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5)

upvoted 1 times

**Ario** 6 months, 2 weeks ago

Selected Answer: D

Azure Policy provides a centralized platform to enforce and assess compliance with a wide range of regulatory standards, including NIST 800-53 assigning a built-in policy definition, you can evaluate the current configuration and compliance status of the Azure resources in the subscriptio against the specified requirements.

upvoted 1 times

**zellck** 8 months ago

Same as Question 30.
https://www.examtopics.com/discussions/microsoft/view/94937-exam-sc-100-topic-2-question-30-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/nist-sp-800-53-r5

upvoted 1 times

Question #36 *Topic 2*

You have an Azure subscription.

Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.

What should you recommend using to enforce the governance requirement?

A. Azure management groups

B. custom Azure roles

C. Azure Policy assignments

D. regulatory compliance standards in Microsoft Defender for Cloud

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**Gurulee** Highly Voted 9 months ago

Selected Answer: C

Specifically, some useful governance actions you can enforce with Azure Policy include:
Ensuring your team deploys Azure resources only to allowed regions,
Enforcing the consistent application of taxonomic tags, and
Requiring resources to send diagnostic logs to a Log Analytics workspace

upvoted 5 times

**WRITER00347** Most Recent 5 months, 1 week ago

To enforce the governance requirement that resources must be created only in specific Azure regions (West Europe or North Europe), you shoul recommend using Azure Policy assignments.

Azure Policy enables you to create, assign, and manage policies that enforce different rules and effects over your resources. In this case, you can define a policy that restricts the creation of resources to the specified regions, and then assign that policy to the appropriate scope (subscriptior resource group, etc.).

Therefore, the correct option is:

C. Azure Policy assignments.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It alsc helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

upvoted 1 times

**kazaki** 8 months, 1 week ago

Why not D

upvoted 4 times

**ijunico** 6 months, 3 weeks ago

because the question is about restrictions for regions for resources, not about any specific regulations.

upvoted 1 times

Question #37 *Topic 2*

HOTSPOT
-

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender.

You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender.

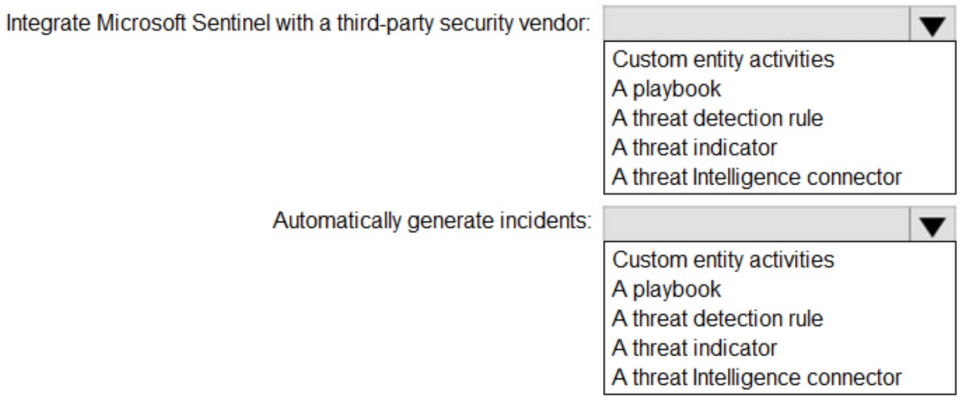
You need to recommend a solution to meet the following requirements:

• Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware.
• Automatically generate incidents when the IP address of a command-and-control server is detected in the events.

What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

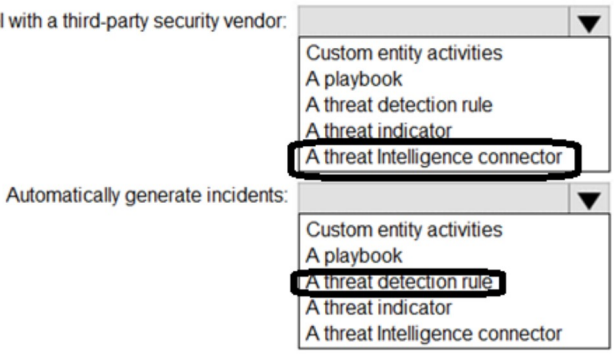
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer Area**

**Correct Answer:**




**Victory007** Highly Voted 5 months, 1 week ago

1. Threat Intelligence connector - Allow you to integrate Microsoft Sentinel with third-party security vendors to access information about known threats, such as malware and command-and-control servers.
2. Threat detection rule- Allow you to define conditions that, when met, will automatically generate an incident in Microsoft Sentinel.
https://learn.microsoft.com/en-us/azure/sentinel/partner-integrations
https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts

upvoted 14 times

**Murtuza** Most Recent 1 week, 2 days ago

Playbooks are used to automatically remediate the incidents after the rule has been created so playbook is not an answer here

upvoted 1 times

**Mblott77** 5 months, 2 weeks ago

1. Playbook used to send data to 3rd party SIEM.
https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
2. Microsoft Threat Intelligence Analytics rule.
https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-built-in
upvoted 2 times

Question #38 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You need to enforce ISO 27001:2013 standards for new resources deployed to the subscription. The solution must ensure that noncompliant resources are automatically detected.

What should you use?

A. Azure Blueprints

B. the regulatory compliance dashboard in Defender for Cloud

C. Azure Policy

D. Azure role-based access control (Azure RBAC)

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**Murtuza** 1 week, 2 days ago
enforce = azure policy
upvoted 1 times

**juanpe147** 1 month ago
in my opinion, if they are new elements, it should be a BluePrint instead an azure Policy
upvoted 1 times

**Victory007** 5 months, 1 week ago
Selected Answer: C
same as before.
upvoted 2 times

Question #39 *Topic 2*

DRAG DROP

-

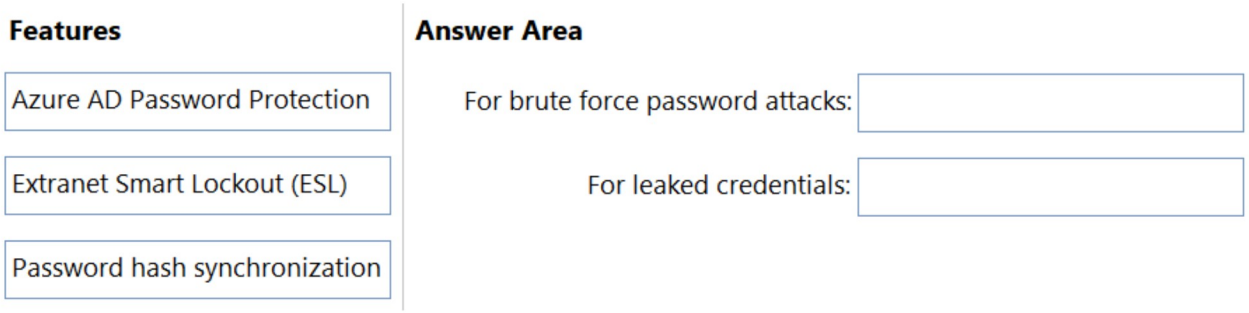
You have a hybrid Azure AD tenant that has pass-through authentication enabled.

You are designing an identity security strategy.

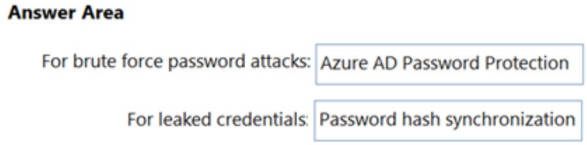
You need to minimize the impact of brute force password attacks and leaked credentials of hybrid identities.

What should you include in the design? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**Luffysan91x** 1 month ago

I chose ESL for the Second Option.

https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout

Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers

upvoted 1 times

**smanzana** 2 months, 3 weeks ago

Box1: Azure AD Password Protection
Box2: Password hash syncronization

upvoted 4 times

**AbdallaAM** 3 months, 3 weeks ago

Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers. By setting smart lockout policies in Azure AD appropriat attacks can be filtered out before they reach on-premises AD DS.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

upvoted 3 times

**calotta1** 4 months, 3 weeks ago

based on the article ... https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

ESL is not possible when using PTA - "Hash tracking functionality isn't available for customers with pass-through authentication enabled as authentication happens on-premises not in the cloud"

Azure AD Password Protection seem to be the answer based on these recommendations:

When using pass-through authentication, the following considerations apply:*

*The Azure AD lockout threshold is less than the AD DS account lockout threshold. Set the values so that the AD DS account lockout threshold i least two or three times greater than the Azure AD lockout threshold.
* The Azure AD lockout duration must be set longer than the AD DS account lockout duration. The Azure AD duration is set in seconds, while th AD duration is set in minutes.

upvoted 2 times

**ruscomike** 1 month, 2 weeks ago

from the same document:
"Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premi Active Directory Domain Services (AD DS) accounts from being locked out by attackers"

ESL is available also for PTA, only the hash tracking is not available (purple box on the doc page).

upvoted 1 times

**Doinitza** 4 months, 1 week ago

Yes, it looks like that ESL is not available for a hybrid environment: "Finally, remember to start looking at moving to a Cloud Authentication model (either with Password Hash Sync or Pass-Through Authentication) so we can do the blocking for you at cloud scale in Azure Active Directory". Link: https://www.linkedin.com/pulse/extranet-smart-lockout-ad-fs-2016-andres-canello

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

this means the current answers are correct.

upvoted 2 times

**KrissB** 4 months, 3 weeks ago

For brute force password attacks: Extranet Smart Lockout (ESL)
For Leaked Credentials: Password Hash Sync. PHS needs to be enabled so Microsoft can compare Password hash' for cloud and hybrid identities those available on the black market.

upvoted 1 times

**KrissB** 4 months, 3 weeks ago

Actually, This is a weird one. Extranet Smart Lockout is an ADFS feature, however here while talking about Hybrid identities, they mention tha the set up is Pass-Through AUth so ADFS is not a solution without backtracking and going against the Microsoft recommended route (shift away from ADFS). Azure AD feature is Smart Lockout.

upvoted 2 times

**kanag1** 5 months ago

For brute force password attacks: Extranet Smart Lockout (ESL)
For leaked Credentials: Azure AD Password Protection

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recogni sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, whil your users continue to access their accounts and be productive.
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

upvoted 3 times

**Cally46** 5 months ago

Looks correct:
1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
2. https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-phs

upvoted 1 times

Question #40 *Topic 2*

HOTSPOT
-

You are designing the security architecture for a cloud-only environment.

You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

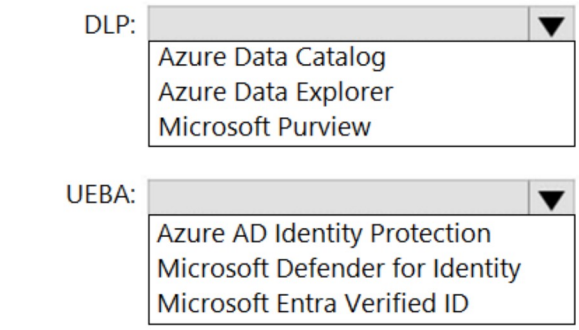
You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

• Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
• Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area.

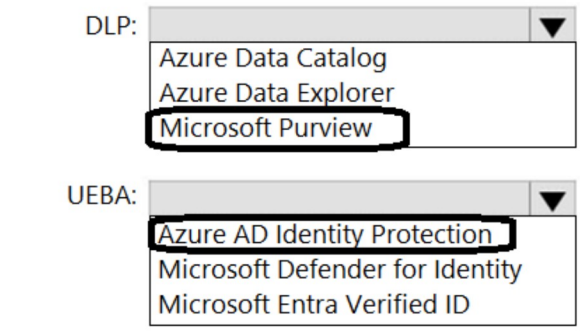
NOTE: Each correct selection is worth one point.

**Answer Area**




**Correct Answer:**

**Answer Area**




**Victory007** Highly Voted 5 months, 1 week ago

1. Purview- For the requirement to enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal, you should include Microsoft Purview in your recommendation. https://learn.microsoft.com/en-us/microsoft-365/security/defender/dlp-investigate-alerts-defender?view=o365-worldwide
2. MS Defender for Identity. Microsoft Defender for Cloud Apps provides user entity behavioral analytics (UEBA) in the cloud. This can be extend to your on-premises environment by integrating with Microsoft Defender for Identity. After you integrate with Defender for Identity, you'll also gain context around user identity from its native integration with Active Directory. https://learn.microsoft.com/en-us/defender-cloud-apps/tutor ueba

upvoted 12 times

**KrissB** Highly Voted 4 months, 3 weeks ago

Purview and Microsoft Defender for Identity. MDI is a pre-requisite UEBA across various security workloads.

upvoted 6 times

**cybrtrk** Most Recent 1 week, 5 days ago

Purview is correct
No active directory in this question, so UEBA should be Azure AD Identity Protection.

upvoted 1 times

**summut** 2 weeks, 1 day ago

1 = Purview
2 = Identity Protection (MDI is a Hybrid solution mainly for monitoring and protecting on-prem identities)

upvoted 1 times

**Arjanussie** 1 month, 1 week ago

It is a design of a cloud only environment and Yes, Azure AD Identity Protection provides User and Entity Behavior Analytics (UEBA) functionality UEBA uses artificial intelligence and machine learning to model how users and devices typically behave. It then compares future behavior agains the baseline to create a risk score. This allows you to analyze large data sets and elevate the highest-priority alerts

upvoted 2 times

**hovlund** 2 months, 2 weeks ago

It is NOT Defender for Identity because its a cloud only environment..., i agree with ServerBrian: Purview and Identity Protection

upvoted 5 times

**Azerty1313** 1 month ago

Agree. Azure ID protect is a better fit as it is Azure only.
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/introducing-investigation-priority-built-on-user-and-entity/ba-p/360853#:~:text=UEBA%20for%20Azure%20ATP%2C%20MCAS%2C%20and%20Azure%20AD%20Identity%20Protection&text=Activities%20and%20events%20from%20these,organization%2C%20should%20they%20be%20compromised.

upvoted 1 times

**smanzana** 2 months, 3 weeks ago

Microsoft Purview and Microsoft Defender for Identity

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Purview and Identity Protection
https://learn.microsoft.com/en-us/azure/security/fundamentals/threat-detection

upvoted 1 times

**sbnpj** 5 months ago

Purview and Defender for Identity

https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-suspicious-activity

upvoted 2 times

Question #41 *Topic 2*

HOTSPOT

-

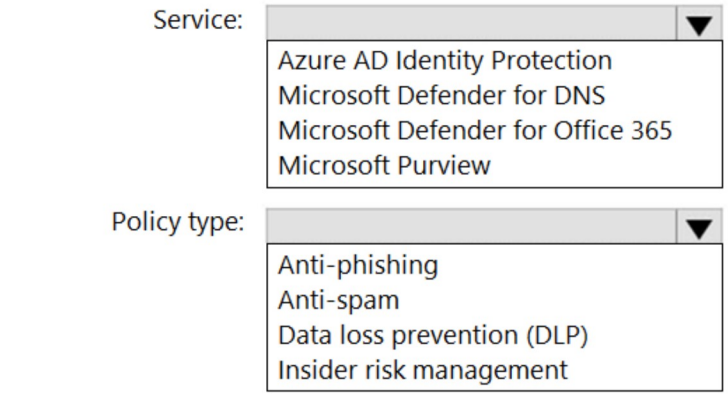
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

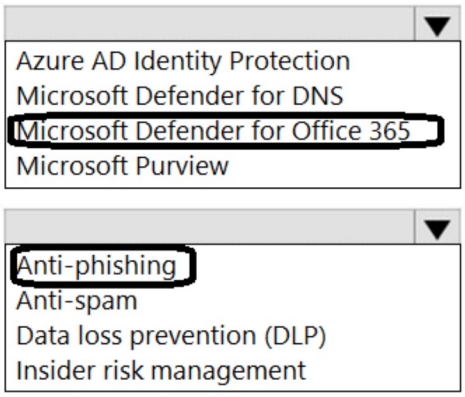
NOTE: Each correct selection is worth one point.

**Answer Area**




**Correct Answer:**

**Answer Area**




**morito** 3 weeks, 1 day ago

For people like me who are unsure whether this belongs to EOP or to Defender for Office 365, here a good comparision: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about?view=o365-worldwide. TLDR: EOP contains some anti-phishing functionality, but only Defender for Office 365 has impersonation protection.

upvoted 1 times

**smanzana** 2 months, 3 weeks ago

Microsoft Defender for Office 365 y Anti-Phishing

upvoted 3 times

**ServerBrain** 4 months, 4 weeks ago

Given answers are 100% correct

upvoted 4 times

**Victory007** 5 months, 1 week ago

1. MS Defender for Office 365. 2. Anti-Phishing . To prevent malicious actors from impersonating the email addresses of internal senders, you should use Microsoft Defender for Office 365 and configure an Anti-phishing policy. Microsoft Defender for Office 365 provides protection agai phishing attacks, including spoofing and impersonation. You can customize the anti-phishing policy to specify the actions to take when a messa

is identified as a phishing attempt. This includes configuring anti-spoofing protection, which helps protect against exact domain spoofing, where attackers forge the domain to look exactly like the domain of the victim's organization or like their business partner's.

upvoted 4 times

Question #42 *Topic 2*

HOTSPOT
-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.

You have multiple project teams. Each team has an AD DS group that syncs with Azure AD.

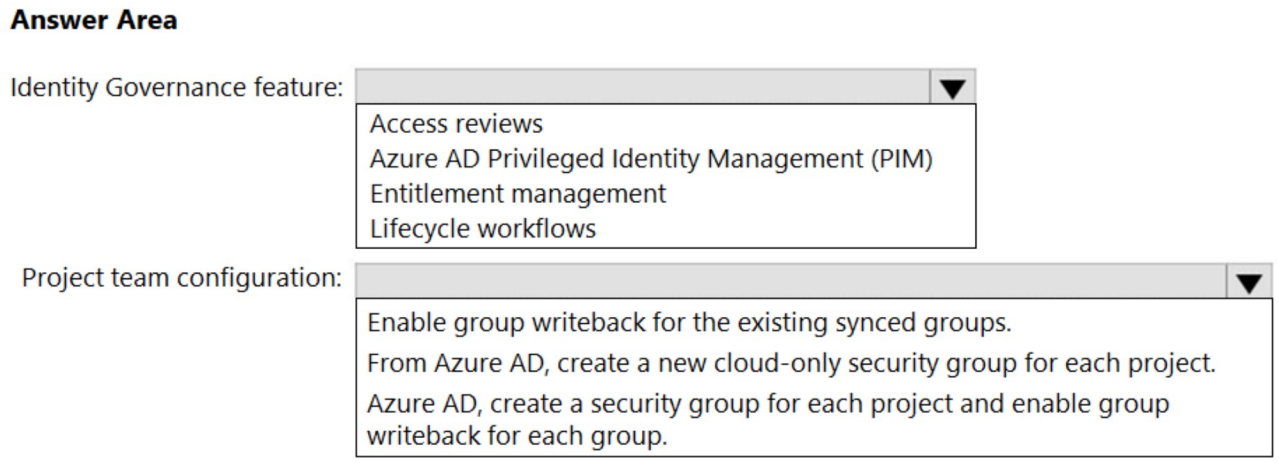
Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

You need to recommend an Azure AD Identity Governance solution that meets the following requirements:

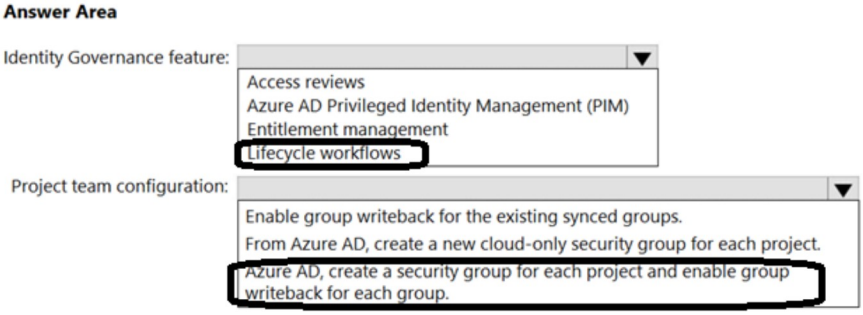
- Project managers must verify that their project group contains only the current members of their project team.
- The members of each project team must only have access to the resources of the project to which they are assigned.
- Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days.
- Administrative effort must be minimized.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**Victory007** Highly Voted 5 months, 1 week ago

1. Access Reviews. 2. Enable group write back for the existing synced group. https://learn.microsoft.com/en-us/azure/active-directory/governanc /access-reviews-overview.

upvoted 26 times

**casualbork** 4 months ago

• Project managers must verify that their project group contains only the current members of their project team.
This means access reviews, Lifecycle Workflow would do all of this automatically based on the user attributes (such as department or team)

You have multiple project teams. Each team has an **AD DS group** that **syncs with Azure AD.** (these being the key to find the correct answer)
Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.

The correct answer is "Enable group write back for the existing synced group."

Therefor, the answer Victory007 have provided is the correct answer.

upvoted 5 times

**ServerBrain** 4 months, 4 weeks ago

You are correct. Azure AD Connect has group writeback enabled, no need to create new groups.

upvoted 1 times

**Murtuza** Most Recent 1 week ago

Project managers must verify = IMPLIES ACCESS REVIEW

upvoted 1 times

**NICKTON81** 3 weeks, 2 days ago

1 - Entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview
2. Enable group write back for the existing synced group.

upvoted 2 times

**harimurti20** 1 month, 1 week ago

Given Answer is correct: Lifecycle Workflow is correct, as per the requirement-Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days.

upvoted 1 times

**smanzana** 2 months, 3 weeks ago

Box1:Access Reviews
Box2: Enable group write back for the existing synced group.

upvoted 2 times

**ConanBarb** 3 months, 3 weeks ago

To add some detail to the discussion: Lifecycle Workflows could have been an option, and actually a better one than Access Reviews, but isn't du to
1) The requirements says "Users must be removed from a project group automatically if the project manager has NOT verified the group's membership for 30 days."
2) LC Workflows requires Microsoft Entra ID Governance licenses (which we can't assume)

Lifecycle Workflows, if valid, would have been better as they are automatic and event driven, (happen instantly) and not every 30 days or so

upvoted 1 times

**sbnpj** 5 months ago

I agree with Victory007, its 1- Access reviews and Enabled Group write back for the existing synced group.

upvoted 2 times

**saurabh123sml** 5 months ago

Given Answer is correct it seems
Lifecycle Workflows
Writeback enabled

upvoted 1 times

Question #43 *Topic 2*

HOTSPOT
-

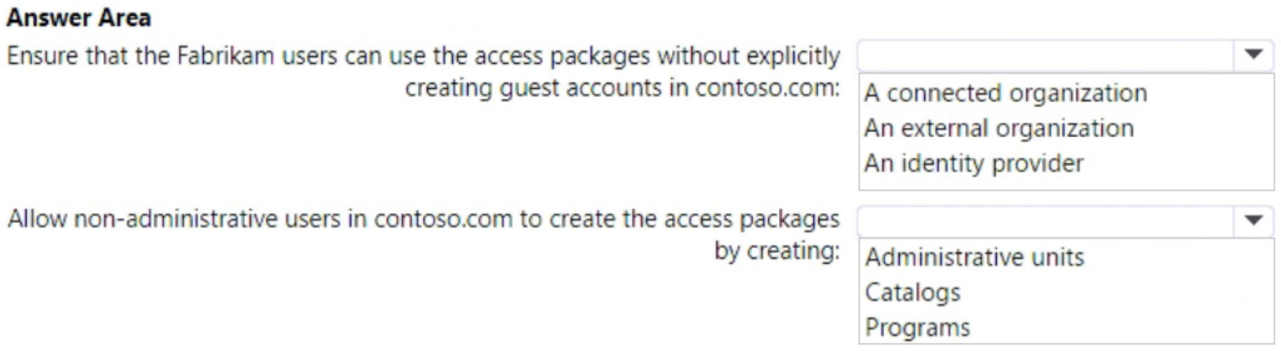
You are designing a privileged access strategy for a company named Contoso, Ltd. and its partner company named Fabrikam, Inc. Contoso has an Azure AD tenant named contoso.com. Fabrikam has an Azure AD tenant named fabrikam.com. Users at Fabrikam must access the resources in contoso.com.

You need to provide the Fabrikam users with access to the Contoso resources by using access packages. The solution must meet the following requirements:

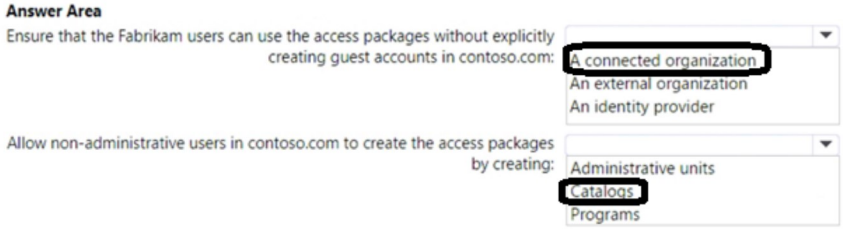
• Ensure that the Fabrikam users can use the Contoso access packages without explicitly creating guest accounts in contoso.com.
• Allow non-administrative users in contoso.com to create the access packages.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**harimurti20** 1 month, 1 week ago
Answer is correct
upvoted 3 times

**xavi1** 2 months, 3 weeks ago
Correct:
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-organization
https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-external-users
upvoted 1 times

Question #44 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app registrations in Azure AD

D. application control policies in Microsoft Defender for Endpoint

**Correct Answer:** *D*

**Ramye** 4 days, 2 hours ago
Yes, Microsoft Defender for Endpoint can do the job, but it is not mentioned in the question at all. So, can this really be the answer?
upvoted 1 times

**harimurti20** 1 month, 1 week ago
D (Application control policies in Microsoft Defender for Endpoint) is correct.
upvoted 1 times

**smanzana** 2 months, 3 weeks ago
D (Application control policies in Microsoft Defender for Endpoint)
upvoted 2 times

**theugly23** 2 months, 3 weeks ago
D is correct
upvoted 1 times

Question #45 *Topic 2*

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.

The company signs a contract with the United States government.

You need to review the current subscription for NIST 800-53 compliance.

What should you do first?

A. From Defender for Cloud, add a regulatory compliance standard.

B. From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

C. From Defender for Cloud, review the Azure security baseline for audit report.

D. From Microsoft Defender for Cloud Apps, create an access policy for cloud applications.

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Murtuza** 1 week, 2 days ago

Selected Answer: A

A is correct

upvoted 1 times

**Arockia** 1 week, 2 days ago

A. From Defender for Cloud, add a regulatory compliance standard.

To review the subscription for NIST 800-53 compliance, you should start by adding the NIST 800-53 regulatory compliance standard within Defender for Cloud. This will ensure that the appropriate compliance checks and assessments are performed against the NIST 800-53 controls fc your Azure resources.

The other options are not the correct first step for reviewing NIST 800-53 compliance:

upvoted 1 times

**harimurti20** 1 month, 1 week ago

Answer is B

upvoted 1 times

**harimurti20** 1 month, 1 week ago

Answer A is correct:
Answer B will be correct if it contains Azure Policy initiative

upvoted 1 times

**Glorpy** 1 month, 1 week ago

Selected Answer: A

Answer is correct:
Defender for Cloud's regulatory standards and benchmarks are represented as security standards.

Defender for Cloud continually assesses the environment-in-scope against standards. Based on assessments, it shows in-scope resources as bei compliant or noncompliant with the standard, and provides remediation recommendations.

upvoted 2 times

**Azerty1313** 1 month, 1 week ago

Answer is B

upvoted 1 times

**theugly23** 2 months, 3 weeks ago

Answer A Correct

upvoted 1 times

Question #46 *Topic 2*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app registrations in Azure AD

B. Azure AD Conditional Access App Control policies

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. adaptive application controls in Defender for Cloud

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**Murtuza** 1 week, 2 days ago

**Selected Answer: D**

D is correct

upvoted 1 times

**Murtuza** 2 weeks ago

**Selected Answer: D**

D is correct questions keeps repeating in this dump

upvoted 1 times

**theugly23** 2 months, 3 weeks ago

D is correct

upvoted 2 times

Question #47 *Topic 2*

You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.

You need to design a security solution to assess whether all the devices meet the customer's compliance rules.

What should you include in the solution?

A. Microsoft Sentinel

B. Microsoft Purview Information Protection

C. Microsoft Intune

D. Microsoft Defender for Endpoint

**Correct Answer:** *D*

*Community vote distribution*

C (95%) 5%

**shanti0091** Highly Voted 3 months, 1 week ago

Selected Answer: C

Microsoft Intune same repeated question as #25 Microsoft Endpoint Manager.

upvoted 7 times

**harimurti20** Most Recent 1 month, 1 week ago

Answer C, Microsoft Intue is correct

upvoted 3 times

**Glorpy** 1 month, 2 weeks ago

Selected Answer: C

Intune as compliance is assessed through it and not MDE

upvoted 2 times

**DuckChuck** 2 months, 3 weeks ago

Selected Answer: C

Intune is correct

upvoted 4 times

**Igglepiggle** 3 months, 1 week ago

Selected Answer: C

"solution to assess whether all the devices meet the customer's compliance rules"

Answer is MS Intune.
Defender for endpoint is for detection and response (EDR).

upvoted 3 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: C

got this in exam 6oct23. passed with 896 marks. I answered C

upvoted 4 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: D

Repeated Q#25. MD for endpoint is answer

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Sorry this is wrong comment by me. i don't know how to remove it. please ignore this ans D. correct is C

upvoted 2 times

**Topic 3 - Question Set 3**

Question #1 *Topic 3*

You have Microsoft Defender for Cloud assigned to Azure management groups.
You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation.
Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel threat intelligence workbooks

B. Microsoft Sentinel notebooks

C. threat intelligence reports in Defender for Cloud

D. workload protections in Defender for Cloud

**Correct Answer:** *AC*
A: Workbooks provide insights about your threat intelligence
Workbooks provide powerful interactive dashboards that give you insights into all aspects of Microsoft Sentinel, and threat intelligence is no exception. You can use the built-in Threat Intelligence workbook to visualize key information about your threat intelligence, and you can easily customize the workbook according to your business needs. You can even create new dashboards combining many different data sources so you can visualize your data in unique ways. Since
Microsoft Sentinel workbooks are based on Azure Monitor workbooks, there is already extensive documentation available, and many more templates.
C: What is a threat intelligence report?
Defender for Cloud's threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats.
Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:
Activity Group Report: provides deep dives into attackers, their objectives, and tactics.
Campaign Report: focuses on details of specific attack campaigns.
Threat Summary Report: covers all of the items in the previous two reports.
This type of information is useful during the incident response process, where there's an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue in the future.
Incorrect:
Not B: When to use Jupyter notebooks
While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data.
For example, use notebooks to:
Perform analytics that aren't provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features
Create data visualizations that aren't provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees
Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.
Not D: Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. For example, you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your Azure Storage accounts.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

*Community vote distribution*
AC (100%)

**zts** Highly Voted 1 year, 4 months ago
Selected Answer: AC
answer is correct.
upvoted 11 times

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago

correct ans

upvoted 6 times

**zellck** Most Recent 8 months ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence#add-threat-indicators-to-microsoft-sentinel-with-the-microsof
defender-threat-intelligence-data-connector
Bring high fidelity indicators of compromise (IOC) generated by Microsoft Defender Threat Intelligence (MDTI) into your Microsoft Sentinel workspace. The MDTI data connector ingests these IOCs with a simple one-click setup. Then monitor, alert and hunt based on the threat intelligence in the same way you utilize other feeds.

upvoted 3 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 2 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports#what-is-a-threat-intelligence-report
When Defender for Cloud identifies a threat, it triggers a security alert, which contains detailed information regarding the event, including suggestions for remediation. To help incident response teams investigate and remediate threats, Defender for Cloud provides threat intellige reports containing information about detected threats.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence#introduction-to-threat-intelligence
For SIEM solutions like Microsoft Sentinel, the most common forms of CTI are threat indicators, also known as Indicators of Compromise (IoC Indicators of Attack (IoA). Threat indicators are data that associate observed artifacts such as URLs, file hashes, or IP addresses with known threat activity such as phishing, botnets, or malware. This form of threat intelligence is often called tactical threat intelligence because it's' applied to security products and automation in large scale to detect potential threats to an organization and protect against them. Use threa indicators in Microsoft Sentinel, to detect malicious activity observed in your environment and provide context to security investigators to inform response decisions.

upvoted 1 times

**uffman** 8 months, 3 weeks ago

Selected Answer: AC

Correct.

upvoted 1 times

**tester18128075** 1 year, 4 months ago

A and C

upvoted 4 times

Question #2 *Topic 3*

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions.
You are evaluating the security posture of the customer.
You discover that the AKS resources are excluded from the secure score recommendations.
You need to produce accurate recommendations and update the secure score.
Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Defender plans.

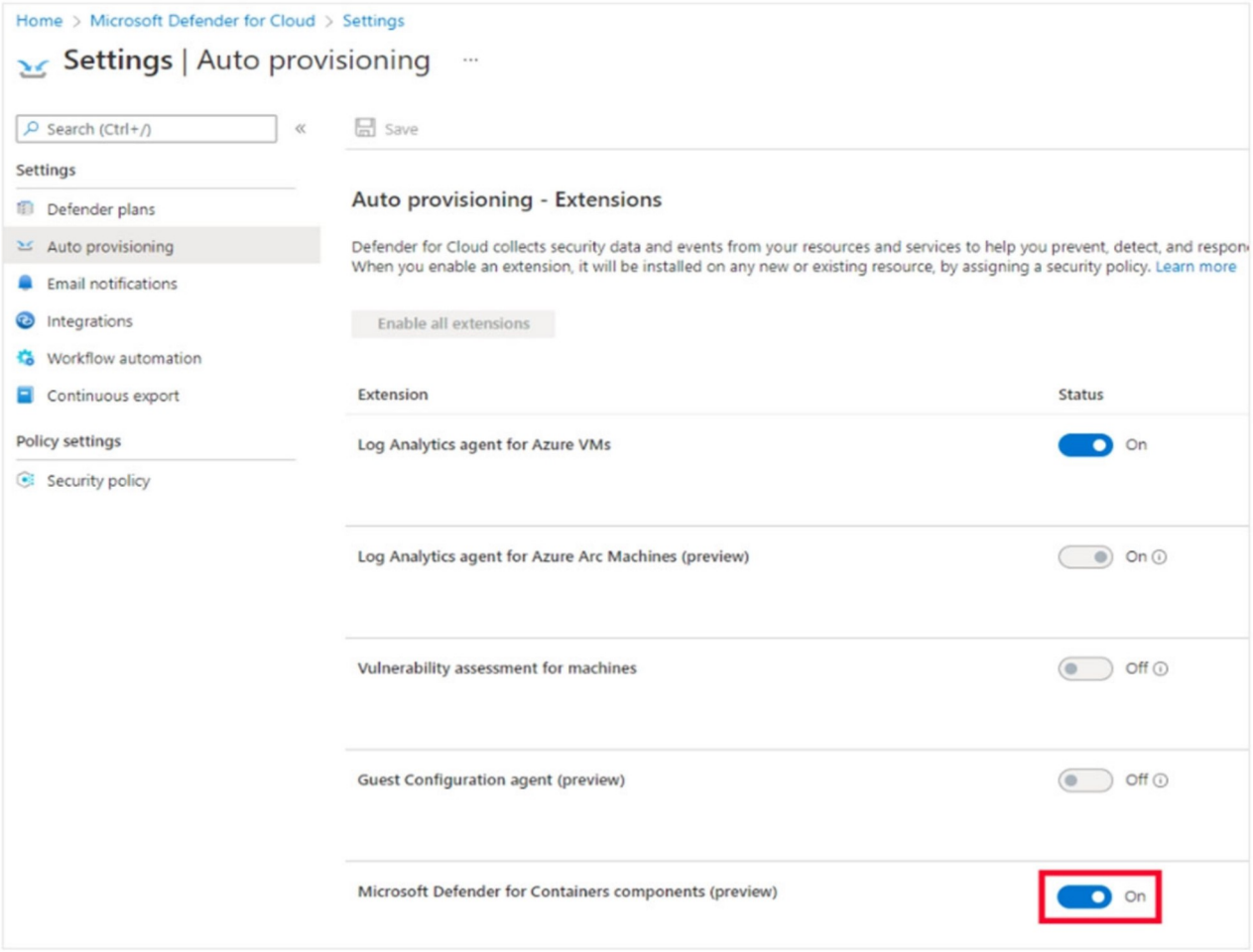
B. Configure auto provisioning.

C. Add a workflow automation.

D. Assign regulatory compliance policies.

E. Review the inventory.

**Correct Answer:** *BD*
D: How are regulatory compliance standards represented in Defender for Cloud?
Industry standards, regulatory standards, and benchmarks are represented in Defender for Cloud's regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.
To see compliance data mapped as assessments in your dashboard, add a compliance standard to your management group or subscription from within the
Security policy page.
When you've assigned a standard or benchmark to your selected scope, the standard appears in your regulatory compliance dashboard with all associated compliance data mapped as assessments.
B: Configure Defender for Containers components
If you disabled any of the default protections when you enabled Microsoft Defender for Containers, you can change the configurations and reenable them via auto provisioning.
1. To configure the Defender for Containers components:
2. Sign in to the Azure portal.
3. Navigate to Microsoft Defender for Cloud > Environment settings.
4. Select the relevant subscription.
5. From the left side tool bar, select Auto provisioning.
6. Ensure that Microsoft Defenders for Containers components (preview) is toggled to On.




Incorrect:

Not A: When you enable Microsoft Defender for Containers, Azure Kubernetes Service clusters, and Azure Arc enabled Kubernetes clusters (Preview) protection are both enabled by default.

To upgrade to Microsoft Defender for Containers, open the Defender plans page in the portal and enable the new plan:

Not C: No need for automation.

Note: Automate responses to Microsoft Defender for Cloud triggers.

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can.

Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

*Community vote distribution*

AB (75%) 14% 12%

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago

I would select A and B

upvoted 41 times

**foxtrott** Highly Voted 1 year, 4 months ago

Selected Answer: AB

I like A and B for this one - enable the defender for containers plan - then ensure it deploys to your container resources with auto provision.

upvoted 24 times

**sbnpj** Most Recent 5 months, 2 weeks ago

Selected Answer: AB

I would go with A&B

upvoted 4 times

**Ario** 6 months, 2 weeks ago

Selected Answer: AE

By enabling Defender plans and reviewing the inventory, you can ensure that the AKS resources are properly evaluated, and their security postu is reflected in the secure score.

upvoted 2 times

**MS_ExamsRule** 7 months, 1 week ago

Although by default Enabling the Defender plan also configures auto-provisioning, to align with CAF you would then configure auto-provisionir to use a centralised rather than the default log analytics workspace.
So its A&B

upvoted 4 times

**zellck** 8 months ago

Selected Answer: AB

AB is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-enable

upvoted 3 times

**zellck** 8 months ago

A streamlined, frictionless, process lets you use the Azure portal pages to enable the Defender for Cloud plan and setup auto provisioning of the necessary components for defending your Kubernetes clusters at scale.

upvoted 1 times

**Tictactoe** 8 months, 1 week ago

AE CORRECT

upvoted 2 times

**alifrancos** 9 months ago

Selected Answer: AD

For me it's A & D,
it's simple, first you should active the Defender Plan, and microsoft say that auto provisioned id activated by default, so, we cannot shoose it because it's given by microsoft,
and for the secure score, we should have policy defenition assigned, else we will not increase secure score

upvoted 2 times

**Gurulee** 9 months ago

Selected Answer: AB

Since AKS was observed as excluded, it needs to be re-enabled and auto provisioned.

upvoted 6 times

**vitodobra** 9 months, 3 weeks ago

Selected Answer: AE

Para producir recomendaciones precisas y actualizar la puntuación segura en Microsoft Defender para la nube en relación con los recursos de A se recomienda:

A. Habilitar los planes de Defender para la suscripción de Azure que contiene los recursos de AKS. Esto permitirá que Microsoft Defender para la nube recolecte datos de seguridad de los recursos y proporcionará recomendaciones específicas de seguridad.

E. Revisar el inventario de recursos de AKS en cada suscripción de Azure y asegurarse de que se están siguiendo las mejores prácticas de seguric Esto ayudará a identificar cualquier problema de seguridad que pueda existir y tomar medidas para abordarlos.

upvoted 1 times

**josh_josh** 10 months, 1 week ago

Selected Answer: AE

The correct answer is A and E. No one can counter this statement. prove me wrong

upvoted 2 times

**ChaBum** 10 months, 1 week ago

so, you're guessing!

upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

Selected Answer: AE

The two actions that should be recommended in Microsoft Defender for Cloud to produce accurate recommendations and update the secure sc are:

A. Enable Defender plans: Enabling Defender plans for Azure Kubernetes Service will enable the Defender for Kubernetes solution to collect and analyze security events and provide recommendations for improving the security posture of the AKS resources. Defender for Kubernetes integra with Azure Security Center and Azure Monitor to provide a unified view of security posture and insights.

E. Review the inventory: Reviewing the inventory in Microsoft Defender for Cloud will enable you to identify all the AKS resources and Docker images deployed across the four Azure subscriptions. This will help you assess the security posture of the resources, identify potential vulnerabilities and misconfigurations, and prioritize remediation actions.

upvoted 6 times

**Fal991l** 10 months, 2 weeks ago

Option B (Configure auto provisioning), option C (Add a workflow automation), and option D (Assign regulatory compliance policies) are not directly related to addressing the issue of excluded AKS resources from secure score recommendations. These options may be helpful in othe scenarios, such as automating remediation actions or ensuring compliance with specific regulations. However, for the given scenario, enablin Defender plans and reviewing the inventory are the most relevant actions.

upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

That's from ChatGPT. Does it sound interesting?

upvoted 1 times

**Gurulee** 10 months, 4 weeks ago

Tricky...I can understand B,D. " When you enable Microsoft Defender for Containers, Azure Kubernetes Service clusters, and Azure Arc enabled Kubernetes clusters (Preview) protection are both enabled by default."

upvoted 1 times

**Gurulee** 9 months ago

After reviewing closer, since AKS was found excluded, my answer would be A, B

upvoted 3 times

**awssecuritynewbie** 11 months ago

Selected Answer: AB

A and B for sure! I have tested it in the lab trust me

upvoted 5 times

**awssecuritynewbie** 11 months, 1 week ago

Selected Answer: AB

for sure A and B

upvoted 2 times

**Navynine** 1 year ago

Selected Answer: AB

A and B

upvoted 4 times

**TJ001** 1 year ago

AB for me

upvoted 3 times

Question #3 *Topic 3*

Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks.
The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:
⇨ Prevent exposing the public IP addresses of the virtual machines.
⇨ Provide the ability to connect without using a VPN.
⇨ Minimize costs.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a hub and spoke network by using virtual network peering.

B. Deploy Azure Bastion to each virtual network.

C. Deploy Azure Bastion to one virtual network.

D. Create NAT rules and network rules in Azure Firewall.

E. Enable just-in-time VM access on the virtual machines.

**Correct Answer:** *AC*
Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
Incorrect:
Not B: Two Azure Bastions would increase the cost.
Reference:
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

*Community vote distribution*
AC (97%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: AC
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion
upvoted 22 times

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago
correct answer (so good job Guys!)
upvoted 11 times

**Ario** Most Recent 6 months, 2 weeks ago
Selected Answer: BE
By deploying Azure Bastion to each virtual network and enabling JIT VM access on the virtual machines, you can provide the developers with secure and convenient access to the virtual machines over SSL from the Azure portal, while also meeting the requirements of preventing public exposure, avoiding the use of a VPN, and minimizing costs.
upvoted 1 times

**edurakhan** 7 months, 3 weeks ago
Exam 5/25/2023
upvoted 3 times

**zellck** 8 months ago
Selected Answer: AC
AC is the answer.

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peere VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

upvoted 3 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 2 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: AC

This seems the only logical combination.

upvoted 1 times

**awssecuritynewbie** 11 months, 1 week ago

Selected Answer: AC

Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity t VMs created in the local or peered virtual networks.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastic service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
Incorrect:
Not B: Two Azure Bastions would increase the cos

upvoted 2 times

**JeeBi** 11 months, 3 weeks ago

Why not C and E? Because E costs more? It would be safer...

upvoted 1 times

**walkaway** 11 months, 3 weeks ago

Then you will need two different Azure Bastion hosts.

upvoted 2 times

**tester18128075** 1 year, 4 months ago

A and C is cost optimal solution

upvoted 4 times

**HardcodedCloud** 1 year, 4 months ago

Selected Answer: AC

Perfect answer

upvoted 7 times

Question #4 *Topic 3*

HOTSPOT -

You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

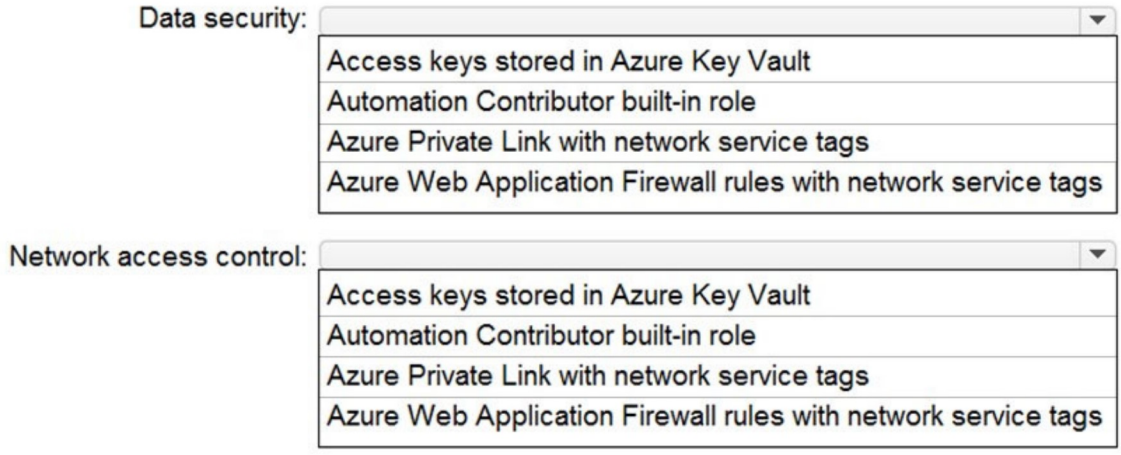
You need to recommend a solution to secure the components of the copy process.

What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

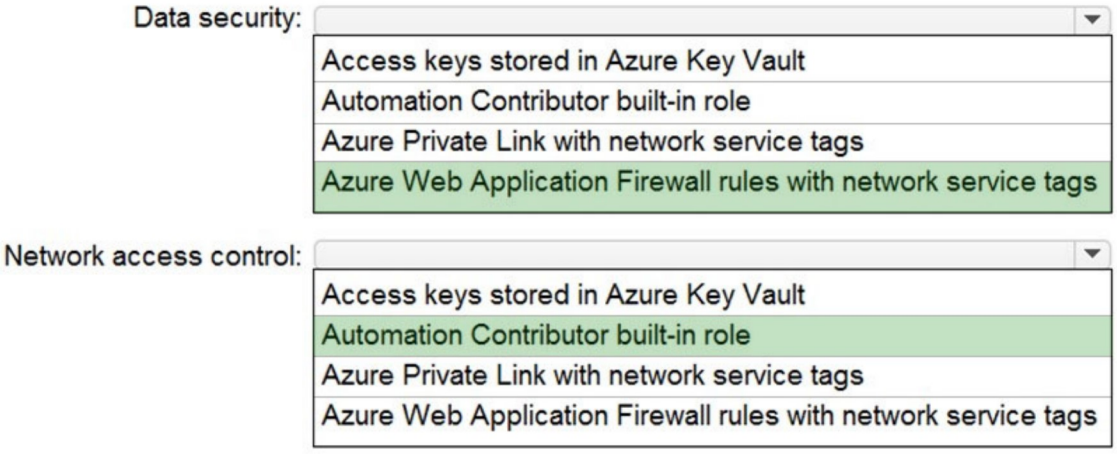
Hot Area:

**Answer Area**




**Correct Answer:**

**Answer Area**




Box 1: Azure Web Application Firewall with network service tags

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to define network access controls on network security groups, Azure Firewall, and user-defined routes.

Incorrect:

* Not Azure private link with network service tags
Network service tags are not used with Private links.
Box 2: Automation Contributor built-in role
The Automation Contributor role allows you to manage all resources in the Automation account, except modifying other user's access permissions to an
Automation account.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago
wrong one, I would select - Key Vault for box1 and for box 2 is Private Link
upvoted 85 times

**prabhjot** 1 year, 4 months ago
Ans is wrong - Azure key vault is for Application ad Data Security so key vault - Box1 and Private link is for Vnet security so Box2 =Private link
upvoted 14 times

**HardcodedCloud** Highly Voted 1 year, 4 months ago
Data Security : Access Keys stored in Azure Key Vault
Network access control : Azure Private Link with network service tags
upvoted 37 times

**Arockia** Most Recent 1 week, 2 days ago
• Data safety: Lock keys in Key Vault, network isolation with Private Link & service tags for secured Azure Data Lake Gen2 copy via Automation runbook.

• Network control: Private Link & service tags shield your Azure Data Lake Gen2 copy process from the public internet for enhanced security.
upvoted 1 times

**Murtuza** 1 week, 2 days ago
App GW with WAF cant play a role because it applies to client facing which is not the ASK in the question.
upvoted 1 times

**JG56** 1 month, 2 weeks ago
in exam Nov 23, Agree with Alex
upvoted 3 times

**smanzana** 2 months, 3 weeks ago
Box1:Key Vault
Box2:Private Link
upvoted 2 times

**ian2387** 2 months, 3 weeks ago
Have we managed to figure out the correct answer?
Data: Azure key vault
Network: Private link with service tags. I have my doubts if service tags are supported by azure private links.
upvoted 1 times

**rahulnair** 3 months ago
A & C -
Secure the assets in Azure Automation including credentials, certificates, connections and encrypted variables. These assets are protected in Azure Automation using multiple levels of encryption. By default, data is encrypted with Microsoft-managed keys. For additional control over encryption keys, you can supply customer-managed keys to use for encryption of Automation assets. These keys must be present in Azure Key Vault for Automation service to be able to access the keys.

Use Azure Private Link to securely connect Hybrid runbook workers to Azure Automation. Azure Private Endpoint is a network interface that connects you privately and securely to a an Azure Automation service powered by Azure Private Link. Private Endpoint uses a private IP address from your Virtual Network (VNet), to effectively bring the Automation service into your VNet.

https://learn.microsoft.com/en-us/azure/automation/automation-security-guidelines
upvoted 2 times

**ConanBarb** 3 months, 3 weeks ago
Hey all,
Lets exclude the nonsensical options first:
Automation Contributor role is the RBAC role for working with the Automation service, "design-time" if you will, and hence has nothing to do with securing data run-time.

Private link with network service tags is nonse for N/W security. There is no such thing. Network service tags is used in NSGs and firewall rules.

Hence, even though these options seem strange as well but in theory relevant:
Data Security: Key vault
N/W Security: App GW with WAF

upvoted 3 times

**uffman** 8 months, 3 weeks ago

Box1: Key Vault
Box2: Private Link

upvoted 1 times

**KrisDeb** 11 months, 1 week ago

Azure Automation Run As Account will retire on September 30, 2023 and will be replaced with Managed Identities. Before that date, you'll need start migrating your runbooks to use managed identities. For more information, see migrating from an existing Run As accounts to managed identity to start migrating the runbooks from Run As account to managed identities before 30 September 2023.

upvoted 3 times

**Toschu** 9 months, 3 weeks ago

Note: This has nothing to do with the question

upvoted 4 times

**janesb** 1 year ago

Data Security : Access Keys stored in Azure Key Vault
Network access control : Azure Private Link with network service tags
https://learn.microsoft.com/en-us/azure/automation/automation-security-guidelines

upvoted 5 times

**Azzzurrre** 1 year ago

None of the answers provided is a good answer. They are fragmentary or just wrong.
Key Vault with access keys is a bad answer because using shared access keys is only recommended if a service accessing the storage cannot use managed identity or a certificate to authenticate.

"Azure Private Link with network service tags" doesn't mean anything. Network Service Tags can be used in NSG rules, and in routing rules, if eit were specified, but they aren't.

upvoted 6 times

**EM1234** 8 months, 2 weeks ago

these are both good points. I was also confused how everyone keeps saying to use private link with service tags. Service tags are not used wi private links / endpoints.
I would still go with A for data security since key vault can be very explicitly secured but the point you made is great.
For the second question, I would go with the app gateway with WAF since it is at least controlling network access. Honestly though, I think something has been written wrong here. The answers dont make sense.

upvoted 1 times

**TJ001** 1 year ago

Data Security : Access Keys stored in Azure Key Vault
Network access control : Azure Private Link with network service tags

upvoted 3 times

**cychoia** 1 year, 2 months ago

https://learn.microsoft.com/en-us/azure/automation/automation-security-guidelines

upvoted 6 times

**tester18128075** 1 year, 4 months ago

Data Security : Key Vault
Network Access Control : Private links/endpoints

upvoted 4 times

**PlumpyTumbler** 1 year, 4 months ago

Both given answers are incorrect. Follow the user comments. It seems like everyone knows this so far.
Data Security = Access Keys stored in Azure Key Vault
Network access control = Azure Private Link with network service tags

https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security

upvoted 15 times

Question #5 *Topic 3*

You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.
What should you include in the recommendation?

A. Compliance Manager

B. Microsoft Defender for Cloud Apps

C. Microsoft Endpoint Manager

D. Microsoft Defender for Endpoint

**Correct Answer:** *D*
Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint. It enables your organization to track and regulate access to websites based on their content categories. Many of these websites, while not malicious, might be problematic because of compliance regulations, bandwidth usage, or other concerns.
Note: Turn on web content filtering
From the left-hand navigation in Microsoft 365 Defender portal, select Settings > Endpoints > General > Advanced Features. Scroll down until you see the entry for Web content filtering. Switch the toggle to On and Save preferences.
Configure web content filtering policies
Web content filtering policies specify which site categories are blocked on which device groups. To manage the policies, go to Settings > Endpoints > Web content filtering (under Rules).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering

*Community vote distribution*
D (92%) 8%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: D
Click on the arrow next to "Adult content" and Gambling is explicitly named as a Defender for Endpoint content filtering site category.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#configure-web-content-filtering-policies
upvoted 15 times

**zellck** Most Recent 8 months ago

Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#what-is-web-conter filtering
Web content filtering is part of the Web protection capabilities in Microsoft Defender for Endpoint and Microsoft Defender for Business. Web content filtering enables your organization to track and regulate access to websites based on their content categories. Many of these websites (even if they're not malicious) might be problematic because of compliance regulations, bandwidth usage, or other concerns.
upvoted 2 times

**Shaz** 8 months, 2 weeks ago

Selected Answer: D
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide
upvoted 2 times

**AWS56** 10 months, 1 week ago

Selected Answer: B
B. Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a cloud-native security solution that helps protect your organization from cyber threats across cloud applications and services, including web browsing. It includes web content filtering capabilities that allow you to block access to websites that contain adult content, such as gambling sites, and other categories of websites that you want to block.

To implement this solution, you can configure web content filtering policies in Microsoft Defender for Cloud Apps and apply them to your Windows 11 devices. This will prevent users from accessing websites that are not allowed by the policy.

Compliance Manager is a solution that helps you manage regulatory compliance requirements for Microsoft cloud services, and Microsoft Endp

Manager and Microsoft Defender for Endpoint are solutions for securing and managing endpoint devices, but neither of these solutions specific provide web content filtering capabilities.

upvoted 1 times

**Toschu** 9 months, 3 weeks ago

Defender for Endpoint has a basic web filter included, and Microsoft Defender for Cloud Apps needs for the web filter to run Defender for Endpoint on the client.
Fun fact: When Defender for Endpoint was first released, a web filter was not included in the price and they wanted that customers pay extra it because it was provided by 3rd party. In the end, after an outcry, it was added as part of the package.

upvoted 1 times

**awssecuritynewbie** 11 months, 1 week ago

Selected Answer: B

this is is also correct with cloudapps you can filter based on category so i would say B

upvoted 1 times

**tester18128075** 1 year, 4 months ago

D is correct

upvoted 2 times

**NNavee** 1 year, 4 months ago

Correct Answer

upvoted 1 times

**JMuller** 1 year, 4 months ago

Selected Answer: D

correct

upvoted 2 times

**re213** 1 year, 4 months ago

Selected Answer: D

Correct Ans

upvoted 3 times

**K1SMM** 1 year, 4 months ago

D is correct !

upvoted 2 times

**Alex_Burlachenko** 1 year, 4 months ago

defo correct

upvoted 2 times

Question #6 *Topic 3*

Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10.
You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
☞ Ensure that only authorized applications can run on the kiosks.
☞ Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Implement Automated investigation and Remediation (AIR) in Microsoft Defender for Endpoint.

B. Onboard the kiosks to Microsoft intune and Microsoft Defender for Endpoint.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

D. Onboard the kiosks to Azure Monitor.

E. Implement Privileged Access Workstation (PAW) for the kiosks.

**Correct Answer:** *BE*
Onboard devices and configure Microsoft Defender for Endpoint capabilities.
Deploying Microsoft Defender for Endpoint is a two-step process.
* Onboard devices to the service
* Configure capabilities of the service
B: Depending on the device, follow the configuration steps provided in the onboarding section of the Defender for Endpoint portal.
E: A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses credential guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and web traffic is restricted to a limit set of permitted destinations (Deny all).
Note: Privileged Access Workstation (PAW) ₳€" This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised. The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive job tasks. This makes the
PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing. To provide productivity to these users, separate accounts and workstations must be provided for productivity applications and web browsing.
While inconvenient, this is a necessary control to protect users whose account could inflict damage to most or all resources in the organization.
Incorrect:
Not A: What is automated investigation and remediation?
Automated investigation and response capabilities help your security operations team by: Determining whether a threat requires action. Taking (or recommending) any necessary remediation actions. Determining whether and what other investigations should occur. Repeating the process as necessary for other alerts.
Not C: Threat & Vulnerability Management is a component of Microsoft Defender for Endpoint, and provides both security administrators and security operations teams with unique value, including:
- Real-time endpoint detection and response (EDR) insights correlated with endpoint vulnerabilities.
- Invaluable device vulnerability context during incident investigations.
- Built-in remediation processes through Microsoft Intune and Microsoft System Center Configuration Manager.
Note: Microsoft's threat and vulnerability management is a built-in module in Microsoft Defender for Endpoint that can:
Discover vulnerabilities and misconfigurations in near real time.
Prioritize vulnerabilities based on the threat landscape and detections in your organization.
If you've enabled the integration with Microsoft Defender for Endpoint, you'll automatically get the threat and vulnerability management findings without the need for additional agents.
As it's a built-in module for Microsoft Defender for Endpoint, threat and vulnerability management doesn't require periodic scans.
Not D: You do not use Azure Monitor for onboarding.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure https://docs.microsoft.com/en-us/security/compass/privileged-access-devices https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-tvm

*Community vote distribution*

BC (79%) BE (21%)

**Jasper666** Highly Voted 1 year, 4 months ago

I would go for B and C. Vuln management sits on top of defender for endpoint. (https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide)

upvoted 44 times

**cdizzle** 1 year, 2 months ago

Agree with you, I think PAW could get the job done as well but the spirit of the question is for kiosks endpoint. PAW implementations are typ for admin workstations.

upvoted 18 times

**HardcodedCloud** Highly Voted 1 year, 4 months ago

Selected Answer: BC

B & C based on the requirements.

upvoted 24 times

**JG56** Most Recent 1 month, 2 weeks ago

in exam Nov 23, Answer, B,C

upvoted 4 times

**theplaceholder** 3 months, 4 weeks ago

Selected Answer: BC

B&C for sure.

upvoted 3 times

**WRITER00347** 5 months, 1 week ago

The requirements provided emphasize controlling the applications that can run on the kiosks and regularly hardening them against new threats With this focus on application control and threat protection, the correct actions would be:

B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Microsoft Intune can manage and configure the kiosks, allowing control over which applications can run. Microsoft Defender for Endpoint will h to protect the kiosks against threats.
C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

This feature of Microsoft Defender for Endpoint helps to discover, prioritize, and remediate threats and vulnerabilities, helping to harden the kio against new and emerging threats.
So the correct answers are:

B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.
C. Implement threat and vulnerability management in Microsoft Defender for Endpoint.

upvoted 2 times

**sbnpj** 5 months, 2 weeks ago

Selected Answer: BC

it has to be BC, other options dont provide the best solution.

upvoted 2 times

**Ario** 6 months, 2 weeks ago

Selected Answer: BC

Microsoft Intune and Microsoft Defender for Endpoint provide a comprehensive set of security capabilities to manage and protect the Windows kiosks, while threat and vulnerability management helps to proactively identify and remediate vulnerabilities.

upvoted 2 times

**imsidrai** 6 months, 3 weeks ago

recommended solution is not asking for least privilege, so no for PAW
B&C definitely correct

upvoted 1 times

**Gurulee** 9 months ago

Selected Answer: BC

PAW are for admin privileged purposes.

upvoted 4 times

**JayLearn2022** 9 months, 2 weeks ago

Answer: BC
B. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint to ensure that only authorized applications can run on the kiosk This allows for the creation of a custom device configuration profile that can restrict which apps are allowed to run on the kiosks. Intune can alsc

be used to regularly harden the kiosks against new threats.

C. Implement threat and vulnerability management in Microsoft Defender for Endpoint to provide a centralized view of the security posture of tl kiosks. This feature identifies potential vulnerabilities and provides guidance on how to mitigate them, allowing for regular hardening of the kio against new threats.

Option E (Implement Privileged Access Workstation (PAW) for the kiosks) is not a suitable recommendation for securing the mobile self-service kiosks. PAWs are typically used for highly privileged users who need access to sensitive information or systems, and not for standard kiosks. Instead, implementing Microsoft Intune and Microsoft Defender for Endpoint as suggested in option B would provide better security measures f the kiosks.

upvoted 2 times

**OK2020** 10 months, 1 week ago

I would go B & E:
B: Microsoft Defender for Endpoint Intune integration
Microsoft Defender for Endpoint and Microsoft Intune work together to help prevent security breaches. They can also limit the impact of breach ATP capabilities provide real-time threat detection as well as enable extensive auditing and logging of the end-point devices.
https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment

E: PAW
A Privileged workstation provides a hardened workstation that has clear application control and application guard. The workstation uses creden guard, device guard, app guard, and exploit guard to protect the host from malicious behavior. All local disks are encrypted with BitLocker and v traffic is restricted to a limit set of permitted destinations (Deny all).
https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices

upvoted 2 times

**awssecuritynewbie** 10 months, 3 weeks ago

Selected Answer: BC

It has to be B because you do need to onboard MDE come on guys
C = it has vulnerability scanning enabled

upvoted 3 times

**Mo22** 11 months, 1 week ago

Selected Answer: BC

B and C are the recommended actions to secure the kiosks. Implementing threat and vulnerability management in Microsoft Defender for Endpo and onboarding the kiosks to Microsoft Intune and Microsoft Defender for Endpoint will help ensure that only authorized applications can run c the kiosks and that the kiosks are regularly hardened against new threats.

upvoted 3 times

**m7medcs** 11 months, 3 weeks ago

B & C 100%

upvoted 3 times

**walkaway** 11 months, 3 weeks ago

Selected Answer: BC

kiosks are NOT administrative workstations lol. We don't need PAW for kiosks.

upvoted 3 times

**yaza85** 12 months ago

Selected Answer: BC

PAW is the name of the admin workstation concept. Its not a technology and has nothing to do with kiosk. B and C

upvoted 3 times

**Jt909** 1 year ago

Selected Answer: BC

B & C in my opinion

upvoted 4 times

Question #7 *Topic 3*

You have a Microsoft 365 E5 subscription.

You need to recommend a solution to add a watermark to email attachments that contain sensitive data.

What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps

B. Microsoft Information Protection

C. insider risk management

D. Azure Purview

**Correct Answer:** *A*

Microsoft Defender for Cloud Apps File policies.

File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases. Defender for Cloud Apps can monitor any file type based on more than 20 metadata filters (for example, access level, file type).

Reference:

https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

*Community vote distribution*

B (90%) 8%

**Alex_Burlachenko** Highly Voted 1 year, 4 months ago

Better to select B - https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide like for example You ca use sensitivity labels to:

Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, an encryption can also restrict what actions authorized people can take on the content.

Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android.

Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as SalesForce, Box, or DropBox, even if the third-party app or service do not read or support sensitivity labels.

upvoted 38 times

**HardcodedCloud** Highly Voted 1 year, 4 months ago

Selected Answer: B

B is part of Microsoft Information Protection to add Visual markings e.g. watermark for sensitive information.

upvoted 20 times

**Naqsh27** Most Recent 5 days, 16 hours ago

Selected Answer: B

Definitely B - I accidentally enabled this for the entire organisation :-P

upvoted 1 times

**JG56** 1 month, 2 weeks ago

Answer B, in exam Nov 23

upvoted 3 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: B

To add a watermark to email attachments that contain sensitive data in a Microsoft 365 E5 subscription, you should recommend B. Microsoft Information Protection.

Microsoft Information Protection (MIP) is a comprehensive solution that allows you to classify, label, and protect sensitive information in emails documents. It includes the ability to apply watermarks to documents and emails based on sensitivity labels. By configuring sensitivity labels and associated policies, you can automatically add watermarks to email attachments containing sensitive data, helping to protect the information an ensure it is appropriately labeled.

upvoted 2 times

**yoooo9730** 6 months ago

A: https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-dlp

Define which information is sensitive: Before looking for sensitive information in your files, you first need to define what counts as sensitive for y organization. As part of our data classification service, we offer over 100 out-of-the-box sensitive information types, or you can create your own suit to your company policy. Defender for Cloud Apps is natively integrated with Microsoft Purview Information Protection and the same sensiti types and labels are available throughout both services. So when you want to define sensitive information, head over to the Microsoft Purview Information Protection portal to create them, and once defined they'll be available in Defender for Cloud Apps. You can also use advanced classifications types such as fingerprint or Exact Data Match (EDM).

upvoted 1 times

**Ario** 6 months, 2 weeks ago

**Selected Answer: B**

Microsoft Defender for Cloud Apps, insider risk management, and Azure Purview, are not specifically designed to add watermarks to email attachments.

upvoted 1 times

**Ramye** 3 days, 23 hours ago

Information Protection is part of Purview, so Information Protection is specifically mentioned hence this is the best choice, otherwise, Purview

upvoted 1 times

**Holii** 6 months, 2 weeks ago

Well, now it's called Microsoft Purview Information Protection-
and there is no Azure Purview.

upvoted 2 times

**zellck** 8 months ago

**Selected Answer: B**

B is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data, while making sure that use productivity and their ability to collaborate isn't hindered.

You can use sensitivity labels to:
- Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, ar that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, an encryption can also restrict what actions authorized people can take on the content.

upvoted 1 times

**oscarmh** 10 months, 1 week ago

I would chose AIP always for watermarks

upvoted 1 times

**OK2020** 10 months, 1 week ago

I would select D:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
Anyone knows a reason why it's not D: Azure Purview?
Purview You can use sensitivity labels to:

Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, anc that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, an encryption can also restrict what actions authorized people can take on the content.

upvoted 2 times

**AJ2021** 10 months, 1 week ago

**Selected Answer: B**

B is correct

upvoted 1 times

**God2029** 10 months, 3 weeks ago

B is the right choice. A is more for thirdparty App information you have 365 E5 so using 365 Email not of any 3rd Party. Information Protection w help you here to apply the water mark based on the classification of Labels, (Ex:Internal/confidential/Public)

upvoted 1 times

**Gurulee** 10 months, 3 weeks ago

**Selected Answer: B**

Information protection

upvoted 1 times

**dbhagz** 10 months, 4 weeks ago

**Selected Answer: D**

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data - For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark.

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

upvoted 1 times

**dbhagz** 10 months, 4 weeks ago

OK B - There is no Azure Purview

upvoted 1 times

**buguinha** 11 months ago

Selected Answer: B

Information Protection is able to classify and protect email messages.

upvoted 1 times

**Mo22** 11 months, 1 week ago

Selected Answer: B

Microsoft Information Protection (MIP) is a solution that provides data classification, labeling, and protection capabilities to help organizations safeguard sensitive information in email attachments and other file types. With MIP, you can add watermarks to email attachments that contain sensitive data as part of the data labeling and protection process.

upvoted 2 times

Question #8 *Topic 3*

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.
You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface.
What should you include in the recommendation?

A. Azure Firewall Premium

B. Azure Traffic Manager and application security groups

C. Azure Application Gateway Web Application Firewall (WAF)

D. network security groups (NSGs)

**Correct Answer:** *B*
* Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.
* Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.
Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint.
Incorrect:
Not C: Azure Application Gateway Web Application Firewall is too small a scale solution in this scenario.
Note: Attacks against a web application can be monitored by using a real-time Application Gateway that has Web Application Firewall, enabled with integrated logging from Azure Monitor to track Web Application Firewall alerts and easily monitor trends.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

*Community vote distribution*
C (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: C
https://docs.microsoft.com/en-us/learn/modules/specify-security-requirements-for-applications/5-specify-security-strategy-apis
upvoted 30 times

**JaySapkota** Highly Voted 1 year, 4 months ago
I would choose C, Application Gateway with WAF. Not Traffic Manager.
Traffic Manager is a DNS based routing for performance and speed.
upvoted 17 times

**ian2387** Most Recent 2 months, 3 weeks ago
This answer needs to be rectified
upvoted 3 times

**Ramye** 6 days, 10 hours ago
And many others really
upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago
Selected Answer: C
To prevent malicious bots from scanning Azure App Service web apps for vulnerabilities while minimizing the attack surface for customers in Europe and the United States, you should recommend C. Azure Application Gateway Web Application Firewall (WAF).

C. Azure Application Gateway Web Application Firewall (WAF): Azure Application Gateway with the Web Application Firewall (WAF) is specifically designed for web application security. It provides protection against common web vulnerabilities such as SQL injection, cross-site scripting (XSS) and more. It also includes bot protection capabilities, which can help prevent malicious bots from scanning web apps for vulnerabilities. This aligns with the requirement to prevent bot scanning while minimizing the attack surface.

upvoted 3 times

**Ario** 6 months, 2 weeks ago

Selected Answer: C

to prevent malicious bot scanning and minimize the attack surface for the web apps, Azure Application Gateway Web Application Firewall (WAF) the recommended solution.

upvoted 2 times

**Linuxieux** 6 months, 3 weeks ago

The answer is Clear WAF- Azure Web Application Firewall on Azure Application Gateway bot protection overview: https://learn.microsoft.com/er us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 1 times

**PrettyFlyWifi** 7 months, 3 weeks ago

Selected Answer: C

Looks like C to me, check out:
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 2 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview
Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

upvoted 1 times

**Gurulee** 10 months, 3 weeks ago

Selected Answer: C

Application gateway with waf

upvoted 2 times

**tech_rum** 11 months ago

Selected Answer: C

App gw waf

upvoted 1 times

**buguinha** 11 months ago

Selected Answer: C

https://azure.microsoft.com/en-us/updates/new-bot-protection-rule-set-in-public-preview-for-web-application-firewall-waf-with-azure-front-door-service/

upvoted 1 times

**Mo22** 11 months, 1 week ago

Selected Answer: C

Azure Application Gateway Web Application Firewall (WAF) provides centralized protection for your web applications, helps block common attac like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), and helps minimize the attack surface by blocking malicious b from scanning your web apps for vulnerabilities. By using WAF, you can ensure that the web apps are protected against common web applicatic attacks while minimizing the attack surface.

upvoted 1 times

**ad77** 11 months, 4 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 2 times

**nieprotetkniteeetr** 12 months ago

C. Traffic Manager has no anti-bot capability.

upvoted 2 times

**Hullstar** 12 months ago

Selected Answer: C

WAF is the answer here.

upvoted 1 times

**purek77** 12 months ago

Selected Answer: C

It is WAF on Azure Application Gateway.

Ref: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview

upvoted 1 times

**cychoia** 1 year, 2 months ago

**Selected Answer: C**

Use Geomatch custom rules.
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/geomatch-custom-rules

upvoted 2 times

Question #9 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Need to use customer-managed keys instead.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

*Community vote distribution*
B (82%) A (18%)

**zts** Highly Voted 1 year, 4 months ago
Selected Answer: B
This is the link on how-to.
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation
upvoted 8 times

**prabhjot** Highly Voted 1 year, 4 months ago
Ans is correct ( it is No)
upvoted 5 times

**Murtuza** Most Recent 1 week, 6 days ago
The frequency of key rotation for Platform Managed Keys (PMKs) in Azure depends on the specific service or feature you are using. Azure manag the key rotation process for you, but the actual rotation interval may vary.
upvoted 1 times

**Glorpy** 1 month, 1 week ago
Selected Answer: B
Answer is B...while the solution of using Microsoft-managed keys within an encryption scope for blob containers in Azure Storage supports AES-256 encryption for data at rest, for monthly rotation of the encryption keys, the solution would need to be slightly adjusted to use custome managed keys to meet the specific rotation requirement.
upvoted 1 times

**JG56** 1 month, 2 weeks ago
Answer : No , in exam Nov 23
upvoted 2 times

**shanti0091** 3 months, 1 week ago
Selected Answer: A
A is the answer.
upvoted 1 times

**shanti0091** 3 months, 1 week ago
To backup my point, here is a link - https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption#about-encryption key-management
upvoted 1 times

**Ario** 6 months, 2 weeks ago

Selected Answer: A

Yes, the solution of using Microsoft-managed keys within an encryption scope for blob containers in Azure Storage meets the goal of encrypting the data at rest with AES-256 keys and supporting monthly key rotation

upvoted 2 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version
Following cryptographic best practices means rotating the key that is protecting your storage account on a regular schedule, typically at least ev two years. Azure Storage never modifies the key in the key vault, but you can configure a key rotation policy to rotate the key according to your compliance requirements.

upvoted 2 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

The thing is, keys are rotated with microsoft managed keys, but I think you don't know exactly when

upvoted 2 times

**Fal991l** 10 months, 2 weeks ago

Azure Storage encryption with Microsoft-managed keys allows for automatic and seamless key rotation every 30 days by default, which meet the requirement of rotating encryption keys monthly.

upvoted 2 times

**JakeCallham** 1 year, 2 months ago

Selected Answer: B

Nope, answer is B

upvoted 3 times

Question #10 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses Microsoft-managed keys.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Need to use customer-managed keys instead.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

*Community vote distribution*
B (88%) 13%

**Murtuza** 1 week, 6 days ago
The frequency of key rotation for Platform Managed Keys (PMKs) in Azure depends on the specific service or feature you are using. Azure mana the key rotation process for you, but the actual rotation interval may vary.
upvoted 1 times

**Ario** 6 months, 2 weeks ago
**Selected Answer: A**
By adopting TDE with Microsoft-managed keys, you can easily implement and maintain data encryption at rest for your Azure SQL databases, w also meeting the goal of supporting monthly key rotation and using AES-256 keys for encryption.
upvoted 1 times

**zellck** 8 months ago
**Selected Answer: B**
B is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql
Azure SQL transparent data encryption (TDE) with customer-managed key (CMK) enables Bring Your Own Key (BYOK) scenario for data protectic at rest, and allows organizations to implement separation of duties in the management of keys and data. With customer-managed TDE, the customer is responsible for and in a full control of a key lifecycle management (key creation, upload, rotation, deletion), key usage permissions, auditing of operations on keys.
upvoted 1 times

**Gurulee** 10 months, 3 weeks ago
**Selected Answer: B**
Customer managed key
upvoted 2 times

**Philthetill** 1 year, 4 months ago
correct
upvoted 3 times

**zts** 1 year, 4 months ago
**Selected Answer: B**
To provide Azure SQL customers with two layers of encryption of data at rest, infrastructure encryption (using AES-256 encryption algorithm) wi platform managed keys is being rolled out. This provides an addition layer of encryption at rest along with TDE with customer-managed keys,

which is already available. ---- Derived from the link below:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql&viewFallbackFrom=sql server-ver16

upvoted 4 times

Question #11 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
We need to use customer-managed keys.
Azure Storage encryption for data at rest.
Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments.
Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.
Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to manage encryption with your own keys, you have two options. You can use either type of key management, or both:
* You can specify a customer-managed key to use for encrypting and decrypting data in Blob Storage and in Azure Files.
* You can specify a customer-provided key on Blob Storage operations. A client making a read or write request against Blob Storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

*Community vote distribution*
A (100%)

**Murtuza** 1 week, 6 days ago
Unfortunately, the exact frequency of key rotation for PMKs in Azure may not be publicly disclosed.
upvoted 1 times

**JG56** 1 month, 2 weeks ago
in exam Nov 23, agree with zellck.
upvoted 1 times

**zellck** 8 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version
Following cryptographic best practices means rotating the key that is protecting your storage account on a regular schedule, typically at least ev two years. Azure Storage never modifies the key in the key vault, but you can configure a key rotation policy to rotate the key according to your compliance requirements.
upvoted 1 times

**zellck** 7 months, 3 weeks ago
Gotten this in May 2023 exam.
upvoted 3 times

**purek77** 12 months ago

**Selected Answer: A**

Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when you retrie it. The process is completely transparent to users. Storage Service Encryption uses 256-bit Advanced Encryption Standard (AES) encryption.

SSE ref: https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption

Finally: Microsoft-managed keys are rotated appropriately per compliance requirements. If you have specific key rotation requirements, Microso recommends that you move to customer-managed keys so that you can manage and audit the rotation yourself.

upvoted 1 times

**Rocky83** 1 year ago

**Selected Answer: A**

The Microsoft-managed key is rotated appropriately per compliance requirements. Note that the frequency may change without notice. Azure does not expose the logs to indicate rotation to customers. If you have specific key rotation requirements, then we recommend that you move t customer-managed keys. That way, you can manage and audit the rotation yourself.

upvoted 2 times

**Yeero** 1 year, 1 month ago

**Selected Answer: A**

Correct

upvoted 2 times

**damiandeny** 1 year, 1 month ago

**Selected Answer: A**

correct

upvoted 2 times

**Philthetill** 1 year, 4 months ago

correct

upvoted 4 times

**zts** 1 year, 4 months ago

**Selected Answer: A**

seems correct.

upvoted 3 times

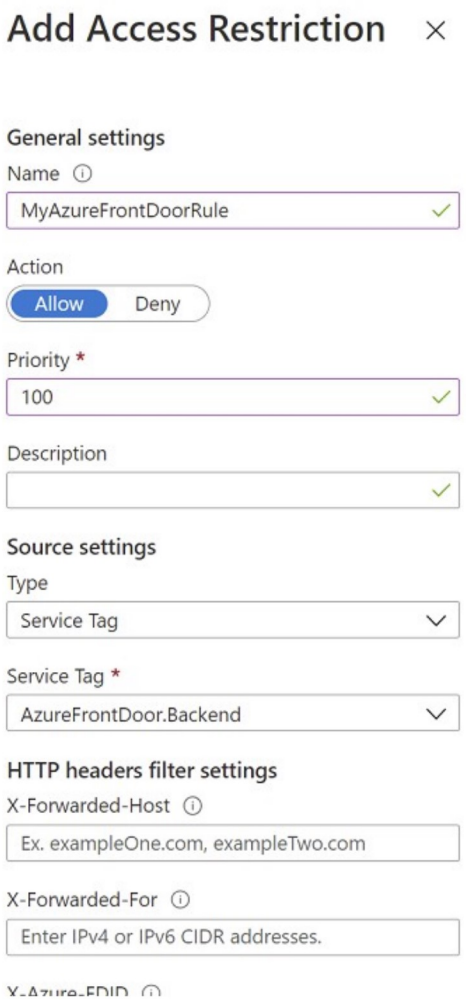
Question #12 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.




Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

*Community vote distribution*
B (71%) A (29%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
These questions repeat in this exam dump. They are found again in a later section. The answer is SERVICE TAGS. The explanations are confused. They say the correct answer in some places and incorrect in others. Focus on the screenshot provided. It shows you the answer. A picture is wort

thousand words.
upvoted 11 times

**AzureJobsTillRetire** 10 months, 1 week ago
This cannot be correct. Service tag is just a list of IP addresses.
upvoted 1 times

**[Removed]** 9 months, 2 weeks ago
This must be correct, as service tag is precisely what we need. Definition of service tag:
A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.
Link to the screenshot, you can see the type of service tag which in our case is AzureFrontDoor.Backend:
https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli#set-a-service-tag-based-rule
upvoted 1 times

**omarrob** Highly Voted 1 year, 1 month ago
A is correct and i was using this method based on an opened ticket with Microsoft Support three years ago where they recommend to do acces restriction using the Frontdoor instance ipv4 and ipv6. that time the frontdoor service tag was not yet available.

so this particular question is correct using the frontdoor backend IP or the service tag or the HTTP header, ALL ARE CORRECT
Below are the front door IP range provided by Microsoft support

147.243.0.0/16
2a01:111:2050::/44
upvoted 6 times

**Arockia** Most Recent 1 week, 1 day ago
To securely restrict access to Azure App Service web apps through Azure Front Door, a more robust approach is required:

1. Service Tag-Based Access Restrictions
2. Custom Headers
upvoted 1 times

**zellck** 8 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t
Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.
upvoted 1 times

**EM1234** 8 months, 1 week ago
Selected Answer: B
When you read the doc you will see that the header filter is critical:

"IP address filtering alone isn't sufficient to secure traffic to your origin, because other Azure customers use the same IP addresses. You should a configure your origin to ensure that traffic has originated from your Front Door profile.

Azure generates a unique identifier for each Front Door profile. You can find the identifier in the Azure portal, by looking for the Front Door ID value in the Overview page of your profile.

When Front Door makes a request to your origin, it adds the X-Azure-FDID request header. Your origin should inspect the header on incoming requests, and reject requests where the value doesn't match your Front Door profile's identifier."

https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?pivots=front-door-standard-premium&tabs=app-service-functions#front-do identifier
upvoted 2 times

**Ajdlfasudfo0** 10 months, 3 weeks ago
Selected Answer: A
You have to restrict traffic to front door backend pool only. This can be done via IP Range, HTTP Header or service tag. So I would go with A.
upvoted 4 times

**JCkD4Ni3L** 1 year, 3 months ago
Selected Answer: B
Service Tag is the correct answer, thus NO (B).
upvoted 3 times

**zts** 1 year, 4 months ago
Selected Answer: B

Service Tag

upvoted 4 times

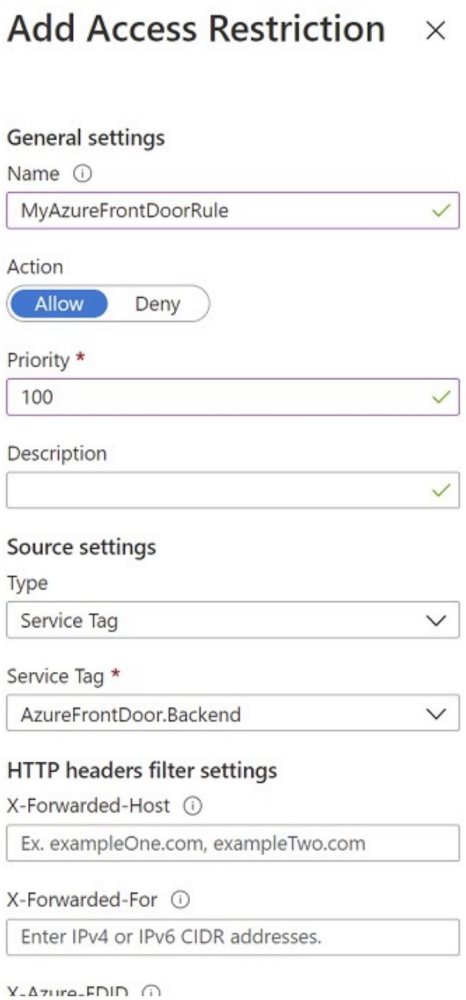
Question #13 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions that allow traffic from the Front Door service tags.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.




Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

*Community vote distribution*
B (53%) A (47%)

**mikenyga** Highly Voted 1 year, 4 months ago
Answer correct.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door (INSTANCE) this is important!

Restrict access to a specific Azure Front Door instance with X-Azure-FDID header restriction
upvoted 25 times

**TP447** 1 year, 1 month ago
Agree. Service Tag would allow for multiple instances so need the specific headers of the Front Door instance to comply with this requiremer
upvoted 4 times

**Jt909** 1 year ago
Exactly. Docs info are here https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli#restrict-access-a-specific-azure-front-door-instance
upvoted 4 times

**BillyB2022** Highly Voted 1 year, 4 months ago
Selected Answer: A
Service Tags
upvoted 9 times

**Murtuza** Most Recent 1 week, 1 day ago
Selected Answer: B
B is the correct choice
upvoted 1 times

**Arockia** 1 week, 1 day ago
To securely restrict access to Azure App Service web apps through Azure Front Door, a more robust approach is required:

1. Service Tag-Based Access Restrictions
2. Custom Headers
upvoted 1 times

**Ario** 6 months, 2 weeks ago
Selected Answer: A
By configuring access restrictions to allow traffic from the Front Door service tags, you can effectively restrict access to the web apps only from t Front Door instance. This approach provides a reliable and scalable solution since the Front Door service tags automatically adapt to any change in IP ranges associated with the Front Door service.
upvoted 1 times

**imsidrai** 6 months, 3 weeks ago
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal
upvoted 1 times

**PrettyFlyWifi** 7 months, 3 weeks ago
Selected Answer: A
https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?pivots=front-door-standard-premium&tabs=app-service-functions#public-ip-address-based-origins
upvoted 1 times

**zellck** 8 months ago
Same as Question 14.
https://www.examtopics.com/discussions/microsoft/view/79383-exam-sc-100-topic-4-question-14-discussion
upvoted 1 times

**zellck** 8 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.
upvoted 1 times

**uffman** 8 months, 3 weeks ago
Selected Answer: B
I would select B, since it states allow connection from the Front Door instance (specific?).
upvoted 2 times

**Fal991l** 10 months, 1 week ago

Selected Answer: A

ChatGTP:
A. Yes

Restricting access to Azure App Service web apps to only allow traffic from the Front Door instance is a good security practice to ensure that the web apps are only accessible through the Front Door instance. One way to achieve this is by using access restrictions that allow traffic from the Front Door service tags.

Azure Front Door service tags represent the IP addresses of the Front Door edge nodes, which can be used to restrict access to the web apps. By configuring access restrictions that only allow traffic from the Front Door service tags, you can ensure that the web apps are only accessible through the Front Door instance.

Therefore, the recommended solution to ensure that the web apps only allow access through the Front Door instance by using access restrictior that allow traffic from the Front Door service tags meets the goal.

upvoted 1 times

**imsidrai** 6 months, 3 weeks ago

GPT is BS in such scenarios

upvoted 3 times

**Bouncy** 10 months, 2 weeks ago

Selected Answer: B

Following the arguments that point out that the question is about a specific instance, not the service itself. Hence B

upvoted 3 times

**AzureJobsTillRetire** 10 months, 4 weeks ago

Selected Answer: B

The given answer is correct.

A service tag represents a group of IP address prefixes from a given Azure service. To say that service tag is used to access the front door does n state clearly which IP addresses are used/allowed, and it does not restrict anything.
https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview

upvoted 2 times

**AzureJobsTillRetire** 10 months, 4 weeks ago

At least it should state that the backend service tag is to be used

upvoted 1 times

**SofiaLorean** 11 months ago

Selected Answer: B

FDID
Correct - B

upvoted 3 times

**Aunehwet79** 11 months, 1 week ago

After researching the different discussions here I am going with B

upvoted 2 times

**Az4U** 11 months, 1 week ago

Selected Answer: B

Given answer is correct.
The question asks to restrict to a specific instance of Front Door, and that's the key.
Service Tag is only part of the solution, we also need to use the HTTP header of the Front Door instance to restrict it to a specific instance only.
Using just Service Tags will allow access from any Front Door instance whether it's hosted by you or not.
The option of HTTP header also appears in the same question series which is the correct choice for what's being asked.

upvoted 6 times

**nieprotetkniteeetr** 12 months ago

Correct is A. https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli

upvoted 1 times

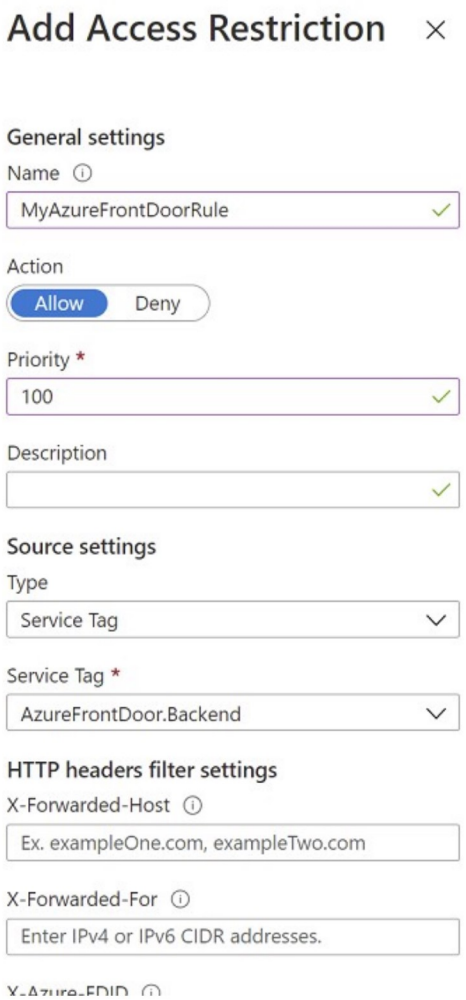
Question #14 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
Restrict access to a specific Azure Front Door instance.
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.




Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

*Community vote distribution*
A (70%) B (30%)

**Petza** Highly Voted 1 year, 4 months ago
The answer seems to be correct.
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-front-door-
upvoted 19 times

**Granwizzard** Highly Voted 1 year, 4 months ago

Selected Answer: A

The answer is correct you can also use FDID on the headers.

upvoted 10 times

**Ario** Most Recent 6 months, 2 weeks ago

Selected Answer: B

While it is possible to configure access restrictions based on custom HTTP headers, relying solely on the Front Door ID header is not a comprehensive solution.

upvoted 2 times

**PrettyFlyWifi** 7 months, 3 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?pivots=front-door-standard-premium&tabs=app-service-functions#public-ip address-based-origins

upvoted 1 times

**zellck** 8 months ago

Same as Question 15.
https://www.examtopics.com/discussions/microsoft/view/79537-exam-sc-100-topic-4-question-15-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t
Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.

upvoted 1 times

**EM1234** 8 months, 1 week ago

Selected Answer: A

When you read the doc you will see that the header filter is critical:

"IP address filtering alone isn't sufficient to secure traffic to your origin, because other Azure customers use the same IP addresses. You should a configure your origin to ensure that traffic has originated from your Front Door profile.

Azure generates a unique identifier for each Front Door profile. You can find the identifier in the Azure portal, by looking for the Front Door ID value in the Overview page of your profile.

When Front Door makes a request to your origin, it adds the X-Azure-FDID request header. Your origin should inspect the header on incoming requests, and reject requests where the value doesn't match your Front Door profile's identifier."

https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?pivots=front-door-standard-premium&tabs=app-service-functions#front-do identifier

upvoted 2 times

**Bouncy** 10 months, 2 weeks ago

Selected Answer: A

Clearly Yes, see comments for previous question variants

upvoted 2 times

**AzureJobsTillRetire** 10 months, 4 weeks ago

Selected Answer: A

The AzureFrontDoor.Backend service tag may contain Backend IP addresses from a few a list Azure Front Doors, eg. Front Door1, Front Door 2, . you want to restrict access to a specific Azure Front Door instance, for example Front Door1, you will have to also access restrictions based on H headers that have the Front Door ID.

upvoted 2 times

**Ssasid** 11 months ago

Yes the answer is correct , its specifially calls out " instance" and to match the defintion given in by MS it should be FD ID not service tag . "Using service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you'll need to further filter the incoming requests based on the unique http header that Azure Front Door sends."

upvoted 1 times

**Aunehwet79** 11 months, 1 week ago

I believe given answer is correct

upvoted 1 times

**nieprotetkniteeetr** 12 months ago

Correct is A. https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli

upvoted 1 times

**Jt909** 1 year ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli#restrict-access-to-a-specific-azure-front-door-instance

upvoted 3 times

**JohnCH** 1 year, 2 months ago

Selected Answer: A

The ans is correct.

upvoted 3 times

**JakeCallham** 1 year, 2 months ago

Selected Answer: A

The url Petza provides states you can use two ways."To lock down your application to accept traffic only from your specific Front Door, you can s up IP ACLs for your backend or restrict the traffic on your backend to the specific value of the header 'X-Azure-FDID' sent by Front Door."

upvoted 3 times

**emiliocb4** 1 year, 3 months ago

Selected Answer: A

the anserver correct is YES and can be used also the service tags

upvoted 4 times

**zts** 1 year, 4 months ago

Selected Answer: B

I would go for B. You need a service tag rule before you can configure http header filtering ---- https://docs.microsoft.com/en-us/azure/app-ser /app-service-ip-restrictions#restrict-access-to-a-specific-azure-front-door-instance

upvoted 6 times

**JakeCallham** 1 year, 2 months ago

wrong! should be yes, see url provided by Petza

upvoted 1 times

**mikenyga** 1 year, 4 months ago

This is true. But question about Azure Front Door (instance), how you can specify instanse with Service Tag?

You need to recommend a solution to ensure that the web apps only allow access through the Front Door (INSTANCE) this is important!

Restrict access to a specific Azure Front Door instance with X-Azure-FDID header restriction

upvoted 3 times

**Nickname01** 1 year, 1 month ago

Answer indeed A
https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?tabs=app-service-functions&pivots=front-door-standard-premium#front-door-identifier
Front Door identifier

IP address filtering alone isn't sufficient to secure traffic to your origin, because other Azure customers use the same IP addresses. You should also configure your origin to ensure that traffic has originated from your Front Door profile.

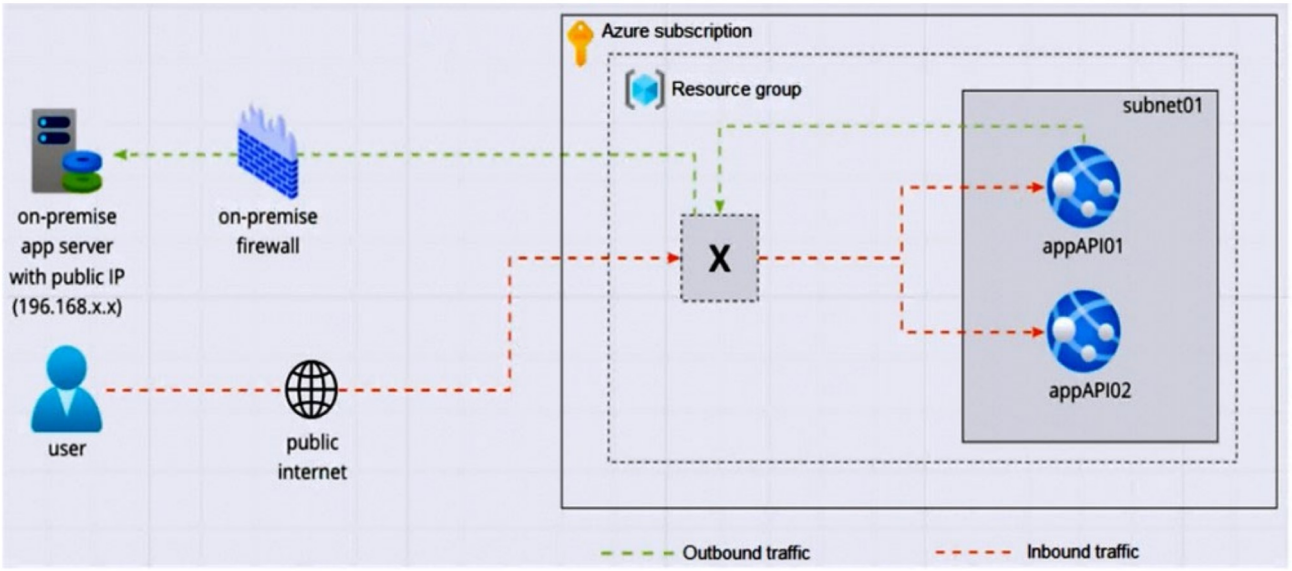
Azure generates a unique identifier for each Front Door profile. You can find the identifier in the Azure portal, by looking for the Front Do ID value in the Overview page of your profile.

When Front Door makes a request to your origin, it adds the X-Azure-FDID request header. Your origin should inspect the header on incoming requests, and reject requests where the value doesn't match your Front Door profile's identifier.

upvoted 1 times

Question #15 *Topic 3*

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)




Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods

B. Azure Firewall with policy rule sets

C. Azure Front Door with Azure Web Application Firewall (WAF)

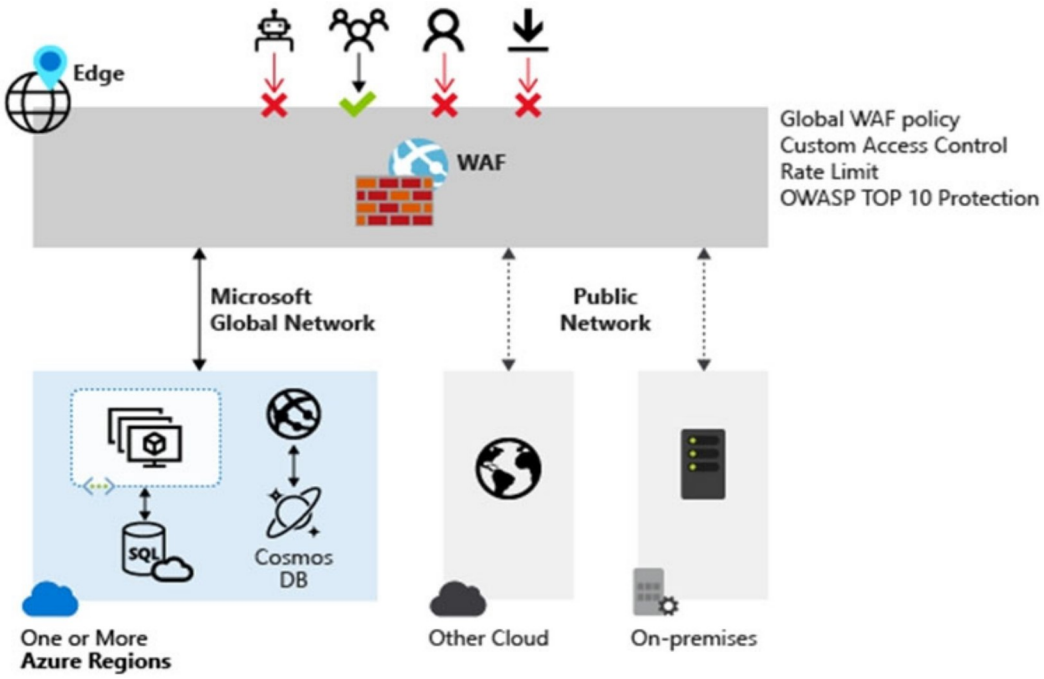
D. Azure Application Gateway v2 with user-defined routes (UDRs)

**Correct Answer:** *C*

Azure Web Application Firewall (WAF) on Azure Front Door provides centralized protection for your web applications. WAF defends your web services against common exploits and vulnerabilities. It keeps your service highly available for your users and helps you meet compliance requirements.

WAF on Front Door is a global and centralized solution. It's deployed on Azure network edge locations around the globe. WAF enabled web applications inspect every incoming request delivered by Front Door at the network edge.

WAF prevents malicious attacks close to the attack sources, before they enter your virtual network.




Incorrect:

Not D: Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

You could use Azure Application Gateway with the Azure Web Application Firewall (WAF).

Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

*Community vote distribution*

B (84%) Other

**Jasper666** Highly Voted 1 year, 4 months ago

I would go for B because there is an expressroute, so part of the trafic is going internally. For accepting internet traffic to the api's I'd go for firev as well. It can work with only one public ip.

upvoted 13 times

**JaySapkota** Highly Voted 1 year, 4 months ago

Why Not D. UDR
User Defined Routes (UDR). Route tables can contain UDRs used by Azure networking to control the flow of packets within a VNet. These route tables can be applied to subnets. One of the newest features in Azure is the ability to apply a route table to the GatewaySubnet, providing the ability to forward all traffic coming into the Azure VNet from a hybrid connection to a virtual appliance.

upvoted 10 times

**TJ001** 1 year ago

There is no compelling case to use App GW in this case . If it was App GW V2 with WAF option then it would have made sense. without WAF Azure FW with routing capability gives better options

upvoted 2 times

**calotta1** Most Recent 4 months, 3 weeks ago

The only answer that makes sense here is AZ-FW because we are talking about traffic between applications residing in Azure and that on-premi not users from the internet.

upvoted 2 times

**Ario** 6 months, 2 weeks ago

Selected Answer: D

Azure Application Gateway acts as a reverse proxy and load balancer, allowing traffic to be routed between the web apps and the on-premises application server. User-defined routes (UDRs) enable you to define custom routing tables for the Azure virtual network

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/environment/firewall-integration#configuring-azure-firewall-with-your-ase

upvoted 1 times

**Gurulee** 10 months, 3 weeks ago

Selected Answer: B

Azure firewall for routing and egress reasons

upvoted 3 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: B

if you also have outgoing traffic that going via the "X" only a firewall makes sense

upvoted 3 times

**buguinha** 11 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/app-service/environment/firewall-integration

upvoted 2 times

**examdog** 11 months, 2 weeks ago

Selected Answer: B

I voted for B. The on-premise firewall does not work for ExpressRoute connection. The on-prem app server is open to the public internet throug the Azure network. To protect the app server, Azure Firewall with policy rule sets is needed to filter all types of traffic, while WAF works only for v requests. In short, the Azure network needs a firewall.

upvoted 4 times

**Hullstar** 12 months ago

Selected Answer: C

I voted for C because we are handling HTTP/s traffic : https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

upvoted 2 times

**Hullstar** 12 months ago

I meant D Application Gateway

upvoted 2 times

**purek77** 12 months ago

Selected Answer: B

For me correct answer is B:

For inbound non-HTTP(S) connections, traffic should be targeting the public IP address of the Azure Firewall (if coming from the public Internet) it will be sent through the Azure Firewall by UDRs (if coming from other Azure VNets or on-premises networks). All outbound flows from Azure VMs will be forwarded to the Azure Firewall by UDRs.

Ref: https://learn.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway#firewall-and-application-gateway-in-parallel

upvoted 4 times

**TJ001** 1 year ago

If FW is used how will you loadbalance between backend webapps?

upvoted 1 times

**TJ001** 1 year ago

my bad that is not how app service works and it manages the load balancing internally . I would go with Azure FW in which case the inbounc addressed via DNAT rules. For outbound to on-premise can route through the Azure FW with force tunnelling implemented or even skip the and use BGP route propagation to route over EXPRESSROUTE . The only issue I have with App GW is we need to cater to inbound and outbo flow and App GW at layer7 needs to have the endpoints configured for both these 1. the inbound to App Services 2. the inbound to on-premises (which is outbound from App service).. UDR is helpful but then there should have clarity in the wordings

upvoted 1 times

**CertShooter** 1 year ago

A possible solution to ensure that the web apps can communicate with the on-premises application server while minimizing the number of publ IP addresses that are allowed to access the on-premises network is to use Azure Firewall with policy rule sets.

Azure Firewall is a cloud-based network security service that protects your Azure virtual network resources. You can use Azure Firewall to filter traffic to and from the on-premises network and the web apps in Azure. By using policy rule sets, you can define rules that specify which public addresses are allowed to access the on-premises network. This will help minimize the number of public IP addresses that are allowed to access t on-premises network.

Other options, such as Azure Traffic Manager with priority traffic-routing methods, Azure Front Door with Azure Web Application Firewall (WAF), and Azure Application Gateway v2 with user-defined routes (UDRs), may not be as suitable for this scenario because they do not provide the sar level of control over access to the on-premises network.

I go for answer B.

upvoted 3 times

**panoz** 1 year, 1 month ago

Selected Answer: B

There is no need for traffic to go over the public internet.

upvoted 2 times

**Ahmed911** 1 year, 1 month ago

**Selected Answer: B**

I believe the answer B

upvoted 2 times

**John0153** 1 year, 1 month ago

**Selected Answer: B**

A very tricky situation
You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. (Azure Firewall with policy rule sets)

The solution must minimize the number of public IP addresses that are allowed to access the on-premises network (public IP's shouldn't be able access the on prem network unless allowed and this questions is directed at on prem network not the Apps, with this in mind the answer is lean towards Azure firewall.)

upvoted 4 times

**cychoia** 1 year, 2 months ago

**Selected Answer: B**

ASE with firewall integration --> https://learn.microsoft.com/en-us/azure/app-service/environment/firewall-integration

upvoted 2 times

Question #16 *Topic 3*

You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts.
You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts.
Which two configurations should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.

B. Enable Microsoft Defender for Identity.

C. Send the Azure Cosmos DB logs to a Log Analytics workspace.

D. Disable local authentication for Azure Cosmos DB.

E. Enable Microsoft Defender for Cosmos DB.

**Correct Answer:** *AD*
A: LT-2: Enable threat detection for Azure identity and access management
Guidance: Azure Active Directory (Azure AD) provides the following user logs, which can be viewed in Azure AD reporting or integrated with Azure Monitor,
Microsoft Sentinel, or other SIEM/monitoring tools for more sophisticated monitoring and analytics use cases:
Sign-ins - The sign-ins report provides information about the usage of managed applications and user sign-in activities.
Audit logs - Provides traceability through logs for all changes done by various features within Azure AD. Examples of audit logs include changes made to any resources within Azure AD, like adding or removing users, apps, groups, roles, and policies.
D: Disable local authentication methods so that your Cosmos DB database accounts exclusively require Azure Active Directory identities for authentication.
Enforcing RBAC as the only authentication method
In situations where you want to force clients to connect to Azure Cosmos DB through RBAC exclusively, you have the option to disable the account's primary/ secondary keys. When doing so, any incoming request using either a primary/secondary key or a resource token will be actively rejected.
Incorrect:
Not C: We use the Azure Active Directory (Azure AD) sign-in logs, not the Azure Cosmos db logs.
Not E: Microsoft Defender for Cosmos DB, though useful from a security perspective, does not help with auditing the users.
Note: Logging and Threat Detection, LT-1: Enable threat detection for Azure resources
Guidance: Use the Microsoft Defender for Cloud built-in threat detection capability and enable Microsoft Defender for your Cosmos DB resources. Microsoft
Defender for Cosmos DB provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your
Cosmos DB resources.
Reference:
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline https://docs.microsoft.com/en-us/azure/cosmos-db/policy-reference https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac#disable-local-auth

*Community vote distribution*
AD (47%) AC (43%) 8%

**BillyB2022** Highly Voted 1 year, 4 months ago
Selected Answer: AC
https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs
upvoted 18 times

**zts** Highly Voted 1 year, 4 months ago
Selected Answer: AD
Enforcing all authentication thru AAD and using RBAC will make auditing more simpler and secure rather than having two sources of authentica the database. So I would go for a and D.
upvoted 17 times

**ca777** 5 months, 1 week ago
It's wrong. To audit all users that access the data in Azure Cosmos DB Core (SQL) API accounts, you should include the following two

configurations :

1. Enable Azure Monitor Logs for Cosmos DB: allows you to collect and analyze data generated by Azure resources, including Azure Cosmos
By enabling Azure Monitor Logs for your Cosmos DB account, you can capture detailed logs related to user access and operations performec
on the data.
2. Enable Audit Logs for Cosmos DB: Cosmos DB provides built-in auditing functionality that allows you to record events related to the datab
account. Enabling the Cosmos DB audit logs will capture events such as login attempts, database CRUD operations, and any changes made t
the configuration of the database account.

So the answer is : AC

upvoted 1 times

**mikenyga** 1 year, 4 months ago

You need to recommend a solution to audit all users that (ACCESS THE DATA) in the Azure Cosmos DB accounts.
How you can audit access the data with sign in log???

upvoted 3 times

**zts** 1 year, 3 months ago

Apologies for the word, but you might want to consider a career out of cybersecurity. You can never access a data unless you are authenticated.
This is the answer to your question. --
When using the Azure Cosmos DB RBAC, diagnostic logs get augmented with identity and authorization information for each data operat
This lets you perform detailed auditing and retrieve the Azure AD identity used for every data request sent to your Azure Cosmos DB account.

This additional information flows in the DataPlaneRequests log category and consists of two extra columns:

aadPrincipalId_g shows the principal ID of the Azure AD identity that was used to authenticate the request.
aadAppliedRoleAssignmentId_g shows the role assignment that was honored when authorizing the request.
Reference link: --> https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac#disable-local-auth

upvoted 9 times

**[Removed]** 1 year ago

This is a ridiculous thing to say: "Apologies for the word, but you might want to consider a career out of cybersecurity." This is a trainin
website where people come to learn. You should absolutely dismount your high horse.

upvoted 54 times

**Murtuza** Most Recent 1 week, 1 day ago

Selected Answer: AD

A, D is correct

upvoted 1 times

**juanpe147** 1 month ago

i go with A&D

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: AD

got this in exam 6oct23. passed with 896 marks. I answered AD

upvoted 1 times

**sbnpj** 5 months ago

Selected Answer: AD

A&D for sure.

upvoted 1 times

**Ario** 6 months, 2 weeks ago

Selected Answer: AC

Definitely AC

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Selected Answer: AC

AC is the answer.

https://learn.microsoft.com/en-us/azure/cosmos-db/monitor-resource-logs?tabs=azure-portal
Diagnostic settings in Azure are used to collect resource logs. Resources emit Azure resource Logs and provide rich, frequent data about the operation of that resource. These logs are captured per request and they're also referred to as "data plane logs". Some examples of the data pla
operations include delete, insert, and readFeed. The content of these logs varies by resource type.

upvoted 1 times

**zellck** 7 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac#audit-data-requests
Diagnostic logs get augmented with identity and authorization information for each data operation when using Azure Cosmos DB role-basec

access control. This augmentation lets you perform detailed auditing and retrieve the Azure AD identity used for every data request sent to y Azure Cosmos DB account.

upvoted 1 times

**Cock** 7 months, 3 weeks ago

Selected Answer: AC

People with AD overthink

upvoted 3 times

**KallMeDan** 8 months, 2 weeks ago

From what I can research on, as long as I have implemented the option A, I do not need to disable the local authentication on cosmos DB. The l authentication logins are also being forwarded to the log analytic workspace. if the local authentication credentials were shared, then that seem create another issue, but that is not stated here to be the case. So option D seems unnecessary as the requirement is not to force Azure AD authentication either. Option C can be a more suitable answer here.

upvoted 3 times

**smudo1965** 9 months, 3 weeks ago

Selected Answer: AC

https://learn.microsoft.com/en-us/azure/cosmos-db/monitor-resource-logs?tabs=azure-portal - Question is about aditing

upvoted 2 times

**Fal991l** 10 months, 1 week ago

Selected Answer: AC

ChatGTP: To audit all users accessing data in Azure Cosmos DB Core (SQL) API accounts, the following two configurations should be included in recommendation:

A. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace: This will enable logging of all sign-in activities, includin successful and failed attempts, by all users accessing the Cosmos DB account. This will provide insight into who is accessing the data and when.

C. Send the Azure Cosmos DB logs to a Log Analytics workspace: This will enable logging of all activities within the Cosmos DB account, includir queries, modifications, and deletions. This will provide insight into what data is being accessed and how it is being used.

upvoted 4 times

**Fal991l** 10 months, 1 week ago

Options B, D, and E are not relevant to auditing user access to Cosmos DB data.

Option B refers to Microsoft Defender for Identity, which is a security solution for on-premises Active Directory environments.

Option D refers to disabling local authentication, which is not a necessary step for auditing user access.

Option E refers to Microsoft Defender for Cosmos DB, which is a security solution for protecting Cosmos DB from cyber-attacks and data breaches but does not provide auditing functionality.

upvoted 2 times

**God2029** 10 months, 3 weeks ago

Purpose is Audit - So sending logs to Log analytics is the action. Question does not say to restrict access to only AD users, it just say audit. So w do you need to disable to local authentication? you just need the logs to see who accessed and what acctions perfomed in the DB, So I would choose A and C

upvoted 1 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

Selected Answer: AD

The given answers are correct.
A is a no-brainer.
I would also choose C if D does not exist as an option. C can be used to audit how users access the data, but without D, C does not work. This is because we would not know how users access the data in the database if DB users are not linked to AD users. For example, if all AD users use or database user to connect to the database, how can you tell from the DB logs which AD user does what?

upvoted 4 times

**awssecuritynewbie** 11 months ago

Selected Answer: AC

I would say A and C because you need to audit the ADD loggings and also the logs of the Cosmos DB to log analytics that can be then sent to sentinel

upvoted 2 times

**examdog** 11 months, 2 weeks ago

Selected Answer: AC

I chose A and C. The request is to audit all user data access, not to limit user access so the audit will be easier.

upvoted 3 times

**JohnBentass** 11 months, 4 weeks ago

AC for me

upvoted 1 times

Question #17 *Topic 3*

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.
You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.
What should you include in the recommendation?

A. Set the AllowSharedKeyAccess property to false.

B. Apply read-only locks on the storage accounts.

C. Set the AllowBlobPublicAccess property to false.

D. Configure automated key rotation.

**Correct Answer:** *B*
A read-only lock on a storage account prevents users from listing the account keys. A POST request handles the Azure Storage List Keys operation to protect access to the account keys. The account keys provide complete access to data in the storage account.
Incorrect:
Not A:
If any clients are currently accessing data in your storage account with Shared Key, then Microsoft recommends that you migrate those clients to Azure AD before disallowing Shared Key access to the storage account.
However, in this scenario we cannot migrate to Azure AD due to the legacy applications.

Note: Shared Key -
A shared key is a very long string. You can simply access Azure storage by using this long string. It's almost like a password. Actually, it's worse: this is a master password. It gives you all sorts of rights on the Azure storage account. You can imagine why this isn't my favorite mechanism of accessing Azure storage. What happens when this key is compromised? You don't get an alert. Perhaps you can set up monitoring to see misuse of your Azure storage account. But it's still less than an ideal situation. Alerts will tell you of damage after it has already occurred.
Not C: Data breaches caused by cloud misconfiguration have been seen for the past few years. One of the most common misconfigurations is granting public access to cloud storage service. Such a data is often unprotected, making them to be accessed without any authentication method. Microsoft recently introduced a new protection feature to help avoid public access on storage account. The feature introduces a new property named allowBlobPublicAccess.
Not D: Key rotation would improve security.
Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources https://docs.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

*Community vote distribution*
B (77%) A (19%) 4%

**zts** Highly Voted 1 year, 4 months ago

Selected Answer: B
A read-only lock on a storage account prevents users from listing the account keys ----> https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json
upvoted 8 times

**Mblott77** Most Recent 5 months, 4 weeks ago

Selected Answer: A
```
Set-AzStorageAccount -ResourceGroupName <resource-group> `
-AccountName <storage-account> `
-AllowSharedKeyAccess $false
```

upvoted 2 times

**Mblott77** 5 months, 4 weeks ago

Set-AzStorageAccount -ResourceGroupName <resource-group> `
-AccountName <storage-account> `
-AllowSharedKeyAccess $false

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#considerations-before-applying-you
locks
A read-only lock on a storage account prevents users from listing the account keys. A POST request handles the Azure Storage List Keys operati
to protect access to the account keys. The account keys provide complete access to data in the storage account. When a read-only lock is configured for a storage account, users who don't have the account keys need to use Azure AD credentials to access blob or queue data. A read only lock also prevents the assignment of Azure RBAC roles that are scoped to the storage account or to a data container (blob container or queue).

upvoted 1 times

**smudo1965** 10 months ago

Selected Answer: B

When a read-only lock is configured for a storage account, users who don't have the account keys need to use Azure AD credentials to access b or queue data. A read-only lock also prevents the assignment of Azure RBAC roles that are scoped to the storage account or to a data container (blob container or queue).

upvoted 3 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: B

reading keys is actually a POST request, therefor a read only lock would work. (the data is NOT readonly, only the control plane)

upvoted 2 times

**awssecuritynewbie** 10 months, 3 weeks ago

Selected Answer: B

a read-only lock

upvoted 2 times

**Mo22** 11 months, 1 week ago

Selected Answer: D

In order to prevent new applications from obtaining the access keys, while minimizing the impact on the legacy applications, it is recommended use a solution that allows you to regularly rotate the access keys, such as automated key rotation (Option D).

upvoted 1 times

**Fal991l** 10 months, 1 week ago

ChatGTP agreed with you.
The best solution to prevent new applications from obtaining the access keys of the storage accounts while minimizing the impact on the leg applications is to configure automated key rotation. This solution will rotate the access keys on a regular basis, making it more difficult for unauthorized applications to gain access to the storage accounts. The legacy applications can continue to use the access keys without interruption, as long as they are updated with the new keys after each rotation.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

Option A (Set the AllowSharedKeyAccess property to false) is not a valid solution because this property is used to enable or disable share key authentication for a storage account. Disabling shared key authentication would impact the legacy applications that are currently usin the access keys for authentication.

Option B (Apply read-only locks on the storage accounts) is not a valid solution because it would prevent any application from modifying storage accounts, including the legacy applications that require write access.

Option C (Set the AllowBlobPublicAccess property to false) is not a valid solution because this property is used to enable or disable public access to blobs in a storage account. Disabling public access would not prevent new applications from obtaining the access keys.

Therefore, the correct answer is D (Configure automated key rotation).

upvoted 1 times

**Funkydave** 6 months ago

don't rely on chatgpt ask it the same question or reply with "why" and it will almost certainly reply apologising for getting the answer wrong.

upvoted 2 times

**TJ001** 1 year ago

legacy application still need to work, then Ready Only Lock (assume only on the management plane) is an option

upvoted 2 times

**CertShooter** 1 year ago

Selected Answer: A

The AllowSharedKeyAccess property is a feature of Azure Storage that controls whether the shared key (also known as the access key) of a stora account can be accessed. When this property is set to false, only the storage account owner can access the shared key. This can help prevent unauthorized access to the storage account by new applications, while still allowing the legacy applications to continue using the shared key for authentication.

Other options, such as applying read-only locks on the storage accounts, setting the AllowBlobPublicAccess property to false, or configuring automated key rotation, may not be as effective at preventing new applications from obtaining the access keys of the storage accounts, or may have a greater impact on the legacy applications.

upvoted 3 times

**KrisDeb** 11 months, 1 week ago

Any source? Because according to this below, apps will stop working correctly after setting this property to false.
https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent?tabs=portal#disable-shared-key-authorization

upvoted 2 times

**panoz** 1 year, 1 month ago

To avoid confusion we should mention that a read only lock applies to the management plane and not the data plane so this lock doesn't affect data access and has no impact to the legacy applications.

upvoted 3 times

**emiliocb4** 1 year, 3 months ago

Selected Answer: B

B is the correct one... preventing the user list the keys

upvoted 4 times

**rdy4u** 1 year, 3 months ago

A read-only lock on a storage account prevents users from listing the account keys.

upvoted 2 times

**K1SMM** 1 year, 4 months ago

Correct B - Lock restrict access keys view
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

upvoted 4 times

Question #18 *Topic 3*

You are designing the security standards for containerized applications onboarded to Azure.
You are evaluating the use of Microsoft Defender for Containers.
In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Instances

B. Windows containers deployed to Azure Kubernetes Service (AKS)

C. Windows containers deployed to Azure Container Registry

D. Linux containers deployed to Azure Container Registry

E. Linux containers deployed to Azure Kubernetes Service (AKS)

**Correct Answer:** *CD*
The new plan merges the capabilities of the two existing Microsoft Defender for Cloud plans, Microsoft Defender for Kubernetes and Microsoft Defender for container registries.
Azure container registries can include both Windows and Linux images.
You can use Defender for Containers to scan the container images stored in your Azure Resource Manager-based Azure Container Registry, as part of the protections provided within Microsoft Defender for Cloud.
To enable scanning of vulnerabilities in containers, you have to enable Defender for Containers. When the scanner, powered by Qualys, reports vulnerabilities,
Defender for Cloud presents the findings and related information as recommendations. In addition, the findings include related information such as remediation steps, relevant CVEs, CVSS scores, and more. You can view the identified vulnerabilities for one or more subscriptions, or for a specific registry.
Note: Defender for Containers includes an integrated vulnerability scanner for scanning images in Azure Container Registry registries. The vulnerability scanner runs on an image:
When you push the image to your registry
Weekly on any image that was pulled within the last 30
When you import the image to your Azure Container Registry
Continuously in specific situations
View vulnerabilities for running images
The recommendation Running container images should have vulnerability findings resolved shows vulnerabilities for running images by using the scan results from ACR registries and information on running images from the Defender security profile/extension.
Incorrect:
Not A: The new plan merges the capabilities of the two existing Microsoft Defender for Cloud plans, Microsoft Defender for Kubernetes and Microsoft Defender for container registries
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-usage https://techcommunity.microsoft.com /t5/microsoft-defender-for-cloud/introducing-microsoft-defender-for-containers/ba-p/2952317 https://docs.microsoft.com/en-us/azure /defender-for-cloud/defender-for-containers-introduction

*Community vote distribution*
DE (73%) 13% 10%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: DE
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-security-requirements-for-containers

https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabilities-for-running-images
upvoted 17 times

**Granwizzard** Highly Voted 1 year, 4 months ago
Selected Answer: DE
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=azure-

aks#registries-and-images
Windows is on preview.

OS Packages Supported
• Alpine Linux 3.12-3.15
• Red Hat Enterprise Linux 6, 7, 8
• CentOS 6, 7
• Oracle Linux 6,6,7,8
• Amazon Linux 1,2
• openSUSE Leap 42, 15
• SUSE Enterprise Linux 11,12, 15
• Debian GNU/Linux wheezy, jessie, stretch, buster, bullseye
• Ubuntu 10.10-22.04
• FreeBSD 11.1-13.1
• Fedora 32, 33, 34, 35

upvoted 8 times

**tocane** Most Recent 6 days, 15 hours ago

Selected Answer: AB

The correct environments where you can use Defender for Containers to scan for known vulnerabilities are:
A. Linux containers deployed to Azure Container Instances
B. Windows containers deployed to Azure Kubernetes Service (AKS)
So, the correct selections would be A and B.

upvoted 1 times

**juanpe147** 1 month ago

D and E are the correct annswers

upvoted 1 times

**slobav** 3 months, 3 weeks ago

C. Windows containers deployed to Azure Container Registry
D. Linux containers deployed to Azure Container Registry

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction
"Vulnerability assessment - Vulnerability assessment and management tools for images stored in Azure Container Registry and Elastic Container Registry"

upvoted 2 times

**sbnpj** 5 months, 1 week ago

Selected Answer: DE

https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-containers#registries-and-images-support-for-aks---powered-by-qualys

upvoted 1 times

**zellck** 8 months ago

Selected Answer: DE

DE is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-containers?tabs=azure-aks#azure-aks

https://learn.microsoft.com/en-us/azure/defender-for-cloud/support-matrix-defender-for-containers?tabs=azure-aks#registries-and-images-support-aks

upvoted 2 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 3 times

**GeVanDerBe** 8 months, 3 weeks ago

C-D, why, see article https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-vulnerability-assessment-azure#faq
"Currently, Defender for Containers can scan images in Azure Container Registry (ACR) and AWS Elastic Container Registry (ECR) only. Docker Registry, Microsoft Artifact Registry/Microsoft Container Registry, and Microsoft Azure Red Hat OpenShift (ARO) built-in container image registr are not supported. Images should first be imported to ACR."

upvoted 5 times

**vitodobra** 9 months, 3 weeks ago

Selected Answer: AD

The two correct options for using Microsoft Defender for Containers to scan for known vulnerabilities are:

A. Linux containers deployed to Azure Container Instances
D. Linux containers deployed to Azure Container Registry

Microsoft Defender for Containers is compatible with Docker containers running on Linux operating systems, so it can scan for known vulnerabilities in Linux containers deployed to Azure Container Instances and Azure Container Registry.

However, it cannot scan for known vulnerabilities in Windows containers deployed to Azure Kubernetes Service or Azure Container Registry, as Microsoft Defender for Containers currently only supports Linux operating systems.

upvoted 1 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: BD

Now that Defender for Containers also supports Windows containers running in AKS, BDE should be the answer.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

ChatGTP:
Microsoft Defender for Containers can be used to scan for known vulnerabilities in the following environments:

A. Linux containers deployed to Azure Container Instances
B. Windows containers deployed to Azure Kubernetes Service (AKS)
C. Windows containers deployed to Azure Container Registry
D. Linux containers deployed to Azure Container Registry
E. Linux containers deployed to Azure Kubernetes Service (AKS)

Therefore, options A, B, C, D, and E are all correct.

upvoted 1 times

**Fal991l** 10 months ago

Correction:
If you choose any of the other options, it would not be the best answer as they are not correct.

Option A: This is correct as Microsoft Defender for Containers can scan Linux containers deployed to Azure Container Instances.

Option B: This is not correct as Microsoft Defender for Containers can only scan Windows containers if they are deployed to a Windows Server 2019 node in an AKS cluster.

Option C: This is not correct as Azure Container Registry is a container registry service, and Microsoft Defender for Containers does not sc container registries.

Option D: This is not correct as Microsoft Defender for Containers cannot scan Linux containers deployed to Azure Container Registry.

Option E: This is not correct as Microsoft Defender for Containers can only scan Linux containers deployed to AKS if they are deployed to Linux node pool.

upvoted 1 times

**Ramye** 3 days, 8 hours ago

ChatGPT will confuse you more :-)

upvoted 1 times

**awssecuritynewbie** 10 months, 3 weeks ago

Selected Answer: DE

Vulnerability assessment: Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service. Learn more in Vulnerability assessment.

upvoted 2 times

**OrangeSG** 11 months, 4 weeks ago

Selected Answer: DE

This question outdated. Support for Windows containers added in Aug 2022 release of Defender for Containers.

Reference
What's new in Microsoft Defender for Cloud?
https://learn.microsoft.com/en-us/azure/defender-for-cloud/release-notes
August 2022
Updates in August include:
• Vulnerabilities for running images are now visible with Defender for Containers on your Windows containers
• Azure Monitor Agent integration now in preview
• Deprecated VM alerts regarding suspicious activity related to a Kubernetes cluster
Vulnerabilities for running images are now visible with Defender for Containers on your Windows containers
Defender for Containers now shows vulnerabilities for running Windows containers.
When vulnerabilities are detected, Defender for Cloud generates the following security recommendation listing the detected issues: Running container images should have vulnerability findings resolved

upvoted 6 times

**Hullstar** 12 months ago

I vote for DE as windows container scanning is still not supported:

Unsupported registries and images: Windows images
'Private' registries (unless access is granted to Trusted Services)
Super-minimalist images such as Docker scratch images, or "Distroless" images that only contain an application and its runtime dependencies without a package manager, shell, or OS

Images with Open Container Initiative (OCI) Image Format Specification

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-container-registries-introduction

upvoted 1 times

**Chandanaa** 1 year ago

Selected Answer: CD

CD

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-vulnerability-assessment-azure

upvoted 1 times

**music_man** 1 year ago

Selected Answer: CD

Given answer correct. Defender for Container can scan images in ACR and AWS ECR only. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-vulnerability-assessment-azure#does-defender-for-containers-scan-images-in-microsoft-container-registry

upvoted 5 times

**CertShooter** 1 year ago

Selected Answer: BE

You can use Microsoft Defender for Containers to scan for known vulnerabilities in the following environments:

Linux containers deployed to Azure Kubernetes Service (AKS): Microsoft Defender for Containers is a security solution that provides vulnerability scanning for container images in Azure Kubernetes Service (AKS). It uses the Azure Container Registry Vulnerability Scanning feature to scan container images for known vulnerabilities before they are deployed to AKS. This can help you identify and remediate vulnerabilities in your container images, and improve the security of your containerized applications.

Windows containers deployed to Azure Kubernetes Service (AKS): Similar to Linux containers, Microsoft Defender for Containers can also be use to scan for known vulnerabilities in Windows containers deployed to AKS. By using this solution, you can ensure that your Windows containers a secure and compliant before they are deployed to production.

Other environments, such as Linux or Windows containers deployed to Azure Container Instances or Azure Container Registry, may not be supported by Microsoft Defender for Containers.

upvoted 2 times

**blopfr** 1 year, 2 months ago

Selected Answer: BE

I think this is a moving picture.

AKS container assessment is in preview for both Linux and windows...
https://learn.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=azure-aks#supported-features-by-environment

also wording is bad, can we really deploy a container to ACR ?

upvoted 6 times

**TJ001** 1 year ago

indeed it is evolving.. it looks now both Windows and Linux are supported atleast by Preview

upvoted 1 times

Question #19 *Topic 3*

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft 365 subscription, and an Azure subscription.
The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
☞ Prevent the remote users from accessing any other resources on the network.
☞ Support Azure Active Directory (Azure AD) Conditional Access.
☞ Simplify the end-user experience.
What should you include in the recommendation?

A. Azure AD Application Proxy

B. web content filtering in Microsoft Defender for Endpoint

C. Microsoft Tunnel

D. Azure Virtual WAN

**Correct Answer:** *A*
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal.
Azure AD Application Proxy is:
Secure. On-premises applications can use Azure's authorization controls and security analytics. For example, on-premises applications can use Conditional
Access and two-step verification. Application Proxy doesn't require you to open inbound connections through your firewall.
Simple to use. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don't need to change or update your applications to work with Application Proxy.
Incorrect:

Not D: Azure Virtual WAN -
Azure Virtual WAN is for end users, not for applications.
Note: Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:
Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).
Site-to-site VPN connectivity.
Remote user VPN connectivity (point-to-site).
Private connectivity (ExpressRoute).
Intra-cloud connectivity (transitive connectivity for virtual networks).
VPN ExpressRoute inter-connectivity.
Routing, Azure Firewall, and encryption for private connectivity.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

*Community vote distribution*
A (100%)

**XtraWest** 3 weeks, 4 days ago
**Selected Answer: A**
A. Azure AD Application Proxy as per Chat GPT
upvoted 2 times

**zellck** 8 months ago
**Selected Answer: A**
A is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal. For example, Application Pr can provide remote access and single sign-on to Remote Desktop, SharePoint, Teams, Tableau, Qlik, and line of business (LOB) applications.

upvoted 2 times

**awssecuritynewbie** 10 months, 3 weeks ago

**Selected Answer: A**

The rest of them do not offer simple and also Conditional access because Azure AD is not being utilized.

upvoted 1 times

**TJ001** 1 year ago

A is perfect

upvoted 2 times

**CertShooter** 1 year ago

**Selected Answer: A**

Azure AD Application Proxy is a feature of Azure AD that allows you to publish on-premises web applications securely to the internet. It acts as a reverse proxy, routing the user's request to the internal web app and returning the response back to the user. By using Azure AD Application Pr you can provide the remote users with access to the internal web apps while preventing them from accessing any other resources on the netwo

Azure AD Application Proxy also supports Azure AD Conditional Access, which allows you to set policies that determine when and how users car access your applications. This can help you ensure that only authorized users are able to access the web apps, and that their access is secure. Additionally, Azure AD Application Proxy simplifies the end-user experience by providing a single sign-on (SSO) experience for the users, which reduce the need for them to remember multiple usernames and passwords.

Other options, such as web content filtering in Microsoft Defender for Endpoint, Microsoft Tunnel, or Azure Virtual WAN, may not be as suitable this scenario because they do not provide the same level of control over access to the internal web apps or the same level of simplicity for the e user experience.

upvoted 2 times

**cychoia** 1 year, 2 months ago

**Selected Answer: A**

This question is testing the candidate on the 'Remote access to on-premises applications through Azure AD Application Proxy'

upvoted 2 times

**zts** 1 year, 4 months ago

**Selected Answer: A**

Answer seems correct.

upvoted 2 times

**PlumpyTumbler** 1 year, 4 months ago

**Selected Answer: A**

https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

upvoted 3 times

Question #20 *Topic 3*

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service.
You are migrating the on-premises infrastructure to a cloud-only infrastructure.
You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.
Which identity service should you include in the recommendation?

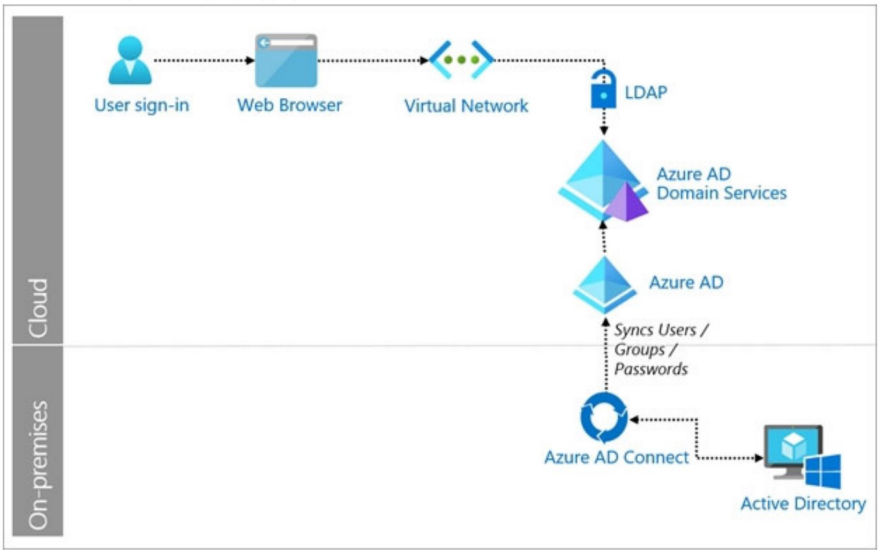
A. Azure Active Directory (Azure AD) B2C

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD)

D. Active Directory Domain Services (AD DS)

**Correct Answer:** *B*
Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services. Directory services, such as Active Directory, store user and account information, and security information like passwords. The service then allows the information to be shared with other devices on the network. Enterprise applications such as email, customer relationship managers (CRMs), and Human Resources (HR) software can use LDAP to authenticate, access, and find information.
Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud-first strategy to modernize their environment by moving off their on-premises LDAP resources to the cloud. The immediate benefits will be:
Integrated with Azure AD. Additions of users and groups, or attribute changes to their objects are automatically synchronized from your Azure AD tenant to AD
DS. Changes to objects in on-premises Active Directory are synchronized to Azure AD, and then to AD DS.
Simplify operations. Reduces the need to manually keep and patch on-premises infrastructures.
Reliable. You get managed, highly available services




Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-ldap

*Community vote distribution*
B (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview
upvoted 14 times

**CertShooter** Highly Voted 1 year ago
Selected Answer: B

Azure AD DS is a managed service that provides domain services such as domain join, group policy support, and LDAP and Kerberos-based authentication for cloud-based applications. It allows you to use your Azure AD directory as a managed domain without the need to set up, maintain, and secure an on-premises domain controller. This can help reduce the administrative effort required to maintain the infrastructure an ensure that the legacy applications continue to function as expected.

Other identity services, such as Azure Active Directory (Azure AD) or Azure Active Directory (Azure AD) B2C, may not be as suitable for this scena because they do not provide the same level of support for legacy applications that rely on LDAP and Kerberos-based authentication. Similarly, using an on-premises Active Directory Domain Services (AD DS) instance would require maintaining additional infrastructure and may not be as cost-effective or efficient as using a managed service like Azure AD DS.

upvoted 5 times

**zellck** Most Recent 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/active-directory-domain-services/overview
Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight direct access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch dom controllers (DCs) in the cloud.

An Azure AD DS managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you do want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

upvoted 1 times

**awssecuritynewbie** 11 months ago

Selected Answer: B

Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud first strategy to modernize their environment by moving off their on-premises LDAP resources to the cloud. The immediate benefits will be:
Integrated with Azure AD. Additions of users and groups, or attribute changes to their objects are automatically synchronized from your Azure A tenant to AD
DS. Changes to objects in on-premises Active Directory are synchronized to Azure AD, and then to AD DS.

upvoted 1 times

Question #21 *Topic 3*

HOTSPOT -

Your company has a Microsoft 365 ES subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (AD DS).

You need to recommend an identity security strategy that meets the following requirements:

☞ Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website

☞ Ensures that partner companies can access Microsoft SharePoint Online sites for the project to which they are assigned

The solution must minimize the need to deploy additional infrastructure components.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| | |
|---|---|
| For the customers: | Azure AD B2B authentication with access package assignments<br>Azure AD B2C authentication<br>Federation in Azure AD Connect with Active Directory Federation Services<br>Pass-through authentication in Azure AD Connect<br>Password hash synchronization in Azure AD Connect |
| For the partners: | Azure AD B2B authentication with access package assignments<br>Azure AD B2C authentication<br>Federation in Azure AD Connect with Active Directory Federation Services<br>Pass-through authentication in Azure AD Connect<br>Password hash synchronization in Azure AD Connect |

**Correct Answer:**

**Answer Area**

| | |
|---|---|
| For the customers: | Azure AD B2B authentication with access package assignments<br>**Azure AD B2C authentication**<br>Federation in Azure AD Connect with Active Directory Federation Services<br>Pass-through authentication in Azure AD Connect<br>Password hash synchronization in Azure AD Connect |
| For the partners: | **Azure AD B2B authentication with access package assignments**<br>Azure AD B2C authentication<br>Federation in Azure AD Connect with Active Directory Federation Services<br>Pass-through authentication in Azure AD Connect<br>Password hash synchronization in Azure AD Connect |

Box 1: Azure AD B2C authentication

Ensures that customers can use their Facebook credentials to authenticate to an Azure App Service website.

You can set up sign-up and sign-in with a Facebook account using Azure Active Directory B2C.

Box 2: Azure AD B2B authentication with access package assignments

Govern access for external users in Azure AD entitlement management

Azure AD entitlement management uses Azure AD business-to-business (B2B) to share access so you can collaborate with people outside your organization.

With Azure AD B2B, external users authenticate to their home directory, but have a representation in your directory. The representation in your directory enables the user to be assigned access to your resources.

Incorrect:

Not: Password hash synchronization in Azure AD connect

The partners are not integrated with AD DS.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration

**TheMCT** Highly Voted 1 year, 4 months ago

The given answers and selection is correct (Box 1 - Azure AD B2C authentication, Box 2 - Azure AD b2b authentication with access package assignments)

upvoted 16 times

**zts** Highly Voted 1 year, 4 months ago

Seems correct: Box 1 --> https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview
Box 2 -- > https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers

upvoted 10 times

**theplaceholder** Most Recent 3 months, 4 weeks ago

given answers are correct (for once)

upvoted 3 times

**zellck** 8 months ago

1. Azure AD B2C authentication
2. Azure AD B2B authentication with access package assignments

https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview
Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b
Azure Active Directory (Azure AD) B2B collaboration is a feature within External Identities that lets you invite guest users to collaborate with y organization. With B2B collaboration, you can securely share your company's applications and services with external users, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an department.

upvoted 1 times

**AKS2504** 1 year ago

Correct selection.

upvoted 1 times

**TJ001** 1 year ago

given answers are right

upvoted 1 times

Question #22 *Topic 3*

You have an Azure subscription that contains virtual machines.
Port 3389 and port 22 are disabled for outside access.
You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:
⇨ Prevent the need to enable ports 3389 and 22 from the internet.
⇨ Only provide permission to connect the virtual machines when required.
⇨ Ensure that administrators use the Azure portal to connect to the virtual machines.
Which two actions should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure Azure VPN Gateway.

B. Enable Just Enough Administration (JEA).

C. Configure Azure Bastion.

D. Enable just-in-time (JIT) VM access.

E. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.

**Correct Answer:** *CD*
C: Bastion provides secure remote access.
It uses RDP/SSH session is over TLS on port 443.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
D: Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.
Meets the requirement: Only provide permission to connect the virtual machines when required
Incorrect:
Not B: Does not address: Only provide permission to connect the virtual machines when required
Just Enough Administration (JEA) is a security technology that enables delegated administration for anything managed by PowerShell. With JEA, you can:
Reduce the number of administrators on your machines using virtual accounts or group-managed service accounts to perform privileged actions on behalf of regular users.
Limit what users can do by specifying which cmdlets, functions, and external commands they can run.
Better understand what your users are doing with transcripts and logs that show you exactly which commands a user executed during their session.
Not E: Does not help with the remote access.
Note: Classic Virtual Machine Contributor: Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
Reference:
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

*Community vote distribution*
CD (81%) CE (19%)

**imsidrai** 6 months, 3 weeks ago
i believe it should be CDE
https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/multilayered-protection-azure-vm
upvoted 2 times

**imsidrai** 6 months, 3 weeks ago
oh only two are required , so it should be Bastion & JIT
upvoted 3 times

**zellck** 8 months ago

Selected Answer: CD

CD is the answer.

https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/multilayered-protection-azure-vm#components
Azure Bastion provides secure and seamless RDP and SSH connectivity to VMs in a network. In this solution, Azure Bastion connects users who u
Microsoft Edge or another internet browser for HTTPS, or secured traffic on port 443. Azure Bastion sets up the RDP connection to the VM. RDP
and SSH ports aren't exposed to the internet or the user's origin.

upvoted 2 times

**zellck** 8 months ago

JIT VM access is a feature of Defender for Cloud that provides just-in-time network-based access to VMs. This feature adds a deny rule to the
Azure network security group that protects the VM network interface or the subnet that contains the VM network interface. That rule minimi
the attack surface of the VM by blocking unnecessary communication to the VM. When a user requests access to the VM, the service adds a
temporary allow rule to the network security group. Because the allow rule has higher priority than the deny rule, the user can connect to the
VM. Azure Bastion works best for connecting to the VM. But the user can also use a direct RDP or SSH session.

upvoted 1 times

**uffman** 8 months, 3 weeks ago

Selected Answer: CD

Correct.

upvoted 1 times

**God2029** 10 months, 3 weeks ago

Going with C and D.

upvoted 1 times

**yaza85** 12 months ago

Jit controls access based on nsg not based on identity. Permissions are given in pim

upvoted 1 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

PIM is fine but not as virtual machine contributors - too much privileges

upvoted 1 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

also virtual machine contributor does not provide connection access

upvoted 1 times

**Jt909** 12 months ago

Selected Answer: CE

Bastion and PIM for "Only provide permission to connect the virtual machines when required"

upvoted 3 times

**CertShooter** 1 year ago

Selected Answer: CD

Configure Azure Bastion: Azure Bastion is a service that allows you to securely connect to your Azure virtual machines over Remote Desktop Protocol (RDP) or Secure Shell (SSH) directly from the Azure portal, without the need to enable ports 3389 or 22 on the virtual machines. Azure Bastion uses Remote Desktop Services and Azure AD for authentication, providing a secure and convenient way to access the virtual machines.

Enable just-in-time (JIT) VM access: JIT VM access is a feature of Azure Security Center that allows you to control and monitor inbound traffic to your virtual machines. By enabling JIT VM access, you can grant administrators access to the virtual machines only when required, and automatically revoke the access when the session ends. This helps prevent unauthorized access to the virtual machines and ensures that access i
granted only to authorized administrators.

Other actions, such as configuring Azure VPN Gateway, enabling Just Enough Administration (JEA), or enabling Azure AD Privileged Identity Management (PIM) roles as virtual machine contributors, may not be directly related to providing secure remote access to the virtual machines.

upvoted 3 times

**blopfr** 1 year, 2 months ago

Selected Answer: CD

correct link
https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/multilayered-protection-azure-vm#architecture

upvoted 3 times

**monkeybiznex** 1 year, 2 months ago

JIT enables on ports exposed to the internet, not to the Bastion vNET.
So... what gives?

upvoted 2 times

**zts** 1 year, 4 months ago

Selected Answer: CD

C. Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses. Provision the service directly in your local or peered virtual network to get support for all the VMs within it --> https://azure.microsoft.com/en-us/services/azure-bastion/#overview
D --> https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview?tabs=defender-for-container-arch-aks

upvoted 4 times

**TheMCT** 1 year, 4 months ago

The given answer is correct: C & D

upvoted 4 times

Question #23 *Topic 3*

Your company has on-premises Microsoft SQL Server databases.
The company plans to move the databases to Azure.
You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.
What should you include in the recommendation?

A. Azure SQL Managed Instance

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

D. SQL Server on Azure Virtual Machines

**Correct Answer:** *A*
Azure SQL Managed Instance is the intelligent, scalable cloud database service that combines the broadest SQL Server database engine compatibility with all the benefits of a fully managed and evergreen platform as a service. SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise
Edition) database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable for existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.
Note: Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking. Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.
Incorrect:
Not D: SQL Server does not support dynamic data masking.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql
https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

*Community vote distribution*
A (52%) C (48%)

**ele123** Highly Voted 1 year, 4 months ago

Selected Answer: C
Azure SQL Database is a general-purpose relational database, provided as a managed service. Categorized as a platform as a service (PaaS), Azu SQL Databases are built on standardized hardware and software that is owned, hosted, and maintained by Microsoft. When using Azure SQL Database, you pay-as-you-go, with the option to scale up or out with no service interruption.

Within Azure SQL Database, you have the option to deploy a managed instance. Azure SQL Database Managed Instance is a collection of systen and user databases with a shared set of resources. In addition to all the PaaS benefits of Azure SQL Database, this option provides a native virtu network (VNet) and near 100 percent compatibility with on-premises SQL Server. Azure SQL Database Managed Instance provides you with full Server access and feature compatibility for migrating SQL Servers to Azure.

Recommendation: Choose Azure SQL Database for your modern cloud applications, or when you have time constraints in development and marketing.
upvoted 24 times

**ca777** 5 months, 1 week ago
Azure SQL Database Managed Instance is a fully managed offering that provides near 100% compatibility with on-premises SQL Server. It minimizes operational requirements as Microsoft manages the underlying infrastructure, including patching, backups, and high availability. S answer is : A.
upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago
No, clearly C.
Reasons are in the key requirements phrases:
"minimize operational requirements for patching"
"The solution must minimize costs."

SQL Database beats Managed Instance in both requirements

Hence C
upvoted 2 times

**ConanBarb** 3 months, 3 weeks ago
Sorry, I take that back. It says "move" databases, which implies MI. For SQLDB it should have said "migrate".
A
upvoted 1 times

**AzureJobsTillRetire** 10 months, 3 weeks ago
Have you considered the cost of migration of on-premise Microsoft SQL Server databases to Azure? To use Azure SQL Databases, you will ha to re-develop most if not all of the applications build upon on-premise Microsoft SQL Server databases. Migrating on-premise Microsoft SQI Server databases to SQLMI is the most cost effective way.
upvoted 5 times

**ConanBarb** 3 months, 3 weeks ago
Do you see that as stated requirements in the question? No. even if you're right, using implicit assumptions (however sound) is not how exam questions work.
upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago
Sorry, I take that back. It says "move" DBs -> MI. "migrate" -> SQLDB (just as a rule of thumb in MS exams, not necessarily in real life)
upvoted 1 times

**TheMCT** Highly Voted 1 year, 4 months ago
Selected Answer: A
SQL managed Instance is best for most migrations to the cloud.
upvoted 21 times

**AzureJobsTillRetire** 10 months, 3 weeks ago
This is correct. If this question is in any of those AZ- exams, you will see no doubt A is the answer. I do not think SC-100 is of any differences.
upvoted 2 times

**AnonymousJhb** 1 year, 2 months ago
this is not the context of this question. You cannot implement dynamic data masking at MI level. dynamic data masking can only be implemented at a db level.
upvoted 1 times

**dc2k79** 1 year ago
Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking. Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.
https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

kindly don't write anything just for the sake of writing.
upvoted 9 times

**Ramye** Most Recent 3 days, 6 hours ago
Based on the video with the link below on cost saving and ease of management, going with option A
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azu /defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
upvoted 1 times

**Ramye** 3 days, 6 hours ago
Gee! wish there could be a definite answer 😉
upvoted 1 times

**Murtuza** 1 week, 1 day ago
Selected Answer: A
A is correct with SQL MI
upvoted 1 times

**CSue** 3 weeks, 4 days ago
1. Operational Requirements and Complexity:
If you prefer a fully managed service with minimal operational overhead:
Azure SQL Database is a fully managed service that abstracts away much of the operational complexity, making it a simpler choice for those wh want
a fully managed database without having to worry about underlying infrastructure.
2. Dynamic Data Masking (DDM):
If dynamic data masking is a critical requirement:
Both Azure SQL Managed Instance and Azure SQL Database support Dynamic Data Masking (DDM). You can implement DDM in both services t protect sensitive data at the query result level.
3. Cost Considerations:
If you prioritize cost-effectiveness and flexibility:
Azure SQL Database offers more flexibility in terms of pricing tiers, allowing you to choose the performance level that aligns with your budget a

requirements.
It may be a cost-effective option for many scenarios.
Azure SQL Database is the correct answer

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

I think both A and C are correct. But the question emphasises on cost. Since nothing MI has over the AzSQL, i'd say C is correct.

upvoted 2 times

**ServerBrain** 4 months, 3 weeks ago

Selected Answer: C

since you are migrating databaseS

upvoted 1 times

**WRITER00347** 5 months, 1 week ago

Recommend Azure SQL Database because:

It's fully managed, reducing patching efforts.
Supports dynamic data masking.
Typically more cost-effective than the other options for single databases. Here's why:

Azure SQL Database: It's a fully managed database service, which means Azure handles most of the operational tasks like patching for you. It als supports dynamic data masking out of the box, which allows you to mask sensitive data. It's usually the most cost-effective option for a single database without requiring the overhead of managing an entire instance or VM.

Azure SQL Managed Instance: While it's also a fully managed service and supports dynamic data masking, it might be more expensive than Azu SQL Database, especially if you only need to host a few databases. It's a better option if you need a higher level of compatibility with SQL Server and VNET integration.

upvoted 1 times

**Darkren4eveR** 5 months, 1 week ago

A

https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql-mi

upvoted 2 times

**hw121693** 5 months, 2 weeks ago

Selected Answer: A

"Microsoft SQL Server databases" multiple databases, you should lend an instance and not single database (C)

upvoted 3 times

**Ario** 6 months, 2 weeks ago

Selected Answer: C

Due to Minimize cost on this question we should go with C if cost wasnt an option here then definitely A is the best to go

upvoted 1 times

**imsidrai** 6 months, 3 weeks ago

A is the correct answer
https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql#key-features-and-capabilities

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql

https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql
Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking. Dynamic data masking limits sensitive data exposure by masking it to nonprivileged users.

upvoted 3 times

**uffman** 8 months, 3 weeks ago

Selected Answer: A

Migrating on-prem SQL server db(s), Azure SQL DB MI is the best and most cost-effective way. Also supports dynamic data masking.

upvoted 4 times

**Mo22** 11 months, 1 week ago

Selected Answer: A

Both Azure SQL MI & Azure SQL can do the job, however SQL MI is the best fitting on-prem SQL architecture so within the scope of migration S MI would be seamless here and again both will meet the sec req

upvoted 6 times

**examdog** 11 months, 2 weeks ago

**Selected Answer: A**

For migrating on-prem SQL server dbs, Azure SQL db MI is the choice. Specifically, I cannot imagine an on-prem SQL server without SQL agent jobs. But SQL agent is available only to MI, not for Azure SQL db.

upvoted 2 times

Question #24 *Topic 3*

Your company plans to move all on-premises virtual machines to Azure.

A network engineer proposes the Azure virtual network design shown in the following table.

| Virtual network name | Description | Peering connection |
|---|---|---|
| Hub VNet | Linux and Windows virtual machines | VNet1, VNet2 |
| VNet1 | Windows virtual machines | Hub VNet |
| VNet2 | Linux virtual machines | Hub VNet |
| VNet3 | Windows virtual machine scale sets | VNet4 |
| VNet4 | Linux virtual machine scale sets | VNet3 |

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines.

Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1

B. 2

C. 3

D. 4

E. 5

**Correct Answer:** *C*

The peering network Hub VNet, VNet1 and VNet2 requires one Bastion.

VNet3 also requires one Bastion.

Finally, VNet3 also requires one Bastion.

Note:

VNet peering -

Can I still deploy multiple Bastion hosts across peered virtual networks?

Yes. By default, a user sees the Bastion host that is deployed in the same virtual network in which VM resides. However, in the Connect menu, a user can see multiple Bastion hosts detected across peered networks. They can select the Bastion host that they prefer to use to connect to the VM deployed in the virtual network.

Make sure that you have set up an Azure Bastion host for the virtual network in which the virtual machine scale set resides.

Azure Bastion requires a dedicated subnet: AzureBastionSubnet. You must create this subnet in the same virtual network that you want to deploy Azure Bastion to.

Can I deploy multiple Azure resources in my Azure Bastion subnet?

No. The Azure Bastion subnet (AzureBastionSubnet) is reserved only for the deployment of your Azure Bastion resource.

Reference:

https://docs.microsoft.com/en-us/azure/bastion/configuration-settings#subnet https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-scale-set https://docs.microsoft.com/en-us/azure/bastion/bastion-faq

*Community vote distribution*

B (89%) 11%

**Nico95** Highly Voted 1 year ago

Selected Answer: B

Passed some days ago score < 900

Was in exam, i answered B

upvoted 21 times

**Jacquesvz** 11 months, 1 week ago

Thank you Nico95. appreciate the feedback.

upvoted 2 times

**JaySapkota** Highly Voted 1 year, 4 months ago

Selected Answer: B

Only 2

upvoted 16 times

**Ramye** Most Recent 3 days, 5 hours ago

Given what I know:
- I know 1 Bastion for 1 VNet
- Peered VNets can have 1 Bastion.
- There is only 2 VNets in the description are peered that is VNet1 and VNet2.

So 1 Bastion for the peered (VFNet1 and Vnet2)
and the rest gets 1 Bastion each
So it is 3 Bastion altogether.

So where the answer 2 coming from? is it possible that only 2 the subnets that has Windows machines get Bastion? Then I read Linux machine a supports Bastion.
Help - thx

upvoted 1 times

**Ramye** 3 days, 5 hours ago

I think I got it ...
This all about how this peering is configured ...
- Hub Vnet is peered with VNet1 and VNet2 - so that means 1 Bastion would work for all
-And then VNet3 and VNet4 are also peered - so that means 1 Bastion for them

So 2 would be the answer ..- Final Answer

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 3 times

**techisland2k19** 5 months ago

Selected Answer: B

This question appeared in exam recently. I think B is the option.Why it was marked C?Anyone can confirm it?

upvoted 1 times

**cybrtrk** 5 months, 1 week ago

oh nevermind, the question should be asking: How many "dedicated Azure Bastion subnets" are required, then it makes more sense to me that t answer is 2.

upvoted 1 times

**cybrtrk** 5 months, 1 week ago

aren't people who are saying 2 is the answer forgetting that the bastion requires its own subnet?
Answer is 3.

upvoted 2 times

**Ramye** 3 days, 5 hours ago

yes but if the subnets are peered than you can go with 1 for the peered subnets.
So this answer 2 is also throwing me off as well

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering
Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peere VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host.

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 2 times

**uffman** 8 months, 3 weeks ago

Selected Answer: B

2 is the right answer.

upvoted 1 times

**awssecuritynewbie** 11 months ago

Selected Answer: B

So i thought it was 3 Bastions but when you actually look a bit closer you will see that the Vnet column on the left hand side shows the VNET th

VM is in and the column on right is the Peered VNET so :

VNET 1-2 ARE PEERED
VNET 3-4 ARE PEERED ...THEREFORE KIDS WE NEED ONLY TWO BASTION : B

upvoted 6 times

**Ramye** 3 days, 6 hours ago

Yes, i don't see either where it shows VNet 3 and VNet 4 are peered.
I don't get it how the answer is 2.
I know one VNet requires 1 Bastion
and peered VNets can have 1 Bastion.
So there is only 2 VNets are peered that is VNet1 and VNet 2.
so how the answer is 2? pls explain - thx
I know you can have 1 Bstion

upvoted 1 times

**tiagofrota** 6 months ago

Where in the question it says vnets 3 and 4 are peered?

upvoted 1 times

**KrishnaSK1** 11 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

upvoted 1 times

**TJ001** 1 year ago

2 is right dont overlook peering is the keyword it does not need to be Hub and Spoke(s)

upvoted 2 times

**dc2k79** 1 year ago

2 Bastion Subnets.
1 in Hub VNet.
1 in either VNet 3 or VNet4.

upvoted 3 times

**Gestalt** 1 year ago

Selected Answer: B

should be 2

upvoted 1 times

**minasamy** 1 year, 1 month ago

Selected Answer: B

Only 2 is needed

upvoted 1 times

**TP447** 1 year, 1 month ago

Answer is 2 for me.

upvoted 1 times

**John0153** 1 year, 1 month ago

Selected Answer: B

only 2 you need to look closely at peering and names

1. Hub vnet, vnet 1, vnet 2
2. vnet 3,vnet 4

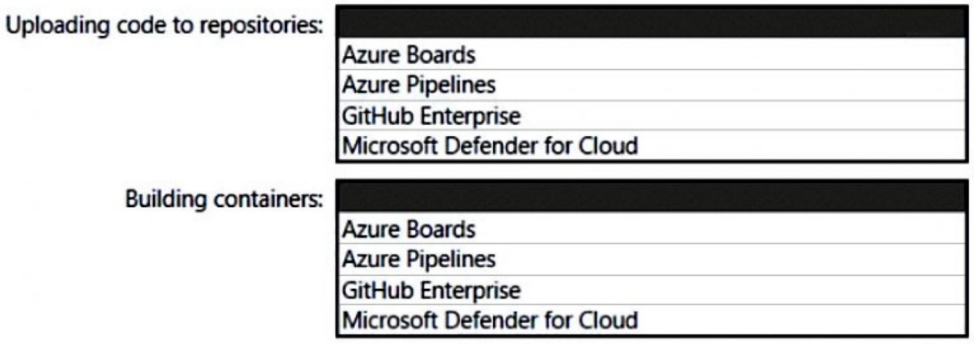
upvoted 5 times

Question #25 *Topic 3*

HOTSPOT -
Your company has an Azure App Service plan that is used to deploy containerized web apps.
You are designing a secure DevOps strategy for deploying the web apps to the App Service plan.
You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:
- Uploading the code to repositories
- Building containers

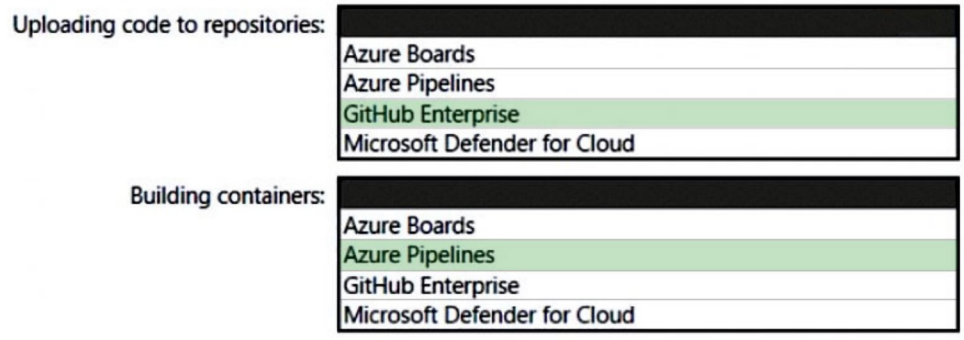
Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

**Answer Area**




**Correct Answer:**

**Answer Area**




Box 1: GitHub Enterprise -
A GitHub Advanced Security license provides the following additional features:
Code scanning - Search for potential security vulnerabilities and coding errors in your code.
Secret scanning - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also detects secrets when they are pushed to your repository.
Etc.
Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub Enterprise Cloud.

Box 2: Azure Pipelines -
Building Containers with Azure DevOps using DevTest Pattern with Azure Pipelines

The pattern enabled as to build container for development, testing and releasing the container for further reuse (production ready).
Azure Pipelines integrates metadata tracing into your container images, including commit hashes and issue numbers from Azure Boards, so that you can inspect your applications with confidence.
Incorrect:
* Not Azure Boards: Azure Boards provides software development teams with the interactive and customizable tools they need to manage their software projects.
It provides a rich set of capabilities including native support for Agile, Scrum, and Kanban processes, calendar views, configurable dashboards, and integrated reporting.
* Not Microsoft Defender for Cloud
Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.
You cannot use Microsoft Defender for Cloud to scan code, it scans images.
Reference:
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-security
https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-container-dev-test-release/

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Agreed
upvoted 16 times

**TJ001** Highly Voted 1 year ago
As a sequence in the process I like to see as below ; hence the given answers are correct.
GitHub Actions (repo commit stage)
Azure pipeline (building the docker image stage)
Container Images published to ACR (Defender for Containers)
Containers running in AKS (Defender for Containers)
upvoted 9 times

**Victory007** Most Recent 5 months, 1 week ago
Answer is Right. 1. Git Hub & Pipeline.
You can integrate code scanning tools with GitHub Enterprise to automatically scan the code when it is uploaded to repositories. GitHub offers code scanning as a feature that analyzes the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identifi by the analysis are shown in GitHub, allowing developers to find, triage, and prioritize fixes for existing problems in their code.
You can integrate code scanning tools with Azure Pipelines to automatically scan the code when building containers. Azure Pipelines is a cloud service that you can use to automatically build, test, and deploy your code. You can configure Azure Pipelines to use various code scanning tool such as Microsoft Security Code Analysis, to automatically scan your code for vulnerabilities during the build process.
upvoted 1 times

**cychoia** 1 year, 2 months ago
Answer is correct
upvoted 4 times

**JakeCallham** 1 year, 2 months ago
A is wrong, you can do code scans in Azure pipelines as well. This doesn't make sense at all.
upvoted 1 times

**dc2k79** 1 year ago
When uploading to the repo, you will scan the code in the repo.
upvoted 1 times

**Learing** 1 year, 2 months ago
Yes but not during upload to git, which is a requirement
upvoted 2 times

**tonuywildthing22** 1 year, 4 months ago
Answer is correct
upvoted 4 times

Question #26 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
We need to use customer-managed keys.
Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics against the threat of malicious offline activity by encrypting data at rest. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.
In Azure, the default setting for TDE is that the Database Encryption Key (DEK) is protected by a built-in server certificate. The built-in server certificate is unique for each server and the encryption algorithm used is AES 256.
TDE protector is either a service-managed certificate (service-managed transparent data encryption) or an asymmetric key stored in Azure Key Vault (customer- managed transparent data encryption).
Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.
This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end-to-end rotation.
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

*Community vote distribution*
A (100%)

**zellck** 8 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-overview?view=azuresql
Azure SQL transparent data encryption (TDE) with customer-managed key (CMK) enables Bring Your Own Key (BYOK) scenario for data protectic at rest, and allows organizations to implement separation of duties in the management of keys and data. With customer-managed TDE, the customer is responsible for and in a full control of a key lifecycle management (key creation, upload, rotation, deletion), key usage permissions, auditing of operations on keys.
upvoted 1 times

**CertShooter** 1 year ago
Selected Answer: A
Yes, this solution meets the goal of ensuring that the data at rest is encrypted by using AES-256 keys and supporting rotating the encryption ke monthly.

Transparent Data Encryption (TDE) is a feature of Azure SQL that allows you to encrypt your databases and their backups with AES-256 keys. By using TDE with customer-managed keys (CMKs), you can manage the encryption keys yourself, which means that you have full control over the keys and can rotate them on a regular basis. This can help ensure that your data at rest is encrypted using AES-256 keys and that the encryption keys are rotated regularly to enhance security.
upvoted 4 times

**JakeCallham** 1 year, 2 months ago
Selected Answer: A
Anser is yes, see provided link:

https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-key-rotation?view=azuresql&tabs=azure-portal#automatic-key-rotation

upvoted 4 times

**JOKERO** 1 year, 3 months ago

I would say no, because TDE is asymmetric key (can't be AES)
In this scenario, the key used for encryption of the Database Encryption Key (DEK), called TDE protector, is a customer-managed asymmetric key stored in a customer-owned and customer-managed Azure Key Vault
To provide Azure SQL customers with two layers of encryption of data at rest, infrastructure encryption (using AES-256 encryption algorithm) wi platform managed keys is being rolled out.

upvoted 2 times

**JakeCallham** 1 year, 2 months ago

You are wrong: https://learn.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-byok-key-rotation?view=azuresql&tabs=azure-portal

you can do it. answer is Yes

upvoted 2 times

**Jacquesvz** 1 year, 1 month ago

Agreed. I also found this article that talks to the TDE using AES 256: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver16#enable-tde

upvoted 1 times

**zts** 1 year, 4 months ago

Selected Answer: A

The requirement says: "solution must support rotating the encryption keys monthly" - you cannot do this if Microsoft manage the keys.

upvoted 3 times

**PlumpyTumbler** 1 year, 4 months ago

CMK to configure monthly rotation. If Microsoft is managing the key, you don't control it. CMK is more expensive because that's a resource in y subscription.

From the docs:
"By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You ha full control and responsibility for the key lifecycle, including rotation and management."

upvoted 4 times

**WickedMJ** 1 year, 4 months ago

So what is the answer?

upvoted 1 times

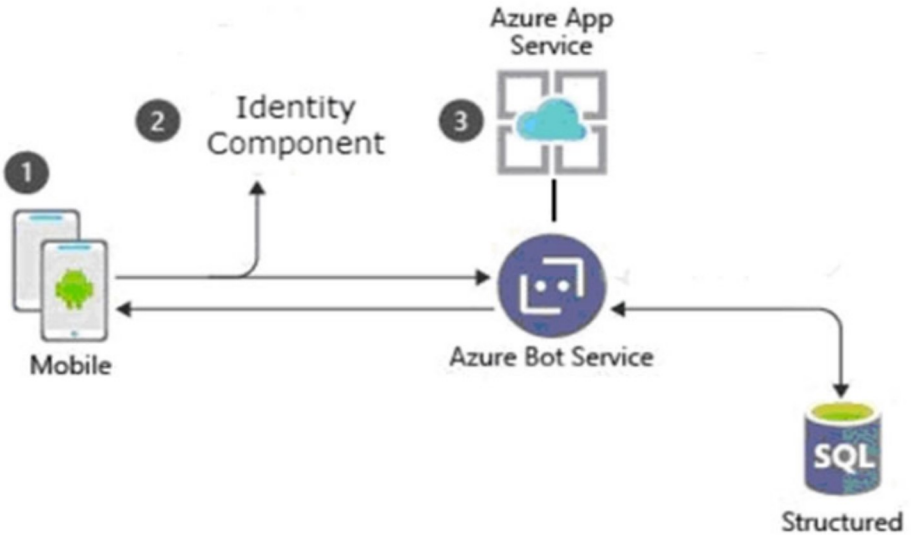
**JakeCallham** 1 year, 2 months ago

Answer is yes

upvoted 1 times

Question #27 *Topic 3*

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.




You need to design an identity strategy for the app. The solution must meet the following requirements:

- Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
- Use a customer identity store.
- Support fully customizable branding for the app.

Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2B

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD) B2C

D. Azure AD Connect

**Correct Answer:** *C*

Azure Active Directory B2C (Azure AD B2C), an identity store, is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page (SPA), and other applications.
You can set up sign-up and sign-in with a Facebook/Google account using Azure Active Directory B2C.

Branding -
Branding and customizing the user interface that Azure Active Directory B2C (Azure AD B2C) displays to your customers helps provide a seamless user experience in your application. These experiences include signing up, signing in, profile editing, and password resetting. This article introduces the methods of user interface (UI) customization.
Incorrect:
Not D: Azure AD Connect is a tool for connecting on-premises identity infrastructure to Microsoft Azure AD.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/
https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

*Community vote distribution*

C (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: C

Very obvious. Second link shows technical procedures for Facebook, Apple, Amazon, Google, etc. I've used most of them. Good answer and resources here.

upvoted 8 times

**cyber_sa** Most Recent 3 months, 1 week ago

Selected Answer: C

got this in exam 6oct23. passed with 896 marks. I answered C

upvoted 1 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview
Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

upvoted 1 times

**uffman** 8 months, 3 weeks ago

Selected Answer: C

Correct.

upvoted 1 times

**TJ001** 1 year ago

AAD B2C create a custom tenant and done deal

upvoted 3 times

**MCSA11** 1 year, 2 months ago

C. Azure Active Directory (Azure AD) B2C

upvoted 3 times

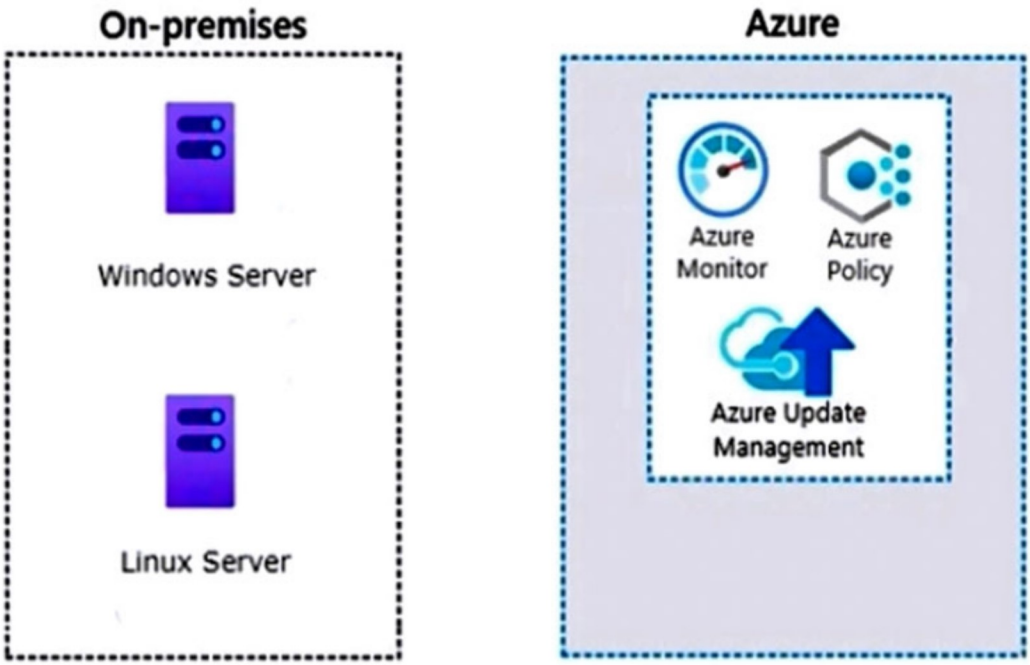
**tonuywildthing22** 1 year, 4 months ago

Correct Answer C

upvoted 1 times

Question #28 *Topic 3*

Your company has a hybrid cloud infrastructure.
Data and applications are moved regularly between cloud environments.
The company's on-premises network is managed as shown in the following exhibit.




You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:
☞ Govern virtual machines and servers across multiple environments.
☞ Enforce standards for all the resources across all the environments by using Azure Policy.
Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. on-premises data gateway

B. Azure VPN Gateway

C. guest configuration in Azure Policy

D. Azure Arc

E. Azure Bastion

**Correct Answer:** *CD*
C: Azure Policy's guest configuration feature provides native capability to audit or configure operating system settings as code, both for machines running in Azure and hybrid Arc-enabled machines. The feature can be used directly per-machine, or at-scale orchestrated by Azure Policy.
Configuration resources in Azure are designed as an extension resource. You can imagine each configuration as an additional set of properties for the machine.
Configurations can include settings such as:

Operating system settings -
Application configuration or presence

Environment settings -
Configurations are distinct from policy definitions. Guest configuration utilizes Azure Policy to dynamically assign configurations to machines.
D: Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.
Microsoft recently [2019/2020] released Azure Arc, which unlocks new hybrid scenarios for organizations by bringing new Azure services and management features to any infrastructure.
By the time of writing this post, the public preview supports the following operating systems:

Windows Server 2012 R2 and newer

Ubuntu 16.04 and 18.04 -
Register the required Resource Providers in Azure
First, we need to register the required resource providers in Azure. Therefore, take the following steps:
Open a browser and navigate to the Azure portal at: https://portal.azure.com/
Login with your administrator credentials.
Open Cloud Shell in the top right menu, and add the following lines of code to register the Microsoft.HybridCompute and the Microsoft.GuestConfiguration resource providers:
Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute
Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration
This will result in the following output:

```
Azure:/
PS Azure:\> Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute

ProviderNamespace : Microsoft.HybridCompute
RegistrationState : Registering
ResourceTypes     : {machines, operations}
Locations         : {West US 2, West Europe, Southeast Asia}


Azure:/
PS Azure:\> Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration

ProviderNamespace : Microsoft.GuestConfiguration
RegistrationState : Registering
ResourceTypes     : {guestConfigurationAssignments, software, softwareUpdates, softwareUpdateProfile…}
Locations         : {East US 2, South Central US}
```

Note that the resource providers are only registered in specific locations.
(Networking
During installation and runtime, the agent requires connectivity to Azure Arc service endpoints. If outbound connectivity is blocked by the firewall, make sure that the following URLs are not blocked:
Required Azure service endpoints include:
Guest Configuration)
Incorrect:
Not A, Not B: Connect the on-premises machine to Azure Arc
To connect the on-premises machine to Azure Arc, we first need install the agent on the on-premises machine (not any Gateways).
Not E: Azure Bastion now supports connectivity to Azure virtual machines or on-premises resources via specified IP address.
Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.
Reference:
https://techcommunity.microsoft.com/t5/azure-developer-community-blog/azure-arc-for-servers-getting-started/ba-p/1262062
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/guest-configuration

*Community vote distribution*

CD (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: CD

Simple process of elimination here, even if you're not sure. The other 3 options have nothing to do with governance. However, guest configurati policy is no longer called that. Answers could look different on the real test. Remember this is the Beta dump and SC-100 isn't in Beta anymore.
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

Not the answers:
https://docs.microsoft.com/en-us/data-integration/gateway/service-gateway-onprem

https://docs.microsoft.com/en-us/learn/modules/connect-on-premises-network-with-vpn-gateway/2-connect-on-premises-networks-to-azure-using-site-to-site-vpn-gateways

upvoted 14 times

**zts** 1 year, 4 months ago

its now called Guest configuration extension --> https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/guest-configuration
upvoted 7 times

**rdy4u** Highly Voted 1 year, 3 months ago

Azure Policy Guest Configuration is now called Azure Automanage Machine Configuration
Ref: https://learn.microsoft.com/en-us/azure/governance/machine-configuration/overview
upvoted 6 times

**cyber_sa** Most Recent 3 months, 1 week ago

Selected Answer: CD

got this in exam 6oct23. passed with 896 marks. I answered CD
upvoted 2 times

**zellck** 8 months ago

Selected Answer: CD

CD is the answer.

https://learn.microsoft.com/en-us/azure/azure-arc/overview
Azure Arc simplifies governance and management by delivering a consistent multicloud and on-premises management platform.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-server-management/guest-configuration-policy
You can use the Azure Policy guest configuration extension to audit the configuration settings in a virtual machine. Guest configuration supports
Azure VMs natively and non-Azure physical and virtual servers through Azure Arc-enabled servers.
upvoted 1 times

**KrishnaSK1** 11 months, 2 weeks ago

Selected Answer: CD

https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/tutorial-assign-policy-portal

Azure Policy supports auditing the state of your Azure Arc-enabled server with guest configuration policies. Azure Policy's guest configuration definitions can audit or apply settings inside the machine.

ARC is mandate for governing virtual machines both on-premises and cloud through Azure Connected Machine agent
https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview
upvoted 1 times

**Sec_Arch_Chn** 1 year, 1 month ago

Correct Answer. 'Azure Policy Guest Configuration is now called Azure Automanage Machine Configuration'
Source: https://learn.microsoft.com/en-us/azure/governance/machine-configuration/overview
upvoted 5 times

Question #29 *Topic 3*

A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze logs, audit activities, and search for potential threats across all deployed services
You need to recommend a solution for the customer.
What should you include in the recommendation?

A. Microsoft Defender for Cloud

B. Microsoft Defender for Cloud Apps

C. Microsoft 365 Defender

D. Microsoft Sentinel

**Correct Answer:** *D*
Microsoft Sentinel is a scalable, cloud-native solution that provides:
Security information and event management (SIEM)
Security orchestration, automation, and response (SOAR)
Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.
Microsoft Sentinel is your bird's-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.
Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
Respond to incidents rapidly with built-in orchestration and automation of common tasks.
Microsoft Sentinel natively incorporates proven Azure services, like Log Analytics and Logic Apps. Microsoft Sentinel enriches your investigation and detection with AI. It provides Microsoft's threat intelligence stream and enables you to bring your own threat intelligence.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/overview

*Community vote distribution*
D (100%)

**InformationOverload** Highly Voted 1 year, 4 months ago
Selected Answer: D
hunt is more used now instead of search. But when it says something by hunting/search, its reffering to Microsoft Sentinel
upvoted 10 times

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: D
Version of the test I've seen says "hunt" instead of search. Same answer though.
upvoted 5 times

**zellck** Most Recent 8 months ago
Selected Answer: D
D is the answer.

https://learn.microsoft.com/en-us/azure/sentinel/overview
Microsoft Sentinel is a scalable, cloud-native solution that provides:
- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
upvoted 1 times

**God2029** 10 months, 3 weeks ago
Again another Easy Pick
upvoted 1 times

Question #30 *Topic 3*

HOTSPOT
-

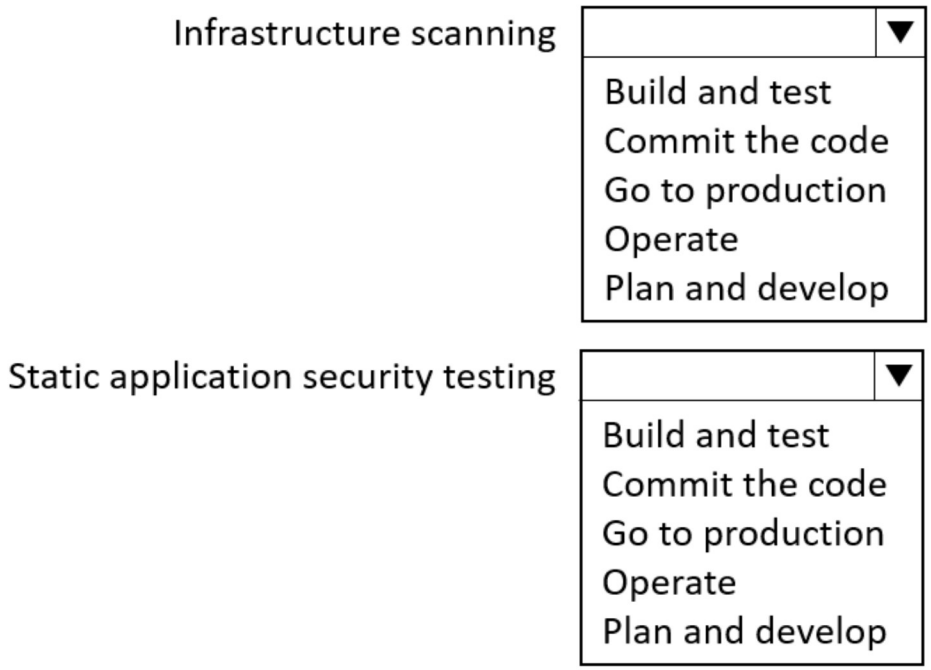
Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines.

You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines.

What should recommend? To answer, select the appropriate options in the answer area.

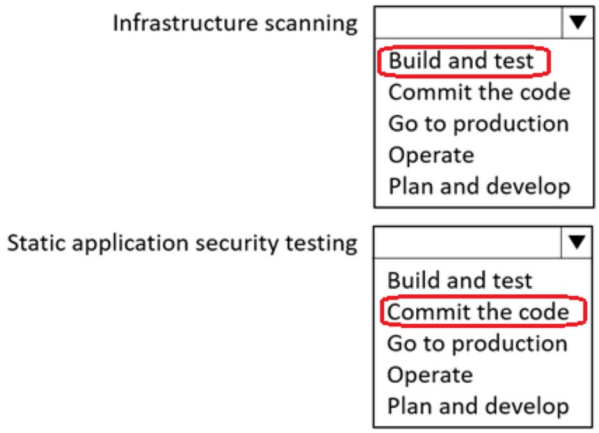
NOTE: Each correct selection is worth one point.

## Answer Area




**Correct Answer:**

**Answer Area**




**cyber_sa** 3 months, 1 week ago
got this in exam 6oct23. passed with 896 marks. I answered as per given answer

upvoted 4 times

**AbdallaAM** 3 months, 4 weeks ago

Correct

https://learning.oreilly.com/api/v2/epubs/urn:orm:book:9780137997299/files/graphics/f0290-01.jpg

upvoted 2 times

**zellck** 8 months ago

1. Build and test
2. Commit the code

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#commit-the-code
Typically, developers create, manage, and share their code in repositories such as GitHub or Azure Repos. This approach provides a central, versi
controlled library of code for developers to collaborate on easily. However, enabling many collaborators on a single codebase also runs the risk
changes being introduced. That risk can lead to vulnerabilities or unintentionally including credentials or tokens in commits.

To address this risk, development teams should evaluate and implement a repository scanning capability. Repository scanning tools perform sta
code analysis on source code within repositories. The tools look for vulnerabilities or credentials changes and flag any items found for remediati
This capability acts to protect against human error and is a useful safeguard for distributed teams where many people are collaborating in the
same repository.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#cloud-configuration-validation-and-infrastructure-scanning

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#static-application-security-testing

upvoted 1 times

**uffman** 8 months, 3 weeks ago

Correct, https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/media/devsecops-controls.png

upvoted 1 times

**awssecuritynewbie** 10 months, 4 weeks ago

The answer is correct!

The Infrastructure scanning is under the build and test phase

Static application security testing is under the commit the code .

upvoted 1 times

**buguinha** 11 months ago

It is correct https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

upvoted 2 times

Question #31 *Topic 3*

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements.

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.

**Correct Answer:** *ACE*

*Community vote distribution*

ACE (70%) ABE (30%)

**zellck** 8 months ago

Selected Answer: ACE

ACE is the answer.

https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-1-use-centralized-identity-and-authentication-system
Security Principle: Use a centralized identity and authentication system to govern your organization's identities and authentications for cloud an non-cloud resources.

https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-protect-identity-and-authentication-systems
Security Principle: Secure your identity and authentication system as a high priority in your organization's cloud security practice.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-3-manage-application-identities-securely-and-automatically
Security Principle: Use managed application identities instead of creating human accounts for applications to access resources and execute code. Managed application identities provide benefits such as reducing the exposure of credentials. Automate the rotation of credential to ensure the security of the identities.

upvoted 2 times

**awssecuritynewbie** 10 months, 3 weeks ago

Selected Answer: ACE

I have tested this

upvoted 2 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

Selected Answer: ACE

https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management

upvoted 2 times

**Bravocado** 10 months, 3 weeks ago

Selected Answer: ACE

The given answer is correct https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management

upvoted 2 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

Selected Answer: ABE

I'm struggling to find "C. Protect identity and authentication systems" in the list below.

IM-1: Standardize Azure Active Directory as the central identity and authentication system
IM-2: Manage application identities securely and automatically

IM-3: Use Azure AD single sign-on (SSO) for application access
IM-4: Use strong authentication controls for all Azure Active Directory based access
IM-5: Monitor and alert on account anomalies
IM-6: Restrict Azure resource access based on conditions
IM-7: Eliminate unintended credential exposure
IM-8: Secure user access to legacy applications
https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v2-identity-management

upvoted 2 times

**Bravocado** 10 months, 3 weeks ago

Look at the latest v3 instead of the v2 - https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-protect-identity-and-authentication-systems

upvoted 3 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

D. Enable threat detection for identity and access management.
This is under Logging and threat detection, and hence this option is out.
https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection

upvoted 1 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

Sorry my bad, the answers should be ACE

B. Manage the lifecycle of identities and entitlements
This is under Privileged access, and hence this option is out
https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access

upvoted 1 times

**awssecuritynewbie** 10 months, 4 weeks ago

Selected Answer: ABE

I would say A B E .
The link posted does not show the rest of them .

upvoted 1 times

**tech_rum** 10 months, 4 weeks ago

correct
https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v2-identity-management

upvoted 2 times

Question #32 *Topic 3*

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure.

You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure.

What should you use to start the threat modeling process?

A. the STRIDE model

B. the DREAD model

C. OWASP threat modeling

**Correct Answer:** *A*

*Community vote distribution*

C (57%) A (43%)

**skr123** Highly Voted 11 months ago

CORRECT
https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
upvoted 10 times

**Azerty1313** 1 month ago

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls
upvoted 1 times

**Murtuza** Most Recent 1 week ago

Sorry typo in my previous comment . I meant DREAD is not MS model to being with its all open source
upvoted 1 times

**Murtuza** 1 week ago

Selected Answer: A

SDLC is old and devops is the new term and STRIDE model is MS own threat model while OWASP and STRIDE are not and they have different purposes. STRIDE is geared towards DEVOPS
upvoted 1 times

**Murtuza** 1 week, 6 days ago

Difference between top down vs bottom up approach in general. This will help answer the question which in this case its C
https://www.simplilearn.com/top-down-approach-vs-bottom-up-approach-article
upvoted 2 times

**Arjanussie** 1 month, 1 week ago

the top-down approach may be simpler because it focuses on the key factors that influence the outcome -simpler is the key word

OWASP threat modeling: This method focuses on asking simple, non-technical questions to get the threat modeling process started.

so i guess C
upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago

For threat modeling using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure, starting with the STRIDE model would be the most appropriate.

The STRIDE model helps identify and categorize potential threats in six categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privileges. This model aligns well with the comprehensive and structured approach advocated by the Microso Cloud Adoption Framework, as it provides a systematic way to identify potential security threats in cloud environments.

While the DREAD model and OWASP Threat Modeling are also valuable, they serve slightly different purposes. The DREAD model is more focuse on assessing the risk level of identified threats, and OWASP provides a broader set of guidelines and tools for web application security, which m not be as directly aligned with the top-down approach of the Microsoft Cloud Adoption Framework.
upvoted 2 times

**slobav** 3 months, 3 weeks ago

Ansver: C
https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started
upvoted 4 times

**sherifhamed** 3 months, 4 weeks ago

Selected Answer: C

C is the answer as Microsoft said
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#threat-modeling-start-simple

upvoted 4 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/security/develop/secure-design#use-threat-modeling-during-application-design
Modeling the application design and enumerating STRIDE threats-Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, a
Elevation of Privilege-across all trust boundaries has proven an effective way to catch design errors early on.

upvoted 2 times

**God2029** 10 months, 3 weeks ago

STRIDE is micrsoft's own Threat Modeling Frame work

upvoted 2 times

Question #33 *Topic 3*

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. SQL Server on Azure Virtual Machines

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

**Correct Answer:** *C*

*Community vote distribution*

C (93%) 7%

**AzureJobsTillRetire** Highly Voted 10 months, 3 weeks ago

Selected Answer: C

Azure SQL Database is the correct option since SQLMI is not in the options

upvoted 7 times

**ConanBarb** Most Recent 3 months, 3 weeks ago

Selected Answer: A

"move" SQL srv db -> Azure M.I.
"migrate" SQL srv db -> Azure SQLDB

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Selected Answer: C

This time the question reads: "The company plans to _move_ the databases to Azure."
(in the previous similar question it said "migrate" )

And "move" to me means using backup-restore to re-host a database from one SQL Server to another.
That threw me off guard from otherwise preferring the SQL Server option.

So strictly interpreting "move" it should be A - SQL Server on VM

However, I anyhow don't think that is the intention, and so C

upvoted 1 times

**Ramye** 2 days, 20 hours ago

The previous question Q23 also said move and not migrate but that question has one more extra answer choice to choose from.

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Typo, I meant "preferring the SQL Database option"

upvoted 1 times

**sherifhamed** 3 months, 4 weeks ago

Selected Answer: C

C is the answer as Microsoft said
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#threat-modeling-start-simple

upvoted 1 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql
Azure SQL Database is a fully managed platform as a service (PaaS) database engine that handles most of the database management functions

such as upgrading, patching, backups, and monitoring without user involvement. Azure SQL Database is always running on the latest stable vers of the SQL Server database engine and patched OS with 99.99% availability. PaaS capabilities built into Azure SQL Database enable you to focus the domain-specific database administration and optimization activities that are critical for your business.

upvoted 2 times

**uffman** 8 months, 3 weeks ago

**Selected Answer: C**

Correct.

upvoted 2 times

Question #34 *Topic 3*

You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs), Azure Firewall, Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure.

What should you include in the recommendation?

A. the Azure landing zone accelerator

B. the Azure Well-Architected Framework

C. Azure Security Benchmark v3

D. Azure Advisor

**Correct Answer:** *A*

*Community vote distribution*

A (88%) 13%

**Murtuza** 1 week, 6 days ago

This question is directly about Azure Landing Zones and nothing else. It has nothing to do with The five pillars of the Azure Well-Architected Framework are reliability, cost optimization, operational excellence, performance efficiency, and security

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Selected Answer: B

Well-architected framework. Simply because it is never wrong and the other alternatives doesn't make any more sense (if any sense at all, such a (no info as to which accelerator would apply if any))

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: A

Confirmed: A is the answer.

upvoted 3 times

**sbnpj** 5 months, 1 week ago

Selected Answer: A

its A landing zone.

upvoted 2 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/app-platform/app-services/landing-zone-accelerator
The Azure App Service landing zone accelerator is an open-source collection of architectural guidance and reference implementation to accelera deployment of Azure App Service at scale. It can provide a specific architectural approach and reference implementation via infrastructure as co templates to prepare your landing zones. The landing zones adhere to the architecture and best practices of the Cloud Adoption Framework.

upvoted 2 times

**ConanBarb** 3 months, 3 weeks ago

The question doesnt mention App Service at all. On the contrary it mentions Bastion which hints at VMs being deployed

upvoted 1 times

**ilan0000** 8 months, 2 weeks ago

Correct
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/app-platform/app-services/landing-zone-accelerator

upvoted 1 times

**MaciekMT** 9 months ago

I believe it's A - the landing zone

upvoted 2 times

Question #35 *Topic 3*

Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.

What should you include in the recommendation?

A. custom roles in Azure Pipelines

B. branch policies in Azure Repos

C. Azure policies

D. custom Azure roles

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**cyber_sa** 3 months, 1 week ago

Selected Answer: B

got this in exam 6oct23. passed with 896 marks. I answered B

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/devops/repos/git/branch-policies-overview?view=azure-devops#adopt-a-git-branching-strategy
There are a few critical branches in your repo that the team relies on always being in good shape, such as your main branch.

Require pull requests to make any changes on these branches. Developers pushing changes directly to the protected branches will have their pushes rejected.

upvoted 3 times

**MaciekMT** 9 months ago

from ChatGPT: Based on the requirements of ensuring that all code changes are submitted through pull requests before being deployed by the CI/CD workflow and aligning with DevSecOps controls guidance, the recommended solution for ensuring this process is followed should be bra policies in Azure Repos.

Branch policies in Azure Repos provide a way to enforce code review policies before a pull request can be completed and merged into a target branch. This ensures that all code changes are submitted through a pull request and reviewed by other members of the team before being deployed by the CI/CD workflow.

Branch policies can be configured to require specific reviewers, require a minimum number of approvals, and block direct pushes to the target branch. This helps to ensure that code changes are thoroughly reviewed and meet the established standards before being merged into the targ branch.

Therefore, the correct answer is B) branch policies in Azure Repos.

upvoted 3 times

Question #36 *Topic 3*

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Your on-premises network contains firewalls that support forwarding event logs in the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls.

You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel.

What should you include in the recommendation?

A. an Azure logic app

B. an on-premises Syslog server

C. an on-premises data gateway

D. Azure Data Factory

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**ConanBarb** 3 months, 3 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-options
https://learn.microsoft.com/en-us/azure/sentinel/connect-common-event-format

upvoted 2 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: B

To ingest events from the firewalls into Microsoft Sentinel, you should include the following recommendation:

B. An on-premises Syslog server

Setting up an on-premises Syslog server is a common approach for collecting and forwarding logs from various devices, including firewalls, to a central location for further processing and analysis. You can configure the Syslog server to receive logs in the Common Event Format (CEF) from your firewalls and then forward those logs to your Microsoft Sentinel workspace. Microsoft Sentinel has built-in support for Syslog, making it a suitable choice for this scenario.

upvoted 3 times

**panda0107** 4 months, 1 week ago

https://learn.microsoft.com/en-us/azure/sentinel/connect-syslog

upvoted 1 times

**ca777** 5 months, 1 week ago

Correct answer

upvoted 1 times

**Victory007** 5 months, 1 week ago

Selected Answer: B

This server can receive the CEF logs from the firewalls and forward them to Microsoft Sentinel using the Syslog connector. This solution allows y to collect and analyze firewall logs in Microsoft Sentinel, even if there is no built-in connector for the firewalls. https://www.microsoft.com /insidetrack/blog/moving-to-next-generation-siem-at-microsoft-with-microsoft-azure-sentinel/

upvoted 1 times

Question #37 *Topic 3*

You have an on-premises datacenter and an Azure Kubernetes Service (AKS) cluster named AKS1.

You need to restrict internet access to the public endpoint of AKS1. The solution must ensure that AKS1 can be accessed only from the public IP addresses associated with the on-premises datacenter.

What should you use?

A. a private endpoint

B. a network security group (NSG)

C. a service endpoint

D. an authorized IP range

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**mohamed1999** 1 month, 1 week ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/aks/limit-egress-traffic

upvoted 1 times

**mohamed1999** 1 month, 1 week ago

Access to the AKS control plane can be protected by API server authorized IP ranges, including the firewall public frontend IP address

upvoted 1 times

**Intrudire** 2 months, 1 week ago

Selected Answer: D

"To secure access to the otherwise publicly accessible AKS control plane / API server, you can enable and use authorized IP ranges."
https://learn.microsoft.com/en-us/azure/aks/api-server-authorized-ip-ranges

upvoted 1 times

**TheCloudGuruu** 2 months, 1 week ago

Selected Answer: D

Using an authorized IP range provides the specific control needed for allowing access only from the designated public IP addresses associated v
the on-premises datacenter.

upvoted 1 times

**smanzana** 2 months, 4 weeks ago

B — NSG

upvoted 1 times

**Ramye** 2 days, 9 hours ago

NSG ties to a VNet. There's no reference to a VNet here.

upvoted 1 times

**shanti0091** 3 months, 1 week ago

Selected Answer: D

Correct answer is D - https://learn.microsoft.com/en-us/azure/aks/limit-egress-traffic

upvoted 2 times

Question #38 *Topic 3*

HOTSPOT
-

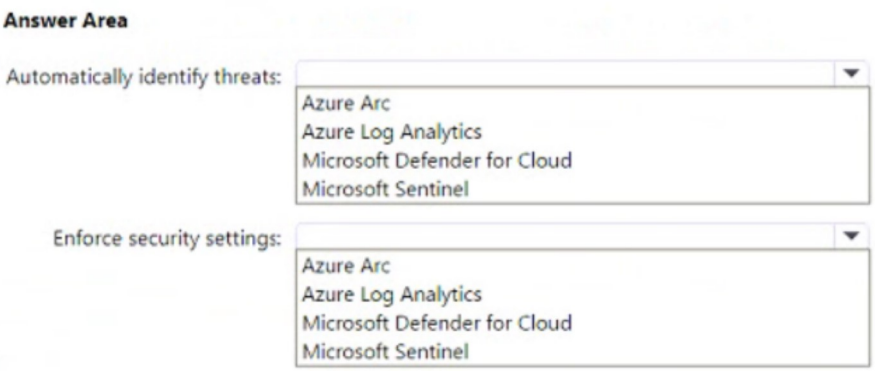
You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.

You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:

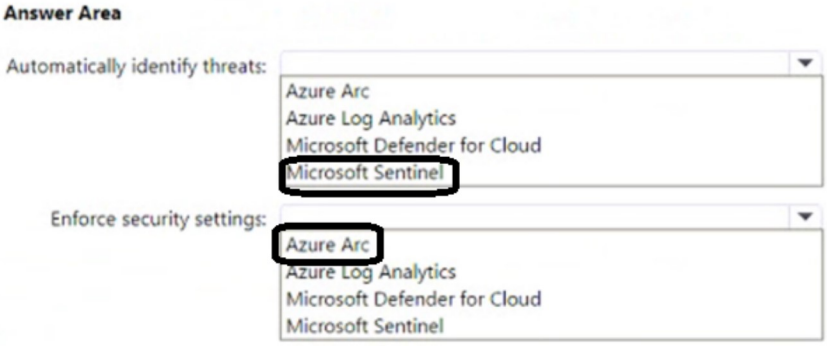
• Automatically identify threats found in AWS CloudTrail events.
• Enforce security settings on AWS virtual machines by using Azure policies.

What should you include in the solution for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**ricorosol** Highly Voted 2 months, 3 weeks ago
1. MS Defender for Cloud
2. Arc
upvoted 5 times

**Murtuza** Most Recent 1 week ago
Sentinel is the correct answer
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/announcing-the-enhanced-microsoft-sentinel-aws-cloudtrail/ba-p/3640884
upvoted 1 times

**mohamed1999** 1 month, 1 week ago
An event in CloudTrail is the record of an activity in an AWS account.
There for the given answer is correct
upvoted 1 times

**Igglepiggle** 3 months ago
Given answer is correct.

https://learn.microsoft.com/en-us/azure/sentinel/connect-aws?tabs=s3

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma
upvoted 3 times

Question #39 *Topic 3*

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux.

You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:

• Identify missing updates and insecure configurations.
• Use the Qualys engine.

What should you use?

A. Microsoft Defender for Servers

B. Microsoft Defender Threat Intelligence (Defender TI)

C. Microsoft Defender for Endpoint

D. Microsoft Defender External Attack Surface Management (Defender EASM)

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**Ramye** 2 days, 9 hours ago
Why not Microsoft Defender for Endpoint since we don't know if Linux machines are servers or not? Thx
upvoted 1 times

**Murtuza** 1 week, 6 days ago
Vulnerability assessment for machines allows you to select between two vulnerability assessment solutions:

Microsoft Defender Vulnerability Management
Microsoft Defender for Cloud integrated Qualys scanner
upvoted 2 times

**cyber_sa** 3 months, 1 week ago
Selected Answer: A
correct answer. MD for servers Plan2 fulfills the requirements
https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-servers-plan
upvoted 1 times

## Topic 4 - Question Set 4

Question #1 *Topic 4*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. app registrations in Azure Active Directory (Azure AD)

B. OAuth app policies in Microsoft Defender for Cloud Apps

C. Azure Security Benchmark compliance controls in Defender for Cloud

D. application control policies in Microsoft Defender for Endpoint

**Correct Answer:** *B*
Microsoft Defender for Cloud Apps OAuth app policies.
OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and
Salesforce. You're also able to mark these permissions as approved or banned. Marking them as banned will revoke permissions for each app for each user who authorized it.
Incorrect:
Not D: Windows Defender Application cannot be used for virtual machines.
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

*Community vote distribution*
D (92%) 8%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: D
This question has been updated on 8/3/22. Potential answers I'd expect to see are:
A. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Notice that only the wrong answers were changed. I'd vote D based on what I know about application control policies.

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create#windows-defender-application-control-policy-rules
upvoted 40 times

**PlumpyTumbler** 1 year, 4 months ago
My first link was for windows, this is a better resource for cloud based endpoint protection.
https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager#what-can-run-when-you-deploy-an-application-control-policy
upvoted 3 times

**rdy4u** Highly Voted 1 year, 3 months ago
The another answer for the same question is "adaptive application controls in Defender for Cloud"
upvoted 17 times

**Ramye** 2 days, 8 hours ago
Thx for this. That question is question #23 in Topic 2.
upvoted 1 times

**sherifhamed** Most Recent 3 months, 3 weeks ago

Selected Answer: D
To ensure that only authorized applications can run on the virtual machines and to block unauthorized applications automatically until an administrator authorizes them, you should recommend:

D. Application control policies in Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides application control policies that allow you to define which applications are allowed or blocked on you Windows machines. You can create rules specifying which applications are authorized to run, and any application that doesn't match these rules can be automatically blocked. This provides a strong layer of security and control over the applications running on your virtual machines.

upvoted 2 times

**AbdallaAM** 3 months, 4 weeks ago

**Selected Answer: D**

D. application control policies in Microsoft Defender for Endpoint - Microsoft Defender for Endpoint provides a feature known as "Application Control." By using application control policies, you can specify which applications are allowed to run on machines, and all other applications not the allowed list will be blocked. This feature directly meets the requirement described.

upvoted 1 times

**Maniact165** 8 months ago

**Selected Answer: D**

Its surely D

upvoted 2 times

**zellck** 8 months ago

**Selected Answer: D**

D is the answer.

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager
prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Applica Control doesn't have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy devices in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-ba protection of Application Control policies deployed through Configuration Manager can be enabled through group policy on capable hardware

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 2 times

**awssecuritynewbie** 10 months, 4 weeks ago

**Selected Answer: D**

for sure D. MDE can implement security application policy controls to prevent installation of an application.

upvoted 1 times

**dbhagz** 10 months, 4 weeks ago

**Selected Answer: D**

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

upvoted 1 times

**Mo22** 11 months, 1 week ago

**Selected Answer: D**

Microsoft Defender for Endpoint provides application control policies which allow administrators to define what applications are allowed to run virtual machines, and block any unauthorized applications from running. This helps to ensure that only authorized applications can run on the virtual machines and improve the overall security posture of the environment. If an unauthorized application attempts to run or be installed, it w be blocked automatically until an administrator authorizes the application.

upvoted 1 times

**examdog** 11 months, 2 weeks ago

**Selected Answer: D**

The link shows that Defender for EndPoint is available for virtual machines and is recommended to be used with Defender for Cloud.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint

upvoted 2 times

**[Removed]** 1 year ago

**Selected Answer: D**

"Application Control lets you strongly control what can run on devices you manage. This feature can be useful for devices in high-security departments, where it's vital that unwanted software can't run." Enable "Enforcement enabled" so that only trusted executables are allowed to r

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

upvoted 1 times

**Learner2022** 1 year, 1 month ago

**Selected Answer: B**

Defender for Endpoint does not include server licenses. D is incorrect.

upvoted 1 times

**Toschu** 9 months, 3 weeks ago

The product is called "Defender for Servers"
upvoted 1 times

**buguinha** 11 months ago
Defender for Endpoint can be installed on Server Platforms
upvoted 1 times

**TP447** 1 year, 1 month ago
Answer is Defender for Endpoint Server so D
upvoted 1 times

**ksksilva2022** 1 year, 1 month ago
Selected Answer: D
https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy
upvoted 1 times

**monkeybiznex** 1 year, 2 months ago
Oauth... LOL!
upvoted 2 times

**Granwizzard** 1 year, 4 months ago
Selected Answer: D
I agree with D.
We could also use: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/detect-block-potentially-unwanted-apps-microsoft-defender-antivirus?view=o365-worldwide

Microsoft Defender for Endpoint is my choice.
upvoted 2 times

**lummer** 1 year, 4 months ago
Certainly D.
https://docs.microsoft.com/en-us/defender-cloud-apps/governance-discovery#block-apps-with-defender-for-endpoint
upvoted 3 times

Question #2 *Topic 4*

Your company plans to provision blob storage by using an Azure Storage account. The blob storage will be accessible from 20 application servers on the internet.
You need to recommend a solution to ensure that only the application servers can access the storage account.
What should you recommend using to secure the blob storage?

A. managed rule sets in Azure Web Application Firewall (WAF) policies

B. inbound rules in network security groups (NSGs)

C. firewall rules for the storage account

D. inbound rules in Azure Firewall

E. service tags in network security groups (NSGs)

**Correct Answer:** *C*
Configure Azure Storage firewalls and virtual networks.
To secure your storage account, you should first configure a rule to deny access to traffic from all networks (including internet traffic) on the public endpoint, by default. Then, you should configure rules that grant access to traffic from specific VNets. You can also configure rules to grant access to traffic from selected public internet IP address ranges, enabling connections from specific internet or on-premises clients. This configuration enables you to build a secure network boundary for your applications.
Storage firewall rules apply to the public endpoint of a storage account. You don't need any firewall access rules to allow traffic for private endpoints of a storage account. The process of approving the creation of a private endpoint grants implicit access to traffic from the subnet that hosts the private endpoint.
Incorrect:
Not B: You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.
Not E: A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

*Community vote distribution*
C (100%)

**smanzana** 2 months, 4 weeks ago
C is ok
upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago
Selected Answer: C
To ensure that only the application servers can access the storage account, you should recommend:

C. Firewall rules for the storage account

Azure Blob Storage supports setting up firewall rules directly on the storage account. You can specify the IP addresses or ranges of your applicat servers to allow access while denying all other incoming traffic. This provides fine-grained control over who can access the storage account.
upvoted 1 times

**WRITER00347** 5 months ago
C. firewall rules for the storage account

You can configure the Azure Storage account firewall to allow traffic only from specific IP addresses or ranges, ensuring that only the designatec application servers can access the blob storage.
upvoted 1 times

**zellck** 8 months ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal
Turning on firewall rules for your storage account blocks incoming requests for data by default, unless the requests originate from a service that operates within an Azure virtual network or from allowed public IP addresses. Requests that are blocked include those from other Azure services from the Azure portal, and from logging and metrics services.

upvoted 1 times

**SelloLed** 1 year, 2 months ago

Selected Answer: C

answer is; C
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

upvoted 4 times

**JakeCallham** 1 year, 2 months ago

Selected Answer: C

I would go for C because the other options are eliminated. It doesnt mention seperate firewall

upvoted 3 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: C

https://docs.microsoft.com/en-us/azure/storage/common/configure-network-routing-preference?tabs=azure-portal#configure-the-routing-preference-for-the-default-public-endpoint

upvoted 4 times

Question #3 *Topic 4*

Your company is developing a modern application that will un as an Azure App Service web app.
You plan to perform threat modeling to identity potential security issues by using the Microsoft Threat Modeling Tool.
Which type of diagram should you create?

A. system flow

B. data flow

C. process flow

D. network flow

**Correct Answer:** *C*
Process flow diagrams are the result of a maturing threat modeling discipline. They genuinely allow incorporation of developers in the threat modeling process during the application design phase. This helps developers working within an Agile development methodology initially write secure code.
Application threat models use process-flow diagrams, representing the architectural point of view. Operational threat models are created from an attacker point of view based on DFDs. This approach allows for the integration of VAST into the organization's development and DevOps lifecycles.
Incorrect:
Not B: Data-flow diagrams are graphical representations of your system and should specify each element, their interactions and helpful context. Data-flow diagrams are made up of shapes that create graphical representations of your system. Each shape represents a unique function. Each interaction is analyzed to help you identify potential threats and ways to reduce risk.
Using shapes correctly allows you to receive better input from colleagues and security teams. Everyone will then understand how the system works. It can also help them avoid going through countless design documents and development plans to get them up and running.
Reference:
https://threatmodeler.com/data-flow-diagrams-process-flow-diagrams/ https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/1b-elements

*Community vote distribution*

B (93%) 7%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: B

The link provided in the explanation is a nice article but this is a Microsoft exam. The answers must come from Microsoft, using vendor terminology.
https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/1b-elements

upvoted 21 times

**rishiraval007** Most Recent 2 months, 2 weeks ago

For performing threat modeling for an application, especially when using the Microsoft Threat Modeling Tool, you should create:

B. Data Flow Diagram (DFD)

Data flow diagrams are the primary choice for threat modeling as they help in visualizing how data moves through the system, where it is stored and how it is processed. This allows you to identify potential security vulnerabilities related to data handling, access points, and data storage. The Microsoft Threat Modeling Tool is particularly geared towards analyzing data flow diagrams to identify potential threats.

upvoted 4 times

**ConanBarb** 3 months, 3 weeks ago

Selected Answer: B

Clearly B

The answer is in the motivation of ExamTopics own answer
Reference:
https://threatmodeler.com/data-flow-diagrams-process-flow-diagrams/
This is not a microsoft page. Something generic

https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/1b-elements
On this Microsoft page it is referred to as Data Flow.

And actually using and looking in the TM tool there is no thing as Process Flow or other. There is only "Data Flow" shapes

upvoted 3 times

**AbdallaAM** 3 months, 4 weeks ago

Selected Answer: B

A. system flow - This is not the typical terminology used in the Microsoft Threat Modeling Tool.

B. data flow - Correct Answer. DFDs (data flow diagrams) are commonly used in the Microsoft Threat Modeling Tool to understand how data mo and interacts within a system.

C. process flow - Process flow diagrams are more about defining the sequence of processes or activities but don't emphasize on how data move or is processed.

D. network flow - While network flow diagrams are useful for understanding network communication patterns, the Microsoft Threat Modeling To emphasizes on data flow diagrams for applications.

upvoted 1 times

**WRITER00347** 5 months ago

When using the Microsoft Threat Modeling Tool, the appropriate type of diagram to create for identifying potential security issues is:

B. data flow

A data flow diagram (DFD) allows you to visualize how data moves through an application, which is crucial in threat modeling to identify potent vulnerabilities and threats.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

upvoted 1 times

**SAMBIT** 11 months, 1 week ago

Selected Answer: B

A data-flow diagram is a way of representing a flow of data through a process or a system (usually an information system). The DFD also provid information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow — there are no decision rules and no loops. Specific operations based on the data can be represented by a flowchart.[1]

Data flow diagram with data storage, data flows, function and interface
Data flow diagram with data storage, data flows, function and interface

upvoted 3 times

**SofiaLorean** 11 months, 2 weeks ago

Answer should be "Data Flow" because Threat modelling techniques map the flow of data within your network and the different stages of a prospective cyber attack. The most popular Threat Modelling techniques are Data Flow Diagrams and Attack Trees.
Reference: https://www.upguard.com/blog/what-is-threat-modelling#:~:text=The%20most%20popular%20Threat%20Modelling%20techniques%20are%20Data,the%20flow%20of%20data%20through%2 n%20organization%27s%20network.

upvoted 1 times

**OrangeSG** 11 months, 3 weeks ago

Selected Answer: B

I have downloaded and tried Microsoft Threat Modelling Tool. It can only draw Data Flow Diagram (DFD).

Reference
Getting started with the Threat Modeling Tool
https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

upvoted 3 times

**TJ001** 1 year ago

Dataflow make sense as it is application/data flow

upvoted 2 times

**dc2k79** 1 year ago

C: Process Flow is the right answer.

upvoted 1 times

**piwiwiwiwiw** 1 year, 1 month ago

For me the critical difference between the data flow and process flow is that the process flow diagram incorporates developers into the process, and is aimed at developers rather than security professionals.
"Which type of diagram should you create? Process flow diagrams are the result of a maturing threat modeling discipline. They genuinely allow incorporation of developers in the threat modeling process during the application design phase"

upvoted 2 times

**Ahmed911** 1 year, 1 month ago

Selected Answer: B

Data Flow

Microsoft Threat Modeling Tool
The Microsoft Threat Modeling Tool makes threat modeling easier for all developers through a standard notation for visualizing system components, data flows, and security boundaries. It also helps threat modelers identify classes of threats they should consider based on the structure of their software design. We designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

upvoted 2 times

**Wedge34** 1 year, 2 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

upvoted 1 times

**SelloLed** 1 year, 2 months ago

Process flow diagrams (PFDs)
These are used by agile teams to build application threat models (ATMs). Agile software development teams can analyse their applications and features by critically examining the communication protocols used to connect the code's building blocks together.

upvoted 1 times

**darren888** 1 year, 3 months ago

Selected Answer: C

Process flow diagrams (PFDs)

These are used by agile teams to build application threat models (ATMs). Agile software development teams can analyse their applications and features by critically examining the communication protocols used to connect the code's building blocks together.
The question refers to applications
https://www.diagrams.net/blog/threat-modelling

upvoted 2 times

**Granwizzard** 1 year, 4 months ago

Selected Answer: B

If you note the URLs provided in the answer both points to data flow.
Building a model: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started#building-a-model

upvoted 2 times

Question #4 *Topic 4*

Your company has an on-premises network and an Azure subscription.
The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.
You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.
You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet- accessible endpoints to the on-premises network.
What should you include in the recommendation?

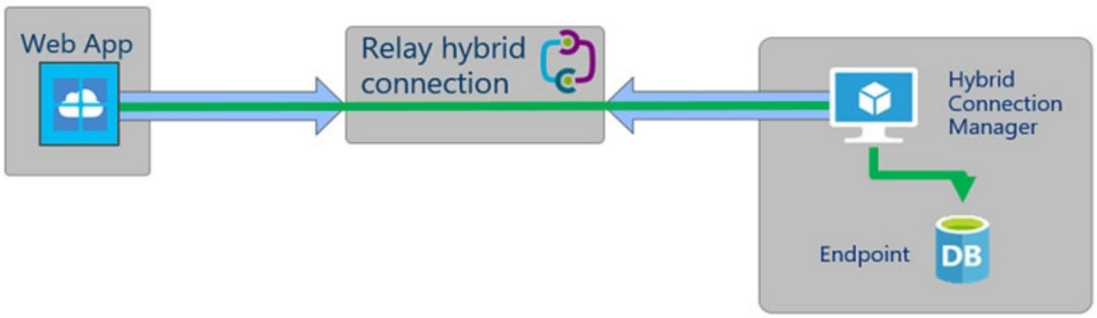
A. virtual network NAT gateway integration

B. hybrid connections

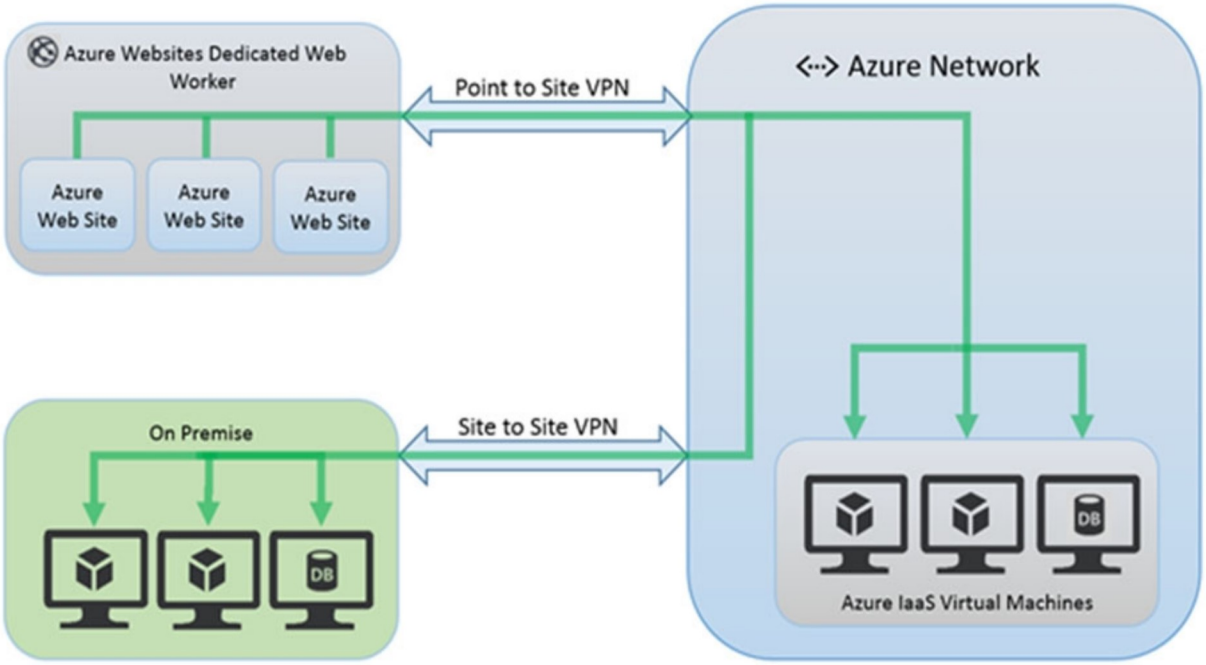
C. virtual network integration

D. a private endpoint

**Correct Answer:** *B*
Hybrid Connections can connect Azure App Service Web Apps to on-premises resources that use a static TCP port. Supported resources include Microsoft SQL
Server, MySQL, HTTP Web APIs, Mobile Services, and most custom Web Services.




Note: You can use an Azure App Service Hybrid Connections. To do this, you need to add and create Hybrid Connections in your app. You will download and install an agent (the Hybrid Connection Manager) in the database server or another server which is in the same network as the on-premise database.
You configure a logical connection on your app service or web app.
A small agent, the Hybrid Connection Manager, is downloaded and installed on a Windows Server (2012 or later) running in the remote network (on-premises or anywhere) that you need to communicate with.
You log into your Azure subscription in the Hybrid Connection manager and select the logical connection in your app service.
The Hybrid Connection Manager will initiate a secure tunnel out (TCP 80/443) to your app service in Azure.
Your app service can now communicate with TCP-based services, on Windows or Linux, in the remote network via the Hybrid Connection Manager.
You could get more details on how to Connect Azure Web Apps To On-Premises.
Incorrect:
Not A: NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway specifies which static IP addresses virtual machines use when creating outbound flows.
However, we need an inbound connection.
Not C: You can Azure web app service VNet integration with Azure VPN gateway to securely access the resource in an Azure VNet or on-premise network.
However, this would require a Site to Site VPN as in the picture below.




Note: Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network. The virtual network integration feature behaves differently when it's used with virtual networks in the same region and with virtual networks in other regions. The virtual network integration feature has two variations:
Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.
Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.
Reference:
https://github.com/uglide/azure-content/blob/master/articles/app-service-web/web-sites-hybrid-connection-connect-on-premises-sql-server.md https://docs.microsoft.com/en-us/answers/questions/701793/connecting-to-azure-app-to-onprem-datbase.html

*Community vote distribution*

B (88%) 13%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: B

Right answer. Link to official docs for reliable information.
https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

upvoted 16 times

**InformationOverload** 1 year, 4 months ago

Correct.

upvoted 1 times

**rishiraval007** Most Recent 2 months, 2 weeks ago

For allowing Azure App Service web apps to access Microsoft SQL Server databases on the on-premises network while minimizing the number c open internet-accessible endpoints, you should include in your recommendation:

B. Hybrid Connections

Hybrid Connections is a feature in Azure App Service that provides a way to access application resources in other networks. It uses a secure, outbound-only connection that doesn't require opening inbound ports to your on-premises network. This makes it a suitable choice for accessi on-premises databases without exposing additional internet-accessible endpoints.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

Within App Service, Hybrid Connections can be used to access application resources in any network that can make outbound calls to Azure over port 443. Hybrid Connections provides access from your app to a TCP endpoint and doesn't enable a new way to access your app. As used in App Service, each Hybrid Connection correlates to a single TCP host and port combination. This enables your apps to access resources on any OS, provided it's a TCP endpoint. The Hybrid Connections feature doesn't know or care what the application protocol is, or what you are accessing. It simply provides network access.

upvoted 1 times

**josh_josh** 10 months, 1 week ago

**Selected Answer: D**

The answer is D

upvoted 2 times

**Toschu** 9 months, 3 weeks ago

Not possible, because there is no VPN between Azure and the local network.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

**Selected Answer: D**

D. A private endpoint should be included in the recommendation.

Private endpoints provide secure access to Azure Services over a private endpoint in your virtual network. Using a private endpoint, you can access Azure services such as Azure Storage, Azure Cosmos DB, Azure SQL Database, and others over a private IP address in your virtual network. With a private endpoint, traffic between your virtual network and the Azure service travels over the Microsoft backbone network, eliminating exposure from the public internet.

In this scenario, using a private endpoint for the Microsoft SQL Server databases on the on-premises network would provide a secure connection between the web apps and the databases without requiring a Site-to-Site VPN or an ExpressRoute connection. This would minimize the number of open internet-accessible endpoints to the on-premises network, which would help enhance security.

upvoted 1 times

**atoon** 4 months, 2 weeks ago

That is not correct. Private Endpoint requires VPN/Expressrout:
https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview
The only correct answer is B.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

Hybrid connections could also be a valid option for allowing Azure App Service web apps to access on-premises databases without requiring a Site-to-Site VPN or an ExpressRoute connection.

Hybrid connections allow you to connect your Azure App Service web apps to on-premises resources securely. A hybrid connection consists of an Azure Relay service endpoint that is used to relay traffic between the App Service app and the on-premises resource.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

To use hybrid connections, you need to install an agent on a machine in your on-premises network that has access to the resource you want to connect to. The agent communicates with the Azure Relay service endpoint, enabling communication between the App Service app and the on-premises resource.

However, compared to private endpoints, hybrid connections can have some additional configuration overhead, require the installation of an agent on the on-premises network, and could add some additional network hops. Therefore, private endpoints are generally considered to be the preferred option for connecting Azure App Service web apps to on-premises resources.

upvoted 1 times

**JakeCallham** 1 year, 2 months ago

**Selected Answer: B**

Answer is the correct answer

https://learn.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections#how-it-works

upvoted 4 times

Question #5 *Topic 4*

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).
You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment.
What should you include during the application design phase?

A. software decomposition by using Microsoft Visual Studio Enterprise

B. dynamic application security testing (DAST) by using Veracode

C. threat modeling by using the Microsoft Threat Modeling Tool

D. static application security testing (SAST) by using SonarQube

**Correct Answer:** *C*
Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It's an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.
Incorrect:
Not B: Advantages of Veracode's DAST test solution
With a blackbox test tool from Veracode, you can:
Simulate the actions of an actual attacker to discover vulnerabilities not found by other testing techniques.
Run tests on applications developed in any language â€" JAVA/JSP, PHP and other engine-driven web applications.
Provide development and QA teams with a report on critical vulnerabilities along with information that lets them recreate the flaws.
Fix issues more quickly with detailed remediation information.
Develop long-term strategies for improving application security across your software portfolio using guidance and proactive recommendations from Veracode's expert.
Not D: SonarQube is a leading automatic code review tool to detect bugs, vulnerabilities and code smells in your code. Using Static Application Security Testing
(SAST) you can do an analysis of vulnerabilities in your code, also known as white-box testing to find about 50% of likely issues.
Reference:
https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

*Community vote distribution*
C (100%)

**prabhjot** Highly Voted 1 year, 4 months ago
100% correct
upvoted 12 times

**zellck** Most Recent 8 months ago
Selected Answer: C
C is the answer.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#plan-and-develop
Typically, modern development follows an agile development methodology. Scrum is one implementation of agile methodology that has every sprint start with a planning activity. Introducing security into this part of the development process should focus on:
- Threat modeling to view the application through the lens of a potential attacker
upvoted 1 times

**Ajdlfasudfo0** 10 months, 3 weeks ago
Selected Answer: C
https://learn.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle
upvoted 1 times

**awssecuritynewbie** 10 months, 4 weeks ago
Selected Answer: C
never would MS recommend a 3rd party tool so it would be C
upvoted 3 times

**TJ001** 1 year ago

Agree with C

upvoted 3 times

**ksksilva2022** 1 year, 1 month ago

**Selected Answer: C**

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

upvoted 3 times

**SelloLed** 1 year, 2 months ago

Answer= C

upvoted 2 times

Question #6 *Topic 4*

DRAG DROP -

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

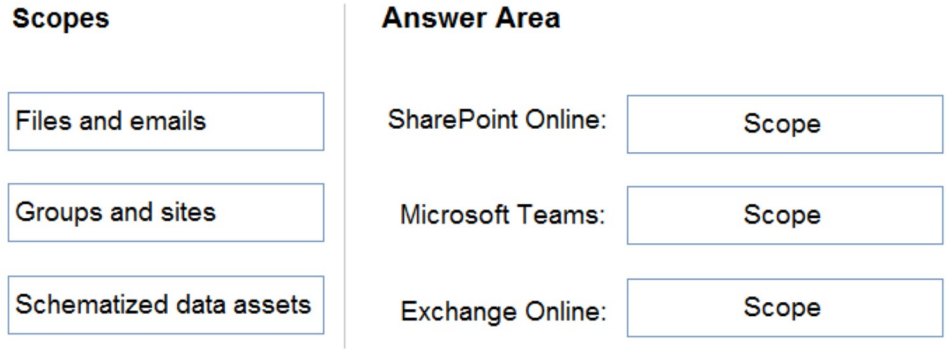
- Microsoft SharePoint Online
- Microsoft Exchange Online
- Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

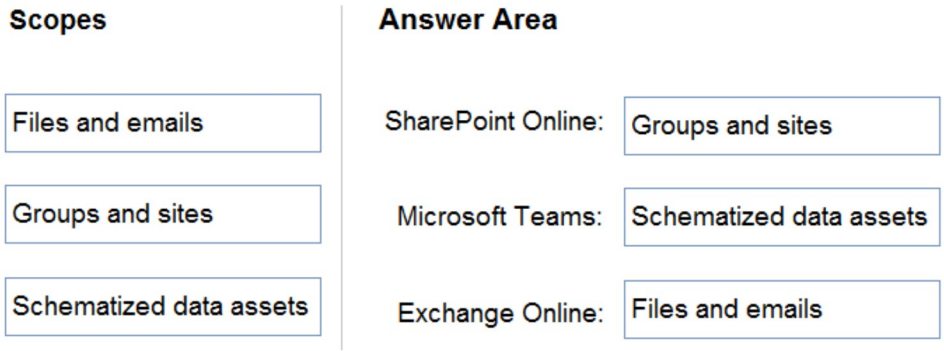
Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may only be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:




**Correct Answer:**




Box 1: Groups and sites -

SharePoint online handles sites.

Azure Active Directory (Azure AD) supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups. Sensitivity labels apply to group across services like Outlook, Microsoft Teams, and SharePoint.

Box 2: Schematized data assets -

Label travels with the data: The sensitivity labels created in Microsoft Purview Information Protection can also be extended to the Microsoft Purview Data Map,

SharePoint, Teams, Power BI, and SQL. When you apply a label on an office document and then scan it into the Microsoft Purview Data Map, the label will be applied to the data asset.

After you enable and configure sensitivity labels for containers, users can additionally see and apply sensitivity labels to Microsoft team sites, Microsoft 365 groups, and SharePoint sites.

Box 3: Files and emails -

Exchange Online handles files and emails.

Reference:

https://docs.microsoft.com/en-us/azure/purview/create-sensitivity-label https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

**Gar23** Highly Voted 1 year, 4 months ago

To me is group and sites for teams and sharepoint then for exchange file and emails

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide Go to label scopes

upvoted 56 times

**cdizzle** 1 year, 2 months ago

This caught me out because I didn't read in the question you could reuse the choices on the left. I thought each answer had to be unique. Thanks Gar!

upvoted 3 times

**SkippyTheMagnificent** 1 year, 4 months ago

Agreed. Great reference, thanks!

upvoted 3 times

**Granwizzard** Highly Voted 1 year, 4 months ago

It also seems that schematized data assets are also in preview, and it doesn't include the requirements.
Extend sensitivity labels to assets in Microsoft Purview Data Map: When you turn on this capability, currently in preview, you can apply your sensitivity labels to files and schematized data assets in Microsoft Purview Data Map. The schematized data assets include SQL, Azure SQL, Azur Synapse, Azure Cosmos, and AWS RDS.

I believe it should be:
- Groups and Sites
- Groups and Sites
- Files and emails

upvoted 19 times

**nieprotetkniteeetr** 12 months ago

You are correct!

upvoted 3 times

**Ramye** Most Recent 2 days, 7 hours ago

The key to answering this question is to know that these scopes are locations where data is stored:
⇨ Microsoft SharePoint Online
⇨ Microsoft Exchange Online
⇨ Microsoft Teams

Now: based on this the answer is:

⇨ Microsoft SharePoint Online - Files and emails. It can't be Groups and Sites because Groups and Sites do not apply to the data stored in that location.
⇨ Microsoft Exchange Online - Files and emails again data in the location
⇨ Microsoft Teams - Groups and Sites. This applies to the location including M365 Group.

upvoted 1 times

**sbnpj** 5 months, 1 week ago

it should be Groups and Sites,Groups and Sites and Files and Emails.

schematized data assets applies for sensitive info like SSN, Bank Account etc.
https://learn.microsoft.com/en-us/purview/how-to-automatically-label-your-content#autolabeling-for-schematized-data-assets

upvoted 3 times

**Kai7** 7 months, 3 weeks ago

It has to be
1) Files and Emails
2) Groups and Sites
3) Files and Emails
Assigning a label to a group or site does NOT label the files stored at the site, but only controls access to the site or group. The problem statem suggests data labelling rather than restricting access to sites/groups first and foremost.

upvoted 2 times

**Ramye** 2 days, 7 hours ago

I think you're correct.

upvoted 1 times

**zellck** 8 months ago

1. Groups and sites
2. Group and sites
3. File and emails

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-sensitivity-labels-can-do
After a sensitivity label is applied to an email, meeting invite, or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:
- Protect content in containers such as sites and groups when you enable the capability to use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites.

upvoted 2 times

**tester18128075** 9 months, 3 weeks ago

Groups and sites – used for teams and sharepoint
Schematized data assets : Used for SQL
Files and emails : Used for emails

upvoted 3 times

**Fal991l** 10 months, 1 week ago

For automatically labeling sensitive data in Microsoft SharePoint Online, Microsoft Exchange Online, and Microsoft Teams, the recommended sc for the sensitivity label policies should be:

For Microsoft SharePoint Online and Microsoft Exchange Online, the scope should be "Files and emails".
For Microsoft Teams, the scope should be "Groups and sites".

upvoted 1 times

**Fal991l** 10 months, 1 week ago

Explanation:

"Files and emails" scope is used for files and emails stored in SharePoint Online and Exchange Online, respectively. This scope will allow the sensitivity label policies to automatically classify and protect sensitive data in files and emails stored in these locations.
"Groups and sites" scope is used for Microsoft Teams. This scope will allow the sensitivity label policies to automatically classify and protect sensitive data in Teams channels and sites.
Since the question is asking about identifying and protecting sensitive data, "Schematized data assets" scope is not relevant here as it is usec for identifying sensitive data based on structured data, such as columns in a database table or Azure Data Factory.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

That's from ChatGPT

upvoted 1 times

**SofiaLorean** 11 months, 1 week ago

Groups & sites: To protect labled Teams, Microsoft 365 Group and Share Point sites
https://learn.microsoft.com/en-us/azure/purview/how-to-automatically-label-your-content
So, SharePoint Online - Groups and sites
Microsoft Teams - Groups and sites
Exchange Online - Files and Emails.

upvoted 4 times

**ad77** 11 months, 4 weeks ago

xtend sensitivity labels to assets in Microsoft Purview Data Map: When you turn on this capability, currently in preview, you can apply your sensitivity labels to files and schematized data assets in Microsoft Purview Data Map. The schematized data assets include SQL, Azure SQL, Azur Synapse, Azure Cosmos DB, and AWS RDS.

upvoted 1 times

**Fcnet** 1 year ago

instead of files and emails we should have items
-Items
-Groups & sites
-Schematized data assets
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

upvoted 1 times

**Fcnet** 1 year ago

Errors in the answer
Labels can be applied to files in storage such as Azure Data Lake or Azure Files as well as to schematized data such as columns in Azure SQL Database or Azure Cosmos DB.
Schematized data assets does not concern Teams nor Sharepoint
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
So
Teams : groups and sites
Sharepoint : groups and sites
Outlook : files and emails

upvoted 3 times

**rdy4u** 1 year, 3 months ago

It should on the latest test, like
Group and sites: Microsoft Teams and SharePoint Online
Items (previously named Files & emails) : Exchange Online
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

upvoted 6 times

**TBE** 9 months, 2 weeks ago

Correct.

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#label-scopes

upvoted 1 times

Question #7 *Topic 4*

Your company is developing a new Azure App Service web app.
You are providing design assistance to verify the security of the web app.
You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection.
What should you include in the recommendation?

A. dynamic application security testing (DAST)

B. static application security testing (SAST)

C. interactive application security testing (IAST)

D. runtime application self-protection (RASP)

**Correct Answer:** *A*
Dynamic application security testing (DAST) is a process of testing an application in an operating state to find security vulnerabilities. DAST tools analyze programs while they are executing to find security vulnerabilities such as memory corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.
Incorrect:
Not B: SAST tools analyze source code or compiled versions of code when the code is not executing in order to find security flaws.
Not C: IAST (interactive application security testing) analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity ג€interactingג€ with the application functionality.
IAST works inside the application, which makes it different from both static analysis (SAST) and dynamic analysis (DAST). This type of testing also doesn't test the entire application or codebase, but only whatever is exercised by the functional test.
Not D: Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application's internal data and state to enable it to identify threats at runtime that may have otherwise been overlooked by other security solutions.
RASP's focused monitoring makes it capable of detecting a wide range of threats, including zero-day attacks. Since RASP has insight into the internals of an application, it can detect behavioral changes that may have been caused by a novel attack. This enables it to respond to even zero-day attacks based upon how they affect the target application.
Reference:
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

*Community vote distribution*
A (92%) 8%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop#test-your-application-in-an-operating-state
upvoted 11 times

**tocane** Most Recent 1 week, 4 days ago
Selected Answer: C
Azure AD Conditional Access policies applies to users, not to applications. but the question is You need to recommend a solution to prevent use on a specific list of countries from connecting to the applications.
upvoted 1 times

**Ramye** 2 days, 6 hours ago
Where do you see this choice "You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications." in this question?
Could be mixing up with another question?
upvoted 1 times

**Ramye** 2 days, 6 hours ago
I just noticed you are referring to the next question,,,
upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago
To test the Azure App Service web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection, you should include in the recommendation:

A. Dynamic Application Security Testing (DAST)

DAST is a testing methodology that involves examining an application during its running state. It's particularly effective at identifying security vulnerabilities that are present when the application is in operation, such as the ones mentioned (insecure server configurations, XSS, SQL injection). DAST tools interact with the application from the outside, simulating an attacker's perspective, which makes them suitable for identify these types of vulnerabilities.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/security/develop/secure-develop#test-your-application-in-an-operating-state
Dynamic application security testing (DAST) is a process of testing an application in an operating state to find security vulnerabilities. DAST tools analyze programs while they are executing to find security vulnerabilities such as memory corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.

upvoted 1 times

**TJ001** 1 year ago

Perfect Answer A
Static for non running code
Dynamic for any running code(deployed in the infra) checks

upvoted 4 times

**Jacquesvz** 11 months, 1 week ago

100%, Well explained 😎👍

upvoted 1 times

Question #8 *Topic 4*

Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD).
You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications.
What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps

B. sign-in risk policies in Azure AD Identity Protection

C. Azure AD Conditional Access policies

D. device compliance policies in Microsoft Endpoint Manager

E. user risk poticies in Azure AD Identity Protection

**Correct Answer:** *A*
Microsoft Defender for Cloud Apps Activity policies.
Activity policies allow you to enforce a wide range of automated processes using the app provider's APIs. These policies enable you to monitor specific activities carried out by various users, or follow unexpectedly high rates of one certain type of activity.
After you set an activity detection policy, it starts to generate alerts - alerts are only generated on activities that occur after you create the policy.
Each policy is composed of the following parts:
Activity filters ג€" Enable you to create granular conditions based on metadata.
Activity match parameters ג€" Enable you to set a threshold for the number of times an activity repeats to be considered to match the policy.
Actions ג€" The policy provides a set of governance actions that can be automatically applied when violations are detected.
Incorrect:
Not C: Azure AD Conditional Access policies applies to users, not to applications.
Note: Blocking user logins by location can be an added layer of security to your environment. The following process will use Azure Active Directory conditional access to block access based on geographical location. For example, you are positive that nobody in your organization should be trying to login to select cloud applications from specific countries.
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/user-activity-policies https://cloudcompanyapps.com/2019/04/18/block-users-by-location-in-azure-o365/

*Community vote distribution*
C (94%) 6%

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: C
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location

https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules
upvoted 31 times

**Awake1969** Most Recent 1 month, 3 weeks ago
Selected Answer: C
AAD Conditional Access policies, w/Named Locations
upvoted 3 times

**sherifhamed** 3 months, 3 weeks ago
Selected Answer: C
To prevent users from specific countries from connecting to the applications accessed as custom enterprise applications in Azure AD, you should include the following recommendation:

C. Azure AD Conditional Access policies

Azure AD Conditional Access allows you to create policies that enforce access controls based on various conditions, including location-based conditions. You can create a Conditional Access policy that restricts access to these applications for users coming from specific countries or regi This ensures that only users from allowed countries can connect to the applications while blocking access for users from restricted countries.
upvoted 3 times

**theplaceholder** 3 months, 4 weeks ago

Selected Answer: C

100% C no doubt

upvoted 2 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview#common-signals
Common signals that Conditional Access can take in to account when making a policy decision include the following signals:
IP Location information
- Organizations can create trusted IP address ranges that can be used when making policy decisions.
- Administrators can specify entire countries/regions IP ranges to block or allow traffic from.

upvoted 3 times

**AssilAbdulrahim** 10 months, 3 weeks ago

It is worth noting that there is a BIG difference between AD Conditional Access which prevents users from signing in conditionally (but not connecting) and Cloud Apps Conditional Access App Control which prevents even connecting to the application.
"Conditional Access" is misleading here... I support A. Any support for my choice?

upvoted 1 times

**awssecuritynewbie** 10 months, 3 weeks ago

AD with conditional access will make sure you cannot access the resource if the condition-> location -> set to the specific country!
https://i.ytimg.com/vi/ySzLKylcpNA/maxresdefault.jpg

upvoted 1 times

**buguinha** 11 months ago

Selected Answer: C

Before going to Defender for Cloud Apps a CA policy is enough to allow or block access to an enterprise application. MDCA activity policy is not session policy and it always depend from a CA policy

upvoted 1 times

**killaK** 11 months, 2 weeks ago

Selected Answer: C

definitely C

upvoted 1 times

**TJ001** 1 year ago

Answer C

upvoted 1 times

**JYsmeng** 1 year ago

Selected Answer: C

Conditional Access should be the answer

upvoted 1 times

**inzza** 1 year, 3 months ago

This is conditional access

upvoted 1 times

**InformationOverload** 1 year, 4 months ago

Selected Answer: C

This is conditional access.

upvoted 3 times

**Gar23** 1 year, 4 months ago

Selected Answer: C

Definitely C

upvoted 3 times

**prabhjot** 1 year, 4 months ago

i also think it is C

upvoted 2 times

**tonuywildthing22** 1 year, 4 months ago

C Conditional Access

upvoted 2 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: A

https://docs.microsoft.com/en-us/defender-cloud-apps/policies-information-protection#detect-data-access-from-an-unauthorized-location

upvoted 3 times

**mikenyga** 1 year, 3 months ago

But need to prevent, not detect!
You can prevent with cloud apps ACCESS POLICY not ACTIVITY POLICY.
Answer CD is true.

upvoted 2 times

**SaadKhamis** 10 months, 3 weeks ago

Within the policy under "Governance actions", you can choose "Suspend user", Suspend the user from the application.
I'm not saying A is the correct answer.

upvoted 1 times

Question #9 *Topic 4*

Your company has an Azure subscription that uses Azure Storage.
The company plans to share specific blobs with vendors.
You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be time- limited.
What should you include in the recommendation?

A. Configure private link connections.

B. Configure encryption by using customer-managed keys (CMKs).

C. Share the connection string of the access key.

D. Create shared access signatures (SAS).

**Correct Answer:** *D*
A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:
What resources the client may access.
What permissions they have to those resources.
How long the SAS is valid.
Types of shared access signatures
Azure Storage supports three types of shared access signatures:

User delegation SAS -

Service SAS -

Account SAS -
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

*Community vote distribution*
D (94%) 6%

**TheMCT** Highly Voted 1 year, 4 months ago
Selected Answer: D
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview.
A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control o how a client can access your data. For example:
1. What resources the client may access.
2. What permissions they have to those resources.
3. How long the SAS is valid.
upvoted 8 times

**InformationOverload** Highly Voted 1 year, 4 months ago
Selected Answer: D
Time limited -> SAS
upvoted 7 times

**sherifhamed** Most Recent 3 months, 3 weeks ago
Selected Answer: D
To provide vendors with secure access to specific blobs without exposing the blobs publicly and ensuring that the access is time-limited, you should include the following recommendation:

D. Create shared access signatures (SAS)

Shared access signatures (SAS) are the ideal solution for granting limited, secure access to specific blobs in Azure Storage. With a SAS, you can specify the exact permissions (read, write, delete, etc.) the vendor should have, the start and expiration times for access, and even the specific bl or container they can access. This provides fine-grained control over access and ensures that it's time-limited and limited to specific resources.
upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview
A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control o
how a client can access your data. For example:
- What resources the client may access.
- What permissions they have to those resources.
- How long the SAS is valid.

upvoted 1 times

**init2winit** 9 months, 4 weeks ago

Should be Private Endpoint

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private
Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between th
clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposur
from the public internet.

upvoted 2 times

**janesb** 11 months, 2 weeks ago

Answer is A , please check the word exposing the blobs publicly

upvoted 1 times

**ad77** 11 months, 4 weeks ago

Selected Answer: A

q is: secure access to specific blobs without exposing the blobs publicly so:
sec recomendation is Use private endpoints
https://learn.microsoft.com/en-us/azure/storage/blobs/security-recommendations
recomendation is:
Create a virtual network and bastion host.
Create a virtual machine.
Create a storage account with a private endpoint.
Test connectivity to the storage account private endpoint.

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Wrong. and how will you address the condition that access must be time- limited??

upvoted 1 times

**inzza** 1 year, 3 months ago

Create shared access signatures

upvoted 3 times

Question #10 *Topic 4*

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app.
You need to recommend a solution to the application development team to secure the application from identity-related attacks.
Which two configurations should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure AD workbooks to monitor risk detections

B. Azure AD Conditional Access integration with user flows and custom policies

C. smart account lockout in Azure AD B2C

D. access packages in Identity Governance

E. custom resource owner password credentials (ROPC) flows in Azure AD B2C

**Correct Answer:** *BD*
B: Add Conditional Access to user flows in Azure Active Directory B2C
Conditional Access can be added to your Azure Active Directory B2C (Azure AD B2C) user flows or custom policies to manage risky sign-ins to your applications.
Azure Active Directory (Azure AD) Conditional Access is the tool used by Azure AD B2C to bring signals together, make decisions, and enforce organizational policies.
Not C: Credential attacks lead to unauthorized access to resources. Passwords that are set by users are required to be reasonably complex. Azure AD B2C has mitigation techniques in place for credential attacks. Mitigation includes detection of brute-force credential attacks and dictionary credential attacks. By using various signals, Azure Active Directory B2C (Azure AD B2C) analyzes the integrity of requests. Azure AD B2C is designed to intelligently differentiate intended users from hackers and botnets.
Incorrect:
Not D: Identity Governance though useful, does not address this specific scenario: to secure the application from identity-related attack in an Azure AD B2C environment.
Note: Identity Governance gives organizations the ability to do the following tasks across employees, business partners and vendors, and across services and applications both on-premises and in clouds:

Govern the identity lifecycle -

Govern access lifecycle -
Secure privileged access for administration
Specifically, it is intended to help organizations address these four key questions:
Which users should have access to which resources?
What are those users doing with that access?
Are there effective organizational controls for managing access?
Can auditors verify that the controls are working?
Note: An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package.
Not E: In Azure Active Directory B2C (Azure AD B2C), the resource owner password credentials (ROPC) flow is an OAuth standard authentication flow. In this flow, an application, also known as the relying party, exchanges valid credentials for tokens. The credentials include a user ID and password.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

*Community vote distribution*
BC (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: BC
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

upvoted 16 times

**CertShooter** Highly Voted 1 year ago

Selected Answer: BC

I recommend configuring Azure AD Conditional Access and using smart account lockout in Azure AD B2C.

Azure AD Conditional Access allows you to set policies that determine when and how users can access your application. By integrating Azure AD Conditional Access with user flows and custom policies, you can define rules that ensure only authenticated users can access the application, and you can also set up multifactor authentication for additional security.

Smart account lockout in Azure AD B2C is a feature that helps protect against brute-force attacks by temporarily locking out accounts after a certain number of failed login attempts. This can help prevent unauthorized access to the application by preventing attackers from guessing log credentials.

Options A, D, and E are not relevant to securing the application from identity-related attacks. Option A involves monitoring risk detections, whic not directly related to securing the application. Option D involves access packages in Identity Governance, which is not related to the security of the application. Option E involves custom ROPC flows, which are not relevant to securing the application from identity-related attacks.

upvoted 9 times

**tocane** Most Recent 1 week, 4 days ago

Selected Answer: BC

it should be BC

upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago

To secure the invoicing application that will use Azure Active Directory (Azure AD) B2C from identity-related attacks, the two configurations to recommend are:

B. Azure AD Conditional Access integration with user flows and custom policies: Conditional Access in Azure AD B2C allows you to create and enforce access policies based on various conditions, such as user location, device state, and more. Integrating these policies with user flows and custom policies in Azure AD B2C can enhance the security of the application by ensuring that only authenticated and authorized users can acces under specific conditions.

C. Smart account lockout in Azure AD B2C: The smart account lockout feature in Azure AD B2C helps protect user accounts from brute force attacks. It intelligently locks out accounts when suspicious activities are detected, such as repeated failed sign-in attempts, without affecting legitimate users.

upvoted 2 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: BC

repeated question#24. Answers are BC. explanation can be found in Q#24

upvoted 3 times

**Ramye** 2 days, 6 hours ago

Exactly - they have different answers to the same question. They need to fix it...

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: BC

To secure your application from identity-related attacks when using Azure AD B2C for authentication, you should recommend the following configurations:

B. Azure AD Conditional Access integration with user flows and custom policies: Azure AD Conditional Access allows you to define policies to control access to your application based on specific conditions, such as risk detections or user behavior. Integrating Azure AD Conditional Acces with user flows and custom policies provides additional layers of security to your application's authentication process.

C. Smart account lockout in Azure AD B2C: Smart account lockout policies help protect user accounts from brute-force attacks or suspicious log attempts. When you configure smart account lockout policies in Azure AD B2C, you can define conditions under which accounts are locked or require additional verification, enhancing security.

upvoted 2 times

**zellck** 8 months ago

Selected Answer: BC

BC is the answer.

https://learn.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow
Conditional Access can be added to your Azure Active Directory B2C (Azure AD B2C) user flows or custom policies to manage risky sign-ins to y applications. Azure Active Directory (Azure AD) Conditional Access is the tool used by Azure AD B2C to bring signals together, make decisions, a enforce organizational policies.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/active-directory-b2c/threat-management#how-smart-lockout-works

Azure AD B2C uses a sophisticated strategy to lock accounts. The accounts are locked based on the IP of the request and the passwords entered. The duration of the lockout also increases based on the likelihood that it's an attack. After a password is tried 10 times unsuccessfull (the default attempt threshold), a one-minute lockout occurs. The next time a login is unsuccessful after the account is unlocked (that is, afte the account has been automatically unlocked by the service once the lockout period expires), another one-minute lockout occurs and contin for each unsuccessful login. Entering the same, or similar password repeatedly doesn't count as multiple unsuccessful logins.

upvoted 1 times

**Mo22** 11 months, 1 week ago

Selected Answer: BC

B. Azure AD Conditional Access integration with user flows and custom policies
C. Smart account lockout in Azure AD B2C.

Conditional Access in Azure Active Directory (Azure AD) is a feature that enables you to enforce security policies and control access to applicatic based on specific conditions,

upvoted 2 times

**TJ001** 1 year ago

will go for B and C . have not seen a reference telling Entitlement Mgmt can be used in B2C ..It is available for B2B though

upvoted 2 times

**Learing** 1 year, 2 months ago

Selected Answer: BC

Azure B2C does not support Identity Governance Entitlement management

upvoted 6 times

**InformationOverload** 1 year, 4 months ago

Selected Answer: BC

i go with B and C here

upvoted 7 times

**prabhjot** 1 year, 4 months ago

Identity Governance is the correct selection over all it seems the ans is correct

upvoted 2 times

**prabhjot** 1 year, 4 months ago

B&C is more relevant

upvoted 1 times

**JaySapkota** 1 year, 4 months ago

Selected Answer: BC

Would say B & C

upvoted 2 times

**[Removed]** 1 year, 4 months ago

Am i the only one who sees the stated answer as BD then in the description it says 'Not D'?

upvoted 5 times

**Paimon** 1 year, 1 month ago

It's happens more than you might think.....

upvoted 1 times

**PlumpyTumbler** 1 year, 4 months ago

That's right, it says "Not D: Identity Governance though useful, does not address this specific scenario" Also all documentation of access packages with Identity Governance specifies B2B. Whether it's a learning module or a reference document, B2C is never mentioned. This question is about B2C.

https://docs.microsoft.com/en-us/learn/modules/plan-implement-entitlement-management/2-define-access-packages

upvoted 2 times

Question #11 *Topic 4*

Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating.
The company identifies protected health information (PHI) within stored documents and communications.
What should you recommend using to prevent the PHI from being shared outside the company?

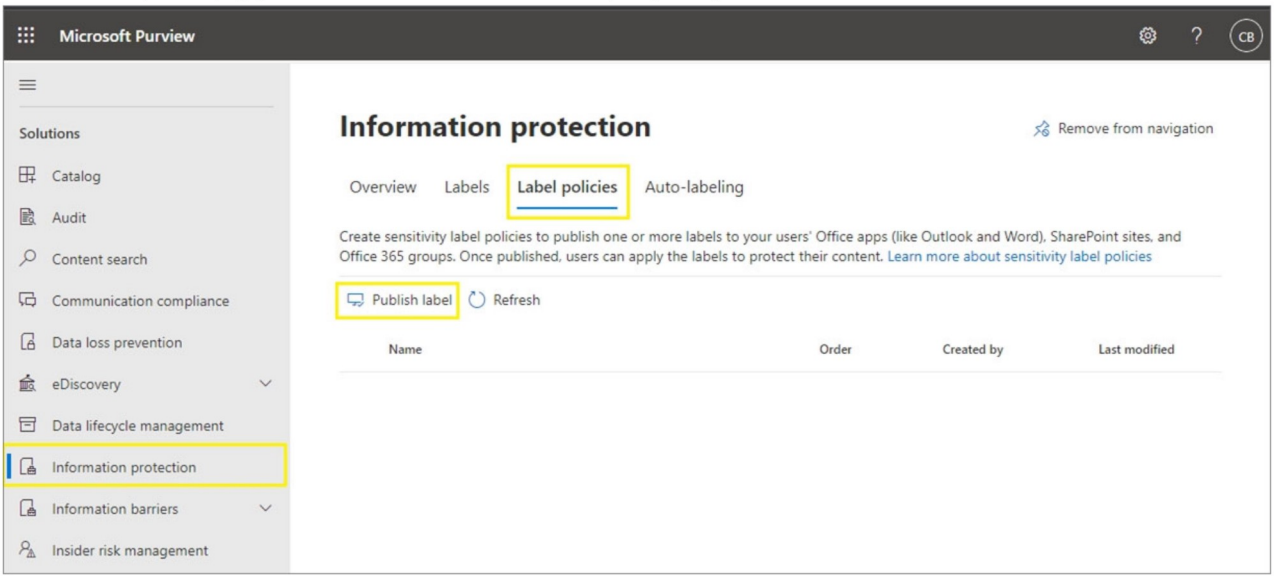
A. sensitivity label policies

B. data loss prevention (DLP) policies

C. insider risk management policies

D. retention policies

**Correct Answer:** *A*
What sensitivity labels can do -
After a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:
* Protect content in containers such as sites and groups when you enable the capability to use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and
SharePoint sites.
* Encrypt emails and documents to prevent unauthorized people from accessing this data. You can additionally choose which users or group have permissions to perform which actions and for how long. For example, you can choose to allow all users in your organization to modify a document while a specific group in another organization can only view it. Alternatively, instead of administrator-defined permissions, you can allow your users to assign permissions to the content when they apply the label.
* Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied. Watermarks can be applied to documents but not email.
* Etc.
Note: Publish sensitivity labels by creating a label policy
1. From the Microsoft Purview compliance portal, select Solutions > Information protection > Label policies
2. On the Label policies page, select Publish label to start the Create policy configuration:




3. On the Choose sensitivity labels to publish page, select the Choose sensitivity labels to publish link. Select the labels that you want to make available in apps and to services, and then select Add.
4. Etc.
Incorrect:
Not B: In this scenario the company itself has identified the sensitive information. This means that sensitive labels are enough, and there is no need for Data loss prevention (DLP) polices.
Note: With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.
Note: Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification

with sensitivity and retention labels.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels https://docs.microsoft.com/en-us/security/compass/information-protection-and-storage-capabilities https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide#publish-sensitivity-labels-by-creating-a-label-policy

*Community vote distribution*

B (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: B

Sensitivity labels classify PHI. DLP uses those labels to prevent it from leaving the protected environment.

upvoted 33 times

**Ramye** Most Recent 2 days, 4 hours ago

DLP all the way.
When you create Labels under DLP you can configure them not to share with people outside of the company.

upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago

To prevent Protected Health Information (PHI) from being shared outside the company, particularly within Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive, you should recommend using:

B. Data Loss Prevention (DLP) policies

Data Loss Prevention policies in Microsoft 365 can help you identify and protect sensitive information like PHI across various applications. These policies can be configured to detect when PHI is being shared and take appropriate actions, such as blocking the sharing or notifying administrators. DLP policies are specifically designed to prevent the accidental or intentional leakage of sensitive data.

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: B

To prevent protected health information (PHI) from being shared outside the company in a Microsoft 365 E5 environment, you should recomme

B. Data Loss Prevention (DLP) policies

Data Loss Prevention policies in Microsoft 365 are specifically designed to prevent sensitive information, such as PHI, from being shared or leake outside the organization. You can create DLP policies that scan content in Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive, a then take actions like blocking sharing, encrypting emails, or notifying administrators when a policy violation occurs. This helps ensure that PHI i handled in accordance with compliance and security requirements.

Sensitivity label policies (option A) can be used to classify and protect documents, but they may not provide the same level of control over data sharing as DLP policies.

upvoted 1 times

**dememere** 7 months, 3 weeks ago

B" should be the answer (DLP policies)

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide
Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or soci security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, a automatically protect sensitive items across:
- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive accounts

upvoted 1 times

**examdog** 11 months, 2 weeks ago

Selected Answer: B

The sensitivity label policy is about who has access and how to access the files. DLP is about whether files can be shared and how they are share

upvoted 3 times

**nieprotetkniteeetr** 12 months ago

Sensitivity labels can be scoped to enforce encryption on domain scope so it's enough.

upvoted 1 times

**TJ001** 1 year ago

DLP sounds correct

upvoted 1 times

**[Removed]** 1 year ago

Selected Answer: B

ABsolutely B. Labels simply categorise, they do not prevent labelled data from being shared. Only DLP policies makes that possible.

upvoted 3 times

**CertShooter** 1 year ago

Selected Answer: B

I recommend using data loss prevention (DLP) policies to prevent protected health information (PHI) from being shared outside the company.

DLP policies in Microsoft 365 allow you to identify, monitor, and protect sensitive information, such as PHI, within your organization. You can cre DLP policies that identify PHI within stored documents and communications and then set rules to prevent the PHI from being shared outside th company. For example, you can create a DLP policy that blocks emails containing PHI from being sent to external recipients, or that prevents documents containing PHI from being shared outside the organization.

Sensitivity label policies allow you to classify and protect sensitive information, but they do not specifically prevent the information from being shared outside the organization. Insider risk management policies are designed to detect and mitigate risks posed by insider threats, but they a not directly related to preventing the sharing of sensitive information. Retention policies allow you to specify how long certain types of informat should be retained, but they do not prevent the sharing of sensitive information.

upvoted 4 times

**mshefiq** 1 year, 2 months ago

DLP is the right answer

upvoted 1 times

**Banzaaai** 1 year, 3 months ago

Selected Answer: B

B. data loss prevention (DLP) policies Most Voted

because PREVENT ..

upvoted 1 times

**InformationOverload** 1 year, 4 months ago

Selected Answer: B

DLP policies

upvoted 4 times

**lummer** 1 year, 4 months ago

It is certainly DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

upvoted 2 times

**JaySapkota** 1 year, 4 months ago

Selected Answer: B

DLP is the correct Answer

upvoted 4 times

**JaySapkota** 1 year, 4 months ago

DLP Policies

upvoted 2 times

Question #12 *Topic 4*

Your company has a Microsoft 365 E5 subscription.
The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online.
You need to recommend a solution to identify documents that contain sensitive information.
What should you include in the recommendation?

A. data classification content explorer

B. data loss prevention (DLP)

C. eDiscovery

D. Information Governance

**Correct Answer:** *B*
Data loss prevention (DLP)
With DLP policies, you can identify, monitor, and automatically protect sensitive information across Office 365. Data loss prevention policies can use sensitivity labels and sensitive information types to identify sensitive information.
Note: Microsoft 365 includes many sensitive information types that are ready for you to use in DLP policies and for automatic classification with sensitivity and retention labels.
Incorrect:
Not A: Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.
Reference:
https://docs.microsoft.com/en-us/security/compass/information-protection-and-storage-capabilities https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer

*Community vote distribution*
A (74%) B (26%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: A
If you have a subscription, go to https://compliance.microsoft.com/dataclassification?viewid=contentexplorer
upvoted 15 times

**3peat** 2 months, 4 weeks ago
DLP falls under solutions in Purview. The answer is B. Content Explorer is just for you to check whether your tenant or environment if it's complying with the policies you have.
upvoted 1 times

**SkippyTheMagnificent** Highly Voted 1 year, 4 months ago
Selected Answer: A
I believe the correct answer is A.
https://docs.microsoft.com/en-us/learn/modules/implement-data-classification-of-sensitive-information/6-view-sensitive-data-content-explore activity-explorer

"Content explorer. This tab provides visibility into the amount and types of sensitive data in an organization. It also enables users to filter by labe or sensitivity type. Doing so displays a detailed view of locations where the sensitive data is stored. It provides admins with the ability to:
index the sensitive documents that are stored within supported Microsoft 365 workloads.
identify the sensitive information they're storing."
upvoted 10 times

**mynk29** 12 months ago
Yes but question is identify the sensitive information not display/review it.

https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer?view=o365-worldwide#sensitive-informati types

"If you know the name of the label, or the sensitive information type, you can type that into the filter box.
Alternately, you can browse for the item by expanding the label type and selecting the label from the list."

DLP policies identifies the data.
upvoted 5 times

**D3D1997** 11 months, 1 week ago

https://learn.microsoft.com/en-us/microsoft-365/compliance/form-a-query-to-find-sensitive-data-stored-on-sites?view=o365-worldwide
With Microsoft Purview Data Loss Prevention (DLP) in SharePoint Online, you can discover documents that contain sensitive data through your tenant

upvoted 2 times

**Ramye** Most Recent 2 days, 4 hours ago

It is Content Explorer- checked in Purview. Wish I should share an image

upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago

For identifying and classifying data, particularly in Microsoft Teams, SharePoint Online, and Exchange Online, you should recommend using:

A. Data Classification Content Explorer

Data Classification Content Explorer is part of the Microsoft 365 compliance center. It allows you to discover, classify, and label content across yo organization's data landscape. It can help you find documents that contain sensitive information by scanning and classifying content based on t sensitivity labels or information types you've defined.

upvoted 2 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: A

got this in exam 6oct23. passed with 896 marks. I answered A

upvoted 3 times

**Ramye** 2 days, 4 hours ago

Thx for sharing. A is the answer

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

To identify and classify documents containing sensitive information in Microsoft Teams, SharePoint Online, and Exchange Online within a Micros 365 E5 subscription, you should recommend:

B. Data Loss Prevention (DLP)

Data Loss Prevention policies allow you to define rules and conditions to automatically identify and classify sensitive information. You can create custom DLP policies that scan content in Microsoft Teams, SharePoint Online, and Exchange Online for specific sensitive data types (such as crec card numbers, Social Security numbers, or custom-defined data) and take actions like blocking, notifying, or encrypting messages or documents when policy violations occur.

Options A, C, and D are not primarily focused on identifying and classifying documents with sensitive information

upvoted 3 times

**sbnpj** 5 months ago

Selected Answer: B

I believe its B, because questions says "you need to recommend a solution to identify documents that contain sensitive information." and DLP policies are used to identify sensitive content across office365.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer?view=o365-worldwide#content-explorer
Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.

upvoted 1 times

**Rocko1** 10 months, 1 week ago

Selected Answer: B

DLP helps prevent data leakage by monitoring and preventing the sharing of sensitive data. DLP policies can be set up to identify sensitive data such as credit card numbers, social security numbers, or other confidential information. You can use DLP to classify and protect data in Microsof Teams, SharePoint Online, and Exchange Online

upvoted 1 times

**AJ2021** 10 months, 1 week ago

Selected Answer: B

A would only be correct if you want to Identify only, read the question "identify and classify " !!
B is correct in this case

upvoted 2 times

**AJ2021** 10 months, 1 week ago

Cancel that or even delete my comment, I need to listen to my own advise, the follow on sentence overules the "identify and classify", so yes

A lol
upvoted 1 times

**Fal991l** 10 months, 1 week ago

Selected Answer: B

ChatGPT: The recommended solution to identify documents that contain sensitive information in Microsoft Teams, SharePoint Online, and Exchange Online is to use Data Loss Prevention (DLP).

DLP in Microsoft 365 allows you to create policies that identify and protect sensitive information types such as credit card numbers, social securi numbers, and other confidential data types. You can use DLP policies to scan content in Teams, SharePoint Online, and Exchange Online for sensitive information types, and take appropriate actions to protect the information.

Therefore, the recommended solution to identify documents that contain sensitive information is to use Data Loss Prevention (DLP) in Microsoft 365.
upvoted 2 times

**MrMozz** 10 months, 3 weeks ago

From below, A is the right answer, "A DLP policy can help protect sensitive information" but "Content explorer shows a current snapshot of the items"
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer?view=o365-worldwide#content-explorer
Content explorer
Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.

Sensitive information types
A DLP policy can help protect sensitive information, which is defined as a sensitive information type. Microsoft 365 includes definitions for many common sensitive information types from across many different regions that are ready for you to use. For example, a credit card number, bank account numbers, and national ID numbers.
upvoted 1 times

**Mo22** 11 months, 1 week ago

Selected Answer: A

While Data Classification Content Explorer can help you identify sensitive information in your content, it does not automatically protect or preve this information from being shared outside of your organization. For that purpose, you would also need to implement Data Loss Prevention (DL policies.
upvoted 2 times

**Tippy** 10 months, 3 weeks ago

Question says "Identify"
upvoted 2 times

**D3D1997** 11 months, 1 week ago

Selected Answer: B

"h Microsoft Purview Data Loss Prevention (DLP) in SharePoint Online, you can discover documents that contain sensitive data throughout your tenant"
https://learn.microsoft.com/en-us/microsoft-365/compliance/form-a-query-to-find-sensitive-data-stored-on-sites?view=o365-worldwide
upvoted 2 times

**Phantasm** 11 months, 1 week ago

My final answer is A and B: data classification content explorer and data loss prevention (DLP). Both solutions allow you to identify documents th contain sensitive information, and the specific solution that you recommend might depend on the specific requirements and constraints of the company.

If I had to choose only one, I would recommend data loss prevention (DLP), as it provides a comprehensive set of tools for identifying, monitorir and protecting sensitive data across an organization's networks and cloud services, including Microsoft Teams, SharePoint Online, and Exchange Online.

So this case: B 99999999999999999999999-n%
upvoted 2 times

**examdog** 11 months, 2 weeks ago

Selected Answer: B

I chose B. Data Classification is not a full-fledged solution. It is a tool for other solutions. DLP is a solution and is listed under Solutions menu at Purview portal.
upvoted 2 times

**OrangeSG** 11 months, 3 weeks ago

Selected Answer: A

Information protection solution with Microsoft Purview has 3 parts:
• Know your data
• Protect your data
• Prevent data loss

The requirement “identify documents that contain sensitive information.” Is related to Know your data, so IA would go for A. data classification

content explorer.

Data Classification Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified sensitive information type in your organization.

Reference
Deploy an information protection solution with Microsoft Purview
https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection-solution

upvoted 5 times

Question #13 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend configuring gateway-required virtual network integration.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.
Incorrect:
Virtual Network (VNet) integration for an Azure service enables you to lock down access to the service to only your virtual network infrastructure. The VNet infrastructure also includes peered virtual networks and on-premises networks.
VNet integration provides Azure services the benefits of network isolation and can be accomplished by one or more of the following methods:
Deploying dedicated instances of the service into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
Using Private Endpoint that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your
VNet, effectively bringing the service into your virtual network.
Accessing the service using public endpoints by extending a virtual network to the service, through service endpoints. Service endpoints allow service resources to be secured to the virtual network.
Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services

*Community vote distribution*
B (100%)

**Ramye** 2 days, 4 hours ago
This is the repeat question - remember the answer would be that is tied with Header or Service Tag
upvoted 1 times

**zellck** 8 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t
Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.
upvoted 1 times

**InformationOverload** 1 year, 4 months ago
Selected Answer: B
user service tags
upvoted 2 times

**PlumpyTumbler** 1 year, 4 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure-front-door-instance

upvoted 3 times

Question #14 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions that allow traffic from the Front Door service tags.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services

*Community vote distribution*
B (60%) A (40%)

**emiliocb4** Highly Voted 1 year, 3 months ago
Selected Answer: B
if you want to block the access to A SPECIFIC front door instance the answer is B... if you want to block to any front door instance is A.... i will go B in this case
upvoted 10 times

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: A
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure-front-door-instance
upvoted 9 times

**mikenyga** 1 year, 4 months ago
Why A? Access Front Door instance, not any Front Door.
Filter by http header : X-Azure-FDID
upvoted 6 times

**Gurulee** 10 months, 1 week ago
Agreed
upvoted 1 times

**Learing** 1 year, 2 months ago
You actually need both, as headers can be set freely by whoever is calling
upvoted 1 times

**TJ001** 1 year ago
It is combination of service tag and X-Azure-FDID header so this is a case where both are needed. It is explicitly mentioned in the link ( use together)
https://learn.microsoft.com/en-us/azure/frontdoor/origin-security?tabs=app-service-functions&pivots=front-door-standard-premium#public-ip-address-based-origins
upvoted 2 times

**Murtuza** Most Recent 1 week, 1 day ago
Selected Answer: B
Answer is correct: B
upvoted 1 times

**calotta1** 4 months, 3 weeks ago

Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t
Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you'll need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

I'd say B

https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli#restrict-access-to-a-specific-azure-front-door-instance

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t
Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.

upvoted 1 times

**uffman** 8 months, 3 weeks ago

Selected Answer: B

Restricting using service tag is not enough, see https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-a-specific-azure-front-door-instance

upvoted 3 times

**smudo1965** 10 months ago

Selected Answer: A

Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t
Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you'll need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

upvoted 1 times

**Gurulee** 10 months, 1 week ago

Selected Answer: B

Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you'll need to further filter the incoming requests based on the unique http header that Azure Front Door sends.

upvoted 2 times

**Gurulee** 10 months, 1 week ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli#restrict-access-to-a-specific-azure-front-door-instance

upvoted 2 times

**AzureJobsTillRetire** 10 months, 3 weeks ago

Selected Answer: B

There are at least three front door service tags. The question is not specific, and it cannot be true.
AzureFrontDoor.Frontend
AzureFrontDoor.Backend
AzureFrontDoor.FirstParty
https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview

upvoted 2 times

**hamshoo** 1 year, 1 month ago

Selected Answer: B

Restricting using service tag is not enough as mentioned below. the answer is correct

https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure-front-door-instance

upvoted 3 times

**JakeCallham** 1 year, 2 months ago

Guys Http headers is correct and service tags is correct. Please look it up before claiming headers is wrong.

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-front-door-

upvoted 3 times

**darkpangel** 1 year, 3 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions

upvoted 2 times

**inzza** 1 year, 3 months ago

Answer is A

upvoted 1 times

**d3an** 1 year, 3 months ago

Selected Answer: B

HTTP header required to restrict to the specific Front Door instance(s).

upvoted 3 times

**darren888** 1 year, 4 months ago

B is correct
To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http heade
that Azure Front Door sends. The app service would qualify as a specific instance the service tag is not enough

upvoted 3 times

**InformationOverload** 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 2 times

Question #15 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
Restrict access to a specific Azure Front Door instance
Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions

*Community vote distribution*
A (73%) B (27%)

**lummer** Highly Voted 1 year, 4 months ago
Answer is correct: A.
Azure Front Door is a globally distributed multi-tenant service. So, the infrastructure for Front Door is shared across all its customers. to ensure t your specific tenant is sending the data you need a HTTP Header with the ID of your Frontdoor tenant. The service tag alone will allow any frontdoor tenant to contact your web app.
upvoted 15 times

**Granwizzard** Highly Voted 1 year, 4 months ago
Selected Answer: A
We can use both Service Tags or headers with the FDID.

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-front-door-
upvoted 9 times

**Murtuza** Most Recent 1 week, 1 day ago
Selected Answer: A
Answer is correct: A.
upvoted 1 times

**zellck** 8 months ago
Selected Answer: A
A is the answer.

https://learn.microsoft.com/en-us/azure/app-service/overview-access-restrictions#restrict-access-to-a-specific-azure-front-door-instance
Traffic from Azure Front Door to your application originates from a well known set of IP ranges defined in the AzureFrontDoor.Backend service t Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front Door. To ensure traffic only originates from your specific instance, you need to further filter the incoming requests based on the unique http header that Azure Front Door sends called X-Azure-FDID. You can find the Front Door ID in the portal.
upvoted 1 times

**dc2k79** 1 year ago
A is correct.
Both Network Service Tags and specialized HTTP Headers are used.
upvoted 1 times

**rad9899** 1 year, 2 months ago
Selected Answer: A
A is correct
upvoted 2 times

**JakeCallham** 1 year, 2 months ago

**Selected Answer: A**

Guys, Http header AND service tags are correct. This is a situation where there are more than one solutions.

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-front-door-

upvoted 3 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

well actually no: you have to combine both solutions, like stated in the ms doc

upvoted 1 times

**darren888** 1 year, 4 months ago

Correct answer is A
To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http heade
that Azure Front Door sends.more granular than service tags alone which is what the Azure app service requires.more secure agree with Lumme

upvoted 5 times

**BillyB2022** 1 year, 4 months ago

**Selected Answer: B**

Service tag

upvoted 6 times

**JakeCallham** 1 year, 2 months ago

Http header AND service tags are correct. This is a situation where there are more than one solutions.

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-front-doo

upvoted 2 times

Question #16 *Topic 4*

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription.
The company uses the following devices:
- Computers that run either Windows 10 or Windows 11
- Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored.
What should you include in the recommendation?

A. eDiscovery

B. Microsoft Information Protection

C. Compliance Manager

D. retention policies

**Correct Answer:** *B*
Protect your sensitive data with Microsoft Purview.
Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.
Note: You can use Microsoft Information Protection: Microsoft Purview for Auditing and Analytics in Outlook for iOS, Android, and Mac (DoD).
Incorrect:
Not A: Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft Purview to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365
Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use Microsoft
Purview eDiscovery (Standard) cases to identify, hold, and export content found in mailboxes and sites. If your organization has an Office 365 E5 or Microsoft 365
E5 subscription (or related E5 add-on subscriptions), you can further manage custodians and analyze content by using the feature-rich Microsoft Purview eDiscovery (Premium) solution in Microsoft 365.
Not C: What does compliance Manager do?
Compliance managers ensure that a business, its employees and its projects comply with all relevant regulations and specifications. This could include health and safety, environmental, legal or quality standards, as well as any ethical policies the company may have.
Not D: A retention policy (also called a 'schedule') is a key part of the lifecycle of a record. It describes how long a business needs to keep a piece of information
(record), where it's stored and how to dispose of the record when its time.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

*Community vote distribution*
B (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago
Selected Answer: B
Another no brainer. A, C, and D are not technologies that can provide the desired solution.
upvoted 12 times

**zellck** Most Recent 8 months ago
Selected Answer: B
B is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide
Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.
upvoted 1 times

**awssecuritynewbie** 10 months, 4 weeks ago

Selected Answer: B

So many bad choices to be honest.

upvoted 1 times

Question #17 *Topic 4*

You have a Microsoft 365 E5 subscription.
You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.
You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.
Which two components should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies

B. retention label policies

C. eDiscovery cases

D. sensitivity label policies

**Correct Answer:** *AD*
A: Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.

D: Sensitivity labels -
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate.
Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities like
Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.
Incorrect:
Not B: Retention labels help you retain what you need and delete what you don't at the item level (document or email). They are also used to declare an item as a record as part of a records management solution for your Microsoft 365 data.
Not C: eDiscovery cases in eDiscovery (Standard) and eDiscovery (Premium) let you associate specific searches and exports with a specific investigation. You can also assign members to a case to control who can access the case and view the contents of the case. Place content locations on legal hold.
Reference:
https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/ https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

*Community vote distribution*
AD (100%)

**zts** Highly Voted 1 year, 4 months ago
Selected Answer: AD
common sense answer selection :)
upvoted 13 times

**cyber_sa** Most Recent 3 months, 1 week ago
Selected Answer: AD
got this in exam 6oct23. passed with 896 marks. I answered AD
upvoted 3 times

**zellck** 8 months ago
Selected Answer: AD
AD is the answer.

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide
Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or soci
security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with
people who shouldn't have it. This practice is called data loss prevention (DLP).

In Microsoft Purview, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, ar

automatically protect sensitive items across:
- Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive accounts

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate isn't hindered.

upvoted 1 times

**Aunehwet79** 11 months, 1 week ago

Agree with given answers

upvoted 1 times

**Mo22** 11 months, 1 week ago

**Selected Answer: AD**

A and D, "data loss prevention (DLP) policies" and "sensitivity label policies," should be included in the recommendation.

DLP policies are designed to detect, monitor, and protect sensitive information across SharePoint Online and other Microsoft 365 services. They be used to identify and block the sharing of confidential data such as Personally Identifiable Information (PII) by using rule-based detection, reporting, and remediation.

Sensitivity label policies, on the other hand, are used to classify, protect, and monitor sensitive data within SharePoint Online. They can be used automatically label content based on specific conditions and to apply restrictions on how the content can be accessed or shared. These policies help prevent confidential information from being shared outside the organization or with unauthorized users.

upvoted 2 times

**JCkD4Ni3L** 1 year, 3 months ago

**Selected Answer: AD**

AD obviously

upvoted 2 times

Question #18 *Topic 4*

Your company has the virtual machine infrastructure shown in the following table.

| Operation system | Location | Number of virtual machines | Hypervisor |
|---|---|---|---|
| Linux | On-premises | 100 | VMWare vSphere |
| Windows Server | On-premises | 100 | Hyper-V |

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.

You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.

What should you include in the recommendation?

A. Use geo-redundant storage (GRS).

B. Maintain multiple copies of the virtual machines.

C. Encrypt the backups by using customer-managed keys (CMKS).

D. Require PINs to disable backups.

**Correct Answer:** *D*

Azure Backup -

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication.

As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.

Authentication to perform critical operations

As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN when you perform Stop Protection with Delete data and Change Passphrase operations.

Reference:

https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature#prevent-attacks

*Community vote distribution*

D (100%)

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#azure-backup

upvoted 9 times

**catblack** Highly Voted 1 year, 4 months ago

Agree with D

upvoted 6 times

**cyber_sa** Most Recent 3 months, 1 week ago

Selected Answer: D

got this in exam 6oct23. passed with 896 marks. I answered D

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: D

keyword is resiliency, not redundancy

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature#authentication-to-perform-critical-operations

As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN when you perform Stop Protect with Delete data and Change Passphrase operations.

upvoted 2 times

**JCkD4Ni3L** 1 year, 3 months ago

D is the correct answer

upvoted 2 times

Question #19 *Topic 4*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. adaptive application controls in Defender for Cloud

B. app protection policies in Microsoft Endpoint Manager

C. OAuth app policies in Microsoft Defender for Cloud Apps

D. Azure Active Directory (Azure AD) Conditional Access App Control policies

**Correct Answer:** *A*

*Community vote distribution*

A (78%) C (22%)

**purek77** Highly Voted 1 year ago

Actually there seems no correct answer here. Requirement is clear "the application must be blocked automatically until an administrator authori the application", but looking at Adaptative Application controls details:

No enforcement options are currently available. Adaptive application controls are intended to provide security alerts if any application runs othe than the ones you've defined as safe.

Source - https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls#are-there-any-options-to-enforce-the-application-controls

upvoted 5 times

**Aunehwet79** 11 months, 2 weeks ago

Agree none of these are fully correct - this question appears three times in this questions list and the other comments refer to A as the best a well

upvoted 2 times

**Ramye** 2 days, 2 hours ago

yes - same questions - 5x actually
Question#23 Under Topic 2
Question#46 Under Topic 2
Question#1 Under Topic 4
Question#26 under Topic 4

upvoted 1 times

**nieprotetkniteeetr** 12 months ago

The best of this is A.

upvoted 2 times

**sherifhamed** Most Recent 3 months, 3 weeks ago

Selected Answer: A

A. Adaptive application controls in Defender for Cloud

Adaptive application controls, often referred to as application whitelisting, allow you to specify which applications are authorized to run on your virtual machines and block all others. If an unauthorized application attempts to run, it will be blocked until an administrator authorizes it. This control provides a strong layer of security against unapproved or malicious applications.

The other options (B, C, and D) are not primarily designed for controlling which applications can run on Windows Server 2019 virtual machines i your Azure subscription

upvoted 1 times

**Xavier_Alonso** 4 months, 2 weeks ago

A is the answer.
How to block intentional or unintentional deletion of backup data? https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#how-to-block-intentional-or-unintentional-deletion-of--backup-data

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

upvoted 2 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the following instructions.

When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.

upvoted 1 times

**Gurulee** 10 months ago

Selected Answer: A

Although none of the options can block the app, A is the best choice. The correct solution should be Windows Defender Application Control and AppLocker.

upvoted 3 times

**AMDf** 1 year ago

Selected Answer: A

Correct

upvoted 2 times

**sfok** 1 year ago

A is correct

upvoted 1 times

Question #20 *Topic 4*

HOTSPOT

-

You have a hybrid cloud infrastructure.

You plan to deploy the Azure applications shown in the following table.

| Name | Type | Requirement |
|---|---|---|
| App1 | An Azure App Service web app accessed from Windows 11 devices on the on-premises network | Protect against attacks that use cross-site scripting (XSS). |
| App2 | An Azure App Service web app accessed from mobile devices | Allow users to authenticate to App2 by using their LinkedIn account. |

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

App1:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

**Correct Answer:**

**Answer Area**

App1:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies (selected)
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access (selected)
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

**exampracticeemail** Highly Voted 11 months, 1 week ago

in exam 6th Feb 23

upvoted 14 times

**purek77** Highly Voted 1 year ago

I believe answers are correct.

Reference for mobile app + B2C + LinkedIn - https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-linkedin?pivots=b2
user-flow

Reference for WAF - https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

upvoted 6 times

**Jacquesvz** 1 year ago

Agreed:
* B2C for Bring your own identity.
* WAF to protect against XSS

upvoted 5 times

**zellck** Most Recent 8 months ago

1. Azure Application Gateway WAF policies
2. Azure AD B2C custom policies with Conditional Access

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview
Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-identity-protection-overview
Enhance the security of Azure Active Directory B2C (Azure AD B2C) with Azure AD Identity Protection and Conditional Access. The Identity Protection risk-detection features, including risky users and risky sign-ins, are automatically detected and displayed in your Azure AD B2C tenant. You can create Conditional Access policies that use these risk detections to determine actions and enforce organizational policies. Together, these capabilities give Azure AD B2C application owners greater control over risky authentications and access policies.

upvoted 1 times

**awssecuritynewbie** 10 months, 4 weeks ago

The answer is correct

upvoted 2 times

Question #21 *Topic 4*

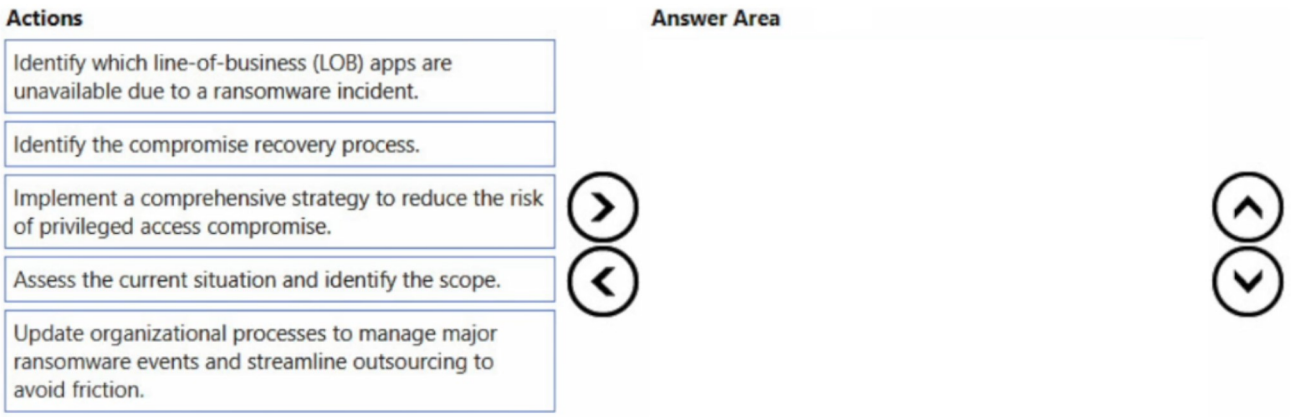
DRAG DROP

-

Your company wants to optimize ransomware incident investigations.

You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.

Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.




**Correct Answer:**

Answer Area

1. Assess the current situation and identify the scope.
2. Identify which line-of-business (LOB) apps are unavailable due to a ransomware incident.
3. Identify the compromise recovery process.

**Stubentiger** Highly Voted 1 year ago

looks ok.
https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach

upvoted 14 times

**cyber_sa** Most Recent 3 months, 1 week ago

got this in exam 6oct23. passed with 896 marks. I answered AS PER GIVEN ANSWER

upvoted 3 times

**ServerBrain** 4 months, 4 weeks ago

looks logical

upvoted 1 times

**zellck** 8 months ago

1. Assess the current situation and identify the scope.
2. Identify which LOB apps are unavailable due to a ransomware incident.
3. Identify the compromise recovery process.

https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach#the-dart-approach-to-conducti ransomware-incident-investigations
The following are three key steps in DART ransomware investigations:
1. Assess the current situation
2. Identify the affected line-of-business (LOB) apps
3. Determine the compromise recovery (CR) process

upvoted 1 times

**OCHT** 10 months, 1 week ago

I prefer 4 , 1 , 3 also.

Regarding the alternative sequence of 4, 1, and 2, while identifying the compromise recovery process is an important step, it may not be the mo urgent or critical one, especially if the scope of the incident and the impacted LOB applications are not yet known. Therefore, it is more effective prioritize identifying the scope and impacted LOB applications first, and then move on to identifying the compromise recovery process and implementing measures to reduce the risk of privileged access compromise.

A comprehensive and proactive approach to cybersecurity is essential to prevent and mitigate the impact of cyber incidents. This includes adopt best practices and following established incident response procedures, continuously monitoring systems and networks for potential threats, anc regularly reviewing and updating security policies and procedures to adapt to changing threats and circumstances

upvoted 1 times

**Fal991l** 10 months, 1 week ago

ChatGTP:
The recommended plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach, in the cor sequence, is as follows:

Assess the current situation and identify the scope: This step involves identifying which systems have been impacted and the extent of the dama caused by the ransomware attack.

Identify which line-of-business (LOB) apps are unavailable due to a ransomware process: This step involves identifying which LOB apps are affec by the ransomware attack and determining the impact on business operations.

Implement a comprehensive strategy to reduce the risk of privileged access compromise: This step involves implementing security best practice prevent future ransomware attacks, such as limiting privileged access and enforcing multi-factor authentication.

upvoted 1 times

**Fal991l** 10 months, 1 week ago

n general, it's important to follow the incident response plan for your organization, which may include additional steps beyond those listed h

Therefore, the correct order of actions is 4, 1, and 3.

Option 2 and 5 are not mentioned in the DART approach for ransomware incident investigation, so they are not included in the plan.

upvoted 1 times

**xero180sx** 9 months, 2 weeks ago

4, 1, 2
2 is listed in there.

1. Assess the current situation
2. Identify the affected line-of-business (LOB) apps
3. Determine the compromise recovery (CR) process

https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach

upvoted 1 times

**Ajdlfasudfo0** 10 months, 3 weeks ago

correct, https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-dart-ransomware-approach#the-dart-approach-to-conducting-ransomware-incident-investigations

upvoted 3 times

Question #22 *Topic 4*

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

A. From Microsoft Defender for Endpoint, perform a security scan.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. Disable Microsoft OneDrive sync and Exchange ActiveSync.

**Correct Answer:** *D*

*Community vote distribution*

D (92%) 8%

**Stubentiger** Highly Voted 1 year ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide

upvoted 10 times

**Ramye** Most Recent 1 day, 23 hours ago

I can understand answer should be D to the contaiment but any of the articles shared below talk about stopping sync with OneDrive and Exchar Can anyone spot this?

upvoted 1 times

**juanpe147** 1 month, 1 week ago

Sorry, the correct link for my comment is this one:
https://learn.microsoft.com/en-us/microsoft-365/security/defender/playbook-responding-ransomware-m365-defender?view=o365-worldwide#eradication-and-recovery

upvoted 1 times

**juanpe147** 1 month, 1 week ago

i go with A, in the Security best practices for recovery the first option of the answers available is "to make a Scan", the second one is recover file a cleaned Computer.

Disable Microsoft OneDrive Sync and Exchane Active SYNC doesnt appear in the recovery Plan, only during the Attack.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/playbook-responding-ransomware-m365-defender?view=o365-worldwide#step-3-prevent-the-spread

upvoted 1 times

**JD57005** 1 month, 3 weeks ago

I think It's B. Keyword is Recovery https://learn.microsoft.com/en-us/microsoft-365/security/defender/playbook-responding-ransomware-m365-defender?view=o365-worldwide#eradication-and-recovery

upvoted 1 times

**Argo14** 2 months ago

I would say A: Run a full, current antivirus scan
https://learn.microsoft.com/en-us/microsoft-365/security/defender/playbook-responding-ransomware-m365-defender?view=o365-worldwide#step-5-remove-malware

upvoted 3 times

**rishiraval007** 2 months, 2 weeks ago

The first step in the recovery plan for a ransomware attack, following Microsoft Security Best Practices, would be:

B. Recover files to a cleaned computer or device.

Recovering files to a cleaned computer or device is crucial because it ensures that you are restoring data in a safe environment, free from the ransomware infection. This step helps to prevent the re-infection of your systems and data.

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Selected Answer: B

I'd say B (since this is about "define the recovery steps" which is interpret as _after_ the attack, not during)

BTW: _During_ an attack, step no 2 is: "Contact your local or federal law enforcement agencies."
https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#what-to-do-during-an-attack

So not even during an attack is "Disable Exchange ActiveSync and OneDrive sync" the first step in the list.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/playbook-responding-ransomware-m365-defender?view=o365-worldwide#step-3-prevent-the-spread
Use this list to keep the attack from spreading to additional entities.
- Disable Exchange ActiveSync and OneDrive sync
Pausing OneDrive sync helps protect your cloud data from being updated by potentially infected devices.

upvoted 1 times

**shahnawazkhot** 9 months, 1 week ago

The key point here is to stop the spread of data encryption by the ransomware. Therefore, answer "D" appears a correct option.

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

sorry, disagree. The point is to "define the recovery steps", i.e. not stopping the spread

upvoted 1 times

**Rocko1** 10 months, 1 week ago

Selected Answer: D

Answer is "d" https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide#step-2-disable-exchange-activesync-and-onedrive-sync

upvoted 1 times

**SinceLaur** 10 months, 1 week ago

I would go with B. D is more a preventive measure, but not a recovery process.

upvoted 2 times

**God2029** 10 months, 3 weeks ago

Answer make sense. First - Isolate the incident

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

"define the recovery steps"

upvoted 1 times

Question #23 *Topic 4*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. OAuth app policies in Microsoft Defender for Cloud Apps

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. application control policies in Microsoft Defender for Endpoint

D. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

**Correct Answer:** *A*

*Community vote distribution*

C (92%) 8%

**Ramye** 1 day, 23 hours ago

This is the 5th time this question is listed and the answer for this occurrence is different than other ones.

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

**Selected Answer: C**

C. Application control policies in Microsoft Defender for Endpoint

Application control policies, also known as application whitelisting, allow you to specify which applications are authorized to run on your virtual machines and block all others. If an unauthorized application attempts to run, it will be blocked until an administrator authorizes it. This control provides a strong layer of security against unapproved or potentially malicious applications.

The other options (A, B, and D) are not primarily designed for controlling which applications can run on Windows Server virtual machines in you Azure subscription

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

**Selected Answer: A**

With answer C, i do not see where there is reference indicating admin approval for blocked apps.

A is the answer:

https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

upvoted 1 times

**zellck** 8 months ago

**Selected Answer: C**

C is the answer.

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager
prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Applica Control doesn't have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy devices in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-ba protection of Application Control policies deployed through Configuration Manager can be enabled through group policy on capable hardware

upvoted 1 times

**KallMeDan** 8 months, 3 weeks ago

This is the other version of the same question I have seen and the answer was A:
"You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled. The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019. You need to recomm a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application. Which security control should you

recommend?
A. adaptive application controls in Defender for Cloud
B. app protection policies in Microsoft Endpoint Manager
C. OAuth app policies in Microsoft Defender for Cloud Apps
D. Azure Active Directory (Azure AD) Conditional Access App Control policies"

upvoted 2 times

**Gurulee** 10 months, 1 week ago

Selected Answer: C

App Control for apps on endpoints.
Whereas, oauth policies allow you to ban/disable Azure Cloud Enterprise Applications.

upvoted 1 times

**Gurulee** 10 months, 1 week ago

Selected Answer: C

Application Control lets you strongly control what can run on devices you manage. This feature can be useful for devices in high-security departments, where it's vital that unwanted software can't run.

upvoted 1 times

**God2029** 10 months, 3 weeks ago

It is C

upvoted 1 times

**awssecuritynewbie** 10 months, 4 weeks ago

Selected Answer: C

C 4 sure

upvoted 1 times

**buguinha** 10 months, 4 weeks ago

Selected Answer: C

C is the correct. MDCA does not control the servers. Microsoft Defender does

upvoted 1 times

**MKnight25** 10 months, 4 weeks ago

Selected Answer: C

Application control is the correct answer.

upvoted 3 times

**dbhagz** 10 months, 4 weeks ago

Selected Answer: C

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC
https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager

upvoted 2 times

**tech_rum** 10 months, 4 weeks ago

C is the correct answer

upvoted 1 times

**Ssasid** 11 months ago

Its C Application control policies
https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview

upvoted 1 times

Question #24 *Topic 4*

Your company is developing an invoicing application that will use Azure AD B2C. The application will be deployed as an App Service web app.

You need to recommend a solution to the application development team to secure the application from identity-related attacks.

Which two configurations should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies

B. smart account lockout in Azure AD B2C

C. access packages in Identity Governance

D. custom resource owner password credentials (ROPC) flows in Azure AD B2C

**Correct Answer:** *AB*

*Community vote distribution*

AB (100%)

**zellck** 8 months ago

Same as Question 10.
https://www.examtopics.com/discussions/microsoft/view/79376-exam-sc-100-topic-4-question-10-discussion

upvoted 2 times

**zellck** 8 months ago

Selected Answer: AB

AB is the answer.

https://learn.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow
Conditional Access can be added to your Azure Active Directory B2C (Azure AD B2C) user flows or custom policies to manage risky sign-ins to y applications. Azure Active Directory (Azure AD) Conditional Access is the tool used by Azure AD B2C to bring signals together, make decisions, a enforce organizational policies.

upvoted 1 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/active-directory-b2c/threat-management#how-smart-lockout-works
Azure AD B2C uses a sophisticated strategy to lock accounts. The accounts are locked based on the IP of the request and the passwords entered. The duration of the lockout also increases based on the likelihood that it's an attack. After a password is tried 10 times unsuccessful (the default attempt threshold), a one-minute lockout occurs. The next time a login is unsuccessful after the account is unlocked (that is, afte the account has been automatically unlocked by the service once the lockout period expires), another one-minute lockout occurs and contin for each unsuccessful login. Entering the same, or similar password repeatedly doesn't count as multiple unsuccessful logins.

upvoted 1 times

**Gurulee** 10 months, 1 week ago

Selected Answer: AB

Smart lockout is supported by user flows, custom policies, and ROPC flows. It's activated by default so you don't need to configure it in your use flows or custom policies.

upvoted 2 times

**awssecuritynewbie** 10 months, 4 weeks ago

Selected Answer: AB

Correct answer

upvoted 2 times

Question #25 *Topic 4*

Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

What should you recommend?

A. Compliance Manager in Microsoft Purview

B. Microsoft Defender for Cloud

C. Microsoft Sentinel

D. Microsoft Defender for Cloud Apps

**Correct Answer:** *D*

*Community vote distribution*

B (67%) A (20%) 13%

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: B

B. Microsoft Defender for Cloud

Microsoft Defender for Cloud (formerly known as Azure Security Center) is a comprehensive cloud security management system that helps you monitor and improve the security of your Azure resources. It provides continuous security assessment based on various compliance standards, including NIST CSF. It offers recommendations and best practices to help you align with the NIST CSF and other security frameworks.

The other options (A, C, and D) have different purposes and are not specifically designed for evaluating compliance with NIST CSF

upvoted 4 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: B

Ans is B, all-day!

upvoted 2 times

**Ario** 6 months, 2 weeks ago

Selected Answer: C

While options A (Compliance Manager in Microsoft Purview) and D (Microsoft Defender for Cloud Apps) also offer security-related features, they are more focused on specific areas such as compliance management and application security, respectively. Option B (Microsoft Defender for Clo primarily focuses on protecting cloud workloads. However, for evaluating compliance with the NIST CSF across the Azure environment as a whol Microsoft Sentinel is the most suitable choice.

upvoted 4 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard
Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard. Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and b practices in the standards that you've applied to your subscriptions. The dashboard reflects the status of your compliance with these standards.

When you enable Defender for Cloud on an Azure subscription, the Microsoft cloud security benchmark is automatically assigned to that subscription. This widely respected benchmark builds on the controls from the Center for Internet Security (CIS), PCI-DSS and the National Instit of Standards and Technology (NIST) with a focus on cloud-centric security.

upvoted 1 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 3 times

**El_m_o** 8 months, 3 weeks ago

Selected Answer: B

Regulatory Compliance Dashboard has the Azure compliance data. Compliance Manager aggregates this and Office 365 compliance data. For th question, RCD is more direct and actionable.

upvoted 2 times

**promto** 9 months, 1 week ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#add-a-regulatory-standard-to-your-dashboard

upvoted 2 times

**shinda** 9 months, 1 week ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/review-security-recommendations

upvoted 3 times

**OK2020** 9 months, 1 week ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#add-a-regulatory-standard-to-your-dashboard

upvoted 3 times

**janesb** 9 months, 1 week ago

**Selected Answer: A**

it is the Compliance Manager in Microsoft Purview for sure
https://learn.microsoft.com/en-us/compliance/regulatory/offering-nist-csf#use-microsoft-purview-compliance-manager-to-assess-your-risk

upvoted 3 times

**aris** 9 months, 1 week ago

**Selected Answer: A**

https://learn.microsoft.com/en-us/compliance/regulatory/offering-nist-csf

upvoted 3 times

**_adem** 9 months, 1 week ago

**Selected Answer: B**

https://learn.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages
https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

upvoted 3 times

Question #26 *Topic 4*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

B. Azure AD Conditional Access App Control policies

C. adaptive application controls in Defender for Cloud

D. app protection policies in Microsoft Endpoint Manager

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: C

Answer C is being confirmed

upvoted 1 times

**zellck** 8 months ago

Same as Question 19.
https://www.examtopics.com/discussions/microsoft/view/94349-exam-sc-100-topic-4-question-19-discussion

upvoted 2 times

**zellck** 8 months ago

Selected Answer: C

C is the answer.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning tc analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the following instructions.

When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.

upvoted 1 times

**El_m_o** 8 months, 3 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls

upvoted 2 times

Question #27 *Topic 4*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. Azure AD Conditional Access App Control policies

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app protection policies in Microsoft Endpoint Manager

D. application control policies in Microsoft Defender for Endpoint

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**zellck** 8 months ago

Same as Question 23.
https://www.examtopics.com/discussions/microsoft/view/99695-exam-sc-100-topic-4-question-23-discussion

upvoted 2 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager
prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Applica
Control doesn't have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy
devices in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-ba
protection of Application Control policies deployed through Configuration Manager can be enabled through group policy on capable hardware

upvoted 1 times

**Nail** 7 months, 3 weeks ago

why do you have a link for device guard? That is protecting you from unsafe websites, not apps.

upvoted 1 times

**Nail** 7 months, 3 weeks ago

My bad, I was thinking of application guard. device guard is the old name for WDAC.

upvoted 1 times

**CarisB** 8 months, 3 weeks ago

Selected Answer: D

Windows Defender Application Control (WDAC) seems better, but I go for D

upvoted 3 times

**Nail** 7 months, 3 weeks ago

WDAC and app control policies in MDE are one and the same.

upvoted 2 times

**MaciekMT** 9 months ago

from ChatGPT: Based on the requirements of ensuring that only authorized applications can run on the virtual machines, and that an unauthoriz
application is blocked automatically until an administrator authorizes it, the recommended security control to implement is application control
policies in Microsoft Defender for Endpoint.

Application control policies in Microsoft Defender for Endpoint provide a way to prevent the execution of malicious and unauthorized applicatic
on Windows 10 and Windows Server 2019 machines. Application control policies can be used to block all unknown applications or allow only
trusted applications to run.

Using application control policies, you can create policies that restrict application execution to a specific set of approved applications. When an unknown application attempts to run, it will be blocked until the administrator approves it.

Therefore, the correct answer is D) application control policies in Microsoft Defender for Endpoint.

upvoted 1 times

Question #28 *Topic 4*

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

A. app registrations in Azure AD

B. application control policies in Microsoft Defender for Endpoint

C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

D. Azure AD Conditional Access App Control policies

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**Ramye** 1 day, 22 hours ago

lol - same question 7 times

upvoted 1 times

**theplaceholder** 3 months, 4 weeks ago

the same question 3 times in a row? gg ET >_<

upvoted 1 times

**zellck** 8 months ago

Same as Question 27.
https://www.examtopics.com/discussions/microsoft/view/106549-exam-sc-100-topic-4-question-27-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager
prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Applica Control doesn't have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy devices in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-ba protection of Application Control policies deployed through Configuration Manager can be enabled through group policy on capable hardware

upvoted 1 times

**CarisB** 8 months, 3 weeks ago

Duplicate

upvoted 1 times

Question #29 *Topic 4*

You have a Microsoft 365 subscription.

You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

Which two services should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. Azure Data Catalog

C. Microsoft Purview Information Protection

D. Azure AD Application Proxy

E. Microsoft Defender for Cloud Apps

**Correct Answer:** *AE*

*Community vote distribution*

AE (82%) CE (18%)

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: AE

True, Answer A & E

upvoted 1 times

**tirajvid** 5 months, 1 week ago

Question says "authenticated users". So its passed the conditional access stage. So A seems not right. What is the correct answer set then ?

upvoted 1 times

**Kdosec** 1 month ago

But it also mentioned that "unmanaged devices", we must use Azure AD CA rule to check corporate devices.

upvoted 2 times

**zellck** 8 months ago

Same as Question 27.
https://www.examtopics.com/discussions/microsoft/view/106549-exam-sc-100-topic-4-question-27-discussion

upvoted 1 times

**zellck** 8 months ago

Selected Answer: AE

AE is the answer.

https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad#create-a-block-download-policy-for-unmanaged-devices
Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of a session using its devic a condition, create both a conditional access policy AND a session policy.

upvoted 2 times

**uffman** 8 months, 3 weeks ago

Selected Answer: AE

Seems correct.

upvoted 2 times

**KallMeDan** 8 months, 3 weeks ago

Selected Answer: AE

Conditional access to block sign in from unauthorized device. MDCA to prevent downloads.

upvoted 2 times

**CarisB** 8 months, 3 weeks ago

Selected Answer: AE

https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad#create-a-block-download-policy-for-unmanaged-

devices

upvoted 2 times

**MaciekMT** 9 months ago

AE - according to ChatGPT: To block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices, the recommended solution is to use Azure AD Conditional Access and Microsoft Defender for Cloud Apps.

Azure AD Conditional Access provides policies that enable you to ensure that access to your Microsoft 365 resources is only allowed from truste devices that meet your compliance requirements. You can use Conditional Access policies to block access to SharePoint Online for users on unmanaged devices.

Microsoft Defender for Cloud Apps provides advanced data protection and compliance features for cloud applications, including SharePoint Online. Defender for Cloud Apps allows you to control access to data in SharePoint Online, including blocking file downloads by authenticated users on unmanaged devices.

Therefore, the correct answers are A) Azure AD Conditional Access and E) Microsoft Defender for Cloud Apps.

upvoted 3 times

**gaura** 9 months ago

AE is correct
https://learn.microsoft.com/en-us/sharepoint/block-download-from-sites

upvoted 1 times

**_adem** 9 months, 1 week ago

**Selected Answer: CE**

Looks correct

upvoted 2 times

Question #30 *Topic 4*

HOTSPOT
-

You have an Azure SQL database named DB1 that contains customer information.

A team of database administrators has full access to DB1.

To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information.

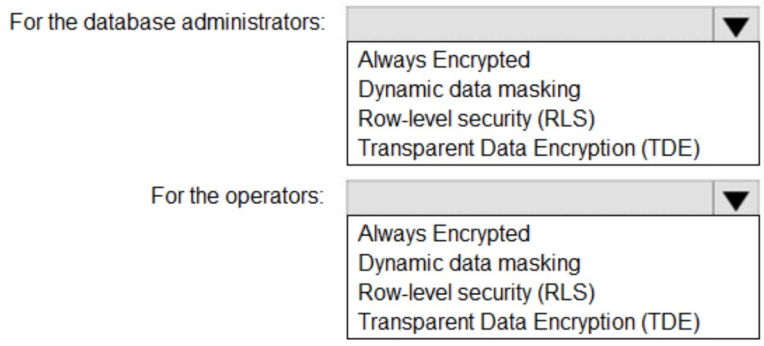
You need to design a security strategy for DB1. The solution must meet the following requirement:

• When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the CreditCard attribute of each customer record.
• When the operators view customer records in App1, they must view only the last four digits of the CreditCard attribute.

What should you include in the design? To answer, select the appropriate options in the answer area.

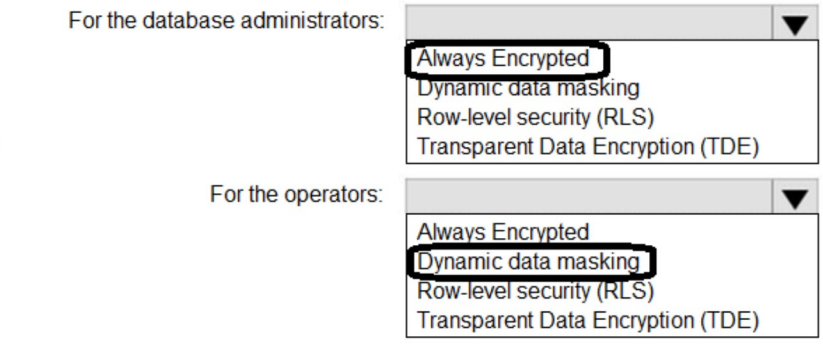
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer Area**

**Correct Answer:**




**Murtuza** 1 week, 5 days ago

ways Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national/regional identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database, Azure SQL Managed Instance, and SQL Server databases. Always Encrypte allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine. This provides a separation between those who own the data and can view it, and those who manage the data but should have no access - on-premises databas administrators, cloud database operators, or other high-privileged unauthorized users.

upvoted 1 times

**Murtuza** 1 week, 5 days ago

What should you use to ensure credit card numbers in an Azure SQL database are protected while data is being processed?
Final answer: To protect credit card numbers in an Azure SQL database while processing, you should use Transparent Data Encryption (TDE) and

Always Encrypted.

upvoted 1 times

**karincauk** 2 weeks ago

1- Always encrypt
"2- Low level "should be correct. because db operator can see last 4 digit.

upvoted 1 times

**ttttt23212121** 3 months, 2 weeks ago

Row Level Security For 1
Dynamic Data Masking for 2

upvoted 3 times

**kanag1** 5 months ago

For the database administrators: Always Encrypted
For the operators: Dynamic Data Masking

Always Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national/regional identification numbers. Alway Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine.

https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver16

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data reveal with minimal effect on the application layer.

https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

upvoted 3 times

**ServerBrain** 4 months, 4 weeks ago

But then when you do Always encrypted the admins are as good as not having full access.

Block 1 should be Row-level security as it's just the CreditCard row they should not see

upvoted 2 times

**ServerBrain** 4 months, 4 weeks ago

looks like i'm wrong...

upvoted 2 times

**Victory007** 5 months, 1 week ago

1. Dynamic Masking. 2. Always Encrypted.
To meet the requirements, you should include Dynamic Data Masking for the operators and Always Encrypted for the database administrators ir your design. Dynamic Data Masking (DDM) is a feature that limits sensitive data exposure by masking it to non-privileged users. It can be used t greatly simplify the design and coding of security in your application.

upvoted 1 times

Question #31 *Topic 4*

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials.

You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. Azure AD B2C

C. an Azure AD enterprise application

D. a relying party trust in Active Directory Federation Services (AD FS)

**Correct Answer:** *A*

*Community vote distribution*

C (100%)

**cyber_sa** 3 months, 1 week ago

Selected Answer: C

got this in exam 6oct23. passed with 896 marks. I answered C

upvoted 4 times

**Lippes** 5 months ago

Selected Answer: C

Enterprise app, C should correct

upvoted 1 times

**sbnpj** 5 months, 1 week ago

Selected Answer: C

you need to configure app as enterprise app

upvoted 1 times

**Victory007** 5 months, 1 week ago

Selected Answer: C

To enable users to authenticate to App1 by using their Azure AD credentials, you should include an Azure AD enterprise application in your recommendation. An Azure AD enterprise application is an instance of an application that is integrated with Azure AD. You can add App1 as an enterprise application in your Azure AD tenant and configure it to support single sign-on (SSO) using Azure AD. This will allow users to authenticate to App1 using their Azure AD credentials.
https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal

upvoted 4 times

**hw121693** 5 months, 1 week ago

Selected Answer: C

Use enterprise app to register that 3rd party app

upvoted 2 times

Question #32 *Topic 4*

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant.

You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1.

What should you include in the design?

A. Microsoft Entra Identity Governance

B. connected apps in Microsoft Defender for Cloud Apps

C. access policies in Microsoft Defender for Cloud Apps

D. Azure AD Application Proxy

**Correct Answer:** *A*

*Community vote distribution*

A (100%)

**sherifhamed** 3 months, 3 weeks ago

**Selected Answer: A**

A. Microsoft Entra Identity Governance

Microsoft Entitlement Management, part of Azure AD Identity Governance, allows you to implement access reviews and request workflows for applications, including third-party SaaS apps like App1. With this solution, you can configure self-service access requests, request approval workflows, and access reviews. Users can request access to App1, provide additional information during the request, and managers can periodic review and verify access.

B. Connected apps in Microsoft Defender for Cloud Apps and C. Access policies in Microsoft Defender for Cloud Apps are more focused on the security and monitoring aspects of cloud applications but do not provide the specific access request and review workflows required for this scenario.

upvoted 2 times

**Victory007** 5 months, 1 week ago

**Selected Answer: A**

Microsoft Entra Identity Governance allows you to balance your organization's need for security and employee productivity with the right proces and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.
https://learn.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview

upvoted 3 times

Question #33 *Topic 4*

You have an Azure subscription.

You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar.

Developers use Azure DevOps to deploy web apps to App Service Environments. When a new app is deployed, a CNAME record for the app is registered in contoso.com.

You need to recommend a solution to secure the DNS record for each web app. The solution must meet the following requirements:

• Ensure that when an app is deleted, the CNAME record for the app is removed also.
• Minimize administrative effort.

What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for DevOps

C. Microsoft Defender for App Service

D. Microsoft Defender for DNS

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

**Ramye** 1 day, 10 hours ago

Mind-boggling how many Defender Services MS has - lol

upvoted 1 times

**kanag1** 5 months ago

Selected Answer: C

Defender for App Service identifies any DNS entries remaining in your DNS registrar when an App Service website is decommissioned - these ar known as dangling DNS entries.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection

Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection

upvoted 1 times

**MiesExam** 5 months, 1 week ago

This answer is correct C: Microsoft Defender for App Service
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-app-service-introduction#dangling-dns-detection

upvoted 4 times

**ca777** 5 months, 1 week ago

Answer is : Microsoft Defender for DNS
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-dns-introduction

upvoted 1 times

**mohamed1999** 1 month, 1 week ago

This is wrong, because it doens't scan the DNS entries for web apps. Also the DNS is not hosted in azure.

upvoted 1 times

**mohamed1999** 1 month, 1 week ago

Defender for App Service also identifies any DNS entries remaining in your DNS registrar when an App Service website is decommissione these are known as dangling DNS entries. When you remove a website and don't remove its custom domain from your DNS registrar, the DNS entry is pointing to a non-existent resource, and your subdomain is vulnerable to a takeover. Defender for Cloud doesn't scan your D registrar for existing dangling DNS entries; it alerts you when an App Service website is decommissioned and its custom domain (DNS ent isn't deleted.

upvoted 4 times

Question #34 *Topic 4*

HOTSPOT
-

You have an on-premises datacenter named Site1.

You have an Azure subscription that contains a virtual network named VNet1 and multiple Azure App Service apps. Site1 is connected to VNet1 by using a Site-to-Site (P2S) VPN connection. The apps are accessed by using public internet connections.

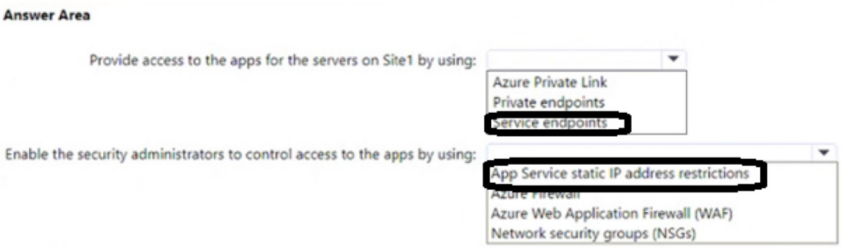
You need to recommend a solution for providing secure access to the apps. The solution must meet the following requirements:

• Servers on Site1 must use a VPN connection to access the apps.
• Access to the apps must be restricted to specific servers on Site1.
• Security administrators for VNet1 must be able to control which servers can access the apps.
• Costs must be minimized.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Correct Answer:**




**Murtuza** 1 week ago
Dont confuse yourself with private end points and private links. The question has nothing to do with extending your private end points to a give business. When the word business its mentioned then private link comes to play
upvoted 1 times

**tocane** 1 week, 3 days ago
1- Prívate endpoint
2-App service static IP address restrictions
upvoted 1 times

**cybrtrk** 1 week, 4 days ago
1. service endpoints use public network, so although private endpoint costs .01/hour this will not use public IPs.
https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview
2. App service static IP address restrictions.
https://learn.microsoft.com/en-us/azure/app-service/overview-inbound-outbound-ips
upvoted 2 times

**Murtuza** 1 week, 5 days ago
The Azure Private Link Service takes this a step further, allowing you to extend your Private Endpoints to business partners or customers. This

service requires an approval process as an added layer of security to prevent unintended access to your internal resources.
upvoted 1 times

**Ramye** 1 day, 10 hours ago
so what are you suggesting the answers are?
upvoted 1 times

**Arjanussie** 1 month, 1 week ago
The most secure way for on-premises servers to access app services in Azure is by using Azure Private Endpoint. This feature allows you to secur connect to your app from on-premises networks that connect to the virtual network using a VPN or ExpressRoute private peering. It also elimina public network access to your app, thus reducing the risk of data exfiltration from your virtual network
upvoted 1 times

**TheCloudGuruu** 1 month, 3 weeks ago
"The apps are accessed by using public internet connections" so I would go with Private Link. and App Service Status IP address restrictions.
upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago
For enabling security administrators to control access to the apps, the best choice would be:

B. Private Endpoints

Here's why:

B. Private Endpoints: They provide secure and direct access to Azure services over a private endpoint in your virtual network. This allows fine-grained access control through network security groups or Azure Firewall. Thus, security administrators can effectively control which servers or clients within the VNet can access the apps.
To enable security administrators to control access to the apps, the best choice among the given options would be:

A. App Service Static IP address restrictions

Here's why:

A. App Service Static IP address restrictions: This feature allows administrators to define a list of IP addresses that are allowed or denied access t the App Service. It's a direct and effective way to control access at the application level, ensuring that only specific servers on Site1 can access th apps.
upvoted 3 times

**smanzana** 2 months, 3 weeks ago
1- Prívate endpoint
2-App service static IP address restrictions
upvoted 1 times

**hcmonteiro** 3 months ago
Why not private endpoint for 1. ?
https://learn.microsoft.com/en-us/azure/app-service/overview-private-endpoint
upvoted 2 times

Question #35 *Topic 4*

DRAG DROP
-

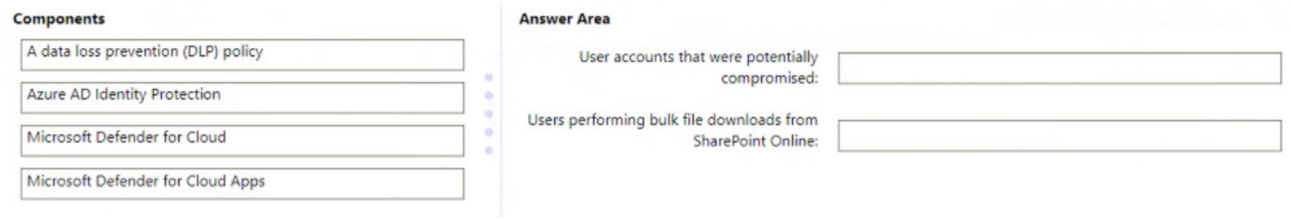
You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

• User accounts that were potentially compromised
• Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.




**Correct Answer:**

**Murtuza** 1 week, 5 days ago

1. Azure AD Identity Protection
2. Microsoft Defender for Cloud Apps

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#nonpremium-user-risk-detectior

https://learn.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration
Detect when a certain user accesses or downloads a massive number of files in a short period of time.

upvoted 3 times

**TheCloudGuruu** 1 month, 3 weeks ago

Answers provided seem correct.

upvoted 2 times

**smanzana** 2 months, 3 weeks ago

It's OK

upvoted 1 times

Question #36 *Topic 4*

HOTSPOT
-

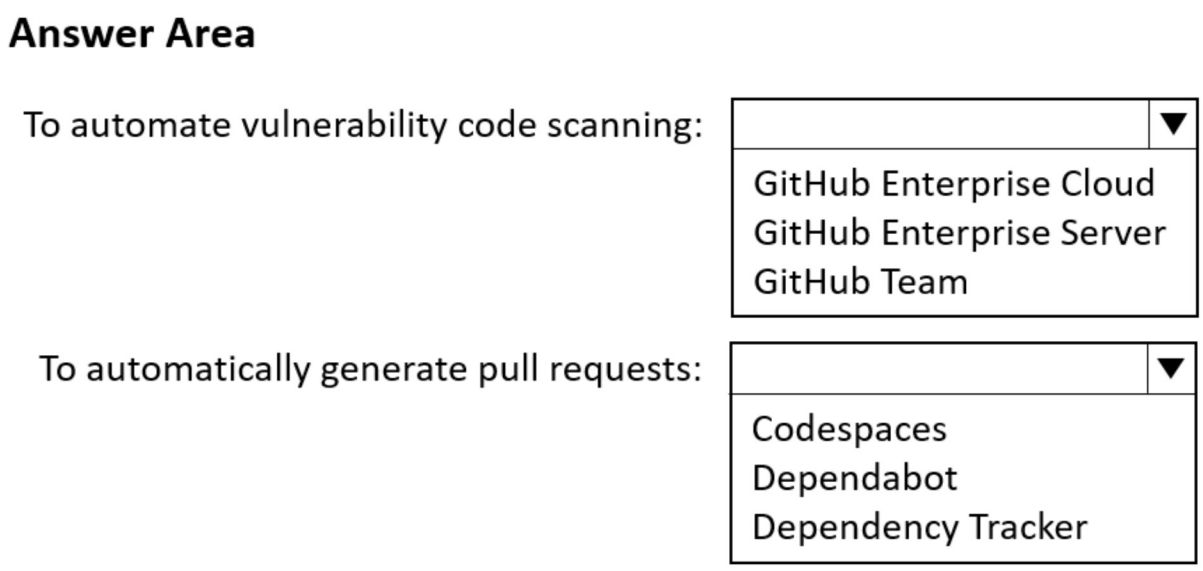
You plan to automate the development and deployment of a Node.js-based app by using GitHub.

You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

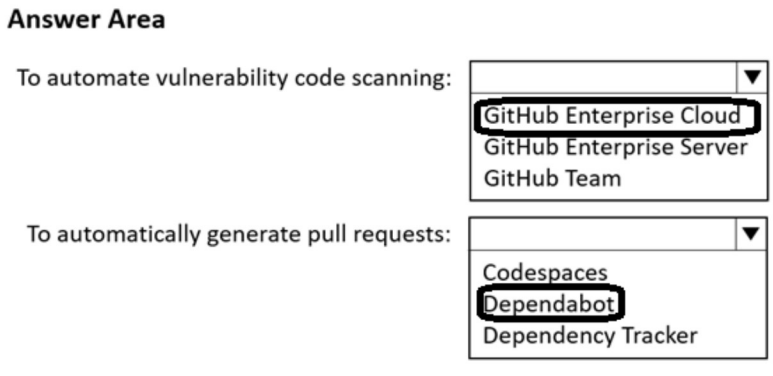
• Automate the generation of pull requests that remediate identified vulnerabilities.
• Automate vulnerability code scanning for public and private repositories.
• Minimize administrative effort.
• Minimize costs.

What should you recommend using? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Correct Answer:**




**Murtuza** 1 week, 5 days ago
Dependabot security updates are automated pull requests that help you update dependencies with known vulnerabilities.
upvoted 1 times

**Murtuza** 1 week, 5 days ago
Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any probler identified by the analysis are shown in GitHub Enterprise Cloud.
upvoted 2 times

**smanzana** 2 months, 3 weeks ago

1- Github enterprise cloud
2- Dependabot
upvoted 4 times

**hcmonteiro** 3 months ago
Dependabot is another tool that automates the process of keeping project dependencies up to date. It helps developers by monitoring the dependencies used in their projects and notifying them when new versions or security updates are available. So in a way could be dependabot
upvoted 3 times

**hcmonteiro** 3 months ago
2. Codespaces
https://docs.github.com/en/codespaces/developing-in-codespaces/using-github-codespaces-for-pull-requests
upvoted 2 times

**kvdvliert** 2 months, 2 weeks ago
Using Codespaces costs money. So this is not the answer.
upvoted 1 times

**hcmonteiro** 3 months ago
1. GitHub Enterprise Cloud
https://docs.github.com/en/enterprise-cloud@latest/code-security/code-scanning/introduction-to-code-scanning/about-code-scanning
https://docs.github.com/en/enterprise-cloud@latest/code-security/code-scanning/introduction-to-code-scanning/about-code-scanning
upvoted 1 times

## Topic 5 - Question Set 5

Question #1 *Topic 5*

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices.

You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

A. controlled folder access

B. application isolation

C. memory scanning

D. machine isolation

E. user isolation

**Correct Answer:** *D*

*Community vote distribution*

D (86%) 14%

**rishiraval007** 2 months, 2 weeks ago

D. Machine Isolation

This is a crucial step in containing the breach. Isolating the compromised machines from the network prevents the spread of ransomware and ot malicious activities.
E. User Isolation

Along with machine isolation, isolating user accounts that have been compromised is essential. This can prevent attackers from using compromi credentials to access other resources.

upvoted 1 times

**cyber_sa** 3 months, 1 week ago

Selected Answer: D

got this in exam 6oct23. passed with 896 marks. I answered D

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach#dart-recommendations-and-be practices

upvoted 2 times

**bmulvIT** 8 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach
"Isolate critical known good application servers,"

upvoted 1 times

**stepman** 7 months ago

The question states, "post-breach response plan for compromised computers", and not referring to the post-breach response plan for the preservation of existing systems. The answer is D

upvoted 2 times

**janesb** 9 months, 1 week ago

Selected Answer: D

correct

upvoted 3 times

Question #2 *Topic 5*

You have an operational model based on the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, databases, files, and storage accounts.

What should you include in the recommendation?

A. business resilience

B. modem access control

C. network isolation

D. security baselines in the Microsoft Cloud Security Benchmark

**Correct Answer:** *D*

*Community vote distribution*

D (100%)

**zellck** 8 months ago

**Selected Answer: D**

D is the answer.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline
Security baseline is one of the Five Disciplines of Cloud Governance within the Cloud Adoption Framework governance model. Security is a component of any IT deployment, and the cloud introduces unique security concerns. Many businesses are subject to regulatory requirements t make protecting sensitive data a major organizational priority when considering a cloud transformation. Identifying potential security threats to your cloud environment and establishing processes and procedures for addressing these threats should be a priority for any IT security or cybersecurity team. The Security Baseline discipline ensures technical requirements and security constraints are consistently applied to cloud environments, as those requirements mature.

upvoted 4 times

**omarmkhan22** 9 months ago

**Selected Answer: D**

Correct.

upvoted 2 times

**technocorgi** 9 months, 1 week ago

**Selected Answer: D**

correct answer

upvoted 2 times

**janesb** 9 months, 1 week ago

**Selected Answer: D**

correct answer

upvoted 2 times

Question #3 *Topic 5*

HOTSPOT
-

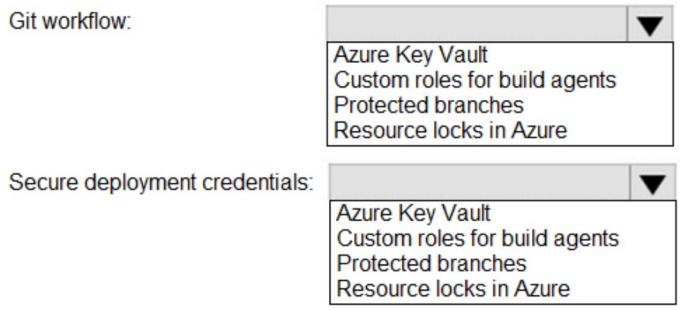
You use Azure Policy with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows.

You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.

What should you include in the recommendation for each stage? To answer, select the appropriate options in the answer area.

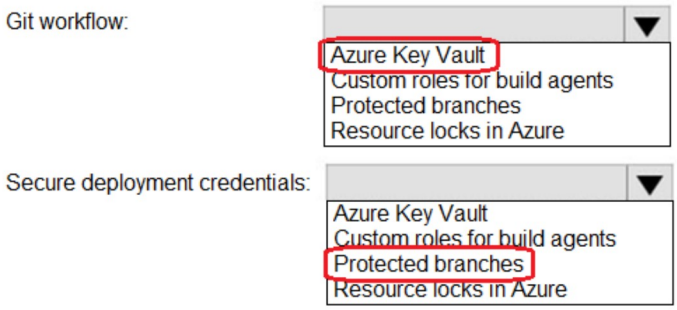
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer Area**

**Correct Answer:**




**janesb** Highly Voted 9 months, 1 week ago
Incorrect Answer
GIT Workflow ---> Protected Branch
Secure Deployment credentials --> Keyvault
Ref : https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops
upvoted 16 times

**OK2020** Highly Voted 9 months, 1 week ago
answers should be the opposite:
1. protected branches
2. Keyvolt

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops
upvoted 12 times

**tocane** Most Recent 1 week, 3 days ago
1. Protected branches
2. Azure Key Vault
upvoted 1 times

**smanzana** 2 months, 3 weeks ago
1. Protected branches
2. Azure Key Vault

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Protected branches
Create custom roles for build agents
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops

upvoted 1 times

**zellck** 8 months ago

1. Protected branches
2. Azure Key Vault

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops#restrict-access-to-protected-branche

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops#azure-key-vault
If your CI platform supports it, consider storing credentials in a dedicated secret store, for example Azure Key Vault. Credentials are fetched at runtime by the build agent and your attack surface is reduced.

upvoted 6 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 4 times

Question #4 *Topic 5*

HOTSPOT
-

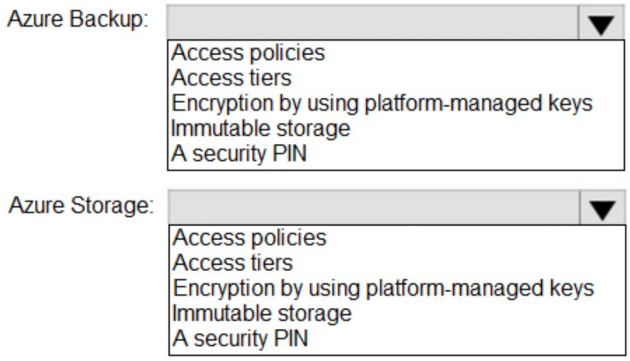
Your company wants to optimize using Azure to protect its resources from ransomware.

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend? To answer, select the appropriate options in the answer area.

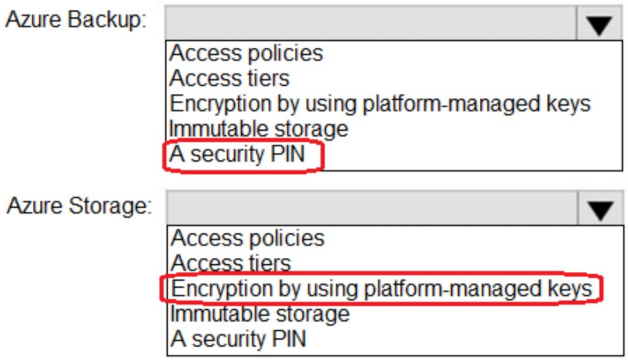
NOTE: Each correct selection is worth one point.

**Answer Area**




**Correct Answer:**

**Answer Area**




**1235813** Highly Voted 8 months, 2 weeks ago

Azure Backup: A security PIN
Azure Storage: Immutable storage

upvoted 14 times

**zellck** Highly Voted 8 months ago

1. Security PIN
2. Immutable storage

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#azure-backup
Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN before modifying online backups.

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#steps-to-take-before-an-attack
Online immutable storage (such as Azure Blob) enables you to store business-critical data objects in a WORM (Write Once, Read Many) state. Th state makes the data non-erasable and non-modifiable for a user-specified interval.

upvoted 7 times

**tocane** Most Recent 1 week, 3 days ago

1. Security PIN
2. Immutable storage

upvoted 1 times

**Murtuza** 1 week, 4 days ago

What is immutable storage against ransomware?
Immutable storage, however, prevents data from being altered or deleted for a specified period. Even if ransomware gains access to the primary data, it cannot modify or encrypt immutable backup copies. This approach ensures the availability of uncorrupted data for recovery.

upvoted 2 times

**smanzana** 2 months, 3 weeks ago

1. Security PIN
2. Immutable storage

upvoted 1 times

**ConanBarb** 3 months, 3 weeks ago

Security pin and Immutable storage

"Encryption by using platform-managed keys for Azure Storage" is always on by default, so doesn't makes sense. And even if it did, it doesn't protect against ransomware encryption. It protects the confidentiality of data.

upvoted 1 times

**calotta1** 4 months, 3 weeks ago

This is my understanding based on this article and why Immutable storage makes sense for the 2nd part: https://learn.microsoft.com/en-us/azu /storage/common/storage-service-encryption

Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud.

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

Azure Storage encryption is enabled for all storage accounts, including both Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled. Because your data is secured by default, you don't need to modify your code or applications to take advantage Azure Storage encryption.

upvoted 2 times

**MaciekMT** 9 months ago

It looks correct to me. A security PIN for backup and Encryption by using platform-managed keys for Azure Storage

upvoted 1 times

**uffman** 8 months, 4 weeks ago

For Azure Backup I agree with a Security PIN. However, for Azure Storage I would argue that Immutable is the strongest, see here: https://learn.microsoft.com/en-us/azure/storage/blobs/security-recommendations#data-protection. Encryption is on by default, we can doul encrypt data with infrastructure encryption but this is not an option.

upvoted 8 times

**DavidSapery** 8 months, 2 weeks ago

Isn't immutable only for blobs?

upvoted 1 times

Question #5 *Topic 5*

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised administrator account cannot be used to delete the backups.

What should you do?

A. From Azure Backup, configure multi-user authorization by using Resource Guard.

B. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.

C. From a Recovery Services vault, generate a security PIN for critical operations.

D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

**Correct Answer:** *C*

*Community vote distribution*

C (55%) A (45%)

**MaciekMT** Highly Voted 9 months ago

Selected Answer: C

Option A is incorrect because multi-user authorization by using Resource Guard is used to provide additional protection for Azure resources, bu does not address the issue of compromised administrator accounts in MABS.

upvoted 19 times

**EM1234** 8 months, 1 week ago

I think this is correct. It is subtle but, being that both a and c do kind of satisfy the requirements, this difference is very important. Thank you MaciekMT.

upvoted 1 times

**DashRyde** Highly Voted 9 months ago

Selected Answer: A

MUA for Azure Backup uses a new resource called the Resource Guard to ensure critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, are performed only with applicable authorization.

ref: https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

upvoted 10 times

**Murtuza** Most Recent 1 week, 1 day ago

Selected Answer: C

Choice C is correct

upvoted 1 times

**Murtuza** 1 week, 4 days ago

Here are the subtle differences in the question. Pay attention to disabled vs deleted backups
As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN when you perform Stop Protect with Delete data and Change Passphrase operations.

Multi-user authorization (MUA) for Azure Backup allows you to add an additional layer of protection to critical operations on your Recovery Services vaults and Backup vaults. For MUA, Azure Backup uses another Azure resource called the Resource Guard to ensure critical operations a performed only with applicable authorization. MUA protects against disabling backups and reducing retention for backups.

upvoted 1 times

**juanpe147** 1 month ago

i think now the recommendation MUA for Azure Backup, so i go with A

upvoted 1 times

**Arjanussie** 1 month, 1 week ago

A : f you have a compromised administrator account, you should configure multi-user authorization by using Resource Guard for your vaults. Th

will prevent the admin from deleting the backups without the approval of another user who owns the Resource Guard. A security PIN is not sufficient to protect your backups, as the compromised admin may be able to access or reset the PIN

upvoted 1 times

**smanzana** 2 months, 3 weeks ago

C. From a Recovery Services vault, generate a security PIN for critical operations

upvoted 1 times

**sherifhamed** 3 months, 3 weeks ago

Selected Answer: C

C. From a Recovery Services vault, generate a security PIN for critical operations.

Configuring a security PIN for critical operations adds an extra layer of security for performing actions like deleting backups. Even if an administrator account is compromised, an attacker would also need access to the security PIN to perform critical operations, such as deleting backups. This aligns with the goal of preventing backups from being deleted, even if an administrator account is compromised.

Options A and D are not directly related to securing backup operations:

Options A and D are not directly related to securing backup operations:

Options A and D are not directly related to securing backup operations:

Options A and D are not directly related to securing backup operations:

Options A and D are not directly related to securing backup operations:

upvoted 3 times

**calotta1** 4 months, 3 weeks ago

A is correct.

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

Selected Answer: A

I'm going with A, the question is about deleting not recovering.

upvoted 1 times

**sbnpj** 5 months, 1 week ago

Selected Answer: A

its clear in the document,
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#what-are-the-best-practices-to-configure-and-protect azure-backups-against-security-and-ransomware-threats

upvoted 1 times

**Potato123Psasas** 5 months, 2 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#what-are-the-best-practices-to-configure-and-protect azure-backups-against-security-and-ransomware-threats

upvoted 1 times

**vicks1x** 6 months, 3 weeks ago

Its A
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#what-are-the-best-practices-to-configure-and-protect azure-backups-against-security-and-ransomware-threats

How to block intentional or unintentional deletion of backup data?
Enable Soft delete is enabled to protect backups from accidental or malicious deletes.

Soft delete is a useful feature that helps you deal with data loss. Soft delete retains backup data for 14 days, allowing the recovery of that backu item before it's permanently lost. For more information, see How to enable, manage and disable soft delete for Azure Backup?

Ensure Multi-user authorization (MUA) is enabled for an additional layer of protection.

MUA for Azure Backup uses a new resource called Resource Guard to ensure critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, are performed only with applicable authorization.

upvoted 1 times

**PrettyFlyWifi** 7 months, 3 weeks ago

I'd argue this could actually be better suited to D - PIM.
Look at:
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#what-are-the-best-practices-to-configure-and-protect azure-backups-against-security-and-ransomware-threats
Use Privileged Identity Management to provide time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, o misused permissions. Learn more.

If you put in place an approval process through PIM, then all admins would need to get the Backup Contributor role.
See: https://learn.microsoft.com/en-us/azure/backup/backup-rbac-rs-vault

upvoted 1 times

**zellck** 8 months ago

Selected Answer: A

A is the answer.

https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq#what-are-the-best-practices-to-configure-and-protect-azure-backups-against-security-and-ransomware-threats
- Ensure Multi-user authorization (MUA) is enabled to protect against rogue admin scenario. MUA for Azure Backup uses a new resource called Resource Guard to ensure critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, are performed only with applicable authorization.

upvoted 4 times

**Shaz** 8 months, 2 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization?tabs=azure-portal&pivots=vaults-recovery-services-vault

upvoted 3 times

**singhaj** 8 months, 2 weeks ago

Answer C: C. From a Recovery Services vault, generate a security PIN for critical operations. because resource guard is not a feature of Azure Backup, so it cant be A

upvoted 1 times

**zellck** 8 months ago

Azure Backup supports Resource Guard.

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization?pivots=vaults-recovery-services-vault&tabs=azure-portal

upvoted 3 times

Question #6 *Topic 5*

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out.

What should you include in the recommendation?

A. device compliance policies

B. Privileged Access Workstations (PAWs)

C. Customer Lockbox for Microsoft Azure

D. emergency access accounts

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**calotta1** 4 months, 3 weeks ago

I can see why some may confuse the 'break-glass' account to this question, but clearly asks to NOT be locked! Which means you've already had access to the environment, whatever that maybe. You don't need emergency account at that point.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices#device-roles-and-profiles
Privileged Access Workstation (PAW) – This is the highest security configuration designed for extremely sensitive roles that would have a signific or material impact on the organization if their account was compromised. The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensit job tasks. This makes the PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: emai and web browsing. To provide productivity to these users, separate accounts and workstations must be provided for productivity applications ar web browsing. While inconvenient, this is a necessary control to protect users whose account could inflict damage to most or all resources in th organization.

upvoted 1 times

**MaciekMT** 9 months ago

Selected Answer: B

ChatGPT: To limit the scope of damage of ransomware attacks without being locked out, you should recommend Privileged Access Workstations (PAWs).

Privileged Access Workstations (PAWs) are dedicated devices that are used to perform sensitive administrative tasks, such as configuring security settings and managing domain controllers. PAWs provide enhanced security by isolating administrative activities from regular user activities and requiring multi-factor authentication and additional controls.

By using a PAW, administrators can perform sensitive tasks without exposing their credentials to the regular network or potentially malicious content, such as ransomware. This helps to limit the scope of damage of ransomware attacks while also maintaining access to critical systems. Therefore, option B is the correct answer.

upvoted 2 times

**aljdeguzman** 9 months ago

I say D

upvoted 3 times

**janesb** 9 months ago

Selected Answer: B

correct
https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware-phase2
https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-devices

upvoted 3 times

Question #7 *Topic 5*

You design cloud-based software as a service (SaaS) solutions.

You need to recommend a recovery solution for ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend doing first?

A. Develop a privileged identity strategy.

B. Implement data protection.

C. Develop a privileged access strategy.

D. Prepare a recovery plan.

**Correct Answer:** *D*

*Community vote distribution*

D (77%) A (15%) 8%

**MaciekMT** Highly Voted 9 months ago

Selected Answer: D

I vote for D - creating recovery plan.
1.Recognize different types of ransomware
2.Help an organization mitigate risk of a ransomware attack by creating a recovery plan
3.Help an organization mitigate risk of a ransomware attack by limiting the scope of damage
4.Help an organization mitigate risk of a ransomware attack by hardening key infrastructure elements
https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/

upvoted 5 times

**Nian** 8 months, 3 weeks ago

Agree - as stated in the Phase 1 is the learning docs:
https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-fc
ransomware-protection-extortion-based-attacks

upvoted 1 times

**rishiraval007** Most Recent 2 months, 2 weeks ago

D. Prepare a recovery plan.

Preparing a recovery plan is essential as it lays out the specific actions and protocols to be followed in the event of a ransomware attack. A well-defined recovery plan ensures that you can quickly and effectively respond to an attack, minimize damage, and restore operations as soon as possible.

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/training/modules/design-resiliency-strategy-common-cyberthreats-like-ransomware/3-ransomware-protectic
Microsoft best practices for ransomware protection are based on a three step approach:
- Prepare your recovery plan
- Limit the scope of the damage
- Make it hard to get in

upvoted 2 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 3 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware#phase-1-prepare-your-recovery-plan

upvoted 1 times

**zellck** 8 months ago

Selected Answer: D

D is the answer.

https://learn.microsoft.com/en-us/training/modules/design-resiliency-strategy-common-cyberthreats-like-ransomware/3-ransomware-protectic
Microsoft best practices for ransomware protection are based on a three step approach:
- Prepare your recovery plan
- Limit the scope of the damage
- Make it hard to get in

upvoted 1 times

**Burnie** 8 months, 3 weeks ago

Selected Answer: D

Phase 1 of ransomware protection is to develop a recovery plan.
The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom.

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-for-ransomware-protection-extortion-based-attacks

upvoted 2 times

**Burnie** 8 months, 3 weeks ago

Phase 1 of ransomware protection is to develop a recovery plan.
The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom.

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-for-ransomware-protection-extortion-based-attacks

upvoted 1 times

**janesb** 9 months, 1 week ago

Selected Answer: C

it should be privileged access strategy
https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-strategy

upvoted 1 times

**janesb** 9 months ago

My initial analysis was Option C, but I think , Option A is More Accurate

upvoted 1 times

**shinda** 9 months, 1 week ago

Selected Answer: A

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/4-recommer
microsoft-ransomware

upvoted 2 times

Question #8 *Topic 5*

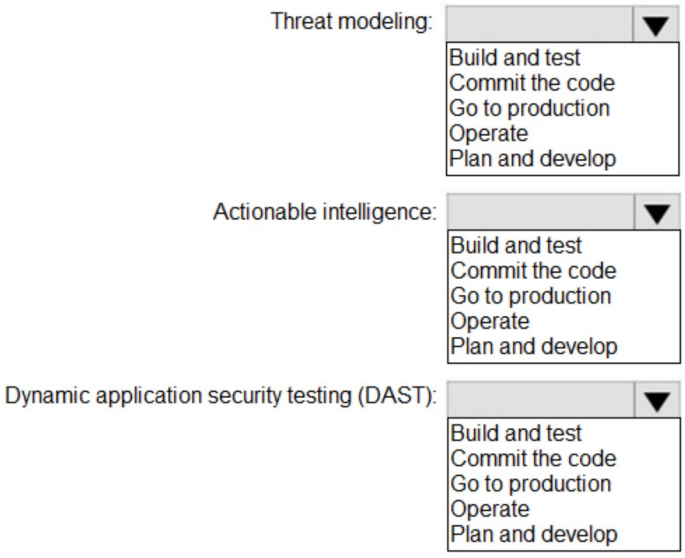
HOTSPOT
-

You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.

During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.

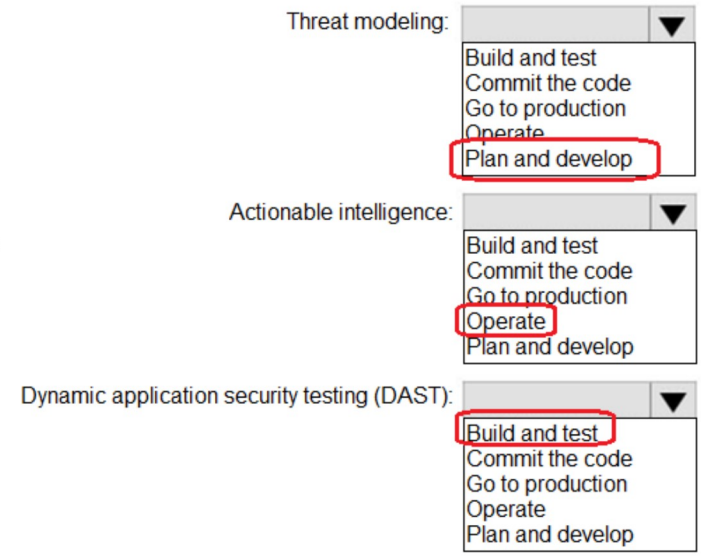
NOTE: Each correct selection is worth one point.

**Answer Area**




**Correct Answer:**

**Answer Area**




**technocorgi** Highly Voted 9 months, 1 week ago
Selected answers are correct!
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls list them in the right place
upvoted 6 times

**Cock** Most Recent 7 months, 2 weeks ago
In the exam 29.05.2023

upvoted 3 times

**zellck** 8 months ago

1. Plan and develop
2. Operate
3. Build and test

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#plan-and-develop
Typically, modern development follows an agile development methodology. Scrum is one implementation of agile methodology that has every sprint start with a planning activity. Introducing security into this part of the development process should focus on:
- Threat modeling to view the application through the lens of a potential attacker
- IDE security plug-ins and pre-commit hooks for lightweight static analysis checking within an integrated development environment (IDE).
- Peer reviews and secure coding standards to identify effective security coding standards, peer review processes, and pre-commit hooks.

upvoted 4 times

**zellck** 8 months ago

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#actionable-intelligence
The tools and techniques in this guidance offer a holistic security model for organizations who want to move at pace and experiment with ne technologies that aim to drive innovation. A key element of DevSecOps is data-driven, event-driven processes. These processes help teams identify, evaluate, and respond to potential risks. Many organizations choose to integrate alerts and usage data into their IT service management (ITSM) platform. The team can then bring the same structured workflow to security events that they use for other incidents and requests.

upvoted 1 times

**aris** 9 months, 1 week ago

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

upvoted 3 times

Question #9 *Topic 5*

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. unit testing

B. penetration testing

C. dependency checks

D. threat modeling

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

**smanzana** 2 months, 3 weeks ago

B is ok

upvoted 1 times

**zellck** 8 months, 1 week ago

Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls#dynamic-application-security-testing
A penetration test consists of several action points, one of which is dynamic application security testing (DAST). DAST is a web application securi test that finds security issues in the running application by seeing how the application responds to specially crafted requests. DAST tools are als known as web application vulnerability scanners.

upvoted 3 times

**zellck** 7 months, 3 weeks ago

Gotten this in May 2023 exam.

upvoted 4 times

**still42** 9 months ago

The automated penetration testing (with manual assisted validation) should also be part of the DAST.

Source: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-devops-security#ds-5-integrate-dynamic-application-security-testin into-devops-pipeline

upvoted 1 times

**janesb** 9 months, 1 week ago

Selected Answer: B

Penetration testing is apart of Dynamic Application Security Testing (DAST)

upvoted 2 times

Question #10 *Topic 5*

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online, SharePoint Online, and Teams in near-real-time (NRT) in response to the following Azure AD events:

• A user account is disabled or deleted.
• The password of a user is changed or reset.
• All the refresh tokens for a user are revoked.
• Multi-factor authentication (MFA) is enabled for a user.

Which two features should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. Azure AD Application Proxy

C. a sign-in risk policy

D. Azure AD Privileged Identity Management (PIM)

E. Conditional Access

**Correct Answer:** *AE*

*Community vote distribution*

AE (80%) AD (20%)

**sherifhamed** 3 months, 3 weeks ago

**Selected Answer: AE**

A. Continuous Access Evaluation (CAE)

E. Conditional Access

upvoted 2 times

**zellck** 8 months, 1 week ago

**Selected Answer: AE**

AE is the answer.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation
Timely response to policy violations or security issues really requires a "conversation" between the token issuer (Azure AD), and the relying party (enlightened app). This two-way conversation gives us two important capabilities. The relying party can see when properties change, like networ location, and tell the token issuer. It also gives the token issuer a way to tell the relying party to stop respecting tokens for a given user because account compromise, disablement, or other concerns. The mechanism for this conversation is continuous access evaluation (CAE). The goal for critical event evaluation is for response to be near real time, but latency of up to 15 minutes may be observed because of event propagation tim however, IP locations policy enforcement is instant.

upvoted 2 times

**zellck** 8 months, 1 week ago

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation#scenarios
There are two scenarios that make up continuous access evaluation, critical event evaluation and Conditional Access policy evaluation.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation#critical-event-evaluatior
Continuous access evaluation is implemented by enabling services, like Exchange Online, SharePoint Online, and Teams, to subscribe to critic Azure AD events. Those events can then be evaluated and enforced near real time. Critical event evaluation doesn't rely on Conditional Acces policies so it's available in any tenant. The following events are currently evaluated:
- User Account is deleted or disabled
- Password for a user is changed or reset
- Multifactor Authentication is enabled for the user
- Administrator explicitly revokes all refresh tokens for a user
- High user risk detected by Azure AD Identity Protection

upvoted 3 times

**MaciekMT** 9 months ago

Selected Answer: AE

according to ChatGPT: To automatically restrict access to Microsoft Exchange Online, SharePoint Online, and Teams in near-real-time (NRT) in response to the specified Azure AD events, you should recommend the following two features:

A. Continuous Access Evaluation: It provides real-time access decisions based on the user's current risk and compliance status. It ensures that or authorized and compliant devices can access the resources.

E. Conditional Access: It allows you to define access policies based on conditions such as user, device, location, and risk level. With Conditional Access, you can enforce multi-factor authentication, block access, or limit access to specific applications or resources based on the user's risk lev and compliance status.

upvoted 4 times

**mohsan001** 9 months ago

CHTGPT4 A and E should be included in the recommendation. Option C (a sign-in risk policy) and Option D (Azure AD Privileged Identity Management (PIM)) are also important security features, but they are not directly related to the NRT access restriction of Exchange Online, SharePoint Online, and Teams in response to Azure AD events. Azure AD Application Proxy (Option B) is not necessary for the functionality described in the scenario.

upvoted 1 times

**omarmkhan22** 9 months ago

Selected Answer: AD

I don't see what conditional access has to do with this.

upvoted 2 times

**zellck** 8 months, 1 week ago

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation#conditional-access-polic evaluation
Exchange Online, SharePoint Online, Teams, and MS Graph can synchronize key Conditional Access policies for evaluation within the service itself.

This process enables the scenario where users lose access to organizational files, email, calendar, or tasks from Microsoft 365 client apps or SharePoint Online immediately after network location changes.

upvoted 1 times

**OK2020** 9 months, 1 week ago

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

upvoted 3 times

Question #11 *Topic 5*

HOTSPOT
-

You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

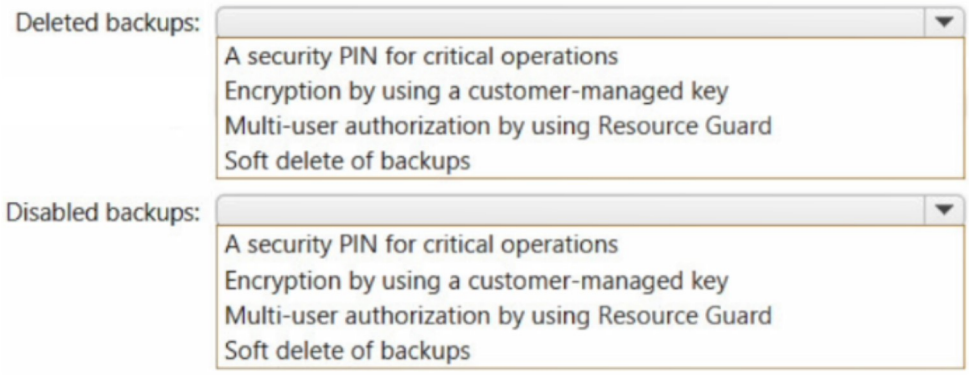
You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

• A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
• A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

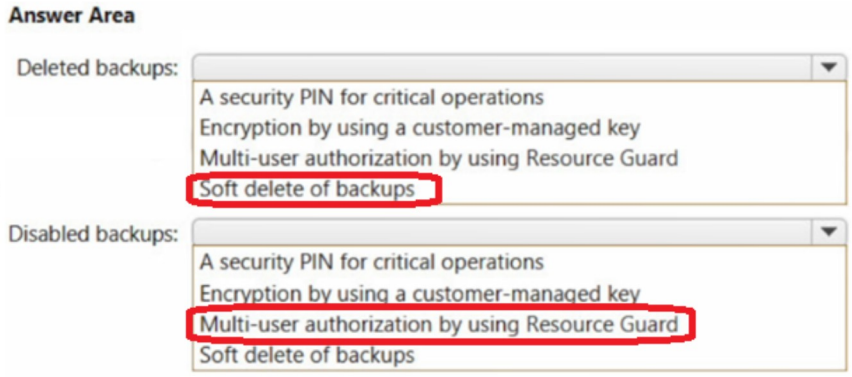
What should you use for each risk? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**




**Correct Answer:**




**MaciekMT** Highly Voted 9 months ago

From ChatGPT: For deleted backups, I would recommend using a security PIN for critical operations - to prevent a compromised administrator account from deleting the backups. This adds an additional layer of security to prevent unauthorized access to the backups.

For disabled backups, I would recommend using Multi-user authorization by using Resource Guard - to prevent a compromised administrator account from disabling the backups. This allows you to specify which users are authorized to perform critical operations and limits the scope of potential attacks.

upvoted 10 times

**Ramye** 1 day, 7 hours ago

ChatGPT may not be reliable. It's not on this question..

upvoted 1 times

**Devon_** 8 months, 3 weeks ago

同意します。
削除： PIN

無効：リソースガード
upvoted 2 times

**Cock** 7 months, 3 weeks ago
66666You can speak Japanese. That's cool
upvoted 4 times

**KallMeDan** 8 months, 3 weeks ago
Would agree here since soft delete will still allow deletion. Security PIN is the preventative control in compromised identity.
upvoted 4 times

**cyber_sa** Highly Voted 3 months, 1 week ago
got this in exam 6oct23. passed with 896 marks. I answered
1. Soft delete of backups
2. Multi-user authorization by using Resource Guard
upvoted 5 times

**Ramye** Most Recent 1 day, 7 hours ago
- Soft Delete - so a copy of the back is stored in the Recycle Bin for 14 Days which can be used to restore

-Multi-user authorization by using Resource Guard - to ensure multiple authorization required for sensitive tasks
upvoted 1 times

**Murtuza** 1 week, 1 day ago
Review this below its the exact same question
https://www.cert2brain.com/Server/Demo.aspx?exam=SC-100
upvoted 1 times

**Murtuza** 1 week, 1 day ago
As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN when you perform Stop Protect with Delete data and Change Passphrase operations.

Multi-user authorization (MUA) for Azure Backup allows you to add an additional layer of protection to critical operations on your Recovery Services vaults and Backup vaults. For MUA, Azure Backup uses another Azure resource called the Resource Guard to ensure critical operations a performed only with applicable authorization. MUA protects against disabling backups and reducing retention for backups.
upvoted 1 times

**Intrudire** 2 months, 1 week ago
Deleted Backups: Soft Delete
Disabled Backups: Resource Guard
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

I don't exactly know how this reconciles with all the previous questions saying PIN was a configuration protection mechanism.
upvoted 2 times

**billy22** 1 month, 2 weeks ago
Ensure soft delete is enabled to protect backups from accidental or malicious deletes

Soft delete is enabled by default on a newly created Recovery Services vault. It protects backup data from accidental or malicious deletes for days at no additional cost, allowing the recovery of that backup item before it's permanently lost. We recommend not to disable this feature. backups are deleted and soft delete isn't enabled, you or Microsoft can't recover the deleted backup data. Use Multi-user authorization (MU as an additional layer of protection for these critical operations on your Recovery Services vault to validate operation before disabling this feature.

Ensure Multi-user authorization (MUA) is enabled to protect against rogue admin scenario.

MUA for Azure Backup uses a new resource called the Resource Guard to ensure critical operations, such as disabling soft delete, stopping ar deleting backups, or reducing retention of backup policies, are performed only with applicable authorization.
upvoted 2 times

**rishiraval007** 2 months, 2 weeks ago
Deleted backups:

C. Multi-user authorization by using Resource Guard
Resource Guard is a feature in Azure Backup that can provide an additional layer of protection for your backup data. It requires more than one person (multi-user authorization) to perform critical operations like deleting backup data, which helps protect against the risk of a compromisec administrator account being used to delete backups.

Disabled backups:

D. Soft delete of backups
Soft delete provides a retention period for deleted backups, meaning that even if backups are deleted (either accidentally or maliciously), they a retained for a set period (by default 14 days) and can be recovered during that time. This can protect against a compromised account attemptin to disable backups on the MARS agent before encrypting the servers, as you would still have a window to recover those backups.
upvoted 1 times

**smanzana** 2 months, 3 weeks ago

1. Soft delete of backups
2. Multi-user authorization by using Resource Guard

upvoted 3 times

**ConanBarb** 3 months, 3 weeks ago

Deleted backups: Multi-user authorization
So this is about the service in Azure. Not the servers on-prem.
https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization?tabs=azure-portal&pivots=vaults-recovery-services-vault
Search for: "For example, disabling soft delete is depicted here"

Disabled backups: security PIN
It's critical to note here that this is about the MARS agent, i.e. on the server "A compromised administrator account used to disable the backups the MARS agent before encrypting the servers". Not anything on Azure.
This guide explains how to manage and protect the MARS agent, and includes setting the PIN.
https://learn.microsoft.com/en-us/azure/backup/backup-azure-manage-mars

upvoted 1 times

**ServerBrain** 4 months, 4 weeks ago

given answers are on point.

https://learn.microsoft.com/en-us/azure/backup/guidance-best-practices

upvoted 1 times

**MaciekMT** 5 months, 3 weeks ago

It looks like soft delete is only available on Azure VM workloads - https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-featur cloud. the question states: "The datacenter contains 100 servers that run Windows Server"

upvoted 2 times

**zellck** 8 months, 1 week ago

1. Soft delete of backups
2. Multi-user authorization by using Resource Guard

https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature-cloud
Concerns about security issues, like malware, ransomware, and intrusion, are increasing. These security issues can be costly, in terms of both mo and data. To guard against such attacks, Azure Backup now provides security features to help protect backup data even after deletion.

One such feature is soft delete. With soft delete, even if a malicious actor deletes a backup (or backup data is accidentally deleted), the backup d is retained for 14 additional days, allowing the recovery of that backup item with no data loss. The additional 14 days of retention for backup da in the "soft delete" state don't incur any cost to you.

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization-concept?tabs=recovery-services-vault

upvoted 2 times

**CarisB** 8 months, 3 weeks ago

I go for soft delete & security PIN

upvoted 2 times

**OK2020** 9 months, 1 week ago

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization-concept?tabs=backup-vault

upvoted 1 times

## Topic 6 - Testlet 1

Question #1 *Topic 6*

**Introductory Info**

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

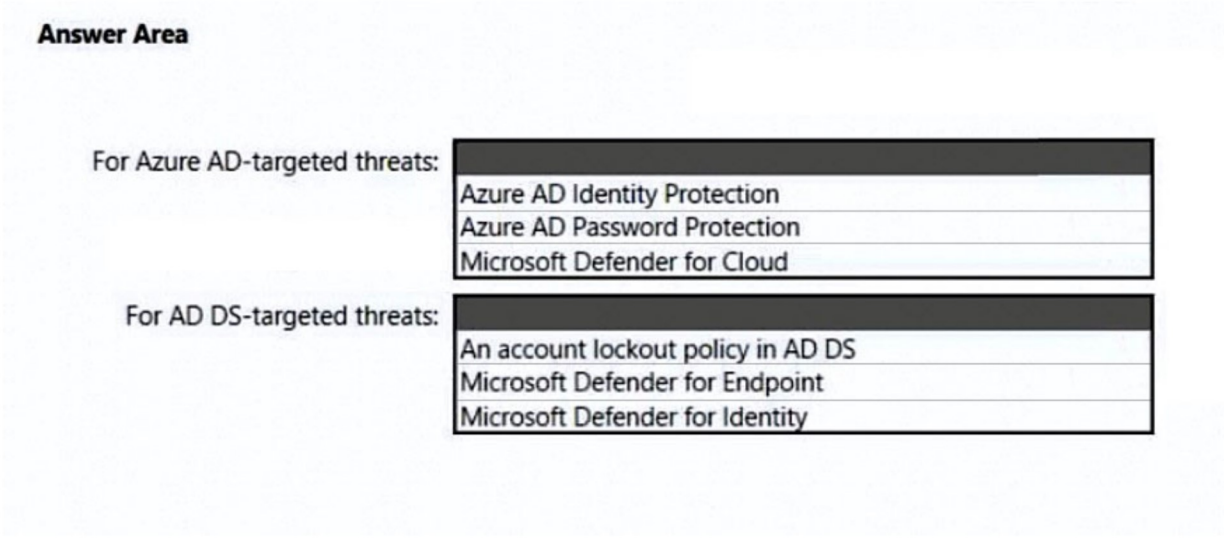
Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:
Detect brute force attacks that directly target AD DS user accounts.
Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

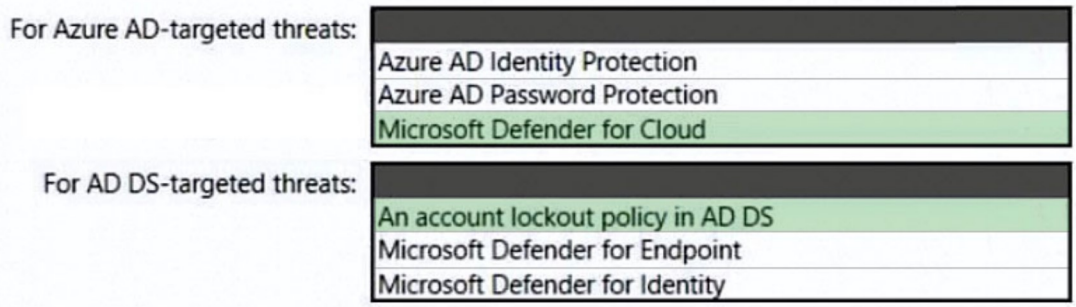
**Question**

HOTSPOT -
You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:




**Correct Answer:**

**Answer Area**




Box 1: Microsoft defender for cloud

Scenario: Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

When Microsoft Defender for Cloud detects a Brute-force attack, it triggers an alert to bring you awareness that a brute force attack took place. The automation uses this alert as a trigger to block the traffic of the IP by creating a security rule in the NSG attached to the VM to deny inbound traffic from the IP addresses attached to the alert. In the alerts of this type, you can find the attacking IP address appearing in the 'entities' field of the alert.

Box 2: An account lockout policy in AD DS

Scenario:

Detect brute force attacks that directly target AD DS user accounts.

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

Verify on-premises account lockout policy

To verify your on-premises AD DS account lockout policy, complete the following steps from a domain-joined system with administrator privileges:

1. Open the Group Policy Management tool.
2. Edit the group policy that includes your organization's account lockout policy, such as, the Default Domain Policy.
3. Browse to Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.
4. Verify your Account lockout threshold and Reset account lockout counter after values.

Reference:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/automation-to-block-brute-force-attacked-ip-detected-by/ba-p/1616825

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#verify-on-premises-account-lockout-policy

**PlumpyTumbler** Highly Voted 1 year, 4 months ago

Box 1: Identity Protection
https://docs.microsoft.com/en-us/defender-cloud-apps/aadip-integration#configure-identity-protection-policies
Box 2: Lockout policy
The case study scenario says "Azure AD Connect is used to implement pass-through authentication." The link below explains "Smart lockout can integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers. By setting smart lockout policies in Azure AD appropriately, attacks can be filtered out before they reach on-premises AD DS."

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#how-smart-lockout-works

Any other solution relies on AD FS. Since the case study doesn't say anything about AD FS, use the lockout policy as described.

That's my last comment, I'm taking the exam in 20 minutes. Thank you all and good day.

upvoted 42 times

**awssecuritynewbie** 10 months, 4 weeks ago

Block 1; Microsoft AD Identity protection
Block 2 ; Microsoft Defender for Identity

The ones saying it is Lockout policy that does not provide protection, there are things like Suspected overpass-the-hash attack (Kerberos) 20 Medium
Account enumeration reconnaissance 2003 Medium

Suspected Brute Force attack (LDAP) 2004 Medium

there are some of the protection and alerts the Defender for identity on perm provides, the password lock out policy will only actually prever the brute force attack...

upvoted 8 times

**Sam_Gutterson** 11 months, 2 weeks ago

I am not sure if these are correct choices however, the case study clearly says 'password has sync has been disabled' under overview. Also, this specific question of the case study clearly says 'Forest' (AD Forest).

upvoted 2 times

**JakeCallham** 1 year, 2 months ago

I agree on both points, 1 cannot be defender as it misses the word apps.

upvoted 2 times

**Brick69** 1 year, 4 months ago

How did you do?

upvoted 5 times

**JaySapkota** Highly Voted 1 year, 4 months ago

Answers should be:
1. Azure AD Identity Protection
Brute Force Detection: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

2. Defender for Identity
MDI can detect brute force attacks: ref: https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts#suspected-bru force-attack-ldap-external-id-2004

upvoted 29 times

**Bubsator** 1 year, 3 months ago

Box 1: Wrong. Identity protection does not provide AAD account smart lockout. Only the Password Protection service can.
Box 2: Correct

upvoted 4 times

**JakeCallham** 1 year, 2 months ago

Box1: Correct, box one doesn't relate to smart lockout?
Box 2: Incorrect

upvoted 3 times

**Murtuza** Most Recent 1 week ago

Case Study says " Implement leaked credential detection in the Azure AD tenant of Litware"

This broad range of signals helps Identity Protection detect risky behaviors like:
Password spray attacks
Leaked credentials

upvoted 1 times

**Kdosec** 2 weeks, 6 days ago

Box 1: Azure AD Identity Protection
Box 2: Microsoft Defender for Identity (the key point "Prevent AD DS user accounts from being locked out by brute force attacks that target Azu AD user accounts." , the requirement is to don't lockout their accounts from Brute-force attacks)

upvoted 1 times

**cybrtrk** 1 month, 2 weeks ago

One of the requirements was to NOT lock out accounts, so account lockout policy won't work.
Defender for identity will detect the ddos attack and it can be configured to force an account password reset vs locking out the account, by configuring it's remediation actions.
https://learn.microsoft.com/en-us/defender-for-identity/manage-action-accounts

upvoted 1 times

**rishiraval007** 2 months, 2 weeks ago

Block 1; Microsoft AD Identity protection
Block 2 ; Microsoft Defender for Identity

upvoted 1 times

**slobav** 3 months, 3 weeks ago

Box 1: Identity Protection
Box 2: Lockout policy
Explanation: https://www.youtube.com/watch?v=YJqZjdzC9xE&list=PLQ2ktTy9rklhzzkSEZvDZT4QSIVUQZD-Y&index=7
SC-100 Question 91

upvoted 1 times

**CatoFong** 4 months ago

"The solution must meet the identity requirement"

Azure AD Identity Protection
Defender for Identity

upvoted 1 times

**zellck** 7 months, 3 weeks ago

1. Azure AD Identity Protection
2. Microsoft Defender for Identity

https://learn.microsoft.com/en-us/defender-for-identity/credential-access-alerts#suspected-brute-force-attack-ldap-external-id-2004
In a brute-force attack, the attacker attempts to authenticate with many different passwords for different accounts until a correct password is fo
for at least one account. Once found, an attacker can log in using that account.

In this detection, an alert is triggered when Defender for Identity detects a massive number of simple bind authentications. This alert detects bru
force attacks performed either horizontally with a small set of passwords across many users, vertically with a large set of passwords on just a few
users, or any combination of the two options. The alert is based on authentication events from sensors running on domain controller and AD FS
servers.

upvoted 3 times

**zellck** 7 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#sign-in-risk
Password spray
- A password spray attack is where multiple usernames are attacked using common passwords in a unified brute force manner to gain
unauthorized access. This risk detection is triggered when a password spray attack has been successfully performed. For example, the attacke
successfully authenticated, in the detected instance.

upvoted 1 times

**KallMeDan** 8 months, 3 weeks ago

box 1 - Microsoft defender for cloud. Identity protection also similar protection but in the requirement for this states "Some premium features c
Azure AD, like Identity Protection and Azure AD Domain Services, require password hash synchronization, no matter which authentication metho
you choose." which is disabled in the case study.
Box 2 - Smart lockout - Some premium features of Azure AD, like Identity Protection and Azure AD Domain Services, require password hash
synchronization, no matter which authentication method you choose.

upvoted 3 times

**KallMeDan** 8 months, 3 weeks ago

Box 2 - Smart lockout - You can integrate Smart Lockout with hybrid deployments that use password hash sync or pass-through authenticati
to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers. By setting smart lockout polic
in Azure AD appropriately, attacks can be filtered out before they reach on-premises AD DS. If you want your Azure AD lockout threshold to
5, then you want your on-premises AD lockout threshold to be 10. This configuration would ensure smart lockout prevents your on-premises
AD accounts from being locked out by brute force attacks on your Azure AD accounts.

upvoted 1 times

**Gurulee** 10 months, 1 week ago

Although the current overview states pwd has sync is disabled, the identity requirements state: "Implement leaked credential detection in the Az
AD tenant of Litware.". Therefore, you need to implement the best controls to meet the requirements.
1: Identity Protection
2: Defender for Identity

upvoted 1 times

**AJ2021** 10 months, 1 week ago

Q1 Microsoft AD Identity protection
Q2 Microsoft Defender for Identity

upvoted 1 times

**PeteNZ** 10 months, 2 weeks ago

This is a tricky one as it does say that password hash sync is disabled... So technically Identity Protection wouldn't work as it requires PHS. Hmm.

upvoted 2 times

**awssecuritynewbie** 10 months, 4 weeks ago

Block 1; Microsoft AD Identity protection
Block 2 ; Microsoft Defender for Identity

The ones saying it is Lockout policy that does not provide protection, there are things like Suspected overpass-the-hash attack (Kerberos) 2002
Medium
Account enumeration reconnaissance 2003 Medium
Suspected Brute Force attack (LDAP) 2004 Medium

there are some of the protection and alerts the Defender for identity on perm provides, the password lock out policy will only actually prevent tl
brute force attack...

upvoted 3 times

**OrangeSG** 11 months, 3 weeks ago

Box 1: Azure AD Identity Protection

Box 2: An account lockout policy in AD DS

Smart lockout can be integrated with hybrid deployments that use password hash sync or pass-through authentication to protect on-premises Active Directory Domain Services (AD DS) accounts from being locked out by attackers.
Not Microsoft Defender for Identity because it can only detect brute force attacks but can not meet requirement of 'Prevent AD DS user accoun from being locked out by brute force attacks'

upvoted 3 times

**TP447** 1 year, 1 month ago

Key for Box 2 is "..attacks that directly target ADDS users" which falls outside of AAD as the attack vector - hence a standard ADDS lockout polic would be the solution.

upvoted 1 times

**SelloLed** 1 year, 2 months ago

Block 1; Microsoft AD Identity protection
Block 2 ; Microsoft Defender for Identity

upvoted 3 times

**Introductory Info**

Case Study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment -

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to

20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Requirements. Planned Changes -

Litware plans to implement the following changes:

Create a management group hierarchy for each Azure AD tenant.

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

▪

Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Requirements. Business Requirements

Litware identifies the following business requirements:

Minimize any additional on-premises infrastructure.

Minimize the operational costs associated with administrative overhead.

Requirements. Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Enable the management of on-premises resources from Azure, including the following:

- Use Azure Policy for enforcement and compliance evaluation.
- Provide change tracking and asset inventory.
- Implement patch management.

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Requirements. Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft

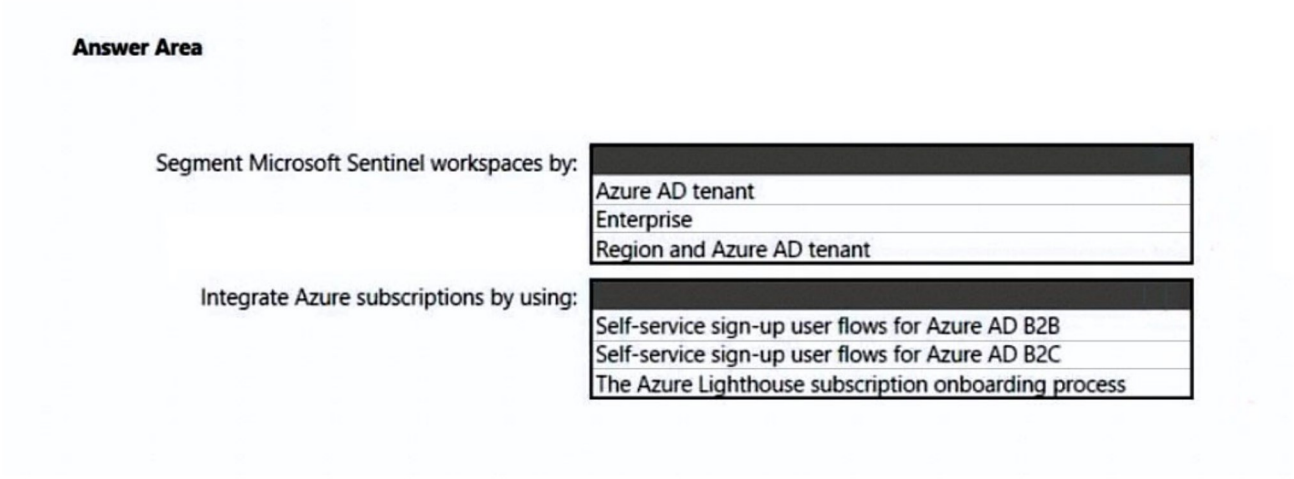
Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Requirements. Identity Requirements

Litware identifies the following identity requirements:
Detect brute force attacks that directly target AD DS user accounts.
Implement leaked credential detection in the Azure AD tenant of Litware.
Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- The management of group properties, membership, and licensing
- The management of user properties, passwords, and licensing
- The delegation of user management based on business units
Requirements. Regulatory Compliance Requirements
Litware identifies the following regulatory compliance requirements:
Ensure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
▪
Use the principle of least privilege.
Requirements. Azure Landing Zone Requirements
Litware identifies the following landing zone requirements:
Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
Provide a secure score scoped to the landing zone.
Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
Minimize the possibility of data exfiltration.
Maximize network bandwidth.
The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:
Be created in a dedicated subscription.
Use a DNS namespace of litware.com.
Requirements. Application Security Requirements
Litware identifies the following application security requirements:
Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

**Question**

HOTSPOT -
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:




**Correct Answer:**

**Answer Area**

Segment Microsoft Sentinel workspaces by:

| |
|---|
| Azure AD tenant |
| Enterprise |
| Region and Azure AD tenant |