# Microsoft.SC-100.v2026-01-20.q141

| | |
|---|---|
| **Exam Code:** | SC-100 |
| **Exam Name:** | Microsoft Cybersecurity Architect |
| **Certification Provider:** | Microsoft |
| **Free Question Number:** | 141 |
| **Version:** | v2026-01-20 |
| **# of views:** | 107 |
| **# of Questions views:** | 1410 |
| https://www.freepdfdumps.com/Microsoft.SC-100.v2026-01-20.q141.html | |

**NEW QUESTION: 1**
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
**Answer: B (LEAVE A REPLY)**
Many networking and security devices and appliances send their system logs over the Syslog protocol in a specialized format known as Common Event Format (CEF). This format includes more information than the standard Syslog format, and it presents the information in a parsed key-value arrangement. The Log Analytics Agent accepts CEF logs and formats them especially for use with Microsoft Sentinel, before forwarding them on to your Microsoft Sentinel workspace.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/connect-common-event-format

**NEW QUESTION: 2**
Hotspot Question
You have the Azure subscriptions shown in the following table.

| Name | Linked Microsoft Entra tenant | Description |
|---|---|---|
| Sub1 | contoso.com | Contain an Azure Backup vault named Vault1 |
| Sub2 | contososecurity.com | Used to manage security resources |

The tenants contain the groups shown in the following table.

| Name | Tenant | Members |
|---|---|---|
| Group1 | contoso.com | Adminisrtator who manage Backup for Sub1 |
| Group 2 | contososecurity.com | Adminisrtator who manage secirity for Sub1 and Sub2 |

You perform the flowing actions:

- Configure multi-user authorization (MUA) for Vault1 by using a resource guard deployed to Sub2.
- Enable all available MUA controls for Vault1.
- In contoso.com, create a Privileged Identity Management (PIM) assignment named Assignment1.
- Configure Assignment1 to enable Group1 to activate the Contributor role for Vault1.

For each of the following statements, select Yes if the statements is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| To enable MUA for Vault1, a resource guard must be deployed to Sub1. | ○ | ○ |
| A user in Group2 must approve changes made by a user in Group1 to the backup policies of Vault1. | ○ | ○ |
| A user in Group1 that activates Assignment1 can disable soft delete for the backups of Vault1, without the approval of a user in Group2. | ○ | ○ |



**Answer:**

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| To enable MUA for Vault1, a resource guard must be deployed to Sub1. | ○ | ● |
| A user in Group2 must approve changes made by a user in Group1 to the backup policies of Vault1. | ● | ○ |
| A user in Group1 that activates Assignment1 can disable soft delete for the backups of Vault1, without the approval of a user in Group2. | ○ | ● |



Explanation:

Box 1: No

No - To enable MUA for Vault1, a resource guard must be deployed to Sub1.

The Backup vault is in Sub1.

You create a Resource Guard in a different tenant than the Backup Fault, to get maximum protection.

Note: The Security admin creates the Resource Guard. We recommend that you create it in a different subscription or a different tenant as the vault.

However, it should be in the same region as the vault.

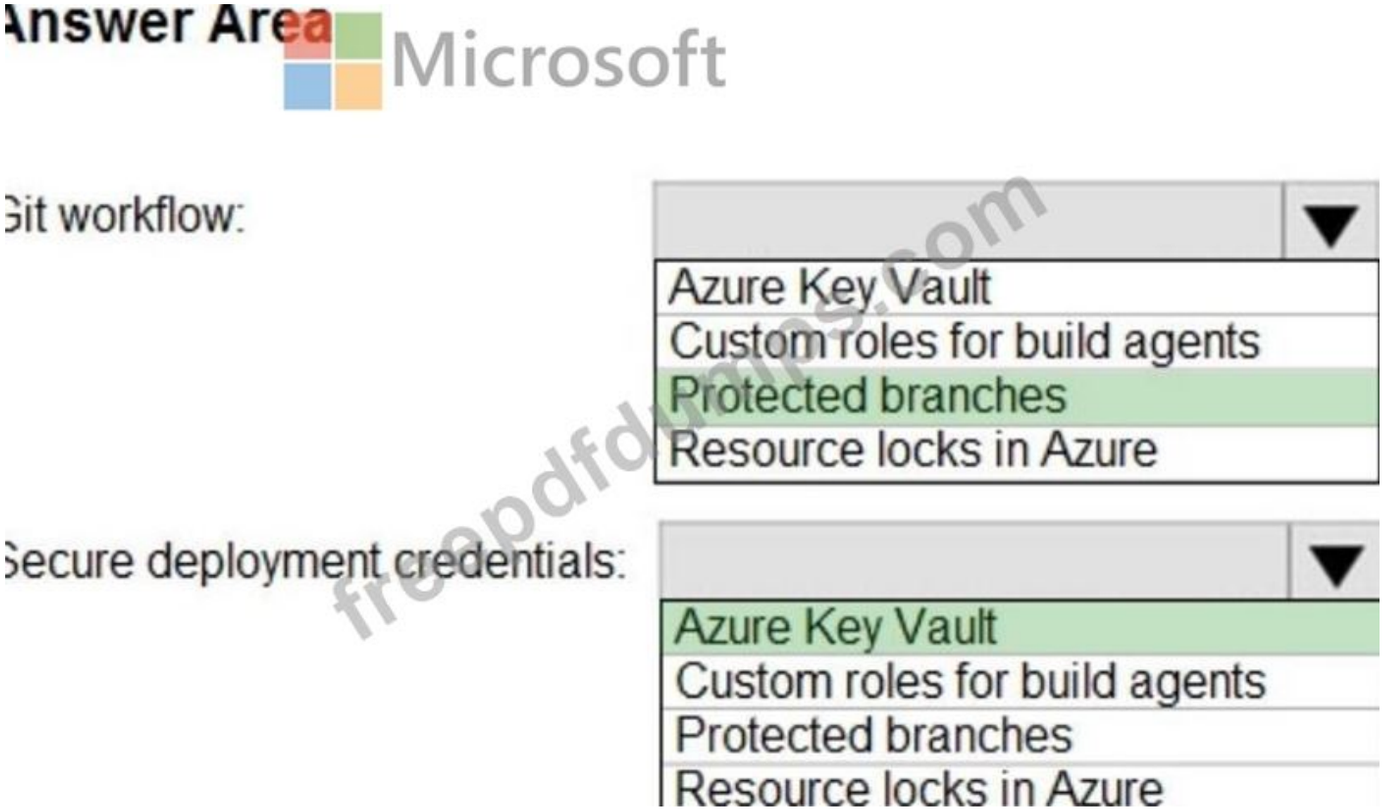
Box 2: Yes

Yes - A user in Group2 must approve changes-made by a user in Group1 to the backup policies of Vault1.
Group1 has administrators who manage Backup for Sub1.
Group2 has administrators who manage security for Sub1 and Sub2.
Box 3: No
No - A user in Group1 that activates Assignment1 can disable soft for the backups of Vault1, without the approval of a user in Group2.
You can't disable the protected operations - Disable soft delete and Remove MUA protection.
Reference:
https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

**NEW QUESTION: 3**
Hotspot Question
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:**

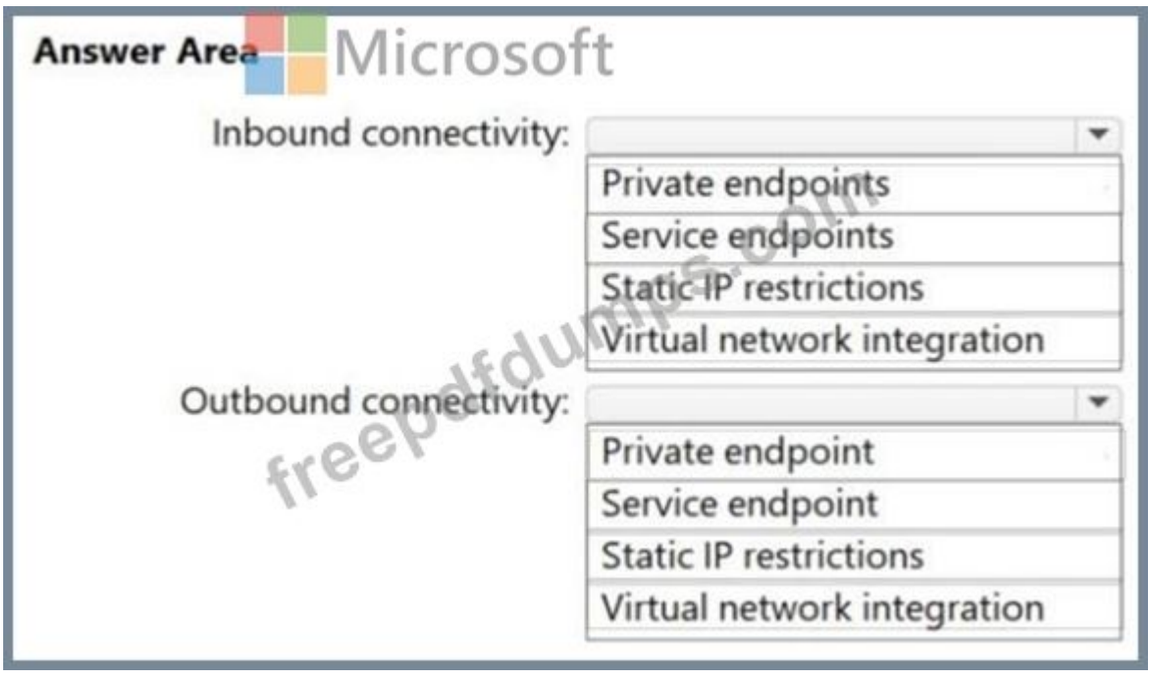
Answer Area





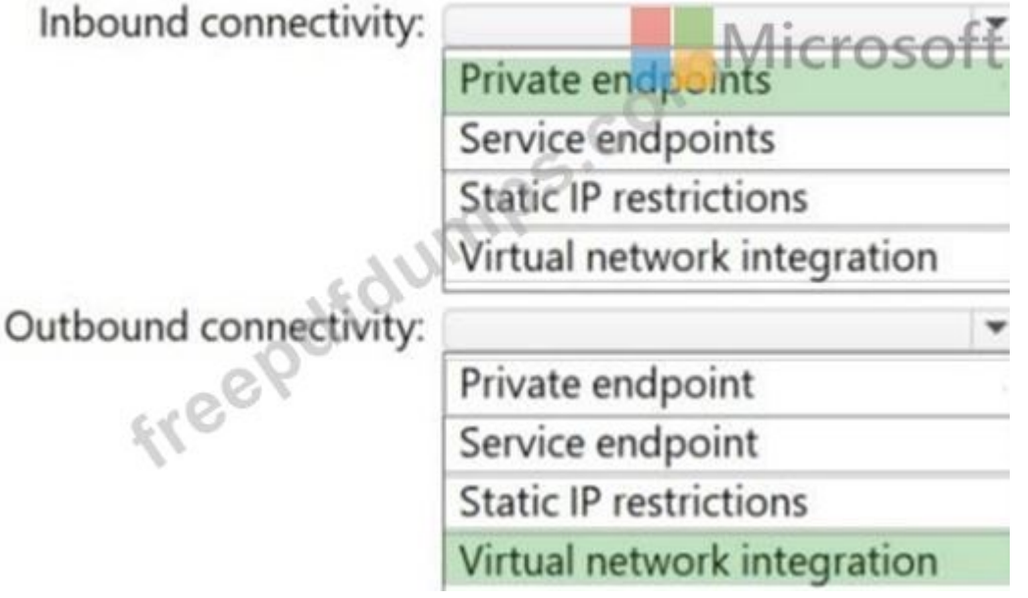

Explanation:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops

**NEW QUESTION: 4**
Hotspot Question
You have an Azure subscription that contains two virtual machines named VM1 and VM2 and an Azure App Service Standard app named App1. VM1 is used to upload data to App1. App1 stores data on VM2.
You need to secure connectivity between the virtual machines and App1. The solution must minimize the risk of data exfiltration.
What should you use to manage connectivity for App1? To answer, select the options in the answer area.
NOTE: Each correct answer is worth one point.




**Answer:**

**Answer Area**




Explanation:

Box 1: Private endpoints

Inbound connectivity

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. Refer to private endpoint for inbound private access.

Box 2: Virtual network integration

Outbound connectivity

How virtual network integration works

Apps in App Service are hosted on worker roles. Virtual network integration works by mounting virtual interfaces to the worker roles with addresses in the delegated subnet. The virtual interfaces used aren't resources customers have direct access to. Because the from address is in your virtual network, it can access most things in or through your virtual network like a VM in your virtual network would.


When virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address is an address from the integration subnet. The private IP assigned to an instance is exposed via the environment variable, WEBSITE_PRIVATE_IP.
Reference:
https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration

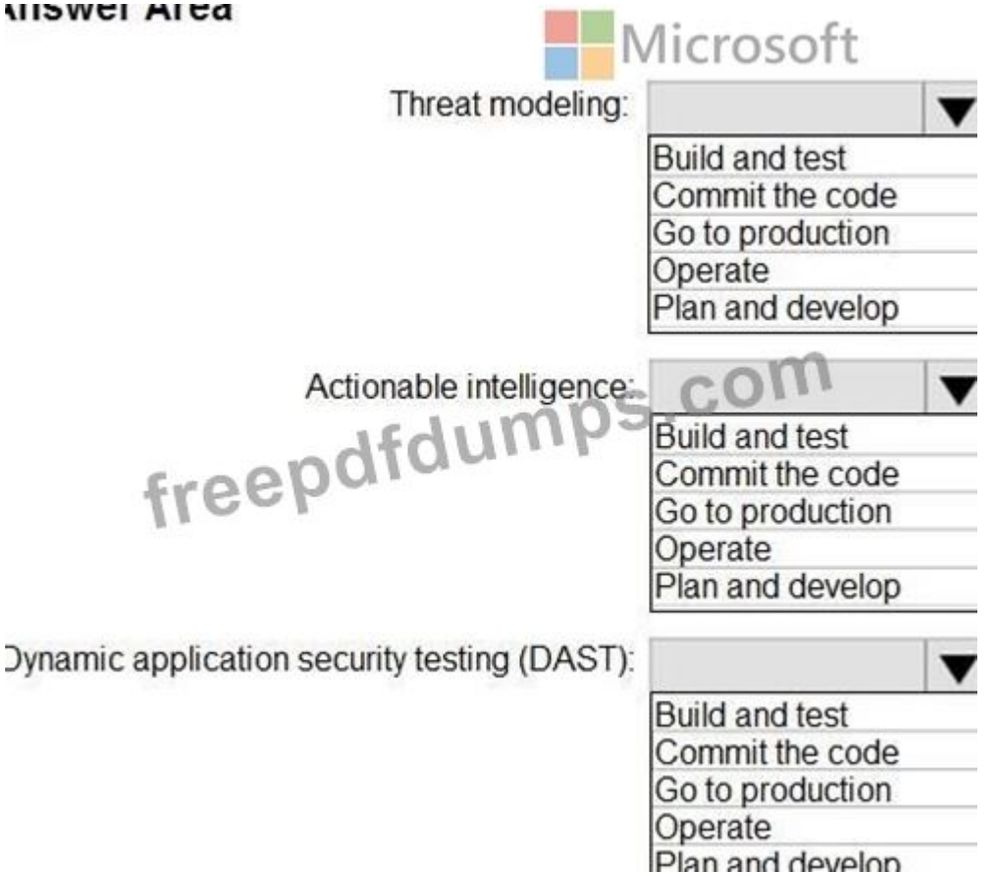
**NEW QUESTION: 5**
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?
**A.** From Defender for Cloud, enable Defender for Cloud plans.
**B.** From Azure Policy, assign a built-in policy definition 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 initiative that has a scope of the subscription.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 6**
You have a Microsoft Entra tenant named contoso.onmicrosoft.com and an Azure subscription named Sub1.
You need to implement Microsoft Entra Verified ID by using Quick Verified ID setup.
What should you create first?
**A.** a security principal in contoso.onmicrosoft.com
**B.** a custom domain in contoso.onmicrosoft.com

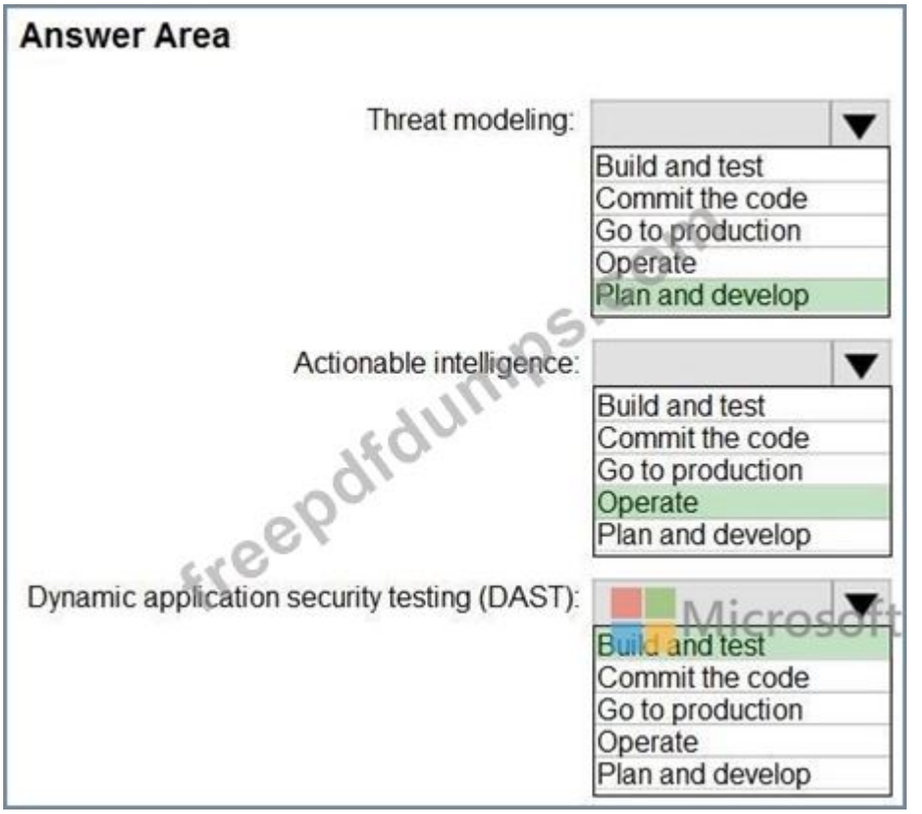
**C.** a user-assigned managed identity in Sub1
**D.** an Azure key vault in Sub1
**Answer: B (LEAVE A REPLY)**
Microsoft Entra Verified ID, Quick Microsoft Entra Verified ID setup
Prerequisites
* You need the Authentication Policy Administrator permission for the directory you want to configure. If you need to perform app registration tasks, you'll also need the Application Administrator permission.
* Ensure that you have a custom domain registered for the Microsoft Entra tenant. If you don't have one registered, the setup defaults to the advanced setup experience.
Reference:
https://learn.microsoft.com/en-us/entra/verified-id/verifiable-credentials-configure-tenant-quick
https://learn.microsoft.com/en-us/entra/identity/users/domains-manage

**NEW QUESTION: 7**
Hotspot Question
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

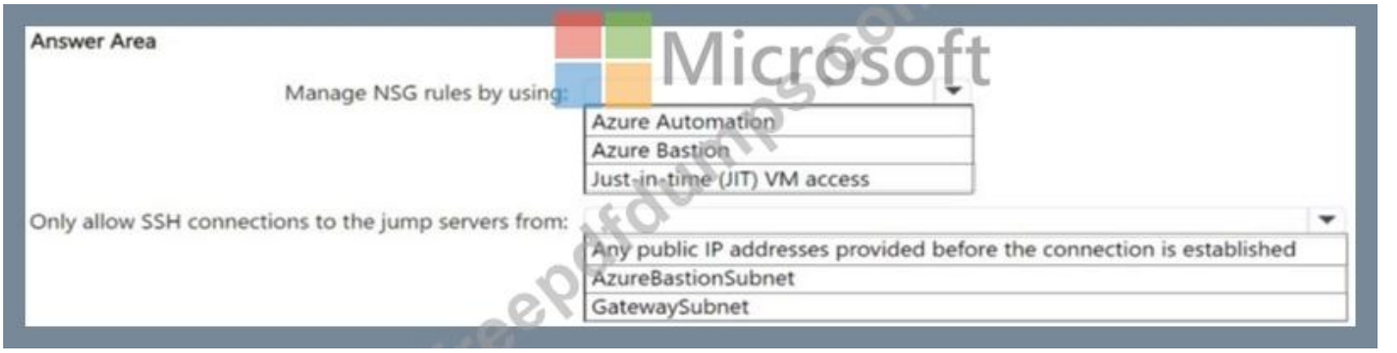


**Answer:**

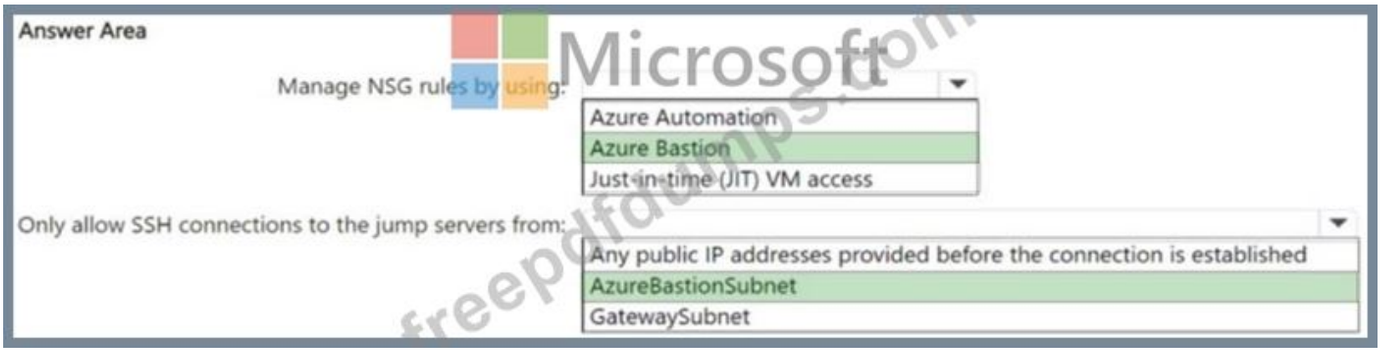



Explanation:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

**NEW QUESTION: 8**
Hotspot Question
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG).
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
- Ensure that each time the support staff connects to a jump server,
they must request access to the server.
- Ensure that only authorized support staff can initiate SSH
connections to the jump servers.
- Maximize protection against brute-force attacks from internal
networks and the internet.
- Ensure that users can only connect to the jump servers from the
internet.
- Minimize administrative effort.
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.




**Answer:**




Explanation:

Box 1: Azure Bastion

Manage NSG rules by using:

Box 2: AzureBastionSubnet

Ensure that only authorized support staff can initiate SSH connections to the jump servers.

Configure Bastion for native client connections

Secure your native client connection

If you want to further secure your native client connection, you can limit port access by only providing access to port 22/3389. To restrict port access, you must deploy the following NSG rules on your AzureBastionSubnet to allow access to select ports and deny access from any other ports.

Reference:

https://learn.microsoft.com/en-us/azure/bastion/native-client

**NEW QUESTION: 9**

Hotspot Question

You have multiple on-premises Hyper-V hosts that contain virtual machines. The virtual machines run Windows Server 2022.

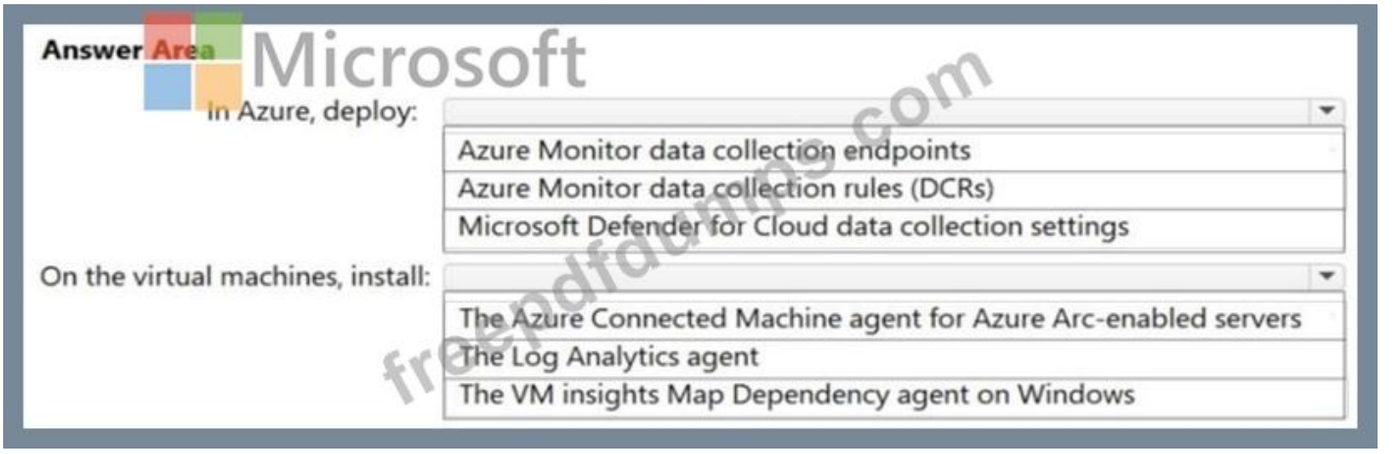
You have an Azure subscription.

You need to recommend a solution to collect Security event logs from the virtual machines by using Microsoft Sentinel. The Solution must meet the following requirements:

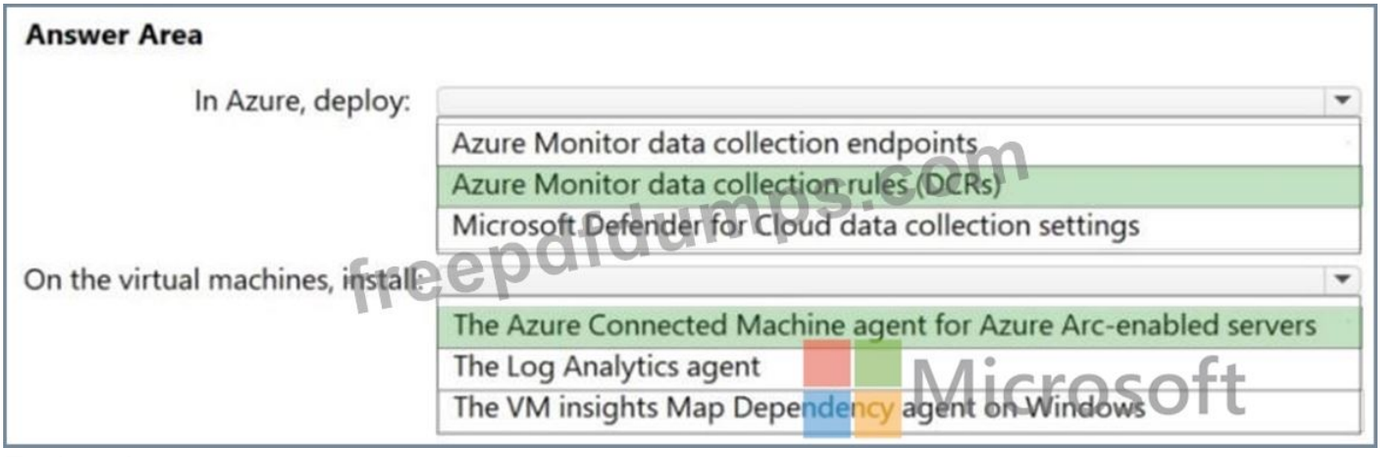
- Leverage the Windows Security Events via AMA data connector.
- Ensure that only specific events are collected.
- Minimize costs.

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

NOTE: Each correct selection is worth one port.




**Answer:**




Explanation:

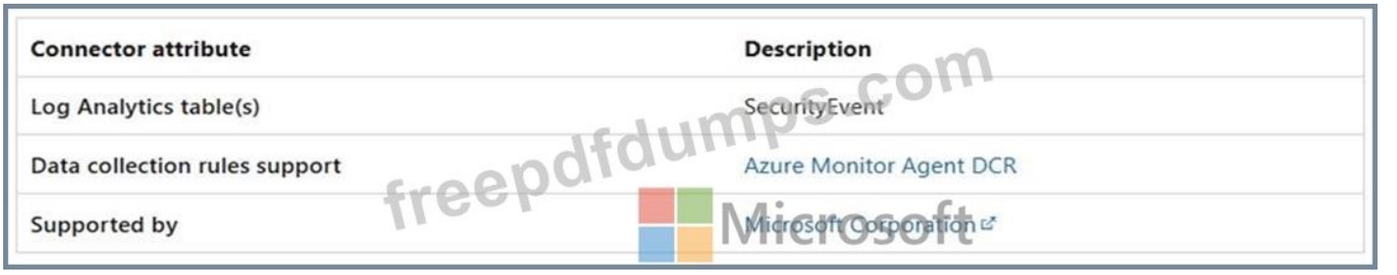
Box 1: Azure Monitor data collection rules (DCRs)

In Azure, deploy

Windows Security Events via AMA connector for Microsoft Sentinel

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Connector attributes



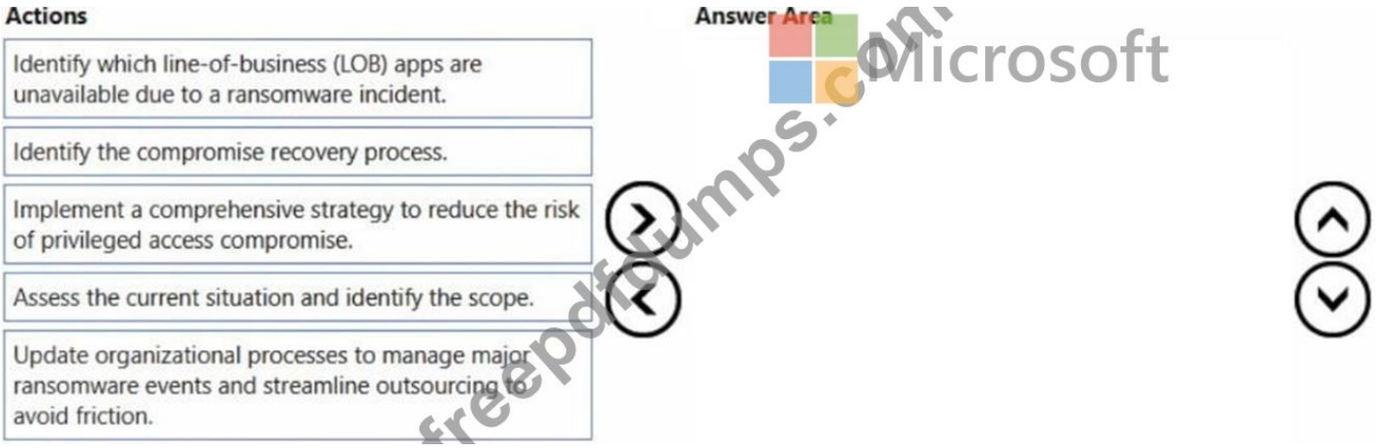
| Connector attribute | Description |
|---|---|
| Log Analytics table(s) | SecurityEvent |
| Data collection rules support | Azure Monitor Agent DCR |
| Supported by | Microsoft Corporation |

Create a data collection rule

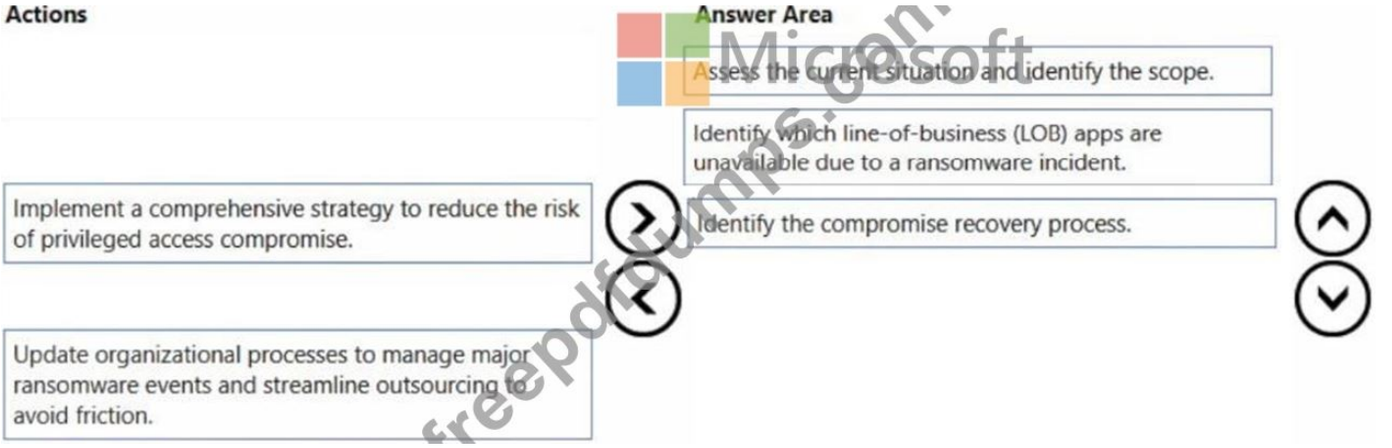
You can define a data collection rule to send data from multiple machines to multiple Log Analytics workspaces, including workspaces in a different region or tenant. Create the data collection rule in the same region as your Log Analytics workspace. You can send Windows event

and Syslog data to Azure Monitor Logs only. You can send performance counters to both Azure Monitor Metrics and Azure Monitor Logs.
Box 2: The Azure Connected Machine agent for Azure Arc-enabled servers
On the virtual machines, install
The Azure Connected Machine agent enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers.
Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent
https://learn.microsoft.com/en-us/windows-server/administration/azure
https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview

**NEW QUESTION: 10**
Drag and Drop Question
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.




**Answer:**




Explanation:

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

**NEW QUESTION: 11**
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.
**Answer: B (LEAVE A REPLY)**
https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/self-healing-in-microsoft-365-defender/ba-p/1729527

**NEW QUESTION: 12**
You are a security administrator for Microsoft 365; you implemented Microsoft Defender for Identity You have created several test accounts with specific configurations for the purpose of vulnerability testing, When attackers try to exploit these accounts, you would like to be alerted to see what areas in the configuration needs improvements.
What features in Microsoft Defender for Identity can you use to meet your objective?
**A.** Sensitivity labels
**B.** System user tags
**C.** Confidential label
**D.** Honeytoken entity tags
**Answer: (SHOW ANSWER)**
Option A is incorrect because a sensitivity label is a tag applied to content containing sensitive data, whether text documents, spreadsheets, or emails. This will not meet the objective.
Option B is incorrect because User tags are identifiers for specific groups of users in Microsoft Defender for Office 365 and will not meet the objective.
Option C is incorrect because a confidential label is a sensitivity label you can use to add a layer of security to your files or emails.
Option D is correct because Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.
Reference:
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity

**NEW QUESTION: 13**
Hotspot Question

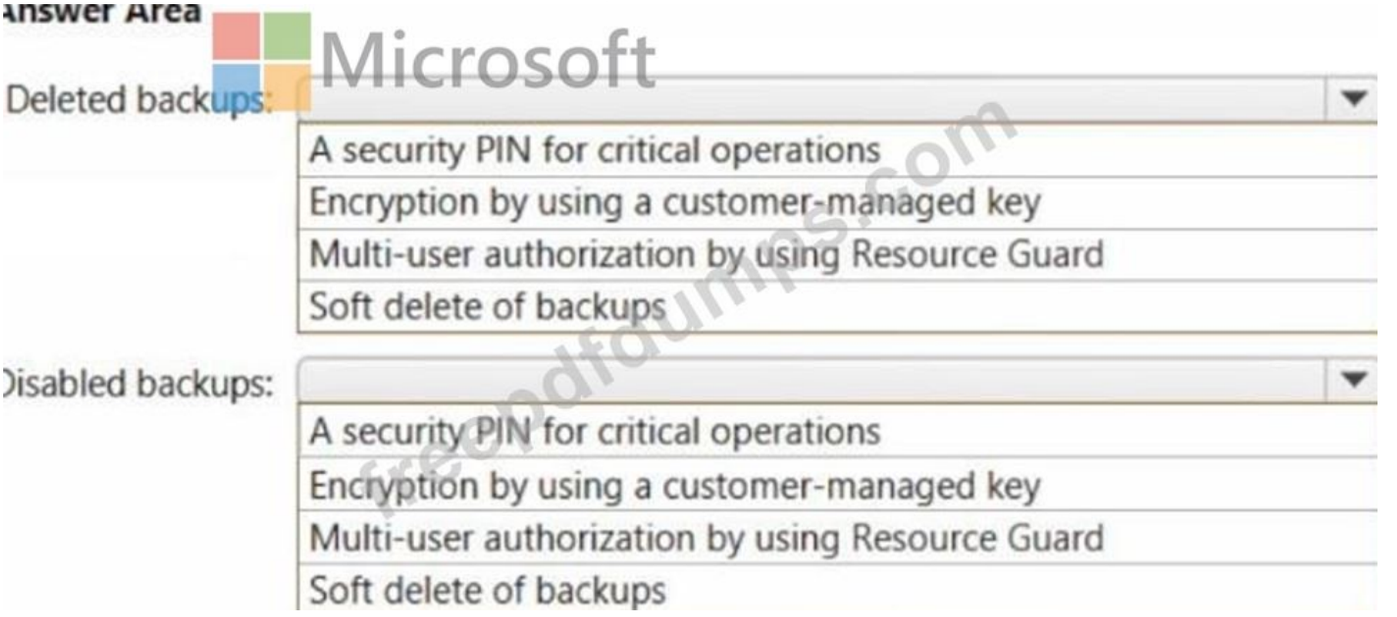
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

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:**


Explanation:

Box 1: Soft delete of backups

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 backup item before it's permanently lost.
Box 2: Multi-user authorization by using Resource Guard
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.
Reference:
https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

**NEW QUESTION: 14**
You have a Microsoft 365 E5 subscription and an Azure subscription.
You need to recommend a solution to enforce the Zero Trust principle of explicit verification for the subscriptions. The solution must be based on Zero Trust guidance in the Microsoft Cybersecurity Reference Architectures (MCRA).
What should you include in the recommendation?
**A.** Conditional Access
**B.** Microsoft Defender for Identity
**C.** Microsoft Defender for Cloud
**D.** Microsoft Entra ID Identity Governance
**Answer: (SHOW ANSWER)**
To enforce Zero Trust explicit subscription verification in Microsoft 365, focus on verifying users and devices before granting access, using Microsoft Entra ID for identity and access management and leveraging Conditional Access policies. This involves configuring authentication methods, managing device compliance, and enforcing access based on user roles and device health.
Reference:
https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/

**NEW QUESTION: 15**
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 Registry
**B.** Linux containers deployed to Azure Kubernetes Service (AKS)
**C.** Windows containers deployed to Azure Container Registry
**D.** Windows containers deployed to Azure Kubernetes Service (AKS)
**E.** Linux containers deployed to Azure Container Instances

**Answer: A,B (LEAVE A REPLY)**
Defender for Containers assists you with the three core aspects of container security:
Environment hardening - Defender for Containers protects your Kubernetes clusters whether they're running on Azure Kubernetes Service, Kubernetes on-premises/IaaS, or Amazon EKS. Defender for Containers continuously assesses clusters to provide visibility into misconfigurations and guidelines to help mitigate identified threats.
Vulnerability assessment - Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service.
Run-time threat protection for nodes and clusters - Threat protection for clusters and Linux nodes generates security alerts for suspicious activities.
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

**NEW QUESTION: 16**
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.** device compliance policies in Microsoft Endpoint Manager
**D.** Azure AD Conditional Access policies
**E.** user risk policies in Azure AD Identity Protection
**Answer: D (LEAVE A REPLY)**
You create the app and then set the locations and create a Conditional Access policy based on locations.
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

**NEW QUESTION: 17**
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.** insider risk management policies
**B.** data loss prevention (DLP) policies
**C.** sensitivity label policies
**D.** retention policies
**Answer: B (LEAVE A REPLY)**
Sensitivity labels classify PHI. DLP uses those labels to prevent it from leaving the protected environment.
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp- policy?view=o365-worldwide

**NEW QUESTION: 18**
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.** the regulatory compliance dashboard in Defender for Cloud
**B.** Azure role-based access control (Azure RBAC)
**C.** Azure Blueprints
**D.** Azure Policy
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 19**
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?

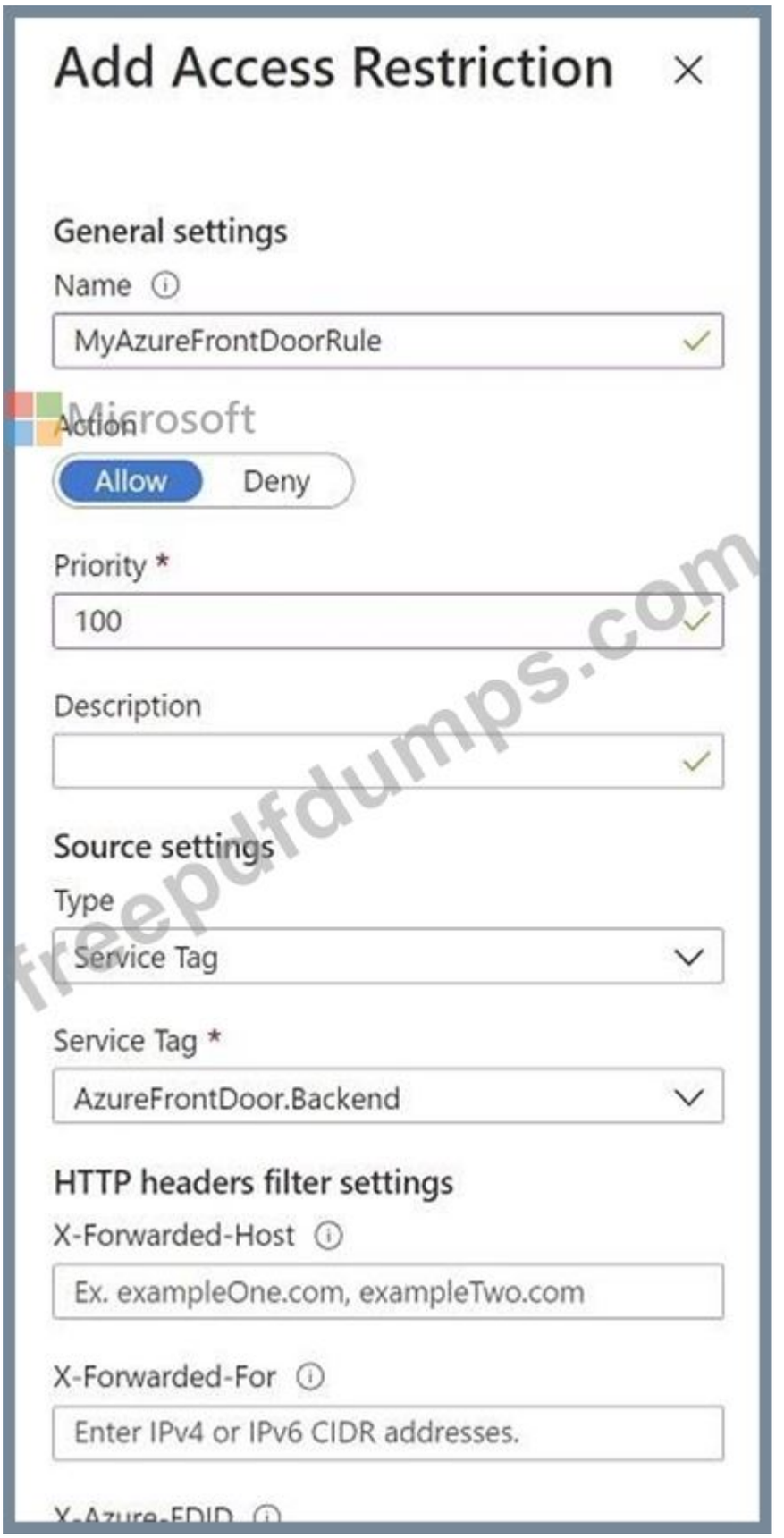
**A.** Yes

**B.** No

**Answer: A (LEAVE A REPLY)**

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

**NEW QUESTION: 20**
You have a Microsoft Entra tenant that contains 10 Windows 11 devices and two groups named Group1 and Group2. The Windows 11 devices are joined to the Microsoft Entra tenant and are managed by using Microsoft Intune.
You are designing a privileged access strategy based on the rapid modernization plan (RaMP). The strategy will include the following configurations:
- Each user in Group1 will be assigned a Windows 11 device that will be configured as a privileged access device.
- The Security Administrator role will be mapped to the privileged access security level.
- The users in Group1 will be assigned the Security Administrator role.
- The users in Group2 will manage the privileged access devices.
You need to configure the local Administrators group for each privileged access device. The solution must follow the principle of least privilege.
What should you include in the solution?
**A.** Only add Group2 to the local Administrators group.
**B.** Configure Windows Local Administrator Password Solution (Windows LAPS) in legacy Microsoft LAPS emulation mode.
**C.** Add Group2 to the local Administrators group. Add the user that is assigned the Security Administrator role to the local Administrators group of the user's assigned privileged access device.
**Answer: (SHOW ANSWER)**
Separate and manage privileged accounts
Emergency access accounts
What: Ensure that you are not accidentally locked out of your Microsoft Entra organization in an emergency situation.
Why: Emergency access accounts rarely used and highly damaging to the organization if compromised, but their availability to the organization is also critically important for the few scenarios when they are required. Ensure you have a plan for continuity of access that accommodates both expected and unexpected events.
Reference:
https://learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan

**NEW QUESTION: 21**
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
**Answer: C (LEAVE A REPLY)**
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.
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

**NEW QUESTION: 22**
You have a Microsoft 365 subscription that contains 1,000 Microsoft Exchange Online mailboxes. Incoming email from the internet is scanned for security threats by using a third-party cloud service.
You are evaluating whether to replace the third-party service with Microsoft Defender for Office 365.
What should you modify to ensure that all the incoming email is scanned by Defender for Office 365 only?
**A.** the accepted domains in Exchange Online
**B.** the DNS records
**C.** the Exchange Online transport rule
**D.** the Exchange Online connectors
**Answer: (SHOW ANSWER)**
Configure mail flow using connectors in Exchange Online
Connectors are a collection of instructions that customize the way your email flows to and from your Microsoft 365 or Office 365 organization.
What do connectors do?

Connectors are used in the following scenarios:
Enable mail flow between Microsoft 365 or Office 365 and email servers that you have in your on-premises environment (also known as on-premises email servers).
*-> Apply security restrictions or controls to email that's sent between your Microsoft 365 or Office 365 organization and a business partner or service provider.
Relay mail from devices, applications, or other non-mailbox entities in your on-premises environment through Microsoft 365 or Office 365.
Avoid graylisting that would otherwise occur due to the large volume of mail that's regularly sent between your Microsoft 365 or Office 365 organization and your on-premises environment or partners.
Reference:
https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/use-connectors-to-configure-mail-flow

**NEW QUESTION: 23**
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.** Use Azure Monitor notifications when backup configurations change.
**B.** Require PINs for critical operations.
**C.** Perform offline backups to Azure Data Box.
**D.** Encrypt backups by using customer-managed keys (CMKs).
**E.** Enable soft delete for backups.
**Answer: B,E (LEAVE A REPLY)**
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.
Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

**NEW QUESTION: 24**

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)
**Answer: A (LEAVE A REPLY)**
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

**NEW QUESTION: 25**
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
**Answer: D (LEAVE A REPLY)**
The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multi-cloud environment. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.
Controls include:
* Endpoint Security (ES)
Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in cloud environments.
* Data Protection (DP)
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 management and certificate management.
* Etc.
Reference:

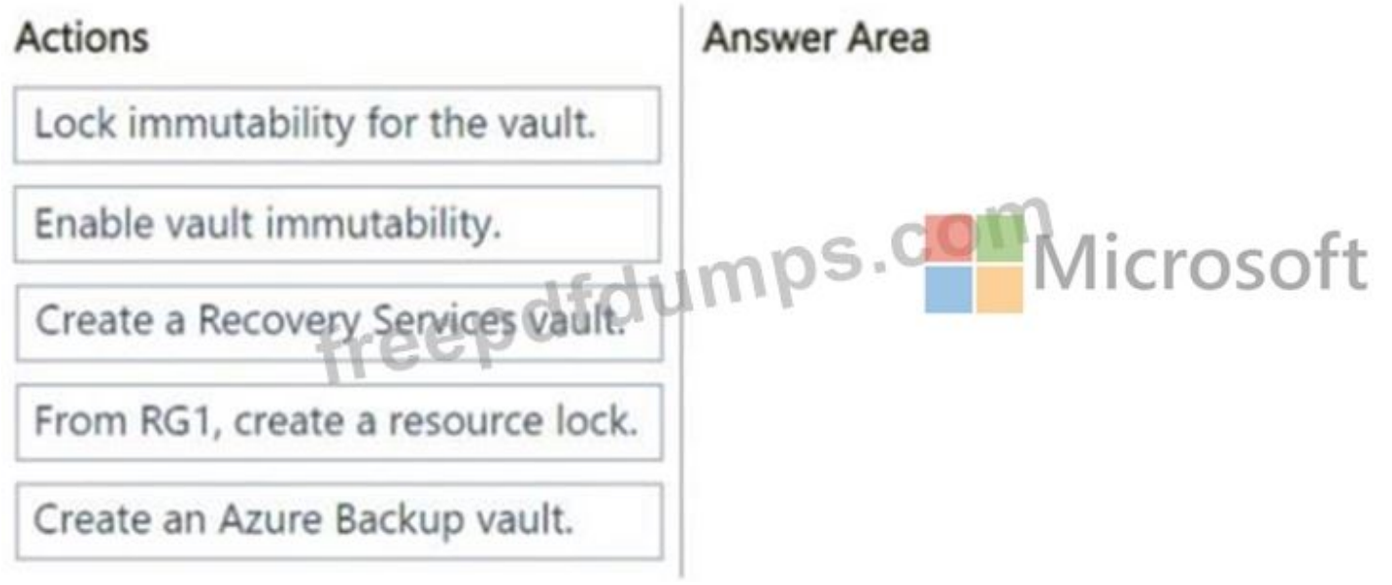
https://learn.microsoft.com/en-us/security/benchmark/azure/overview

**NEW QUESTION: 26**
You have a Microsoft 365 tenant named contoso.com.
You need to ensure that users can authenticate only to contoso.com. The solution must meet the following requirements:
- Prevent the users from authenticating to other Microsoft 365 tenants.
- Minimize administrative effort.
What should you use?
**A.** Microsoft Entra Private Access
**B.** Microsoft Defender for Endpoint
**C.** Microsoft Entra Internet Access
**D.** Microsoft Defender for Cloud Apps
**Answer: A (LEAVE A REPLY)**
Microsoft Entra Private Access unlocks the ability to specify the fully qualified domain names (FQDNs) and IP addresses that you consider private or internal, so you can manage how your organization accesses them. With Private Access, you can modernize how your organization's users access private apps and resources. Remote workers don't need to use a VPN to access these resources if they have the Global Secure Access Client installed. The client quietly and seamlessly connects them to the resources they need.
Private Access provides two ways to configure the private resources that you want to tunnel through the service. You can configure Quick Access, which is the primary group of FQDNs and IP addresses that you want to secure. You can also configure a Global Secure Access app for per-app access, which allows you to specify a subset of private resources that you want to secure. The Global Secure Access app provides a granular approach to securing your private resources.
The features of Microsoft Entra Private Access provide a quick and easy way to replace your VPN to allow secure access to your internal resources with an easy-one time configuration, using the secure capabilities of Conditional Access.
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/concept-private-access
https://learn.microsoft.com/en-us/entra/global-secure-access/concept-internet-access

**NEW QUESTION: 27**
Drag and Drop Question
You have an Azure subscription that contains a resources group named RG1. RG1 contains multiple Azure Files shares.
You need to recommend a solution to deploy a backup solution for the shares. The solution must meet the following requirements:
- Prevent the deletion of backups and the vault used to store the
backups.

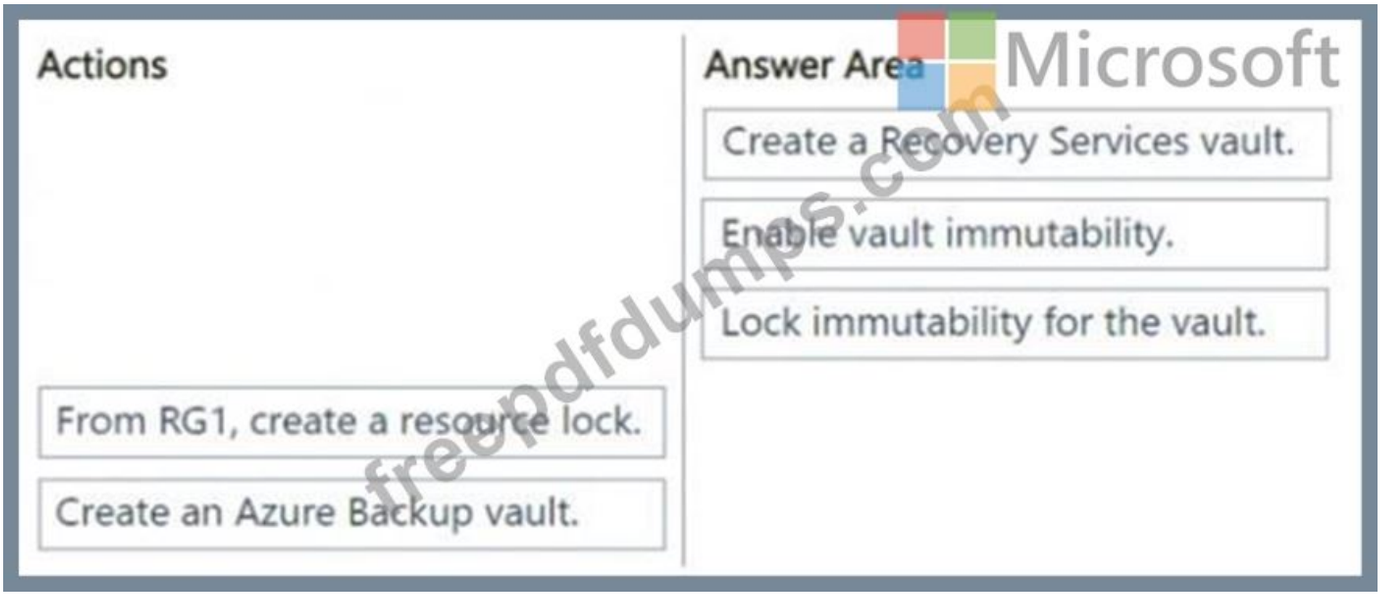
- Prevent privilege escalation attacks against the backup solution.
- Prevent the modification of the backup retention period.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.






**Answer:**






Explanation:

Step 1: Create a Recovery Services vault.

Immutable vault for Azure Backup

Immutable vault can help you protect your backup data by blocking any operations that could lead to loss of recovery points. Further, you can lock the Immutable vault setting to make it irreversible to prevent any malicious actors from disabling immutability and deleting backups.

Step 2: Enable vault immutability

Step 3: Lock immutability for the vault

Making immutability irreversible

The immutability of a vault is a reversible setting that allows you to disable the immutability (which would allow deletion of backup data) if needed. However, we recommend you, after being satisfied with the impact of immutability, lock the vault to make the Immutable vault settings irreversible, so that any bad actors can't disable it. Therefore, the Immutable vault settings accept following three states.
Reference:
https://learn.microsoft.com/en-us/azure/backup/backup-azure-immutable-vault-concept

**NEW QUESTION: 28**
You have a Microsoft 365 tenant that contains two groups named Group1 and Group2.
You use Microsoft Defender XDR to manage the tenants of your company's customers.
You need to ensure that the users in Group1 can perform security tasks in the tenant of each customer. The solution must meet the following requirements:
- The Group1 users must only be assigned the Security Operator role for the customer tenants.
- The users in Group2 must be able to assign the Security Operators
role to the Group1 users for the customer tenants.
- The use of quest accounts must be minimized.
- Administrative effort must be minimized.
What should you include in the solution?
**A.** multi-user authorization (MUA)
**B.** Azure Lighthouse
**C.** Privileged Identity Management (PIM)
**D.** Microsoft Entra B2B collaboration
**Answer: B (LEAVE A REPLY)**
Azure Lighthouse includes multiple ways to help streamline engagement and management:
* Azure delegated resource management: Manage your customers' Azure resources securely from within your own tenant, without having to switch context and control planes. Customer subscriptions and resource groups can be delegated to specified users and roles in the managing tenant, with the ability to remove access as needed.
* Etc.
Reference:
https://learn.microsoft.com/en-us/azure/lighthouse/overview

**NEW QUESTION: 29**
You have on-premises Windows 11 devices that have the Global Secure Access client deployed.
You have a Microsoft 365 subscription that uses Microsoft SharePoint Online and Exchange Online.
You deploy Microsoft Entra Internet Access from the on-premises network to Microsoft 365. The deployment has the Microsoft 365 profile enabled and contains the following:
- Default traffic policies for Microsoft 365 services
- A linked Conditional Access policy that performs compliant network

checks with continuous access evaluation and is applied to all users
- An assignment to all the devices
- An assignment to a remote network associated with the on-premises network

Which Microsoft 365 resources are protected by using continuous access evaluation?

**A.** SharePoint Online only

**B.** Exchange Online only

**C.** both SharePoint Online and Exchange Online

**Answer: A (LEAVE A REPLY)**

Compliant network enforcement reduces the risk of token theft/replay attacks. Compliant network enforcement happens at the authentication plane (generally available) and at the data plane (preview). Authentication plane enforcement is performed by Microsoft Entra ID at the time of user authentication. If an adversary has stolen a session token and attempts to replay it from a device that is not connected to your organization's compliant network (for example, requesting an access token with a stolen refresh token), Entra ID will immediately deny the request and further access will be blocked. Data plane enforcement works with services that support Continuous Access Evaluation (CAE) - currently, *only SharePoint Online*. With apps that support CAE, stolen access tokens that are replayed outside your tenant's compliant network will be rejected by the application in near-real time. Without CAE, a stolen access token will last up to its full lifetime (default 60-90 minutes).

Reference:

https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-compliant-network

**NEW QUESTION: 30**

Hotspot Question

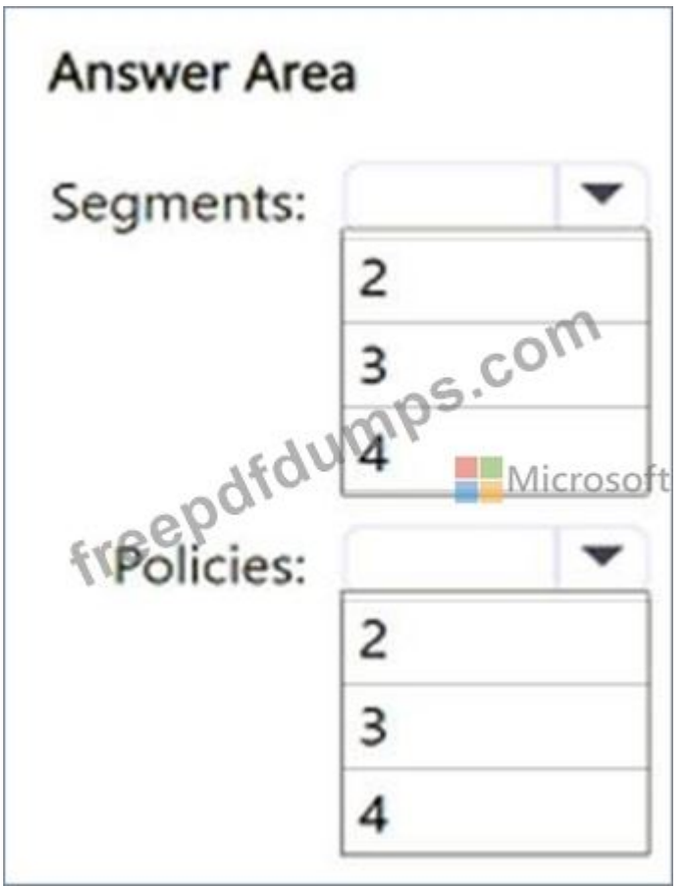
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

Your company has an investment department and a research department. Each department has a compliance team.

You are designing a Microsoft Purview Information Barriers (IBs) solution to restrict communication between the departments. The solution must meet the following requirements:
- The employees in each department must only be able to communicate with the employees in their respective department.
- The employees on the compliance team of each department must be able to communicate with the employees on the compliance team of the other department.

What is the minimum number of segments and IB policies required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**


Explanation:

Box 1: 3

To isolate communication between two departments in Microsoft Teams while allowing communication within each department and also permitting a specific group to communicate across departments, you'll need to configure information barriers. First, define segments for each department and the exception group. Then, create policies that block communication between the department segments, but allow communication within each segment. Finally, create an exception policy that allows communication between the exception group and both departments.
1. Define Segments:
Create a segment for Department A.
Create a segment for Department B.
Create a segment for the exception group.
Box 2: 2
2. Create Information Barrier Policies:
Policy 1: Block Communication between Departments:
Segments Involved: Department A and Department B.
Policy: Block communication (chat, calls, meetings, file sharing) between these two segments.
Policy 2: Allow Exception Group to Communicate:
Segments Involved: Exception Group and Department A.
Policy: Allow communication between the exception group and Department A.
Segments Involved: Exception Group and Department B.
Policy: Allow communication between the exception group and Department B.
Note: With Microsoft Purview Information Barriers and a single segment, communication within that segment is allowed by default. No specific Information Barrier policy is needed to enable communication within a segment. Information Barriers primarily focus on restricting communication between different segments, not within the same segment.
3. Apply Policies:
Apply the created policies within the Microsoft Purview Information Barriers settings.
Ensure all users are assigned to the correct segments.
Apply all policies at once for consistent application.
By following these steps, you can effectively isolate communication between the two departments while enabling cross-departmental communication for the designated exception group.
Reference:
https://learn.microsoft.com/en-us/purview/information-barriers-policies

**NEW QUESTION: 31**
Your company has on-premises datacenters in Seattle, Chicago, and New York City.
You plan to migrate the on-premises workloads to the East US Azure region.
You need to design a governance solution for the management group hierarchy. The solution must be based on Microsoft Cloud Adoption Framework for Azure principles and must ensure that the hierarchy aligns with the Azure landing conceptual architecture.
What should you use to identify which archetype-aligned management groups to create beneath the landing zones management group?

**A.** geographical locations
**B.** the internal billing chargeback structure
**C.** the hybrid connectivity requirements
**D.** software development lifecycle (SDLC) environments
**Answer: C (LEAVE A REPLY)**
Hybrid connectivity in Azure enables you to link your on-premises infrastructure with Azure resources, facilitating a seamless integration between your existing environment and the cloud. This requires establishing secure connections, often using VPN gateways or ExpressRoute, and managing traffic flow between the two environments. Key requirements include network connectivity, security considerations, and often specific configurations for identity and access management.
Reference:
https://learn.microsoft.com/en-us/azure/networking/hybrid-connectivity/



**NEW QUESTION: 32**
You have two Azure subscriptions named Sub1 and Sub2 that contain the vaults shown in the following table.

| Name | Type | Location | Subscription |
|---|---|---|---|
| RSVault1 | Recovery Services vault | East US | Sub1 |
| BackupVault1 | Azure Backup vault | East US | Sub2 |
| RSVault2 | Recovery Services vault | West US | Sub2 |
| BackupVault2 | Azure Backup vault | West US | Sub1 |

You need to design a multi-user authorization (MUA) solution for security operations on the vaults. The solution must meet the following requirements:
- RSVault1 and RSVault2 must require MUA for disabling soft delete, removing MUA protection, and disabling immutability.
- BackupVault1 and BackupVault2 must require MUA for disabling soft delete and removing MUA protection.
What is the minimum number of Resource Guard resources required?
**A.** 1
**B.** 2

**C.** 3
**D.** 4
**Answer: B (LEAVE A REPLY)**
* RSVault1 and RSVault2 must require MUA for disabling soft delete, removing MUA protection, and disabling immutability.
RSVault1 is in Sub1 in East US.
RSVault2 is in Sub2 in West US.
Need two Resource Guards. One in East US, and one in West US.
* BackupVault1 and BackupVault2 must require MUA for disabling soft delete and removing MUA protection.
Need two Resource Guards. One in East US, and one in West US.
As a Resource Guard can be configured both for Recovery Vaults and Backup Vaults, we need only two; one in each region.
Note 1: Create a Resource Guard
The Security admin creates the Resource Guard. We recommend that you create it in a different subscription or a different tenant as the vault.
However, it should be in the same region as the vault.
Note 2: Select operations to protect using Resource Guard
Choose the operations you want to protect using the Resource Guard out of all supported critical operations. By default, all supported critical operations are enabled. However, you (as the security admin) can exempt certain operations from falling under the purview of MUA using Resource Guard.
To exempt operations, follow these steps:
1. In the Resource Guard created above, go to Properties > Recovery Services vault tab.
2. Select Disable for operations that you want to exclude from being authorized using the Resource Guard.
Attention:
You can't disable the protected operations - Disable soft delete and Remove MUA protection.
3. Optionally, you can also update the description for the Resource Guard using this blade.
4. Select Save.
Reference:
https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

**NEW QUESTION: 33**
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.** Privileged Access Workstations (PAWs)
**B.** emergency access accounts
**C.** device compliance policies

**D.** Customer Lockbox for Microsoft Azure

**Answer: A (LEAVE A REPLY)**

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 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.

**NEW QUESTION: 34**

Hotspot Question

You have an Azure subscription.

You have a Microsoft 365 subscription.

You need to assess regulatory compliance of the subscriptions. The solution must meet the following requirements:

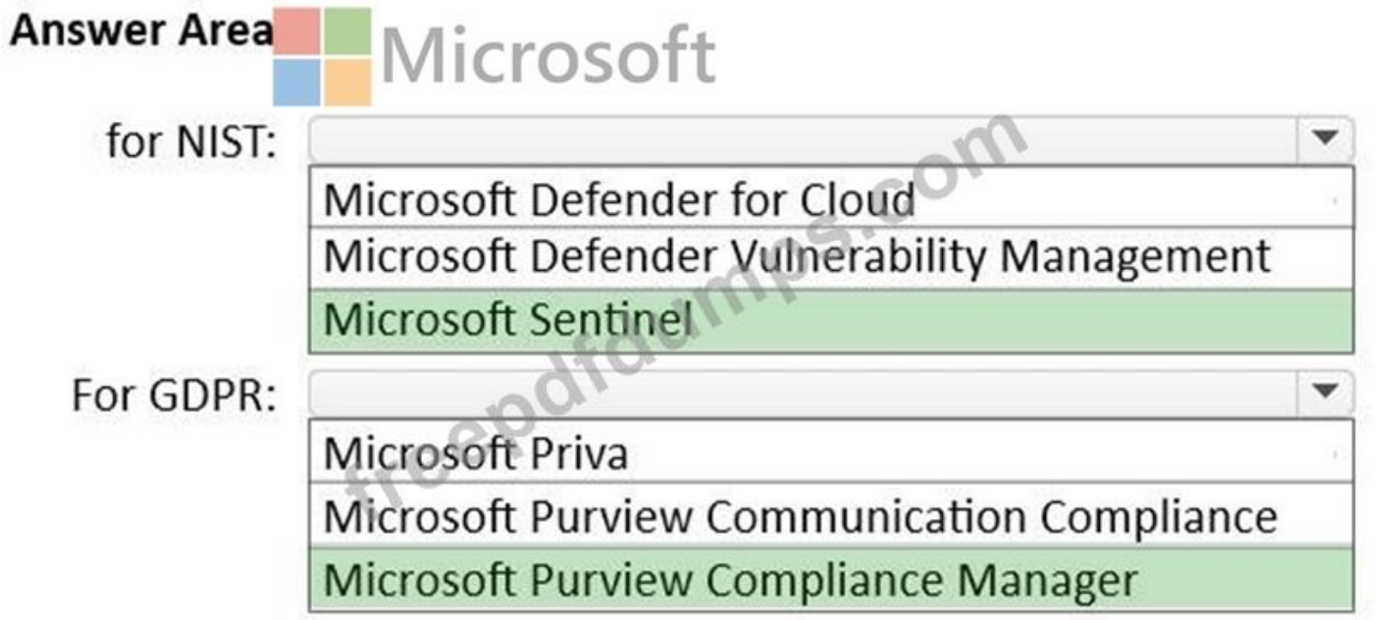
- Identify whether data stored in Azure and Microsoft 365 complies with General Data Protection Regulation (GDPR) regulations.
- Identify whether Azure resources comply with National Institute of Standards and Technology (NIST) standards.
- Provide recommendations on controls to improve compliance.

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

NOTE: Each correct selection is worth one point.


**Answer:**

**Answer Area**






Explanation:

Box 1: Microsoft Sentinel

Identify whether Azure resources comply with National Institute of Standards and Technology (NIST) standards.

Announcing the Microsoft Sentinel: NIST SP 800-53 Solution [February 2022] The Microsoft Sentinel: NIST SP 800-53 Solution enables compliance teams, architects, security analysts, and consultants to understand their cloud security posture related to Special Publication (SP) 800-53 guidance issued by the National Institute of Standards and Technology (NIST). This solution is designed to augment staffing through automation, visibility, assessment, monitoring, and remediation. Content features include an intuitive user interface, policy-based assessments, control cards for guiding alignment with control requirements, alerting rules to monitor configuration drift, and playbook automations for response. The power of this solution lies in its ability to aggregate at big data scale across first- and third-party products to provide maximum visibility into cloud, hybrid, and multi-cloud workloads.



Box 2: Microsoft Purview Compliance Manager

Identify whether data stored in Azure and Microsoft 365 complies with General Data Protection Regulation (GDPR) regulations.

What is the Compliance Manager General Data Protection Regulation (GDPR) assessment? This is the official Microsoft tool that scans your tenant and compares it to the GDPR. It then provides a report and workflow on how to meet this regulation.

Narrowing General Data Protection Regulation (GDPR) to applicable Purview tools We narrow the scope of All General Data Protection Regulation (GDPR) Control Families (5x) the Assessment runs to just the Compliance applicable GDPR Control Families (6x). Then we can take those tactical Control Families and leverage the applicable Microsoft Purview tools that, when applied, can help you meet these Control Families.

Reference:

https://techcommunity.microsoft.com/blog/microsoftsentinelblog/announcing-the-microsoft-sentinel-nist-sp-800-53-solution/3381485

https://techcommunity.microsoft.com/blog/healthcareandlifesciencesblog/microsoft-purview---compliance-score-part-5---gdpr/3639469

**NEW QUESTION: 35**

Case Study 1 - Fabrikam, Inc

OverView

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment
Fabrikam has the following Azure resources:
- A Microsoft Entra tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com
- A single Azure subscription named Sub1
- A virtual network named Vnet1 in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled
- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts
- All the resources in Sub1 are in either the East US or the West Europe region.

Partners
Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:
- An Microsoft Entra named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications.

The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1. The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event
Fabrikam deploys the following compliance environment:
- Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements
The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation. Machines should have a vulnerability assessment solution. All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment
Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification
- ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.
- Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- Azure DevTest labs will be used by developers for testing.
- All the application code must be stored in GitHub Enterprise.
- Azure Pipelines will be used to manage application deployments.
- All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- Internet-accessible applications must prevent connections that originate in North Korea.
- Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
- Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers:

- Every month, the membership of the ContosoDevelopers group must be verified.
- The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

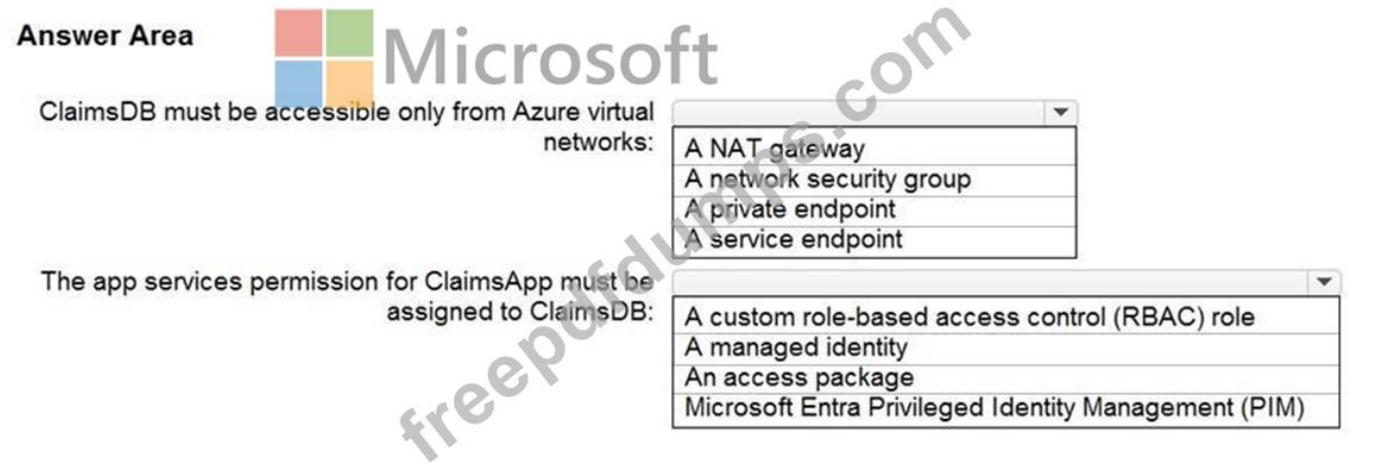
Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Hotspot Question

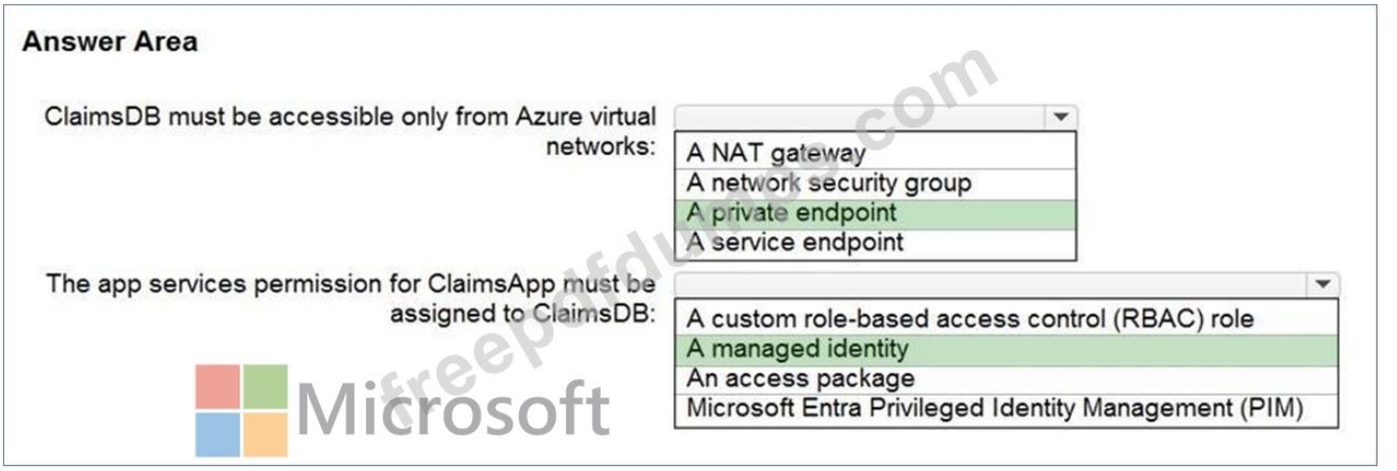
You need to recommend a solution to meet the requirements for connections to ClaimsDB.

What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:

Box 1: A private endpoint

Scenario: An Azure SQL database named ClaimsDB that contains a table named ClaimDetails

Requirements. ClaimsApp Deployment.

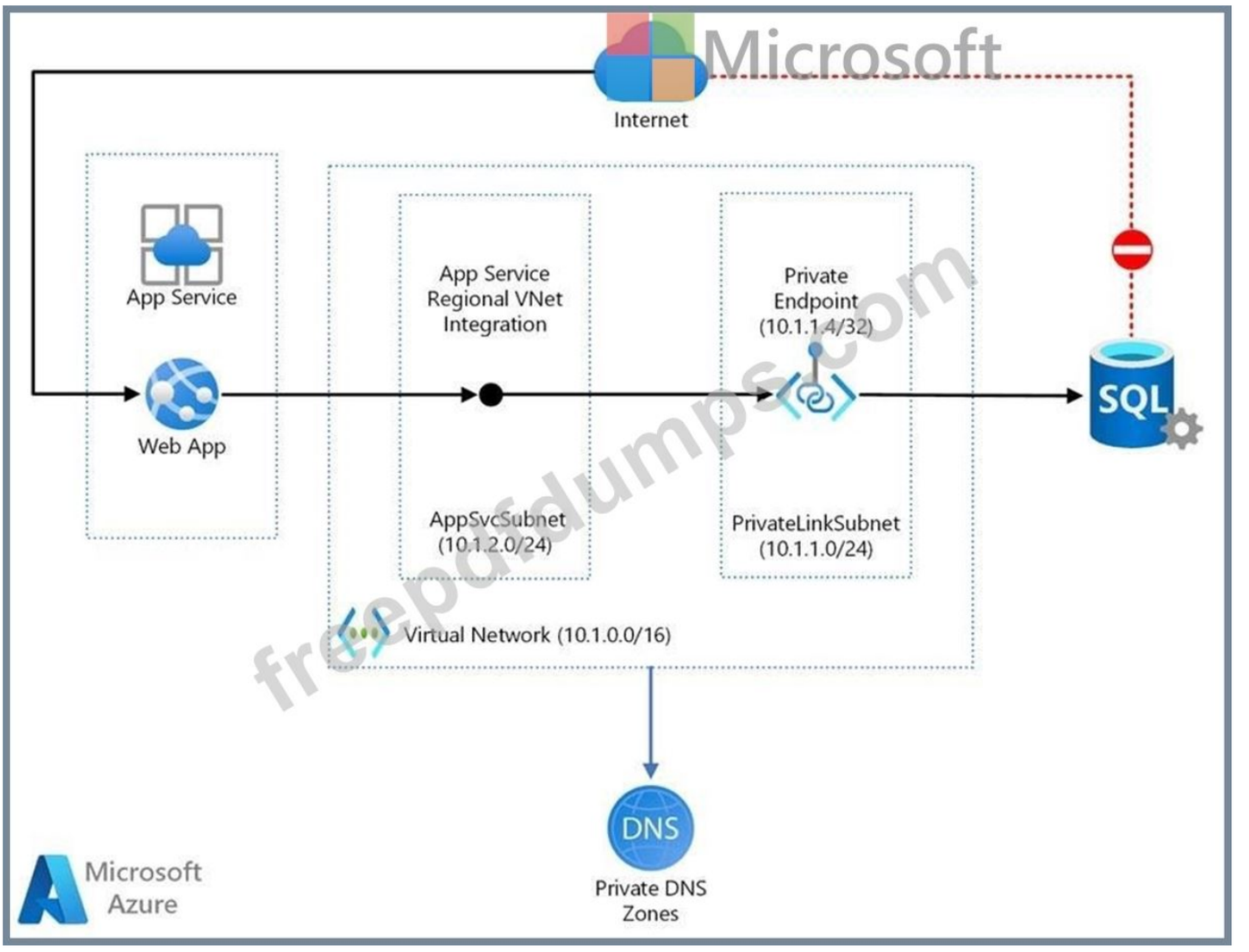
Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specifications:

- ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.

Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.

- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Web app private connectivity to Azure SQL Database.




Workflow

1. Using Azure App Service regional VNet Integration, the web app connects to Azure through an AppSvcSubnet delegated subnet in an Azure Virtual Network.
2. In this example, the Virtual Network only routes traffic and is otherwise empty, but other subnets and workloads could also run in the Virtual Network.
3. The App Service and Private Link subnets could be in separate peered Virtual Networks, for example as part of a hub-and-spoke network configuration.
4. Azure Private Link sets up a private endpoint for the Azure SQL Database in the PrivateLinkSubnet of the Virtual Network.
5. The web app connects to the SQL Database private endpoint through the PrivateLinkSubnet of the Virtual Network.

The database firewall allows only traffic coming from the PrivateLinkSubnet to connect, making the database inaccessible from the public internet.

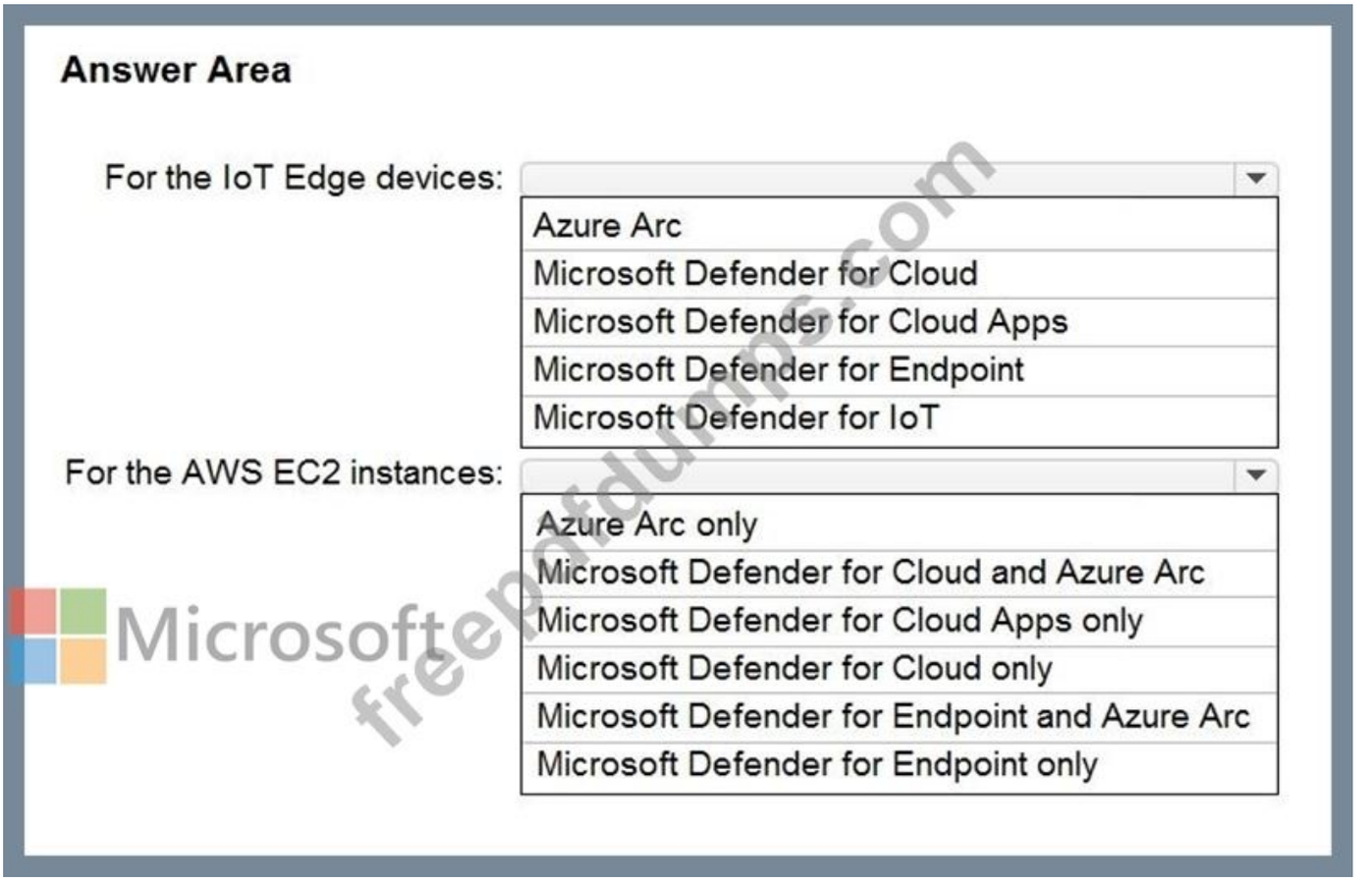
Box 2: A managed identity

Managed identities for Azure resources provide Azure services with an automatically managed identity in Microsoft Entra ID. Using a managed identity, you can authenticate to any service that supports Microsoft Entra authentication without managing credentials.

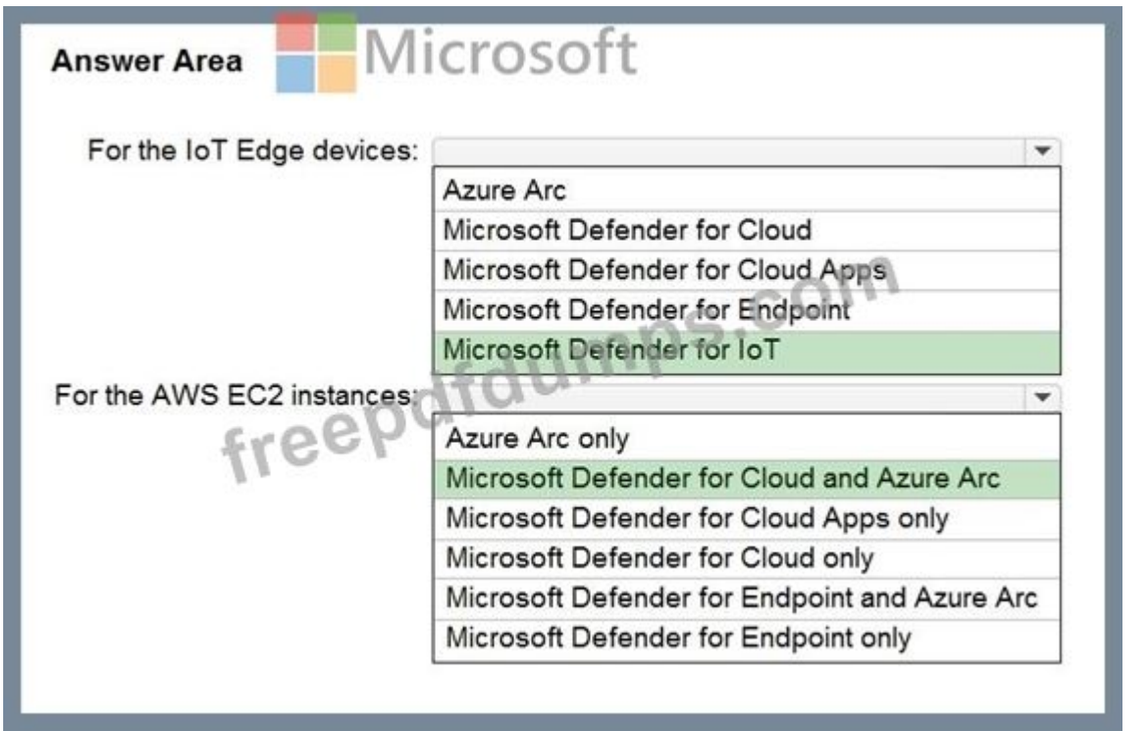
Reference:

https://docs.microsoft.com/en-us/azure/architecture/example-scenario/private-web-app/private-web-app
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-status

**NEW QUESTION: 36**
Hotspot Question
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.




**Answer:**





Explanation:

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/

**NEW QUESTION: 37**
Your on-premises network contains an Active Directory Domain Services (AD DS) domain named corp.contoso.com and an AD DS-integrated application named App1.
Your perimeter network contains a server named Server1that runs Windows Server.
You have a Microsoft Entra tenant named contoso.com that syncs with corp.contoso.com.
You plan to implement a security solution that will include the following configurations:
- Manage access to App1 by using Microsoft Entra Private Access.
- Deploy a Microsoft Entra application proxy connector to Server1.
- Implement single sign-on (SSO) for App1 by using Kerberos constrained delegation.
For Server1, configure the following rules in Windows Defender Firewall with Advanced Security:
- Rule1: Allow TCP 443 inbound from a designated set of Azure URLs,
- Rule2: Allow TCP 443 outbound to a designated set of Azure URLs,
- Rule3: Allow TCP 80 outbound to a designated set of Azure URLs,
- Rule4: Allow TCP 389 outbound to the domain controllers on corp.contoso.com.
You need to maximize security for the planned implementation. The solution must minimize the impact on the connector.
Which rule should you remove?
**A.** Rule1
**B.** Rule2
**C.** Rule3
**D.** Rule4
**Answer: C (LEAVE A REPLY)**
Rule3 allows TCP 80 outbound traffic to a designated set of Azure URLs. TCP 80 is associated with unencrypted HTTP traffic, which poses a security risk because it does not encrypt data, potentially exposing sensitive information in transit. By removing this rule, you can ensure that all communication Server1 and Azure is encrypted, which aligns with security best practices for minimizing data exposure. Additionally, this change will not between HTTPS (TCP 443) connections are still allowed for necessary communications.

impact the functioning of the application proxy connector, as secure

**NEW QUESTION: 38**
Case Study 2 - Litware, inc.
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 a Microsoft Entra tenant that syncs with an Active Directory Domain Services (AD DS) forest named litware.com and is linked to 20 Azure subscriptions. Microsoft Entra 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, Microsoft Entra 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 Microsoft Entra tenant.
- Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.
- Implement Microsoft Entra 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:
o Use Azure Policy for enforcement and compliance evaluation.
o Provide change tracking and asset inventory.
o 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 Microsoft Entra tenant of Litware.
- Prevent AD DS user accounts from being locked out by brute force attacks that target Microsoft Entra user accounts.
- Implement delegated management of users and groups in the Microsoft Entra tenant of Litware, including support for:
o The management of group properties, membership, and licensing
o The management of user properties, passwords, and licensing
o 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 Microsoft Entra Application Proxy.
- Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.
You need to recommend a solution for securing the landing zones.
The solution must meet the landing zone requirements and the business requirements.
What should you configure for each landing zone?
**A.** Azure DDoS Protection Standard

**B.** an Azure Private DNS zone
**C.** Microsoft Defender for Cloud
**D.** an ExpressRoute gateway
**Answer: B (LEAVE A REPLY)**
A specific virtual network can be linked to only one private zone if automatic registration of VM DNS records is enabled. You can however link multiple virtual networks to a single DNS zone.
https://docs.microsoft.com/en-us/azure/dns/private-dns-overview

**NEW QUESTION: 39**
Hotspot Question
You have a Microsoft 365 E5 subscription. The subscription contains 1,000 devices that run Windows 11 Pro and are enrolled in Microsoft Intune.
You need to recommend a Microsoft Defender for Cloud Apps solution that meets the following requirements:
- When a user downloads a file from Microsoft SharePoint Online, a label must be applied to the file in real time based on the file's contents.
- Only users that use Intune-compliant devices must be able to sign in to Dropbox.
Which type of policy should you recommend for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.


**Answer:**



Explanation:

Box 1: File policy

It is possible to apply a sensitivity label to a file in real-time when it's downloaded from Microsoft SharePoint Online, based on the file's content. This can be achieved by using a combination of file policies in Microsoft Defender for Cloud Apps (formerly Cloud App Security) and sensitivity labels configured within Microsoft Purview Information Protection.

Box 2: Access policy

It is possible to restrict Dropbox sign-ins to Intune-compliant devices using a combination of Intune and Microsoft Entra ID Conditional Access policies. This is achieved by configuring a Conditional Access policy that requires devices to be marked as compliant by Intune before granting access to Dropbox.

Reference:

https://learn.microsoft.com/en-us/purview/sensitivity-labels-sharepoint-onedrive-files

https://learn.microsoft.com/en-us/answers/questions/2115107/restricting-access-to-a-web-application-based-on-d

**NEW QUESTION: 40**

Hotspot Question

Your company has two offices named Office1 and Office2. The offices contain 1,000 on-premises Windows 11 devices that are Microsoft Entra joined.

You have a Microsoft 365 subscription and use Microsoft Intune.

You plan to deploy Microsoft Entra Internet Access from the offices to Microsoft 365.

You enable the Microsoft 365 profile and configure the following:

- A traffic policy for all Microsoft 365 traffic
- A linked Conditional Access policy that has the following configurations:

Applies to all users

Performs compliant network checks

Allows Microsoft 365 traffic from compliant devices

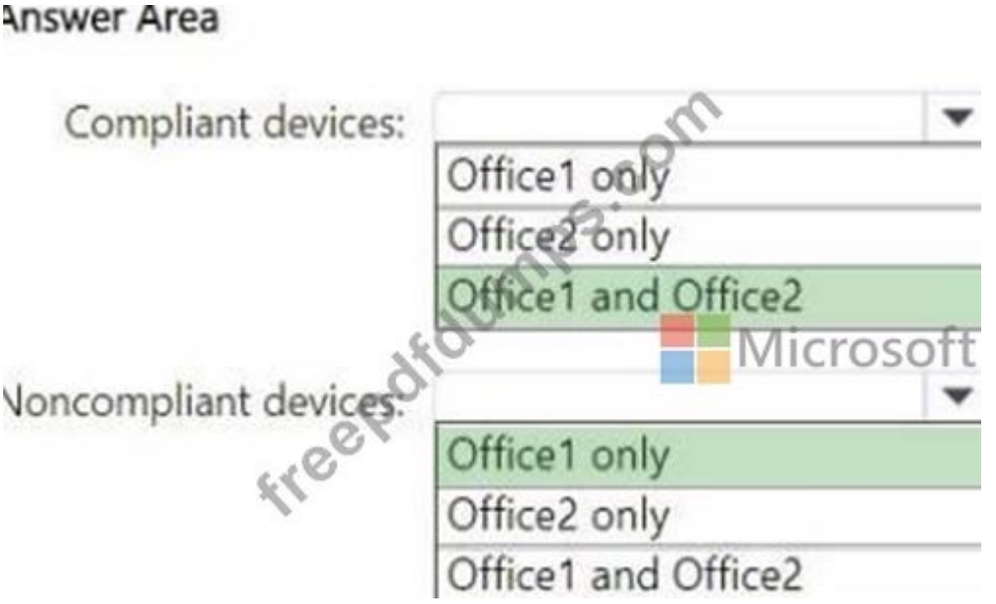
- An assignment to all devices
- An assignment to the remote network associated with Office1

You deploy the Global Secure Access client to all the devices in Office2 and establish connections.

Which users can access Microsoft 365 services from compliant devices, and which users are blocked from accessing Microsoft 365 services when using noncompliant devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


**Answer:**




Explanation:

Box 1: Office1 and Office2

Compliant devices

* Office1

Global Secure Access

Enable compliant network check with Conditional Access

Organizations who use Conditional Access along with the Global Secure Access, can prevent malicious access to Microsoft apps, third-party SaaS apps, and private line-of-business (LoB) apps using multiple conditions to provide defense-in-depth. These conditions might include device compliance, location, and more to provide protection against user identity or token theft.

Global Secure Access introduces the concept of a compliant network within Microsoft Entra ID Conditional Access. This compliant network check ensures users connect from a verified network

connectivity model for their specific tenant and are compliant with security policies enforced by administrators.
The Global Secure Access Client installed on devices or users behind configured remote networks allows administrators to secure resources behind a compliant network with advanced Conditional Access controls. This compliant network feature makes it easier for administrators to manage access policies, without having to maintain a list of egress IP addresses. This removes the requirement to hairpin traffic through organization's VPN.
* Office2
The Global Secure Access client allows organizations control over network traffic at the end-user computing device, giving organizations the ability to route specific traffic profiles through Microsoft Entra Internet Access and Microsoft Entra Private Access. Routing traffic in this method allows for more controls like continuous access evaluation (CAE), device compliance, or multifactor authentication to be required for resource access.
Box 2: Office1 only
Noncompliant devices
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-compliant-network
https://learn.microsoft.com/en-us/entra/global-secure-access/concept-clients

**NEW QUESTION: 41**
Hotspot Question
You are designing a privileged access strategy for a company named Contoso, Ltd. and its partner company named Fabrikam, Inc. Contoso has a Microsoft Entra tenant named contoso.com. Fabrikam has a Microsoft Entra 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.


**Answer:**


**NEW QUESTION: 42**

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.** Enhanced Security Admin Environment (ESAE)

**B.** Microsoft Security Development Lifecycle (SDL)

**C.** Rapid Modernization Plan (RaMP)

**D.** Microsoft Operational Security Assurance (OSA)

**Answer: C (LEAVE A REPLY)**

This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan

**NEW QUESTION: 43**

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.** Disabled

**C.** Modify

**D.** Append

**Answer: (SHOW ANSWER)**

It has to be disabled since deny will send the compliance report as non-complaint.

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

**NEW QUESTION: 44**
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.** insider risk management
**C.** Microsoft Information Protection
**D.** Azure Purview
**Answer: C (LEAVE A REPLY)**
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, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and 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 does not read or support sensitivity labels.
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

**NEW QUESTION: 45**
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.** interactive application security testing (IAST)
**B.** static application security testing (SAST)
**C.** runtime application se/f-protection (RASP)
**D.** dynamic application security testing (DAST)

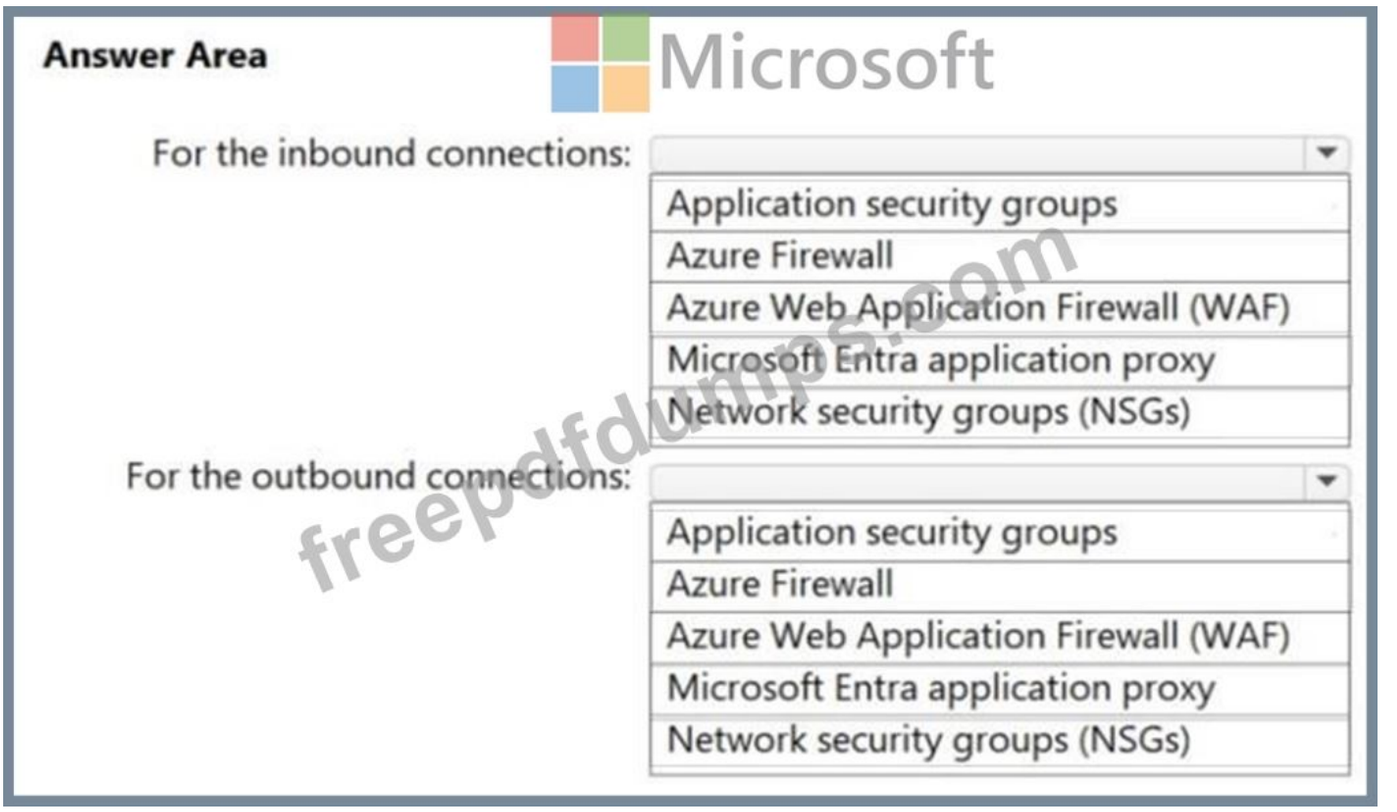
**Answer: D (LEAVE A REPLY)**
DAST tools analyze programs while they are executing to find security vulnerabilities such as memory corruption, insecure server configuration, cross-site scripting, user privilege issues, SQL injection, and other critical security concerns.
Reference:
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

**NEW QUESTION: 46**
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' premises network. The company's security 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.** Migrate the on-premises applications to cloud-based applications.
**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.** Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.
**Answer: D (LEAVE A REPLY)**
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

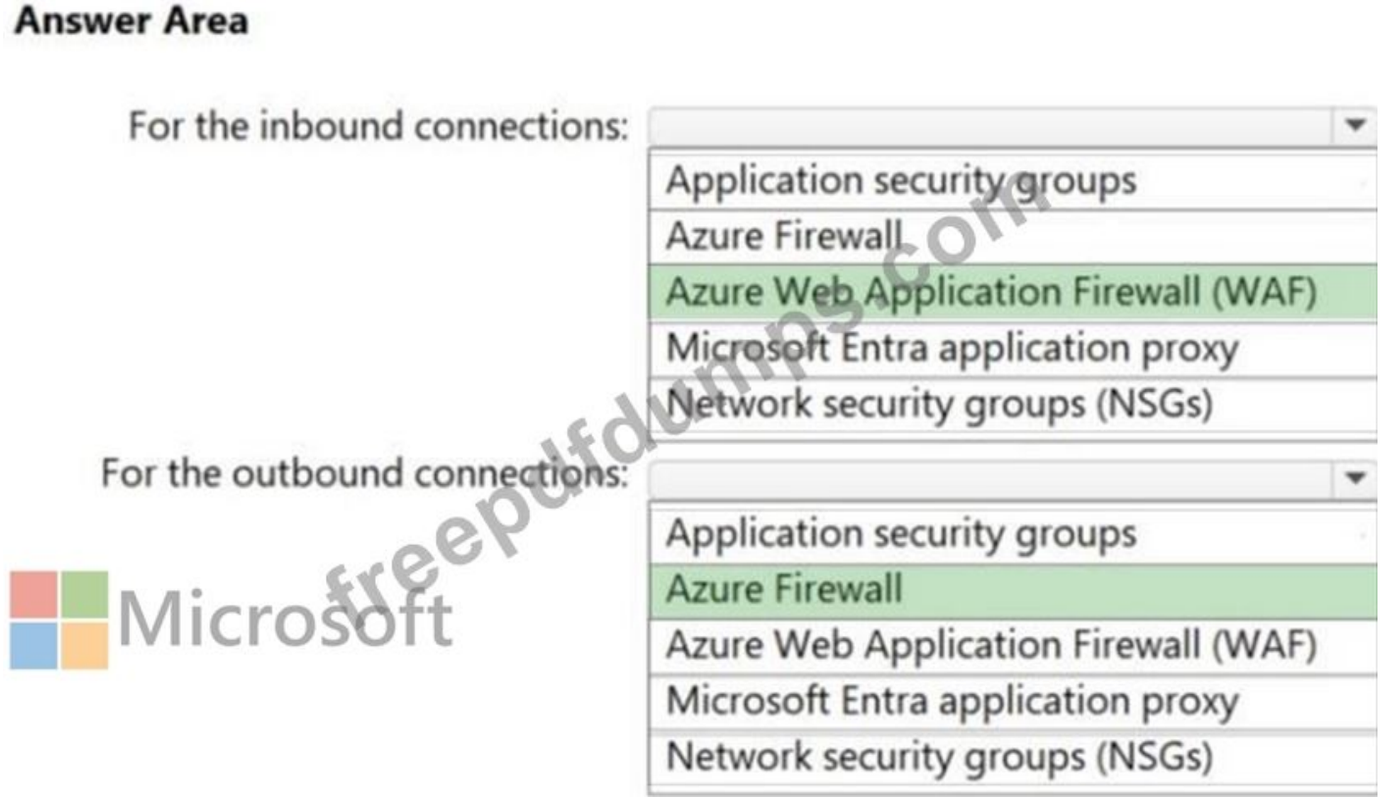
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cloud-apps/ba-p/2835842



**NEW QUESTION: 47**
Hotspot Question
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a 10-node virtual machine scale set that hosts a web search app named App1. Customers access App1 from the internet. The nodes establish outbound HTTP and HTTPS connections to the internet.
You need to recommend a network security solution for App1. The solution must meet the following requirements:
- Inbound connections to App1 that contain security threats specified in the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP) must be blocked.
- Outbound HTTP and HTTPS connections from the virtual machine scale set that contain security threats identified by the Microsoft Defender Threat Intelligence (Defender TI) feed must be blocked.
What should you include in the recommendation? To answer, select the options in the answer area.
NOTE: Each correct answer is worth one point.




**Answer:**




Explanation:

Box 1: Azure Web Application Firewall (WAF)

Inbound connections to App1 that contain security threats specified in the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP) must be blocked.

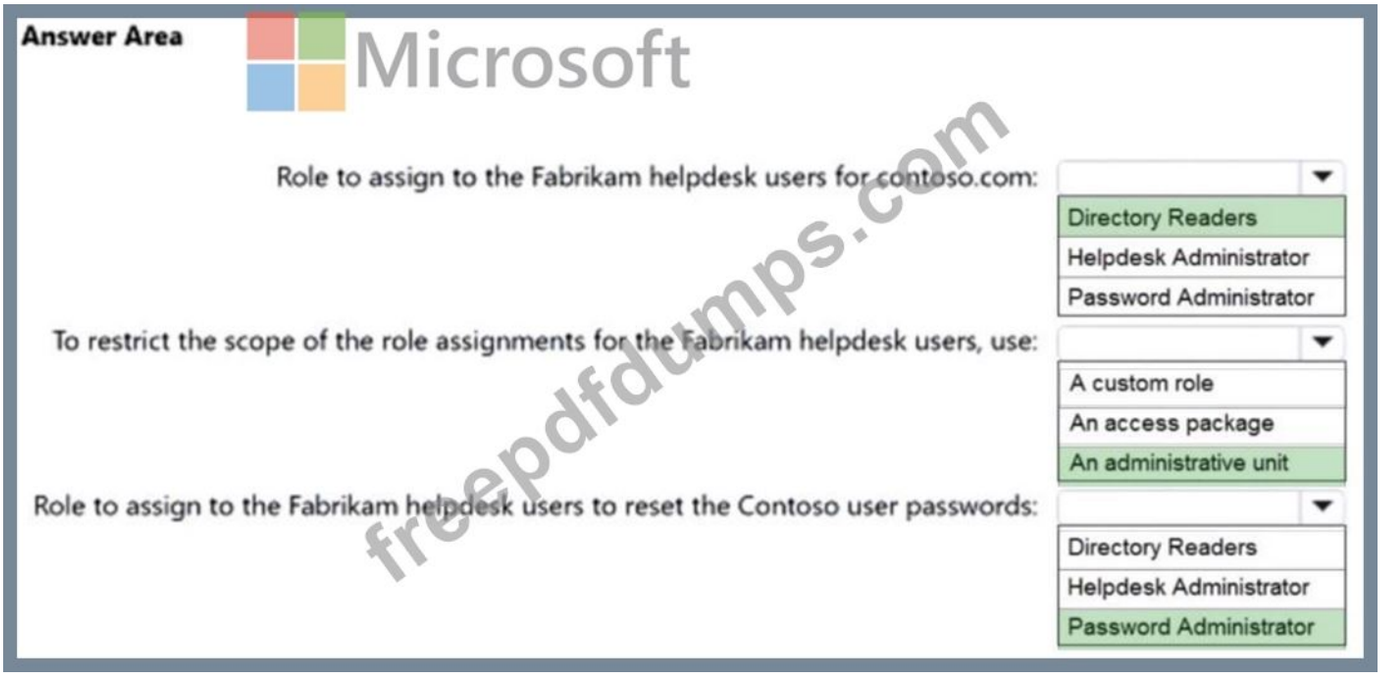
The Azure Web Application Firewall (WAF) on Azure Application Gateway actively safeguards your web applications against common exploits and vulnerabilities. As web applications become

more frequent targets for malicious attacks, these attacks often exploit well-known vulnerabilities such as SQL injection and cross-site scripting.
WAF on Application Gateway is based on the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP).
Box 2: Azure Firewall
Outbound HTTP and HTTPS connections from the virtual machine scale set that contain security threats identified by the Microsoft Defender Threat Intelligence (Defender TI) feed must be blocked.
Azure Firewall threat intelligence-based filtering
You can enable Threat intelligence-based filtering for your firewall to alert and deny traffic from/to known malicious IP addresses, FQDNs, and URLs. The IP addresses, domains and URLs are sourced from the Microsoft Threat Intelligence feed, which includes multiple sources including the Microsoft Cyber Security team. Intelligent Security Graph powers Microsoft threat intelligence and uses multiple services including Microsoft Defender for Cloud.
Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview
https://learn.microsoft.com/en-us/azure/firewall/threat-intel

**NEW QUESTION: 48**
Hotspot Question
Your company, named Contoso, Ltd., has a Microsoft Entra tenant named contoso.com. Contoso has a partner company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabrikam.com.
You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:
- Follow the principle of least privilege.
- Minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**


**Answer:**




Explanation:

Box 1: Directory Readers

To enable a service principal or guest user to use a role assignment scoped to an administrative unit, you must assign the Directory Readers role (or another role that includes read permissions) at a tenant scope.

Box 2: Administrative unit

Assign Microsoft Entra roles with administrative unit scope

In Microsoft Entra ID, for more granular administrative control, you can assign a Microsoft Entra role with a scope that's limited to one or more administrative units. When a Microsoft Entra role is assigned at the scope of an administrative unit, role permissions apply only when managing members of the administrative unit itself, and don't apply to tenant-wide settings or configurations.

For example, an administrator who is assigned the Groups Administrator role at the scope of an administrative unit can manage groups that are members of the administrative unit, but they can't manage other groups in the tenant. They also can't manage tenant-level settings related to groups, such as expiration or group naming policies.
Box 3: Password Administrator
* Password Administrator
Can reset passwords for non-administrators within the assigned administrative unit only. This is a privileged role. Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.
Reference:
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-assign-roles

**NEW QUESTION: 49**
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
**Answer: A,E (LEAVE A REPLY)**
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 device as a condition, create both a conditional access policy AND a session policy.

**NEW QUESTION: 50**
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 end point.
Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

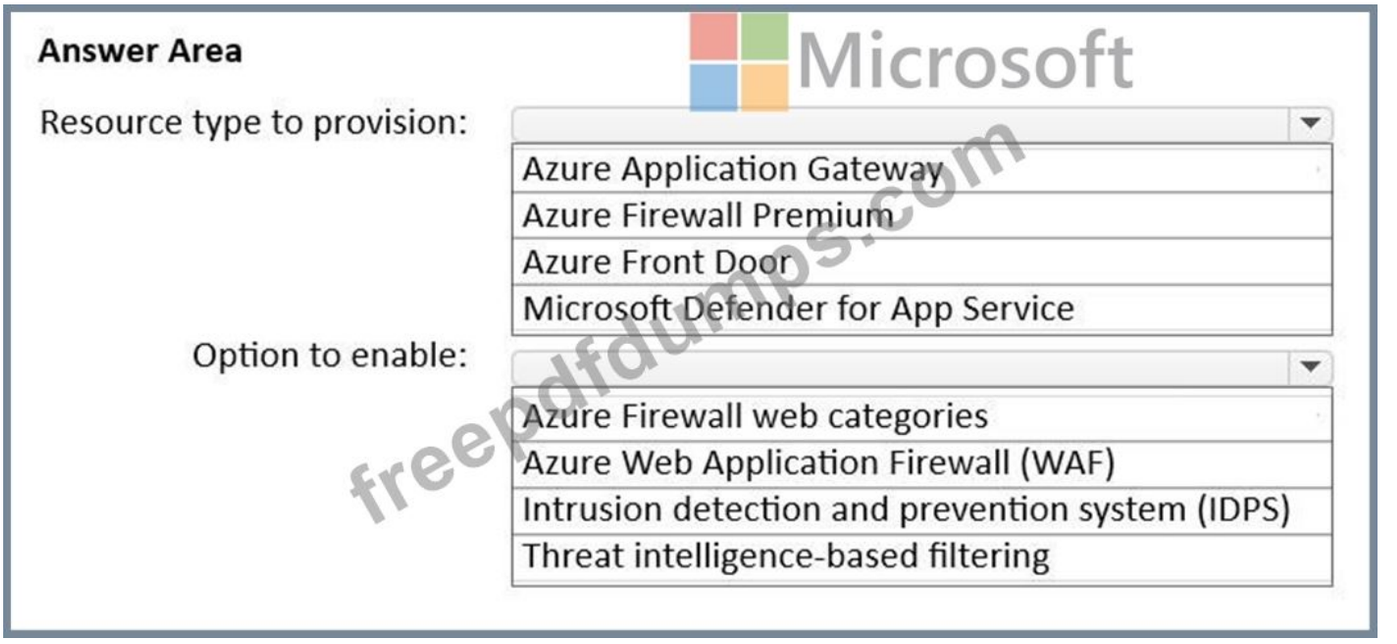
NOTE: Each correct selection is worth one point.
**A.** Microsoft Defender for Endpoint reports the endpoints as compliant.
**B.** Microsoft Intune reports the endpoints as compliant.
**C.** A new Microsoft Entra Conditional Access policy is enforced.
**D.** The client access tokens are refreshed.
**Answer: B,D (LEAVE A REPLY)**
Mobile device management (MDM) solutions like Intune can help protect organizational data by requiring users and devices to meet some requirements. In Intune, this feature is called compliance policies.
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

**NEW QUESTION: 51**
You have an Azure subscription that contains multiple Azure Blob Storage accounts.
You need to recommend a solution to detect threats in files after the files are uploaded to a blob container.
What should you include in the recommendation?
**A.** sensitive data threat detection in Microsoft Defender for Storage
**B.** runtime threat protection in Microsoft Defender for Containers
**C.** vulnerability assessment in Microsoft Defender for Containers
**D.** malware scanning in Microsoft Defender for Storage
**Answer: (SHOW ANSWER)**
Malware Scanning in Defender for Storage helps protect your Azure Blob Storage from malicious content by performing a full malware scan on uploaded content in near real time, using Microsoft Defender Antivirus capabilities. It's designed to help fulfill security and compliance requirements for handling untrusted content.
The Malware Scanning capability is an agentless SaaS solution that allows simple setup at scale, with zero maintenance, and supports automating response at scale.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-malware-scan

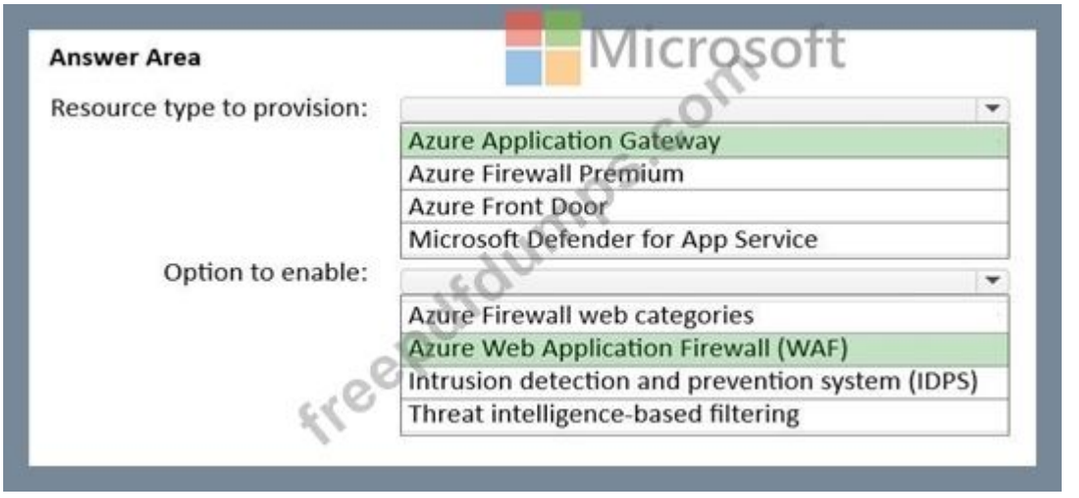
**NEW QUESTION: 52**
Hotspot Question
You have an Azure subscription that contains App Service apps in four Azure regions. Users connect to the apps from the internet.
You plan to block requests to the apps if the requests contain security threats specified in the Core Rule Set (CRS) of the Open Web Application Security Project (OWASP).
You need to design a solution to block the requests. The solution must meet the following requirements:
- Maintain access to the apps in the event of a region outage.
- Minimize the number of resources required.

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:**




Explanation:

Box 1: Azure Application Gateway

The Azure Web Application Firewall (WAF) on Azure Application Gateway actively safeguards your web applications against common exploits and vulnerabilities.

WAF on Application Gateway is based on the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP).

Box 2: Azure Web Application Firewall (WAF)

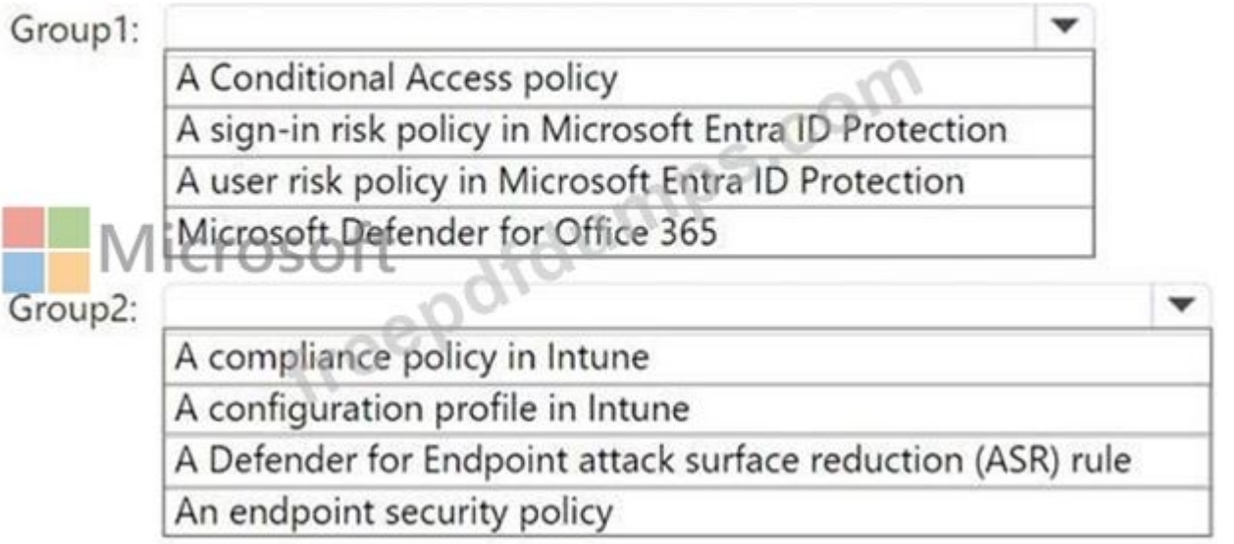
Note: Multi-region load balancing with Traffic Manager, Azure Firewall, and Application Gateway

This architecture is for global, internet-facing applications that use HTTP(S) and non-HTTP(S) protocols. It features DNS-based global load balancing, two forms of regional load balancing, and global virtual network peering to create a high availability architecture that can withstand a regional outage. Traffic inspection is provided by both Azure Web Application Firewall (WAF) and Azure Firewall.

Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview
https://learn.microsoft.com/en-us/azure/architecture/high-availability/reference-architecture-traffic-manager-application-gateway

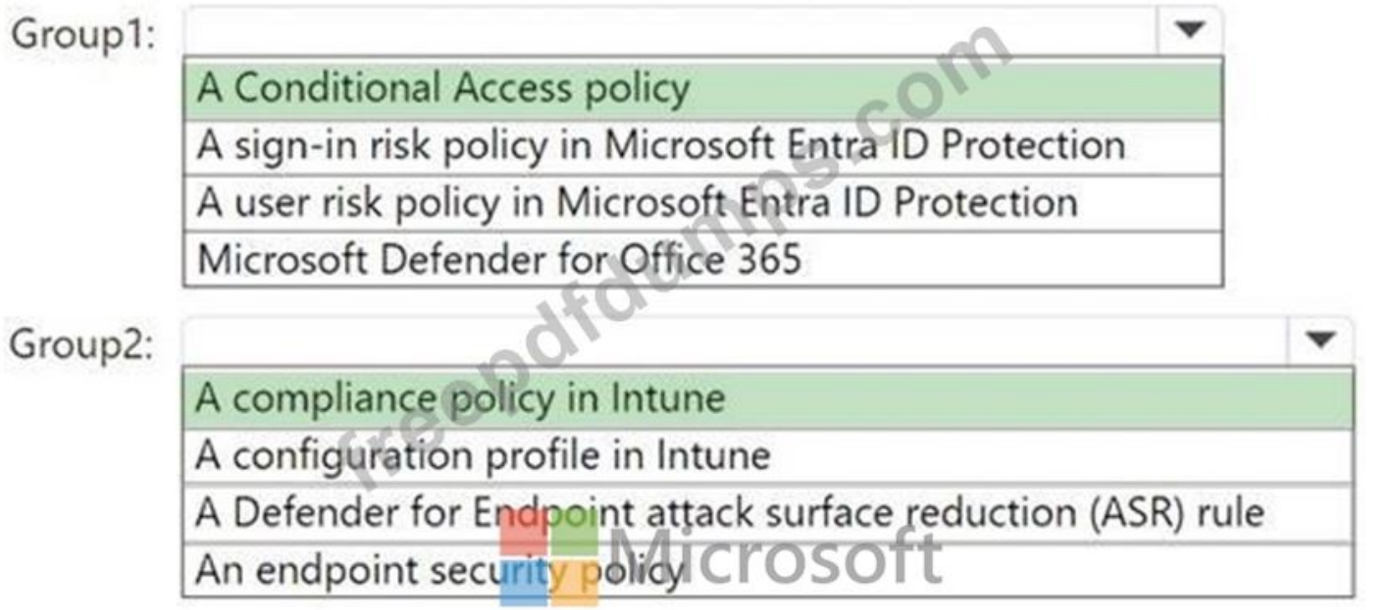
**NEW QUESTION: 53**
Hotspot Question
You have a Microsoft 365 subscription that contains 1,000 users and two groups named Group1 and Group2. All the users have devices that are onboarded to Microsoft Intune and Microsoft Defender for Endpoint. Group1 manages Microsoft Entra and Microsoft 365 services. Group2 manages Intune and Defender for Endpoint.
You need to recommend a solution to prevent users from connecting to Microsoft 365 services from devices that have encryption disabled.
What should you recommend implementing for each group? To answer, select the options in the answer area.
NOTE: Each correct answer is worth one point.

**Answer Area**




**Answer:**

Answer Area




Explanation:

Box 1: A Conditional Access policy

Group1 manages Microsoft Entra and Microsoft 365 services.

Microsoft Entra ID, Conditional Access, Common Conditional Access policy: Require a compliant device, Microsoft Entra hybrid joined device, or multifactor authentication for all users

Organizations who deploy Microsoft Intune can use the information returned from their devices to identify devices that meet compliance requirements such as:

Requiring a PIN to unlock

*-> Requiring device encryption

Requiring a minimum or maximum operating system version

Requiring a device isn't jailbroken or rooted

Box 2: A compliance policy in Intune

Group2 manages Intune and Defender for Endpoint.

Device Compliance settings for Windows 10/11 in Intune includes:

* Encryption

Encryption of data storage on a device:

This setting applies to all drives on a device.

Not configured (default)

Require - Use Require to encrypt data storage on your devices.

DeviceStatus CSP - DeviceStatus/Compliance/EncryptionCompliance

Reference:

https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-compliant-device

https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

**NEW QUESTION: 54**

Hotspot Question

You have a Microsoft Entra tenant. The tenant contains a security group named Group1. Group1 contains the members of your company's IT support team.

You have an Azure subscription. The subscription contains 800 Windows devices that are Microsoft Entra joined and 200 Windows devices that are Microsoft Entra registered.

You have 200 standalone macOS devices.

You deploy 10 Windows devices that are Microsoft Entra joined and have the Microsoft Entra ExtensionAttribute1 value set to SecureWorkstation.

You need to recommend a Conditional Access solution that meets the following requirements:

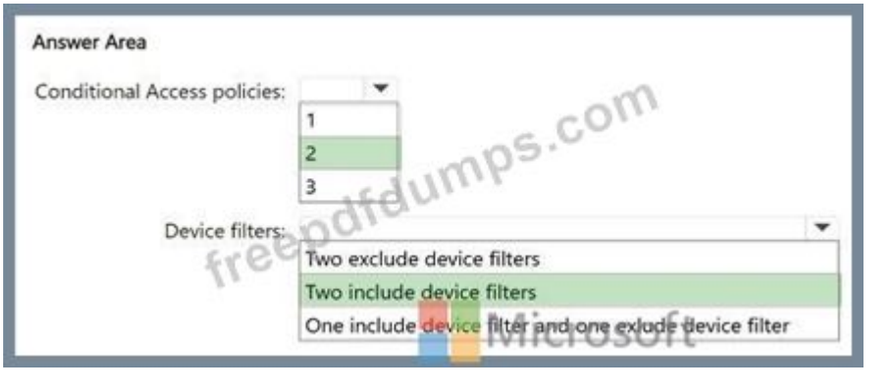
- Only allows access to Microsoft Entra resources from devices that run Windows 10 or Windows 11
- Restricts Windows Azure Service Management API access to the following users:
- The members of Group1
- Users that authenticate by using multifactor authentication (MFA)
- Users that connect from a device that has the SecureWorkstation ExtensionAttribute1

The solution must minimize the number of required policies and maximize security.

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

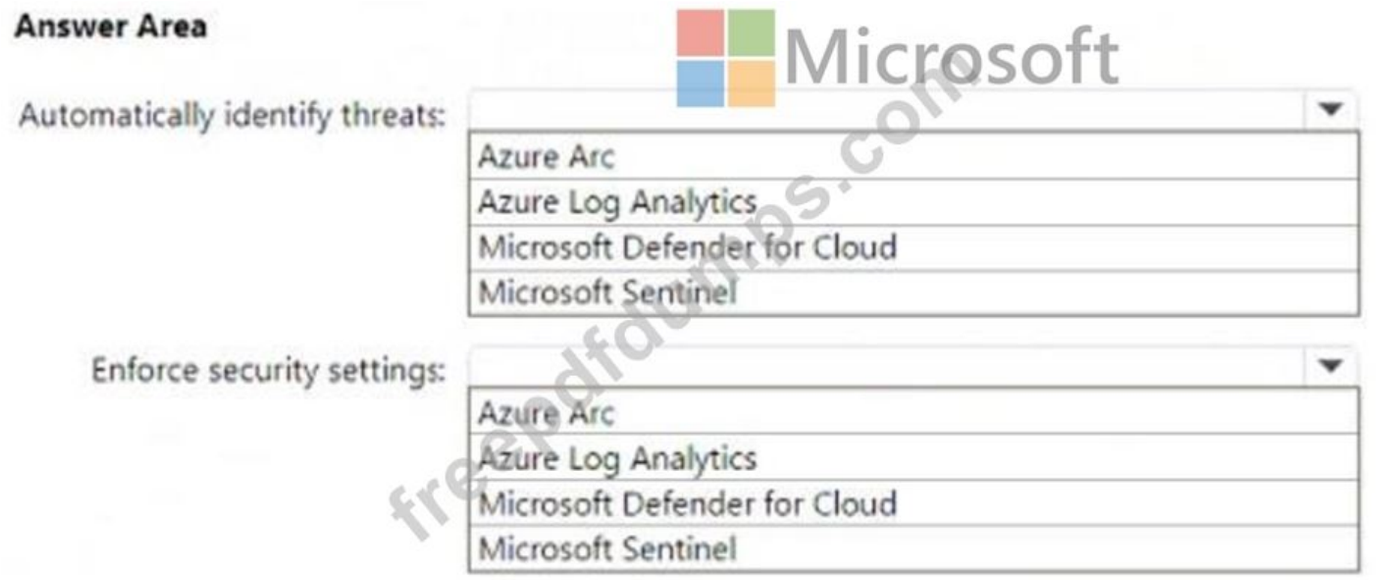
NOTE: Each correct selection is worth one point.


**Answer:**

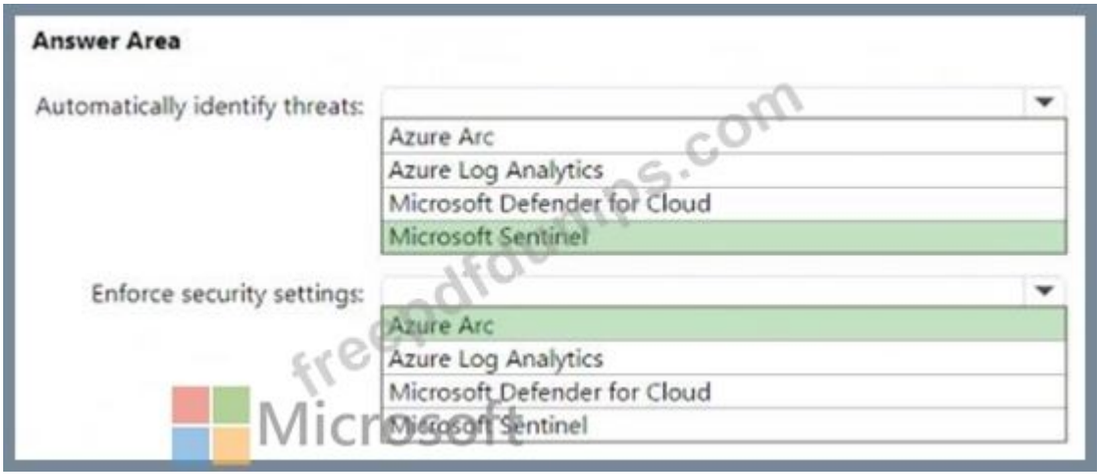


Explanation:
Box 1: 2
* Only allows access to Microsoft Entra resources from devices that run Windows 10 or Windows 11
Create one Conditional Access policy that uses one include device filter which includes only Windows 10 and Windows 11.
* Restricts Windows Azure Service Management API access to the following users:
The members of Group1
Users that authenticate by using multifactor authentication (MFA)
Users that connect from a device that has the SecureWorkstation ExtensionAttribute1 Create a second Conditional Access policy that includes Group1, requires MFA, and one include device for devices that has the SecureWorkstation ExtensionAttribute1. Grant access to Windows Azure Service Management API.
Box 2: Two include device filters
Reference:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-condition-filters-for-devices

**NEW QUESTION: 55**
Hotspot Question
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.




**Answer:**




**NEW QUESTION: 56**

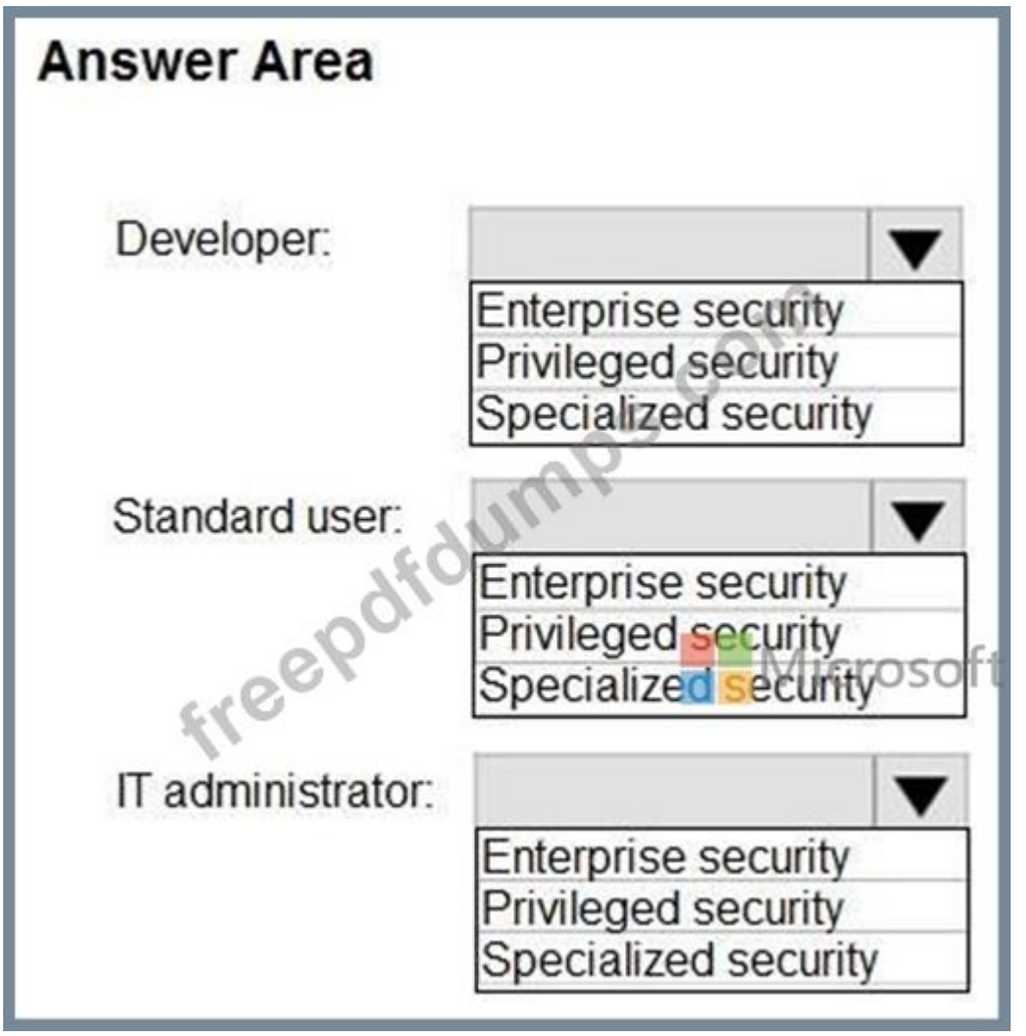
Hotspot Question

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
Developer:
Enterprise security
Privileged security
Specialized security
Standard user:
Enterprise security
Privileged security
Specialized security
IT administrator:
Enterprise security
Privileged security
Specialized security

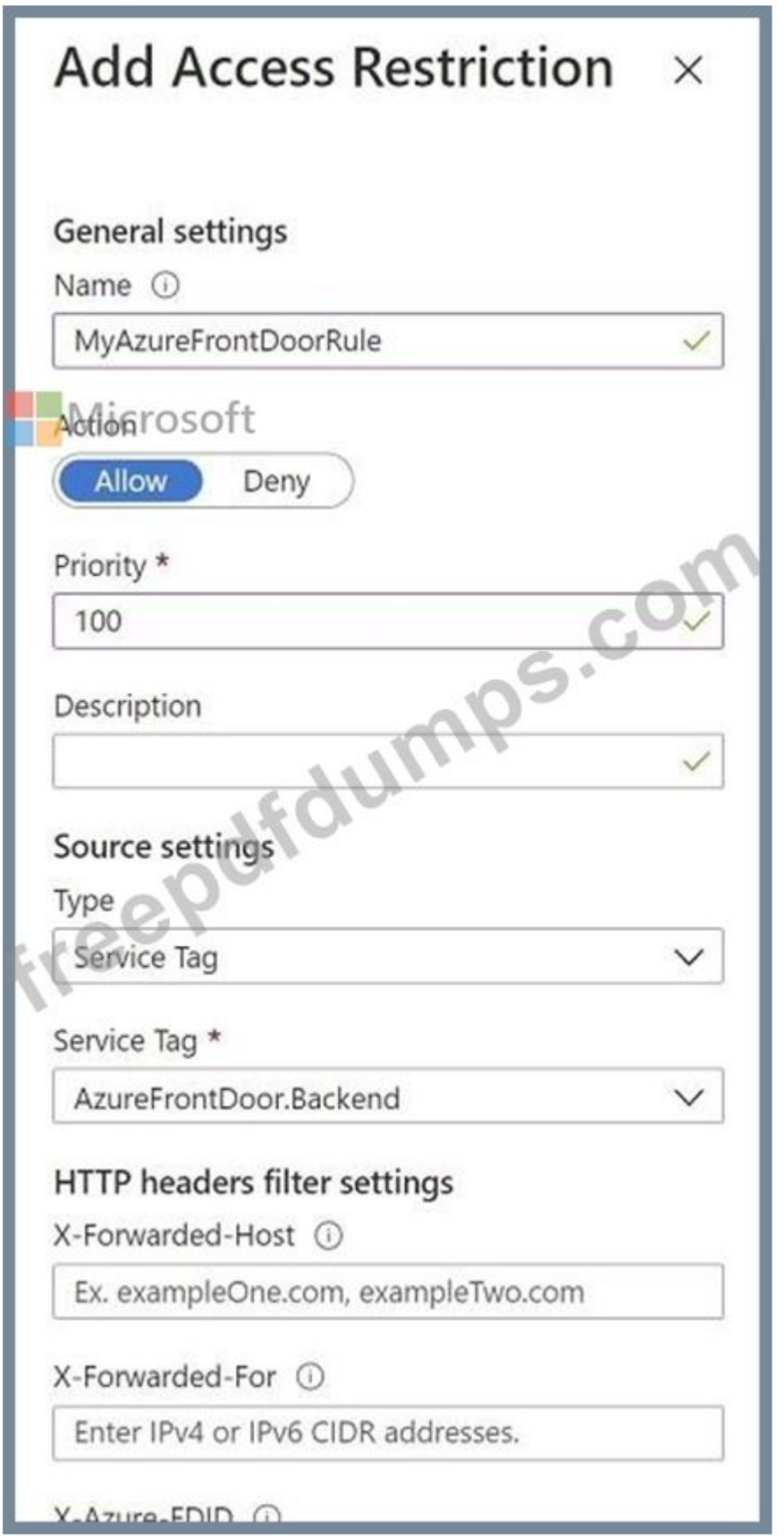
**Answer:**


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

**NEW QUESTION: 57**
You have a multicloud environment that contains an Azure subscription, an Amazon Web Services (AWS) subscription, and a Google Cloud Platform (GCP) subscription.
You plan to assess data security and compliance.
You need to design a Compliance Manager solution that meets the following requirements:
- Provides recommended improvement actions that include detailed implementation guidance
- Automatically monitors regulatory compliance
- Minimizes administrative effort
What should you include in the solution?
**A.** Microsoft Defender for Cloud
**B.** Compliance Manager connectors
**C.** Microsoft Defender for Cloud Apps
**D.** Microsoft Sentinel
**Answer: A (LEAVE A REPLY)**
Microsoft Purview, Configure cloud settings for use with Compliance Manager Compliance Manager integrates with Microsoft Defender for Cloud to provide multicloud support. Organizations must have at least one subscription within Microsoft Azure and then enable Defender for Cloud so that Compliance Manager can receive the necessary signals to monitor

your cloud services. Once you have Defender for Cloud, you need to assign the relevant industry and regulatory standards to your subscriptions.
View available environments
1. In Defender for Cloud, select Environment settings on the left navigation.
2. View the available environments and subscriptions currently visible to MDC for your tenant.
You may need to expand your management groups to view subscriptions, which you can do by selecting Expand all below the search bar. In addition to your Azure subscriptions, you'll also see any Google Cloud Platform (GCP) projects or Amazon Web Services (AWS) accounts connected to Defender for Cloud.
Reference:
https://learn.microsoft.com/en-us/purview/compliance-manager-cloud-settings

**NEW QUESTION: 58**
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
**Answer: B (LEAVE A REPLY)**
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

**NEW QUESTION: 59**
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
**Answer: (SHOW ANSWER)**
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/azure/defender-for-cloud/integration-defender-for-endpoint

**NEW QUESTION: 60**
You have a Microsoft 365 subscription.
You have an Azure subscription.
You need to implement a Microsoft Purview communication compliance solution for Microsoft Teams and Yammer. The solution must meet the following requirements:
- Assign compliance policies to Microsoft 365 groups based on custom
Microsoft Exchange Online attributes.
- Minimize the number of compliance policies.
- Minimize administrative effort.
What should you include in the solution?
**A.** adaptive scopes
**B.** Microsoft 365 Defender user tags
**C.** administrative units
**D.** Microsoft Purview sensitivity labels
**Answer: (SHOW ANSWER)**
When you create a communication compliance policy or a policy for retention, you can create or add an adaptive scope for your policy. A single policy can have one or many adaptive scopes.

An adaptive scope uses a query that you specify, so you can define the membership of users or groups included in that query. These dynamic queries run daily against the attributes or properties that you specify for the selected scope. You can use one or more adaptive scopes with a single policy.
Reference:
https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

**NEW QUESTION: 61**
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.** Create shared access signatures (SAS).
**B.** Share the connection string of the access key.
**C.** Configure private link connections.
**D.** Configure encryption by using customer-managed keys (CMKs)
**Answer: A (LEAVE A REPLY)**
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.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview



**NEW QUESTION: 62**
Hotspot Question
You have an Azure subscription. The subscription contains an Azure SQL database named DB1 that stores customer data.

You have a Microsoft 365 subscription that uses Microsoft SharePoint Online, OneDrive, and Teams.

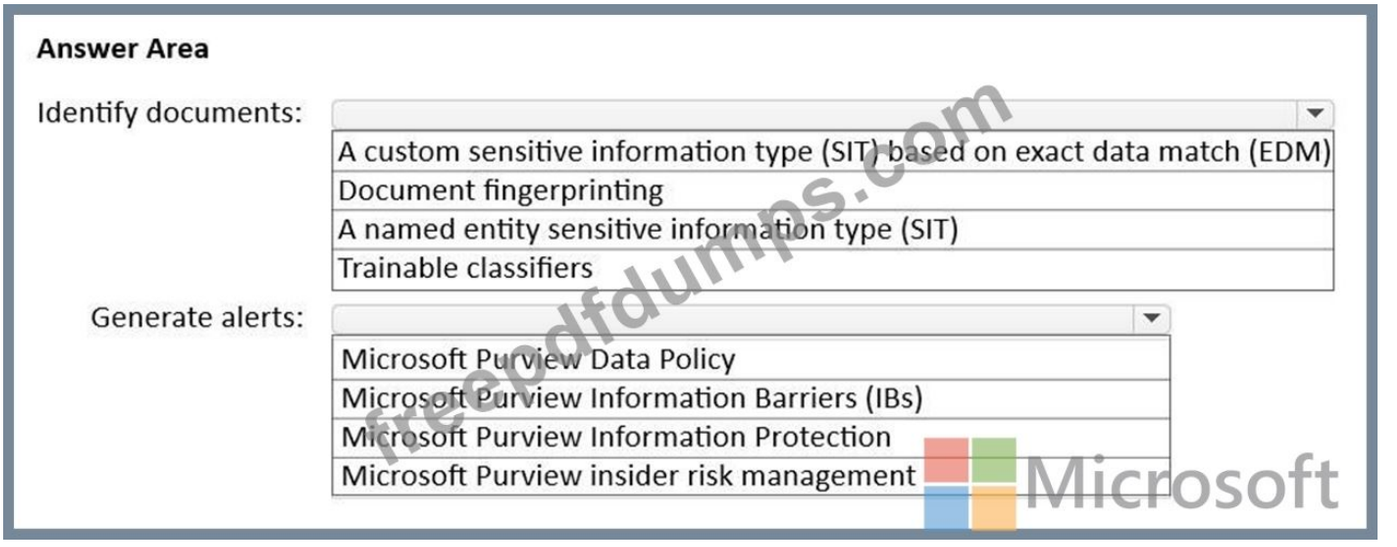
Users frequently create Microsoft Office documents that contain data from DB1.

You need to recommend a Microsoft Purview solution that meets the following requirements:

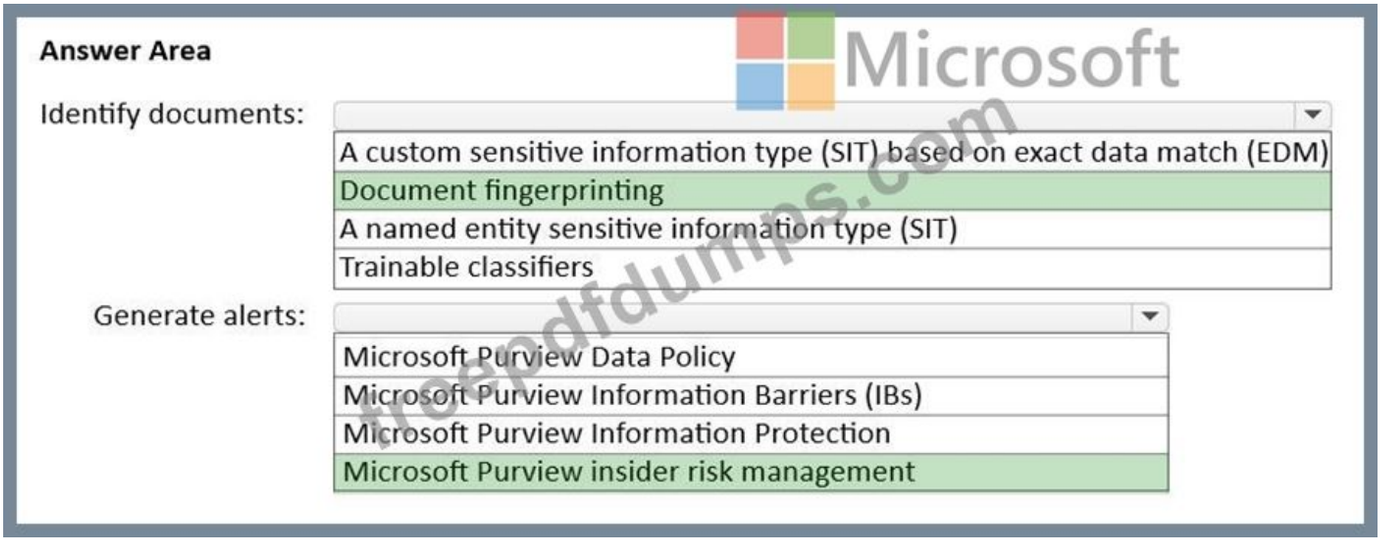
- Identifies Office documents that contain customer addresses and phone numbers sourced from DB1
- Generates an alert if a user downloads an above average number of files that contain data from DB1
- Minimizes the number of false positives

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.




**Answer:**




Explanation:

Box 1: Document fingerprinting

Identifies Office documents that contain customer addresses and phone numbers sourced from DB1 Document fingerprinting is a Microsoft Purview feature that takes a standard form that you provide and creates a sensitive information type (SIT) based on that form. Document

fingerprinting makes it easier for you to protect sensitive information by identifying standard forms that are used throughout your organization.
Document fingerprinting includes the following benefits:
SITs created from document fingerprinting can be used as a detection method in DLP policies scoped to Exchange, SharePoint, OneDrive, Teams, and Devices.
Etc.
Box 2: Microsoft Purview insider risk management
Generates an alert if a user downloads an above average number of files that contain data from DB1 Microsoft Purview, Configure intelligent detections in insider risk management Use can use the Intelligent detections setting in Microsoft Purview Insider Risk Management to:
* Boost the score for unusual file download activities by entering a minimum number of daily events.
* Etc.
File activity detection
You can use this section to specify the number of daily events required to boost the risk score for download activity that's considered unusual for a user. For example, if you enter "25", if a user downloads 10 files on average over the previous 30 days, but a policy detects that they downloaded 20 files on one day, the score for that activity won't be boosted even though it's unusual for that user because the number of files they downloaded that day was less than 25.
Reference:
https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-intelligent-detections

**NEW QUESTION: 63**
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
**Answer: A (LEAVE A REPLY)**
The most simple solution is to host a jumpbox on the virtual network of the data management landing zone or data landing zone to connect to the data services through private endpoints.
Azure Bastion provides a few other core security benefits, including:
* The service integrates with native security appliances for an Azure virtual network, such as Azure Firewall.

Note:
* Platform landing zones: Subscriptions deployed to provide centralized services, often operated by a central team, or a number of central teams split by function (e.g. networking, identity), which will be used by various workloads and applications. Platform landing zones represent key services that often benefit from being consolidated for efficiency and ease of operations. Examples include networking, identity, and management services.
* The Azure App Service landing zone accelerator is an open-source collection of architectural guidance and reference implementation to accelerate deployment of Azure App Service at scale. It can provide a specific architectural approach and reference implementation via infrastructure as code templates to prepare your landing zones. The landing zones adhere to the architecture and best practices of the Cloud Adoption Framework.
Reference:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/cloud-scale-analytics/architectures/connect-to-environments-privately
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/
https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v3
https://learn.microsoft.com/en-us/azure/architecture/framework/

**NEW QUESTION: 64**
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
**Answer: C (LEAVE A REPLY)**
Azure SQL Database is a general-purpose relational database, provided as a managed service. Categorized as a platform as a service (PaaS), Azure 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 system 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 virtual network (VNet) and near 100 percent compatibility with on-premises SQL Server. Azure SQL Database Managed Instance provides you with full SQL Server access and feature compatibility for migrating SQL Servers to Azure.

https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking- overview?view=azuresql

**NEW QUESTION: 65**

You have an Azure subscription that contains the Azure Virtual Machine Scale Sets shown in the following table.

| Name | Configuration |
|---|---|
| VMSS1 | • Orchestration mode: Flexible<br>• Image type: Windows Server virtual machine platform image |
| VMSS2 | • Orchestration mode: Uniform<br>• Image type: Windows Server virtual machine custom image |
| VMSS3 | • Orchestration mode: Flexible<br>• Image type: Linux virtual machine platform image |
| VMSS4 | • Orchestration mode: Uniform<br>• Image type: Linux virtual machine custom image |



You are evaluating Azure Update Manager and automatic virtual machine guest patching.

Which virtual machine scale sets will automatic guest patching support?

**A.** VMSS1 only

**B.** VMSS2 only

**C.** VMSS1 and VMSS3 only

**D.** VMSS2 and VMSS4 only

**E.** VMSS1, VMSS2, VMSS3, and VMSS4

**Answer: C (LEAVE A REPLY)**

* VMSS1 -Yes

Standard Windows virtual machine platform images are supported.

Flexible orchestration mode is supported.

Note: Enabling Automatic Guest Patching on single-instance VMs or Virtual Machine Scale Sets in Flexible orchestration mode allows the Azure platform to update your fleet in phases.

* VMSS2 - No

Custom images are not supported.

* VMSS3 - Yes

Standard Linux virtual machine platform images are supported.

Flexible orchestration mode is supported.

* VMSS4 - No

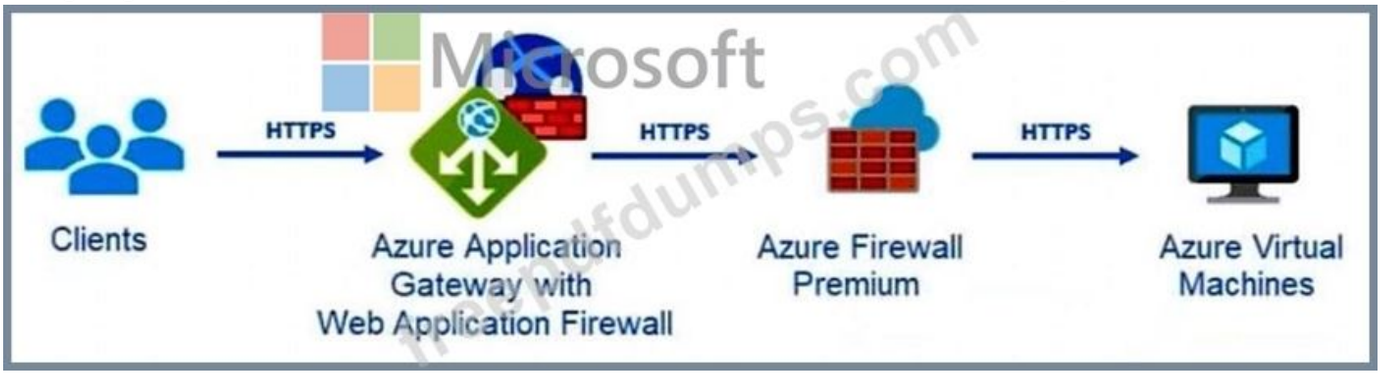
Custom images are not supported.

Note:

Automatic VM guest patching, on-demand patch assessment and on-demand patch installation are supported only on VMs created from images with the exact combination of publisher, offer and sku from the below supported OS images list. Custom images or any other publisher, offer, sku combinations aren't supported. More images are added periodically.

Reference:
https://learn.microsoft.com/en-us/azure/virtual-machines/automatic-vm-guest-patching

**NEW QUESTION: 66**
Hotspot Question
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.

**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 |

**Answer:**

**Answer Area**

| For WAF: |
| --- |
| The Azure Diagnostics extension |
| Azure Network Watcher |
| Data connectors |
| Workflow automation |

| For the virtual machines: |
| --- |
| The Azure Diagnostics extension |
| Azure Storage Analytics |
| Data connectors |
| The Log Analytics agent |
| Workflow automation |



Explanation:
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

**NEW QUESTION: 67**

Case Study 1 - Fabrikam, Inc

OverView

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

Existing Environment

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment

Fabrikam has the following Azure resources:

- A Microsoft Entra tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com
- A single Azure subscription named Sub1
- A virtual network named Vnet1 in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled
- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts
- All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

- An Microsoft Entra named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications.

The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1. The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

- Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation. Machines should have a vulnerability assessment solution. All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

- ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.
- Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- Azure DevTest labs will be used by developers for testing.
- All the application code must be stored in GitHub Enterprise.
- Azure Pipelines will be used to manage application deployments.
- All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- Internet-accessible applications must prevent connections that originate in North Korea.
- Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
- Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers:

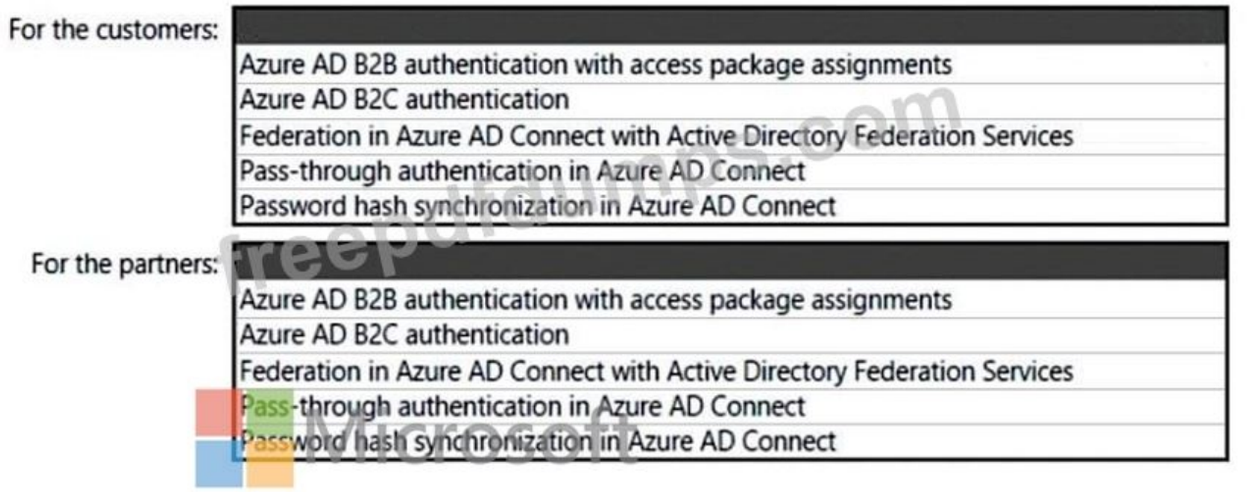
- Every month, the membership of the ContosoDevelopers group must be verified.
- The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.
You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.
What should you include in the recommendation?
**A.** Transparent Data Encryption (TDE)
**B.** Always Encrypted
**C.** row-level security (RLS)
**D.** dynamic data masking
**E.** data classification
**Answer: B (LEAVE A REPLY)**
It is not possible to restrict permissions of a db_owner, and therefore prevent an administrative account from viewing user data. If there's highly sensitive data in a database, Always Encrypted can be used to safely prevent db_owners or any other DBA from viewing it.
Reference:
https://learn.microsoft.com/en-us/azure/azure-sql/database/security-best-practice?view=azuresql

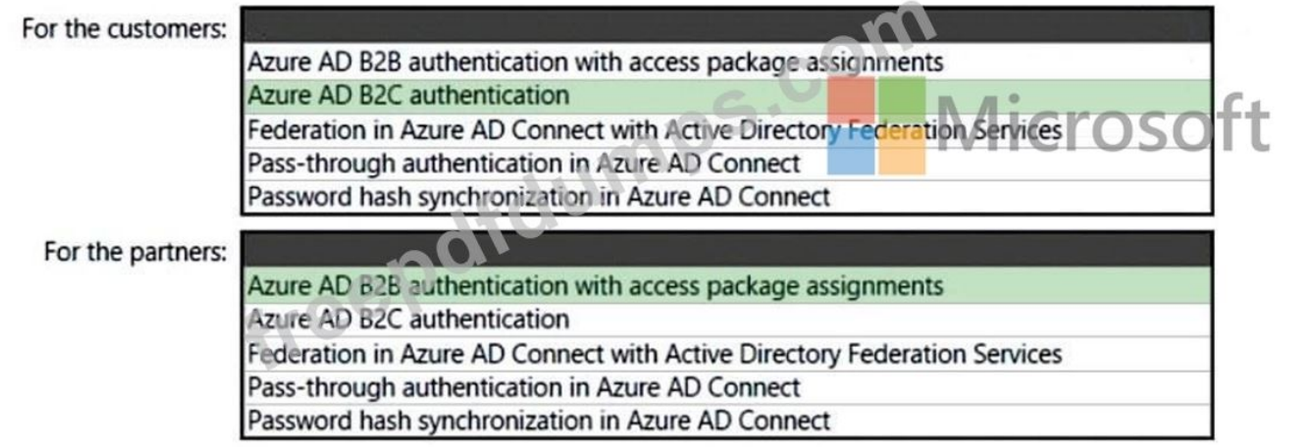
**NEW QUESTION: 68**
Hotspot Question
Your company has a Microsoft 365 E5 subscription, an Azure subscription, on-premises applications, and Active Directory Domain Services (ADDS).
You need to recommend an identity security strategy that meets the following requirements:
- Ensures that customers can 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.

**Answer Area**




**Answer:**

**Answer Area**




Explanation:

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.

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

**NEW QUESTION: 69**
Your organization is in the process of moving its on-premises VMs into Azure; you're using Azure Backup to protect these VMs.
The Chief Information Officer is concerned about ransomware attacks and has asked for an Azure native cost-effective solution that can be initiated in case of a ransomware attack, and a backup restoration is necessary.
What security configurations can you implement?
**A.** Backup to Azure Data Box
**B.** A Veeam backup solution
**C.** Require PINs for critical operations
**D.** Enable soft delete
**Answer: (SHOW ANSWER)**
Option A is incorrect because it's not a cost-effective solution
Option B is incorrect because it's not in the native Azure solution
Options C is correct because 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, Option D is correct because enabling this security feature protects your backup from accident and malicious deletion, adding a layer of security.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

**NEW QUESTION: 70**
You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel 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.** playbooks
**B.** workbooks
**C.** notebooks
**D.** threat intelligence
**Answer: B (LEAVE A REPLY)**
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.

**NEW QUESTION: 71**
Case Study 1 - Fabrikam, Inc
OverView
Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.
Existing Environment
On-premises Environment
The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.
Azure Environment
Fabrikam has the following Azure resources:
- A Microsoft Entra tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com
- A single Azure subscription named Sub1
- A virtual network named Vnet1 in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled
- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts
- All the resources in Sub1 are in either the East US or the West Europe region.
Partners
Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:
- An Microsoft Entra named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications.
The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1. The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

- Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation. Machines should have a vulnerability assessment solution. All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

- ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.
- Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- Azure DevTest labs will be used by developers for testing.
- All the application code must be stored in GitHub Enterprise.
- Azure Pipelines will be used to manage application deployments.
- All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- Internet-accessible applications must prevent connections that originate in North Korea.
- Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
- Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers:
- Every month, the membership of the ContosoDevelopers group must be verified.
- The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

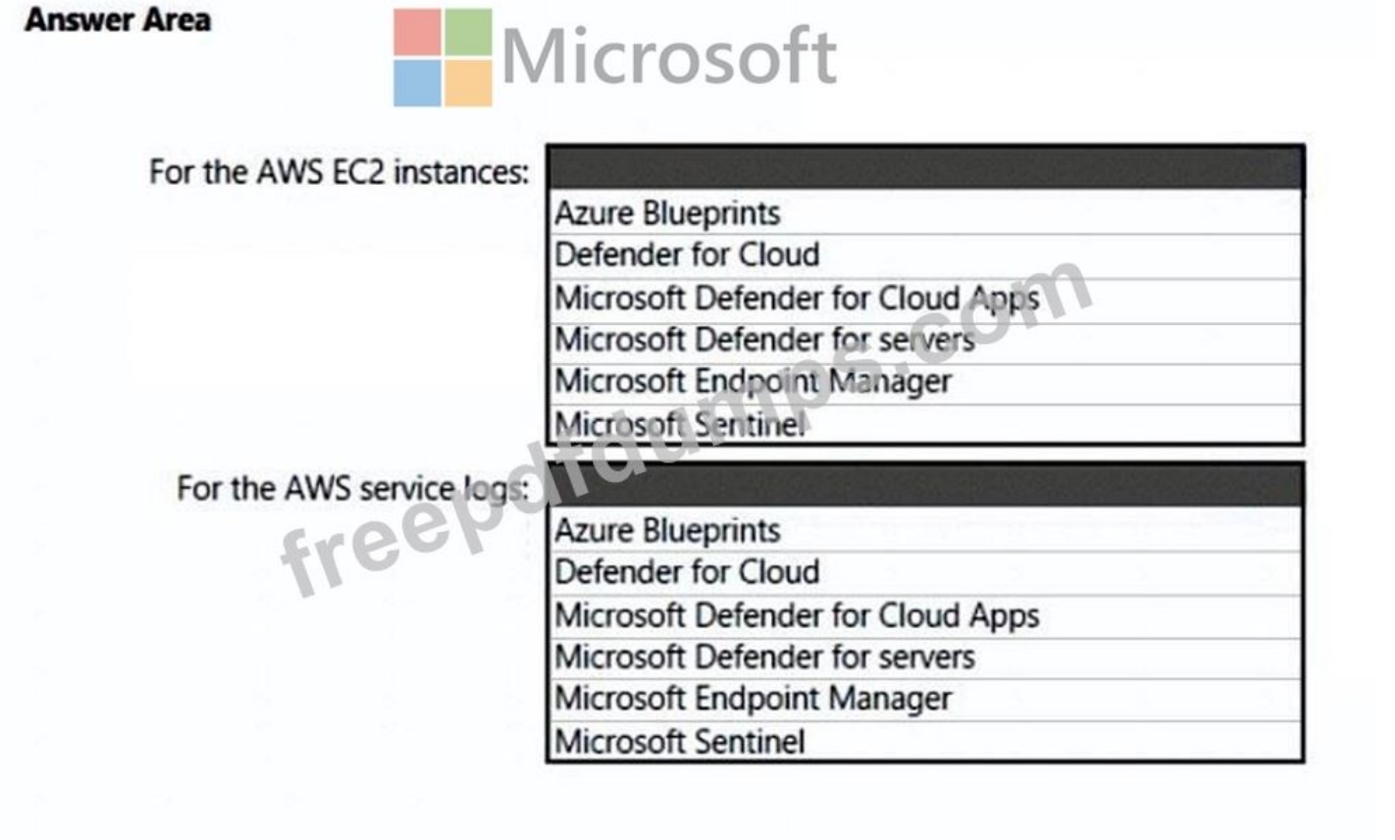
Hotspot Question

You need to recommend a solution to meet the AWS requirements.

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

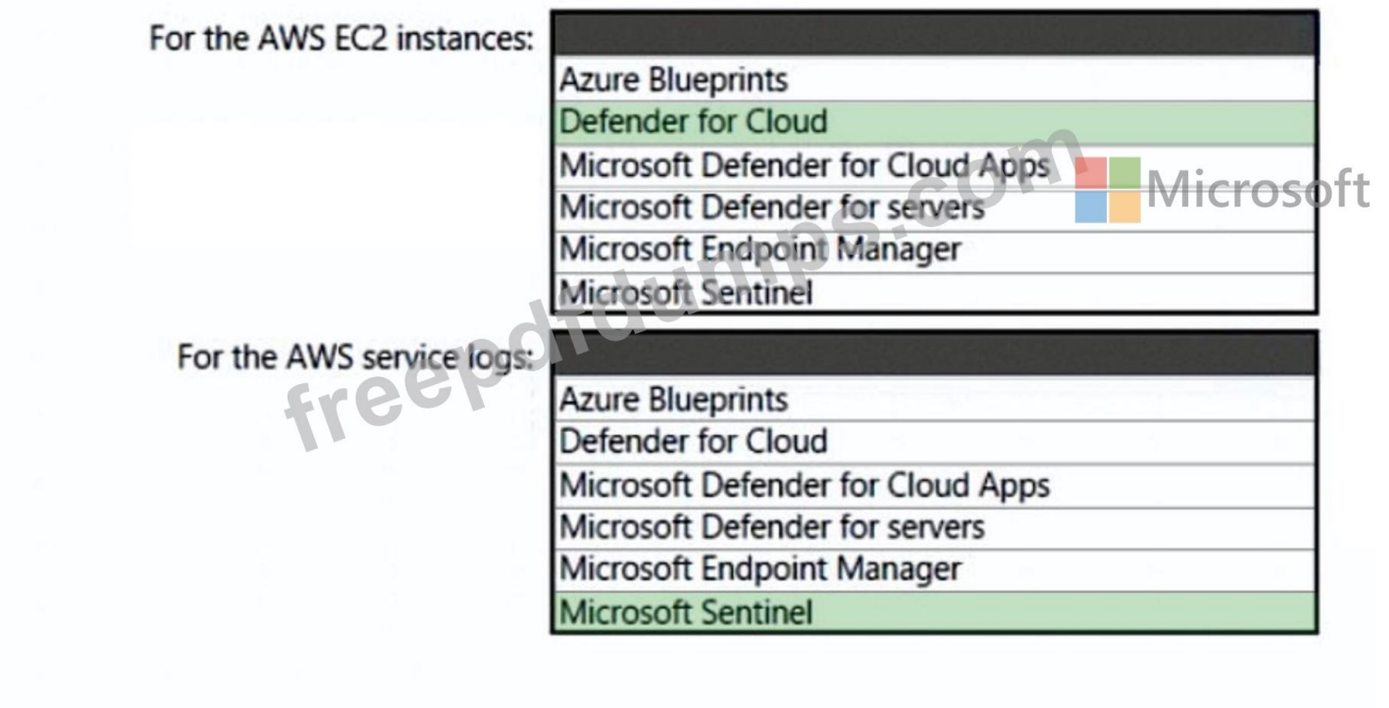
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**

**Answer Area**






Explanation:

Box 1: Defender for Cloud

The requirement is to identify EC2 instances which are noncompliant with secure score recommendations.

Box 2: Microsoft Sentinel

Use the Amazon Web Services (AWS) connectors to pull AWS service logs into Microsoft Sentinel. These connectors work by granting Microsoft Sentinel access to your AWS resource logs. Setting up the connector establishes a trust relationship between Amazon Web Services and Microsoft Sentinel. This is accomplished on AWS by creating a role that gives permission to Microsoft Sentinel to access your AWS logs.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

https://docs.microsoft.com/en-us/azure/sentinel/connect-aws?tabs=s3

**NEW QUESTION: 72**

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
**Answer: (SHOW ANSWER)**
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

**NEW QUESTION: 73**
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
**Answer: (SHOW ANSWER)**
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.

**NEW QUESTION: 74**
You have a Microsoft 365 subscription.
You have an Azure subscription.
You need to implement a Microsoft Purview communication compliance solution for Microsoft Teams and Yammer. The solution must meet the following requirements:
- Assign compliance policies to Microsoft 365 groups based on custom Microsoft Exchange Online attributes.
- Minimize the number of compliance policies.
- Minimize administrative effort.
What should you include in the solution?
**A.** Microsoft Purview Information Protection
**B.** Microsoft 365 Defender user tags
**C.** adaptive scopes
**D.** administrative units
**Answer: C (LEAVE A REPLY)**
When you create a communication compliance policy or a policy for retention, you can create or add an adaptive scope for your policy. A single policy can have one or many adaptive scopes. An adaptive scope uses a query that you specify, so you can define the membership of users or groups included in that query. These dynamic queries run daily against the attributes or properties that you specify for the selected scope. You can use one or more adaptive scopes with a single policy.
Reference:
https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

**NEW QUESTION: 75**
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 SQL Database
**C.** Azure Synapse Analytics dedicated SQL pools
**D.** SQL Server on Azure Virtual Machines
**Answer: (SHOW ANSWER)**
Azure SQL Database is a general-purpose relational database, provided as a managed service. Categorized as a platform as a service (PaaS), Azure 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 system 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 virtual network (VNet) and near 100 percent compatibility with on-premises SQL Server. Azure SQL Database Managed Instance provides you with full SQL Server access and feature compatibility for migrating SQL Servers to Azure.
https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking- overview?view=azuresql

**NEW QUESTION: 76**
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

**Answer: (SHOW ANSWER)**

Its cause Vnet3 and Vnet4 have peering to each other. So a bastion subnet in either Vnet3 or Vnet4 is enough to access them both over the Vnet peering.

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion



**NEW QUESTION: 77**

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

**C.** From Azure Policy, assign a built-in policy definition that has a scope of the subscription.

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

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 78**

You have a multicloud environment that contains Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) subscriptions.

You need to discover and review role assignments across the subscriptions.

What should you use?

**A.** Azure Lighthouse

**B.** Microsoft Defender for Identity

**C.** Microsoft Entra ID Governance

**D.** Microsoft Entra Permissions Management

**Answer: D (LEAVE A REPLY)**

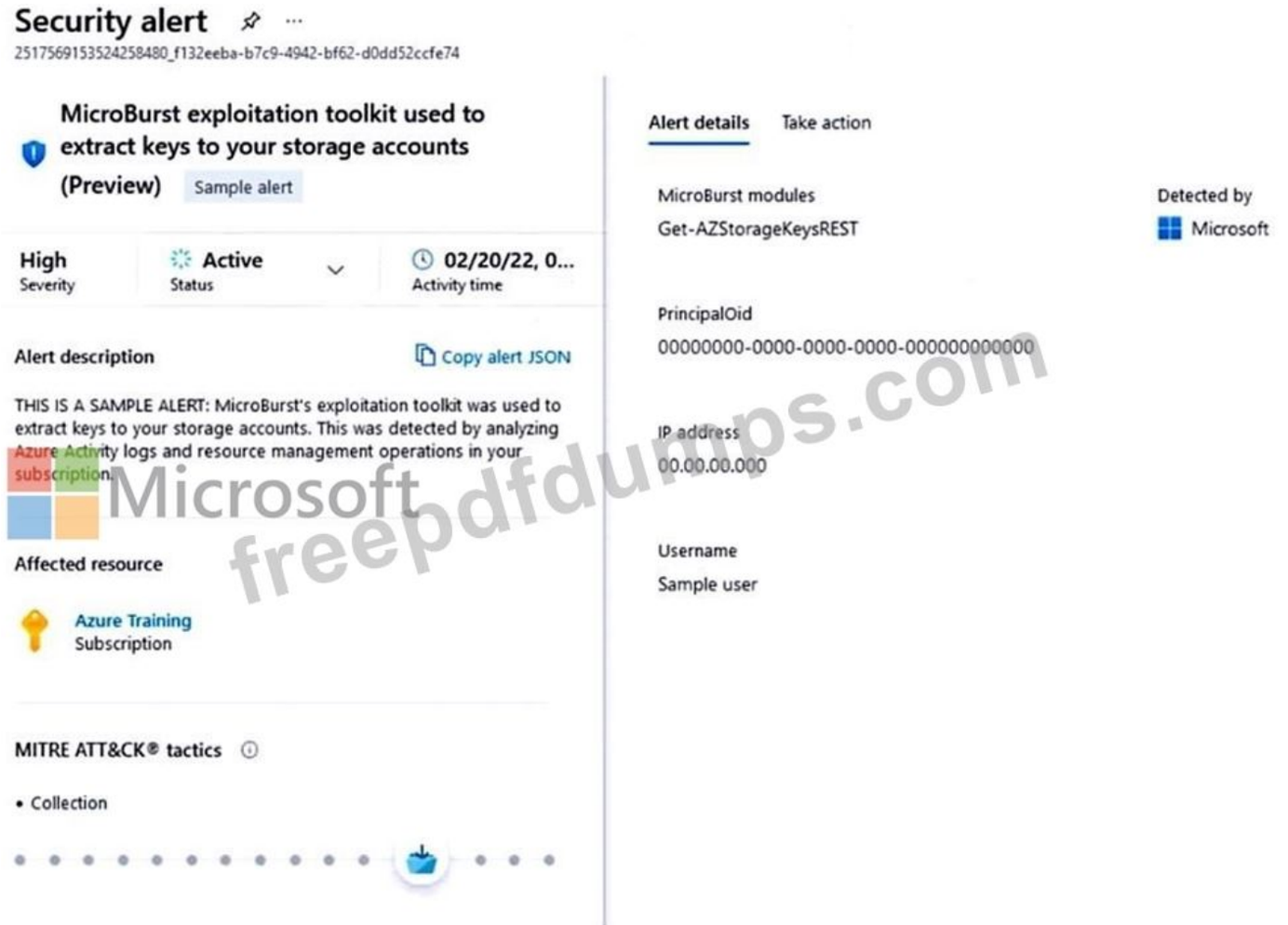
Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) product that provides comprehensive visibility and control over permissions for any

identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP).
Reference:
https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-permissions-management

**NEW QUESTION: 79**
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 Disk Storage
**B.** Azure Storage blob containers
**C.** Azure Storage file shares
**D.** Azure Data Lake Storage Gen2
**Answer: B,D (LEAVE A REPLY)**
B: 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 C: 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

**NEW QUESTION: 80**
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
**Answer: C (LEAVE A REPLY)**
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 access you can't get the key without being authenticated and authorized.
The preventive control here is to manage Shared Key Authorization.

**NEW QUESTION: 81**
You have a multicloud environment that contains an Azure subscription, an Amazon Web Services (AWS) subscription, and a Google Cloud Platform (GCP) subscription.
You plan to implement Cloud Security Posture Management (CSPM) by using Microsoft Defender for Cloud.
You need to design a solution that will provide attack path analysis functionality for each subscription.
What should you include in the solution?
**A.** regulatory compliance
**B.** Microsoft Defender External Attack Surface Management (Defender EASM)
**C.** agentless scanning
**D.** Microsoft Cloud Security Benchmark (MCSB)
**Answer: B (LEAVE A REPLY)**
The Defender CSPM plan utilizes the data collected through the Defender External Attack Surface Management integration to provide the following capabilities within the Defender for Cloud portal:
- Discover of all the internet facing cloud resources through the use of an outside-in scan.
- Attack path analysis which finds all exploitable paths starting from internet exposed IPs.
- Custom queries that correlate all internet exposed IPs with the rest of Defender for Cloud data in the cloud security explorer.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-easm

**NEW QUESTION: 82**
You have a Microsoft Entra tenant that syncs with an Active Directory Domain Services (AD DS) domain. Client computers run Windows and are hybrid-joined to Microsoft Entra.
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.** Microsoft Entra Identity Protection
**C.** Microsoft Entra Privileged Identity Management (PIM)

**D.** Privileged Access Workstations (PAWs)

**Answer: A (LEAVE A REPLY)**

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

**NEW QUESTION: 83**

Hotspot Question

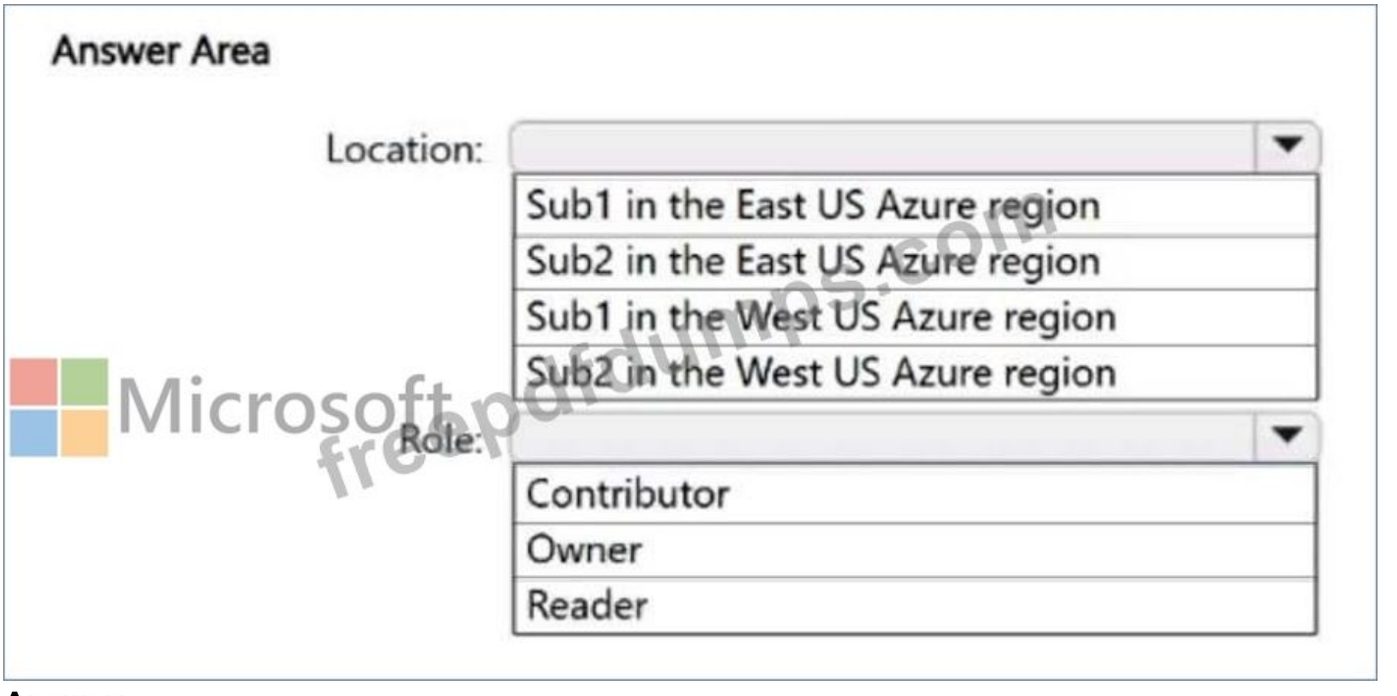
You have the resources shown in the following table.

| Name | Type | Description |
|---|---|---|
| contoso.com | Microsoft Entra tenant | Associated with Sub1 |
| fabrikam.com | Microsoft Entra tenant | Associated with Sub2 |
| Sub1 | Azure subscription | Contains multiple Recovery Services vaults in the US East Azure region |
| Sub2 | Azure subscription | Currently unused |

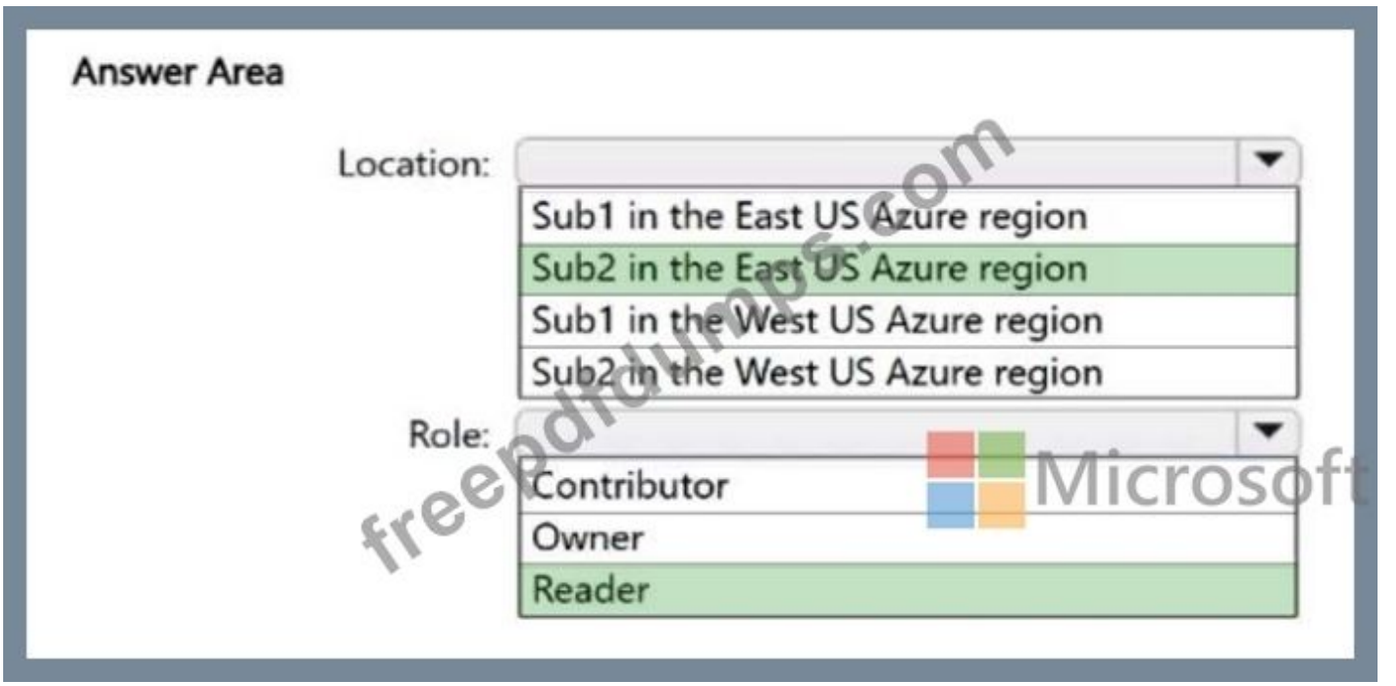
You need to configure multi-user authorization (MUA) for Azure Backup to protect the Recovery Services vaults. The solution must maximize the security of the MUA configuration.

To which location should you deploy Resource Guard, and which role-based access control (RBAC) role should you assign to the team responsible for managing the backup of Resource Guard? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**





Explanation:

Box 1: Sub2 in the US East Azure region

The Recovery service vaults are in Sub1 in the US East Azure region.

We should use the other subscription Sub2 (which also contains the other tenant).

We should use the same region.

Note: Configure Multi-user authorization using Resource Guard in Azure Backup Create a Resource Guard The Security admin creates the Resource Guard. We recommend that you create it in a different subscription or a different tenant as the vault. However, it should be in the same region as the vault. The Backup admin must NOT have Contributor, Backup MUA Admin, or Backup MUA Operator access on the Resource Guard or the subscription that contains it.

Box 2: Reader

Assign permissions to the Backup admin on the Resource Guard to enable MUA To enable MUA on a vault, the admin of the vault must have Reader role on the Resource Guard or subscription containing the Resource Guard.

Reference:

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization

**NEW QUESTION: 84**

Hotspot Question

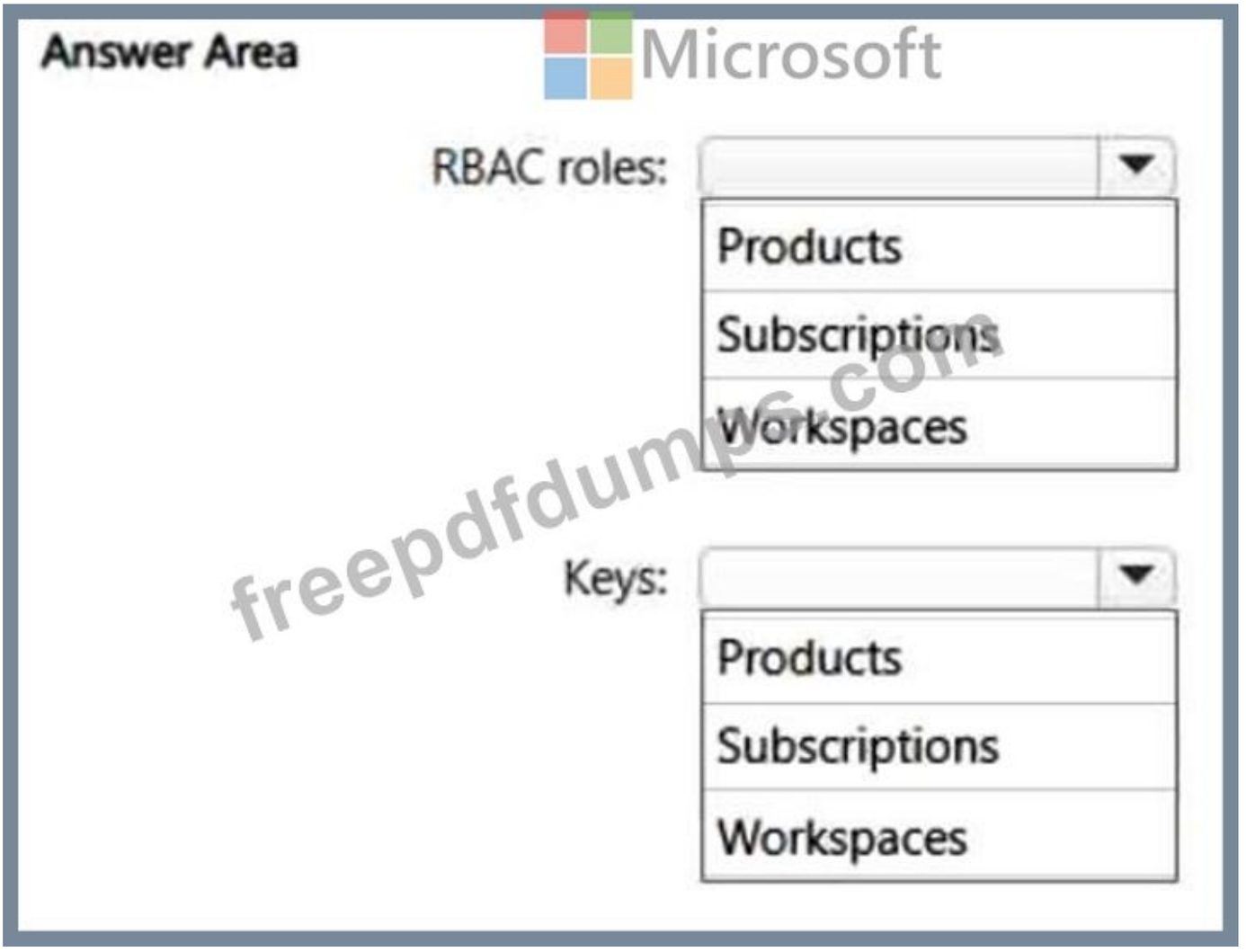
You have an Azure subscription.

You need to use a federated model in Azure API Management to control access to your organization's APIs. The solution must meet the following requirements:

- Support the use of role-based access control (RBAC) to manage the APIs.
- Support the use of keys to control the consumption of the APIs.

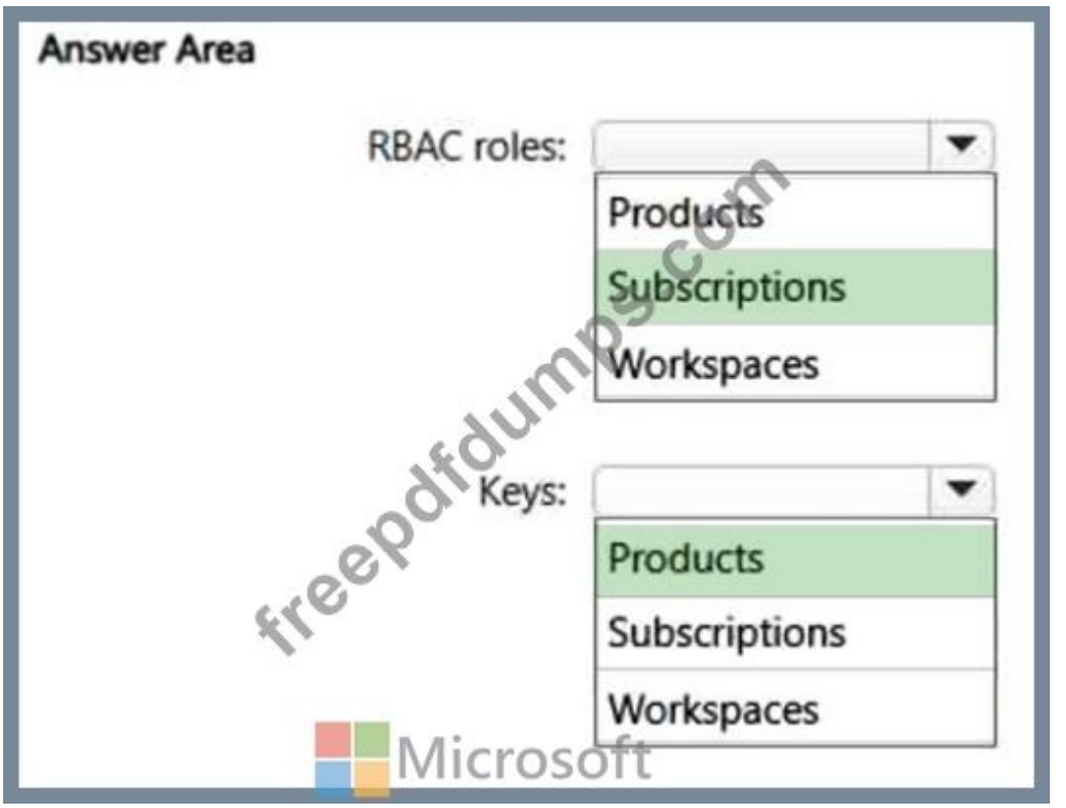
To which scope should you associate each control method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.






**Answer:**




Explanation:

Box 1: Subscriptions

In Azure API Management, RBAC can be used to manage access to APIs within a federated model by assigning roles to users or groups at different scopes (e.g., subscription, resource group, or API Management instance). This allows for granular control over who can manage or access specific APIs, enabling decentralized API development teams to manage their APIs while a central team maintains the infrastructure.

Box 2: Products

In a federated model within Azure API Management, you can control API consumption using keys by leveraging products and subscriptions. This allows teams to manage their APIs independently while still benefiting from centralized governance. Each team can define their own products, which are collections of APIs, and then manage subscriptions to those products. Consumers use subscription keys to access the APIs within the subscribed products.

Reference:

https://learn.microsoft.com/en-us/azure/api-management/api-management-key-concepts

**NEW QUESTION: 85**

Hotspot Question

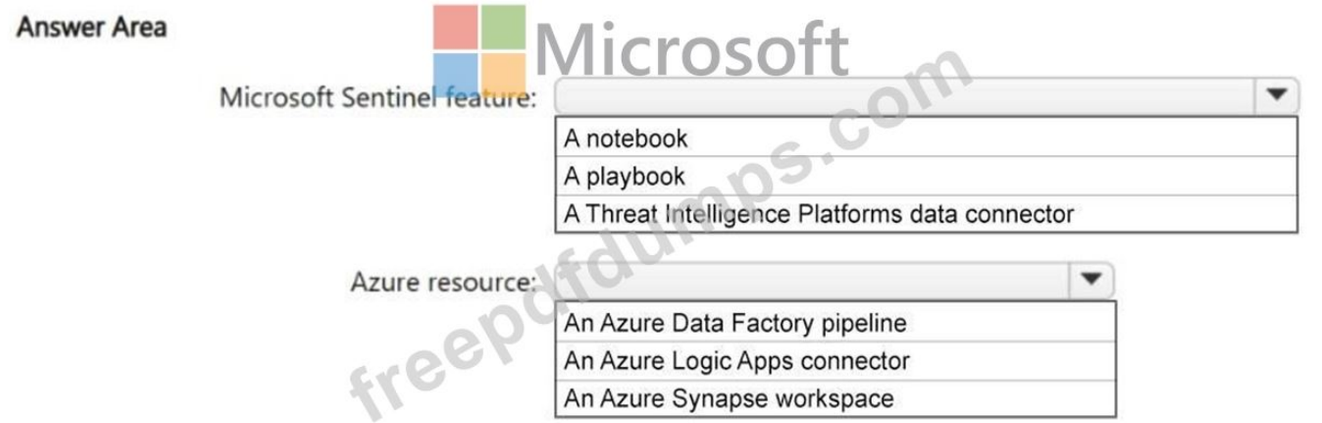
You have an Azure subscription that contains a Microsoft Sentinel workspace named MWS1 and an Azure Data Lake Storage account named lake1. Firewall log data is ingested into MWS1.

You plan to export historical firewall log data from MWS1 to lake1.

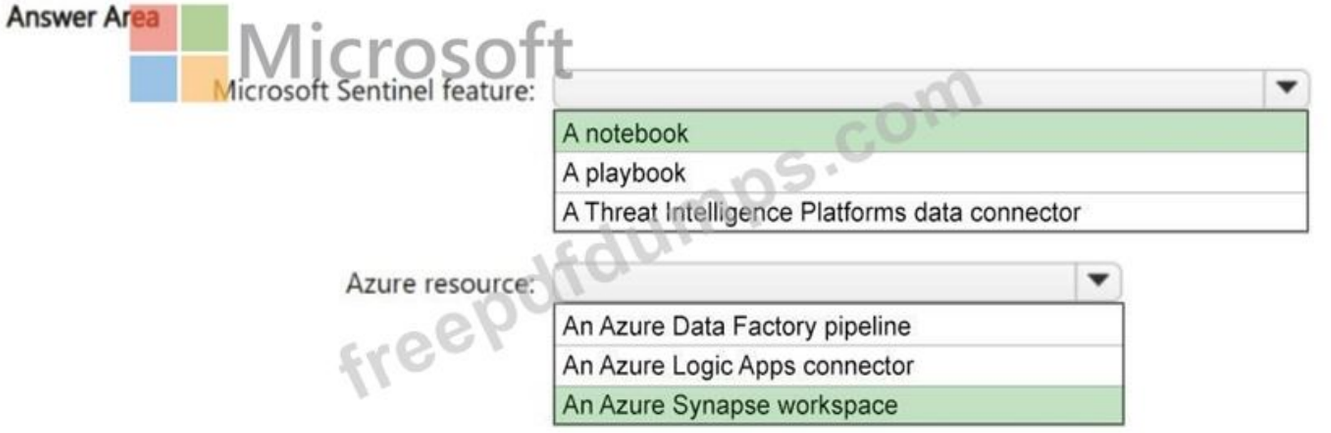
You need to ensure that security analysts can perform threat hunting from MWS1. The solution must ensure that the firewall logs stored in lake1 can be included in threat hunting queries.

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

NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:
Box 1: A notebook
To export historical firewall log data from a Microsoft Sentinel workspace to Azure Data Lake Storage (ADLS) for threat hunting, you can utilize the "Export Historical Data" notebook or a scheduled data export using Log Analytics. The notebook approach allows for more granular control over the export process, including the ability to filter and transform data before exporting it to ADLS, while the scheduled data export offers a more automated and continuous approach.
Box 2: An Azure Synapse workspace
The new historical data export notebook uses Azure Synapse to work with data at scale.
Reference:
https://techcommunity.microsoft.com/blog/microsoftsentinelblog/export-historical-log-data-from-microsoft-sentinel/3413418

**NEW QUESTION: 86**
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
**Answer: (SHOW ANSWER)**
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

**NEW QUESTION: 87**
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
**Answer: A,B (LEAVE A REPLY)**
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 user flows or custom policies.

**NEW QUESTION: 88**
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.

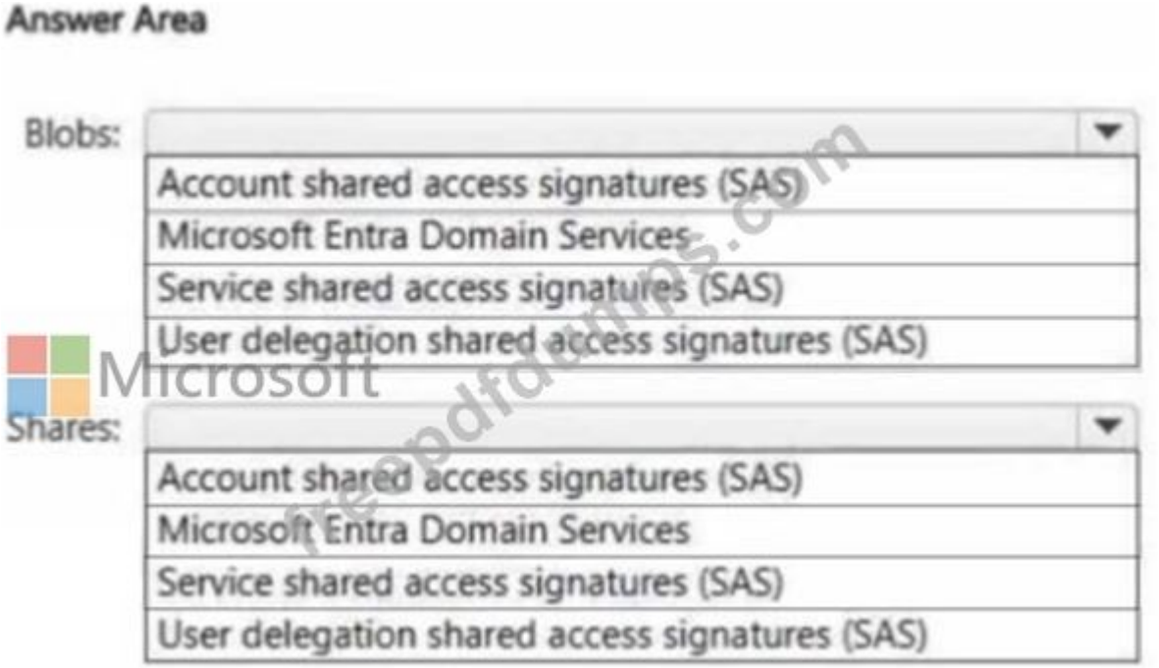
You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.
What should you include in the recommendation?
**A.** custom roles in Azure Pipelines
**B.** branch policies in Azure Repos
**C.** Azure policies
**D.** custom Azure roles
**Answer: B (LEAVE A REPLY)**
Securing Azure Pipelines
YAML pipelines offer the best security for your Azure Pipelines. In contrast to classic build and release pipelines, YAML pipelines:
* Can be code reviewed. YAML pipelines are no different from any other piece of code. You can prevent malicious actors from introducing malicious steps in your pipelines by enforcing the use of Pull Requests to merge changes. Branch policies make it easy for you to set this up.
* Etc.
Reference:
https://learn.microsoft.com/en-us/azure/devops/pipelines/security/overview

**NEW QUESTION: 89**
You have an Azure subscription. The subscription contains 100 virtual machines that run Windows Server. The virtual machines are managed by using Azure Policy and Microsoft Defender for Servers.
You need to enhance security on the virtual machines. The solution must meet the following requirements:
- Ensure that only apps on an allowlist can be run.
- Require administrators to confirm each app added to the allowlist.
- Automatically add unauthorized apps to a blocklist when an attempt is made to launch the app.
- Require administrators to approve an app before the app can be moved
from the blocklist to the allowlist.
What should you include in the solution?
**A.** a compute policy in Azure Policy
**B.** app governance in Microsoft Defender for Cloud Apps
**C.** admin consent settings for enterprise applications in Microsoft Entra ID
**D.** adaptive application controls in Defender for Servers
**Answer: D (LEAVE A REPLY)**
Microsoft Defenders for Cloud's adaptive application controls enhance your security with this data-driven, intelligent automated solution that defines allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes.

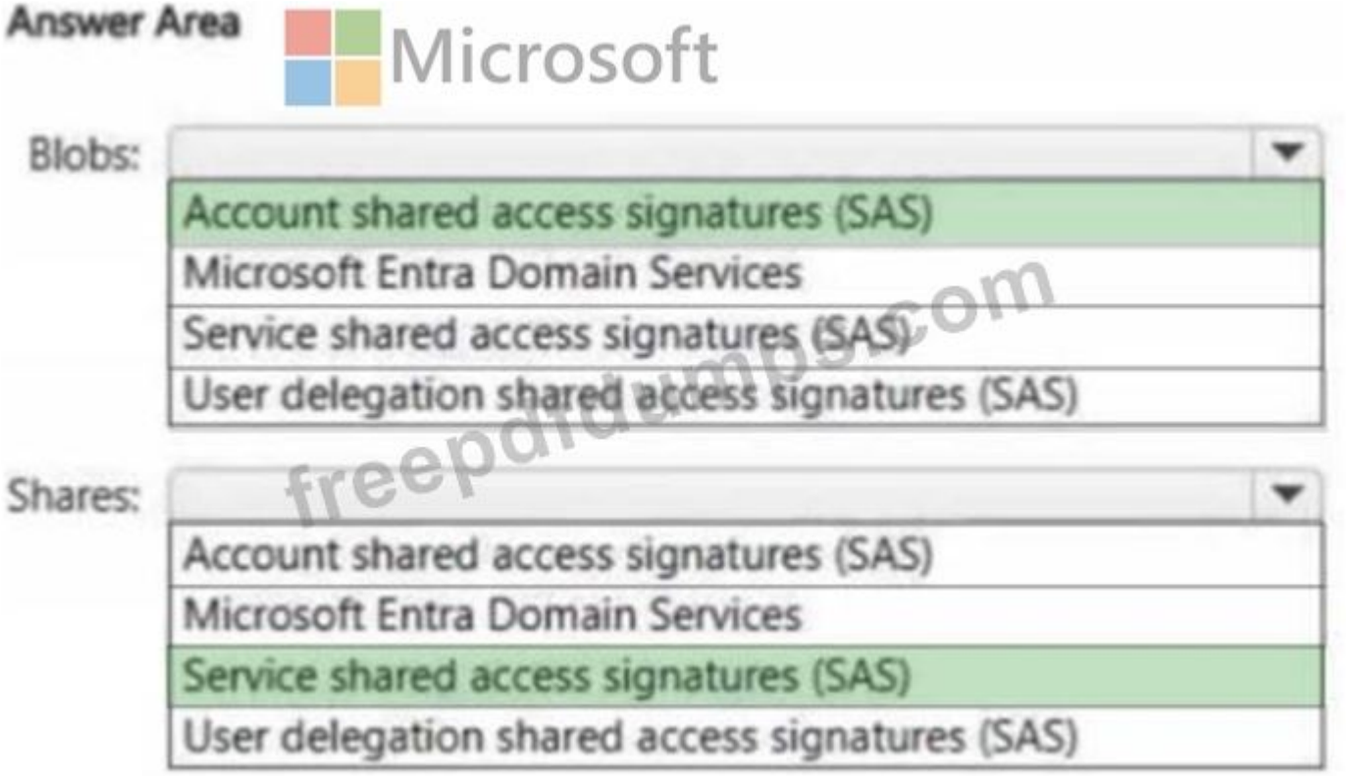
Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations.
Note: Defender for Cloud needs at least two weeks of data to define the unique recommendations per group of machines. Machines that have recently been created, or which belong to subscriptions that were only recently protected by Microsoft Defender for Servers, will appear under the No recommendation tab.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-adaptive-application-controls

**NEW QUESTION: 90**
Hotspot Question
You have an Azure subscription that contains multiple Azure Storage blobs and Azure Files shares.
You need to recommend a security solution for authorizing access to the blobs and shares. The solution must meet the following requirements:
- Support access to the shares by using the SMB protocol.
- Limit access to the blobs to specific periods of time.
- Include authentication support when possible.
What should you recommend for each resource? To answer, select the options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**




**Answer:**




Explanation:
Box 1: Account shared access signature (SAS)
Azure Storage blobs
Limit access to the blobs to specific periods of time
Account SAS
An account SAS is secured with the storage account key. An account SAS delegates access to resources in one or more of the storage services. All of the operations available via a service or user delegation SAS are also available via an account SAS.
Box 2: Service shared access signature (SAS)
Azure Files shares
Support access to the shares by using the SMB protocol.
A shared access signature can take one of the following two forms:
* Ad hoc SAS. When you create an ad hoc SAS, the start time, expiry time, and permissions are specified in the SAS URI. Any type of SAS can be an ad hoc SAS.
*-> Service SAS with stored access policy. A stored access policy is defined on a resource container, which can be a blob container, table, queue, or file share. The stored access policy can be used to manage constraints for one or more service shared access signatures. When you associate a service SAS with a stored access policy, the SAS inherits the constraints--the start time, expiry time, and permissions--defined for the stored access policy.
Reference:
https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview

**NEW QUESTION: 91**

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
**Answer: B (LEAVE A REPLY)**
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



**NEW QUESTION: 92**
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.

**Answer: (SHOW ANSWER)**

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide

**NEW QUESTION: 93**

You have a Microsoft Entra 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 Microsoft Entra Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

**Answer: (SHOW ANSWER)**

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 are performed only with applicable authorization.

Critical operations

The following table lists the operations defined as critical operations and can be protected by a Resource Guard. You can choose to exclude certain operations from being protected using the Resource Guard when associating vaults with it.

* Delete Backup Instance

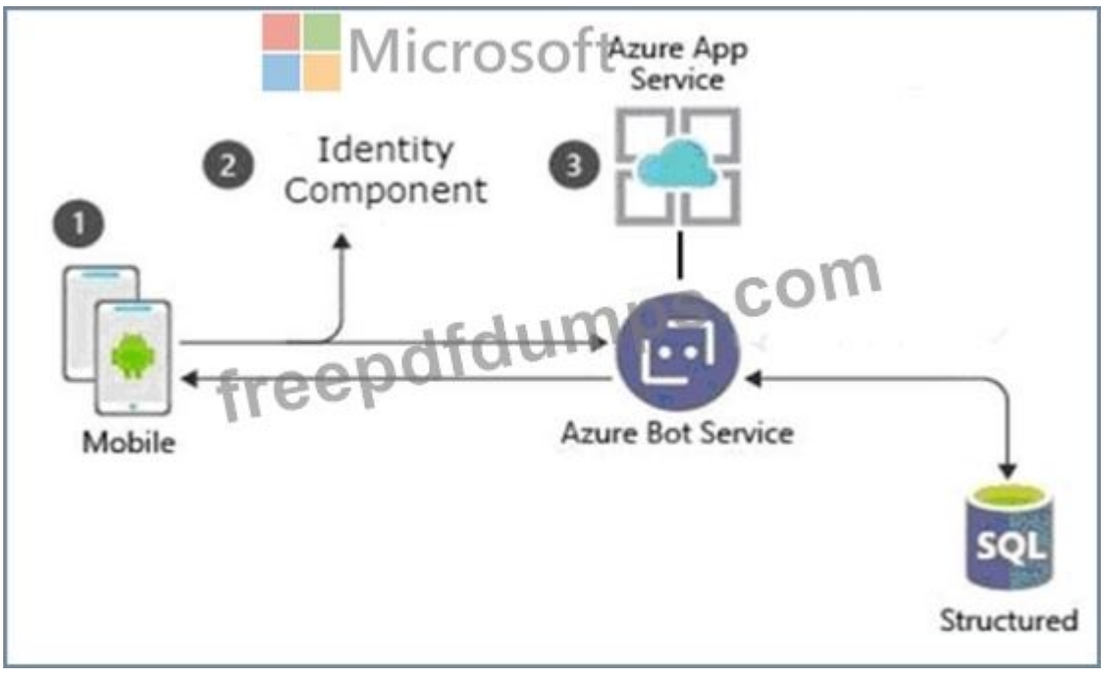
Delete protection by stopping backups and performing delete data.

Reference:

https://learn.microsoft.com/en-us/azure/backup/multi-user-authorization-concept

**NEW QUESTION: 94**

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.
- Be managed separately from the identity store of the customer.
- Support fully customizable branding for each app.

Which service should you recommend to complete the design?

**A.** Azure Active Directory (Azure AD) B2C

**B.** Azure Active Directory (Azure AD) B2B

**C.** Azure AD Connect

**D.** Azure Active Directory Domain Services (Azure AD DS)

**Answer: A (LEAVE A REPLY)**

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.

Reference:

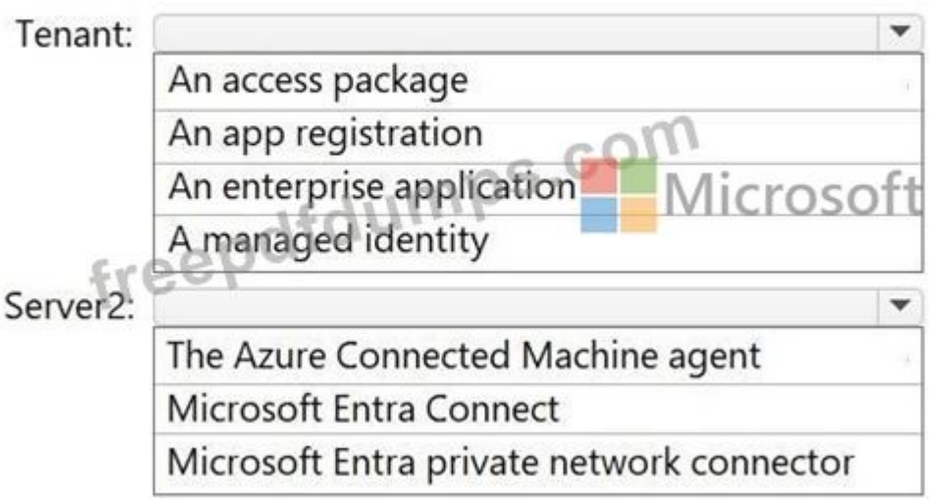
https://docs.microsoft.com/en-us/azure/active-directory-b2c/

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

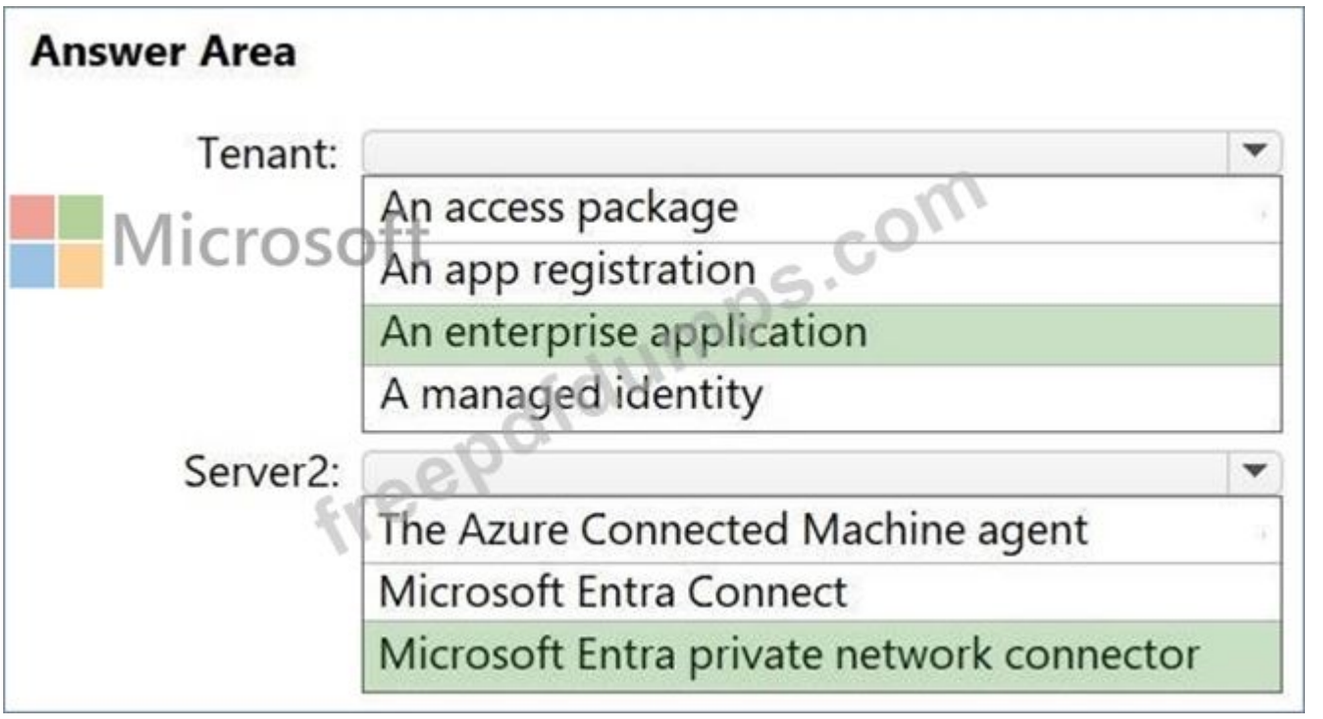
**NEW QUESTION: 95**
Hotspot Question
You have two on-premises servers named Server1 and Server2 that run Windows Server.
Server1 contains an app named App1 and is isolated from the internet.
You have a Microsoft Entra tenant.
You plan to deploy Global Secure Access to provide remote access to App1.
You need to configure the tenant and Server2 to support the planned deployment. The solution must ensure that when users attempt to access App1, they must authenticate by using their Microsoft Entra credentials.
What should you create in the tenant, and what should you install on Server2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

**Answer Area**






**Answer:**




Explanation:

Box 1: An enterprise application

Quick Access and Global Secure Access apps

When you configure the Quick Access and Global Secure Access apps, you create a new enterprise application. The app serves as a container for the private resources that you want to secure. The application has its own Microsoft Entra private network connector to broker the connection between the service and the internal resource. You can assign users and groups to the app, and then use Conditional Access policies to control access to the app.

Box 2: Microsoft Entra private network connector

Global Secure Access, How to configure private network connectors for Microsoft Entra Private Access and Microsoft Entra application proxy Connectors are lightweight agents that sit on a server in a private network and facilitate the outbound connection to the Global Secure Access service. Connectors must be installed on a Windows Server that has access to the backend resources and applications. You can organize connectors into connector groups, with each group handling traffic to specific applications.

User identities must be synchronized from an on-premises directory or created directly within your Microsoft Entra tenants. Identity synchronization allows Microsoft Entra ID to pre-authenticate users before granting them access to application proxy published applications and to have the necessary user identifier information to perform single sign-on (SSO).

Reference:

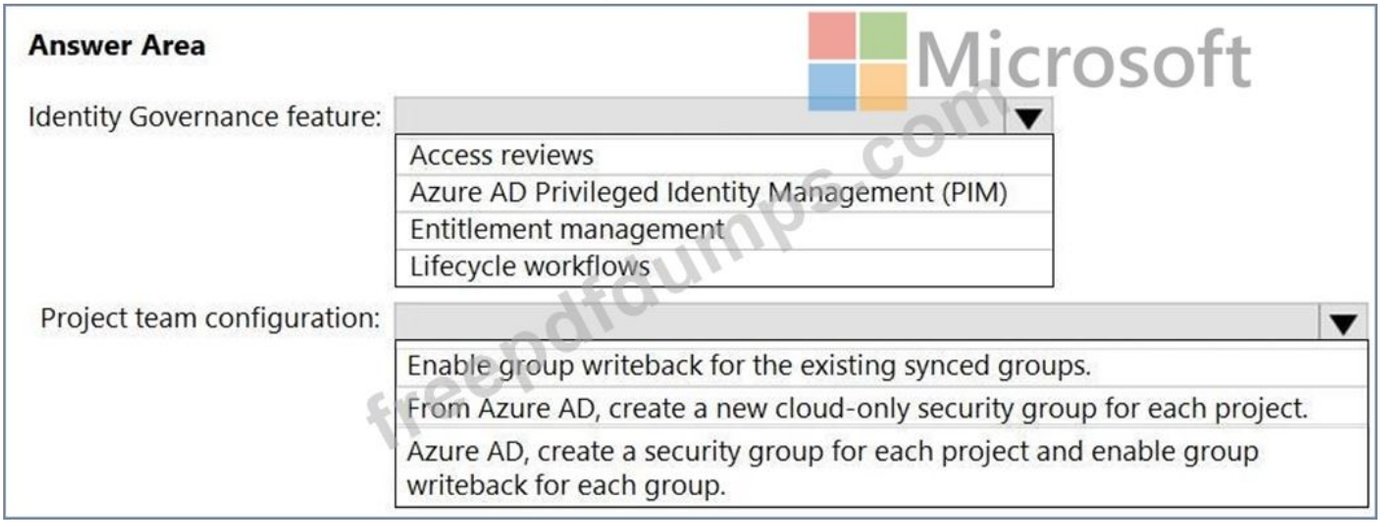
https://learn.microsoft.com/en-us/entra/global-secure-access/concept-private-access

https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors

**NEW QUESTION: 96**

Hotspot Question

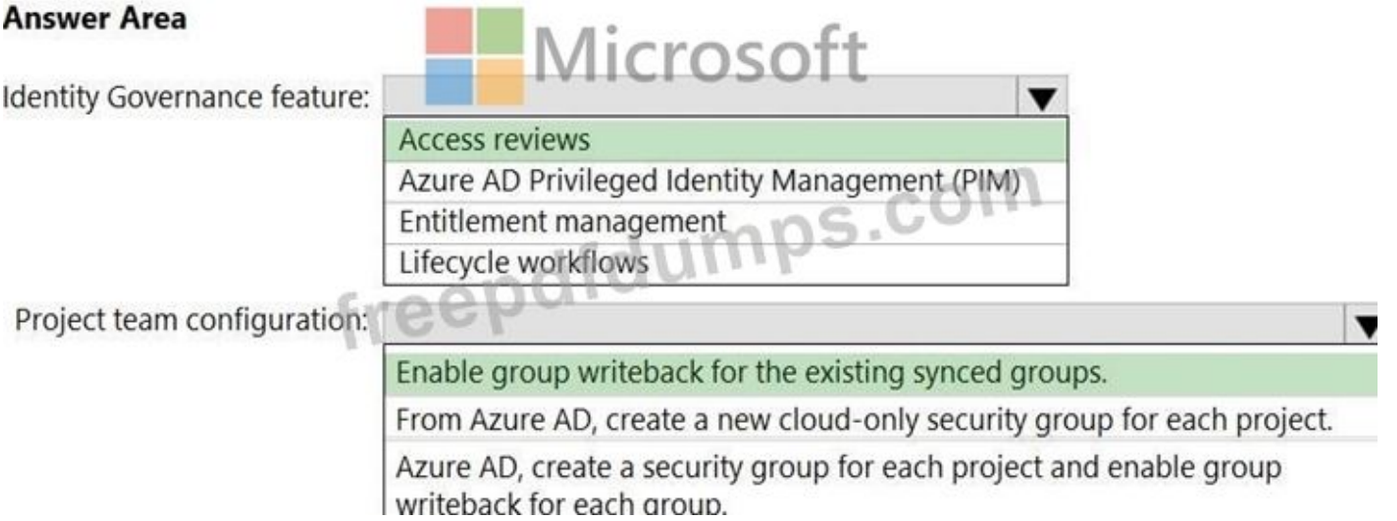
Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains a server that runs Windows Server and hosts shared folders. The domain syncs with Azure AD by using Azure AD Connect. Azure AD Connect has group writeback enabled.
You have a Microsoft 365 subscription 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.





**Answer:**

**Answer Area**



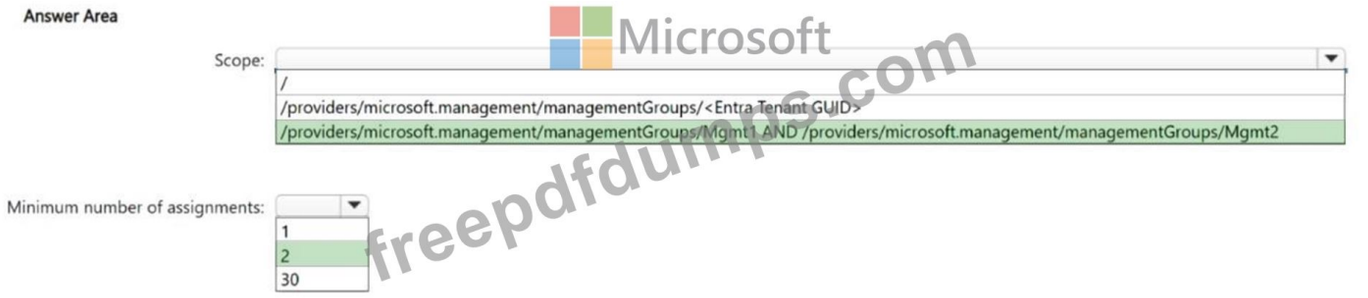

Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview.

**NEW QUESTION: 97**
Hotspot Question
You have a Microsoft Entra tenant named contoso.com. You have 30 Azure subscriptions that are linked to contoso.com. The tenant contains the management groups shown in the following table.

| Name | Description |
|---|---|
| Mgmt1 | Contains 15 subscriptions |
| Mgmt2 | Contains 15 subscriptions |

You need to design a governance solution to manage access to all the Azure Storage accounts across the subscriptions. The solution must meet the following requirements:
- Use custom role-based access control (RBAC) to provide granular
access to control plane and data plane operations.
- Minimize administrative effort.
At which scope should you assign the roles, and what is the minimum number of assignments per role? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.


**Answer:**




Explanation:

Box 1: ..Mgmt1 AND .. Mgmt2

For Microsoft Entra's two management groups, the appropriate scope for assigning roles is the management group level itself. This is because management groups are designed to be a broader scope for managing access and policies across multiple subscriptions.

Box 2: 2

Note:

Broadest Scope:

Management groups are the broadest scope in Azure, encompassing multiple subscriptions.

Reference:

https://learn.microsoft.com/en-us/azure/governance/management-groups/overview

**NEW QUESTION: 98**

Hotspot Question

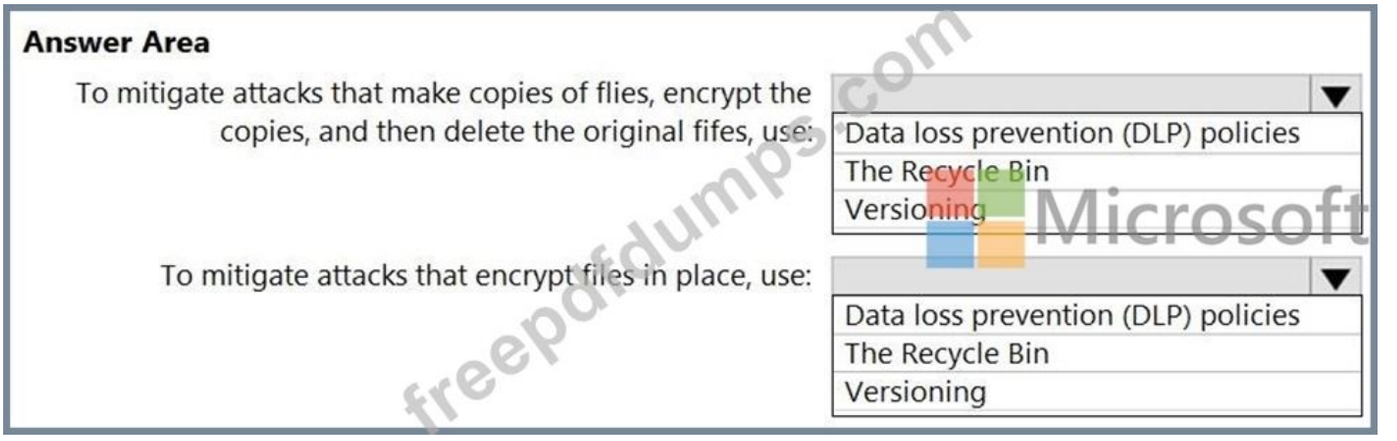
You have a Microsoft 365 E5 subscription that uses Microsoft Purview, SharePoint Online, and OneDrive for Business.

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

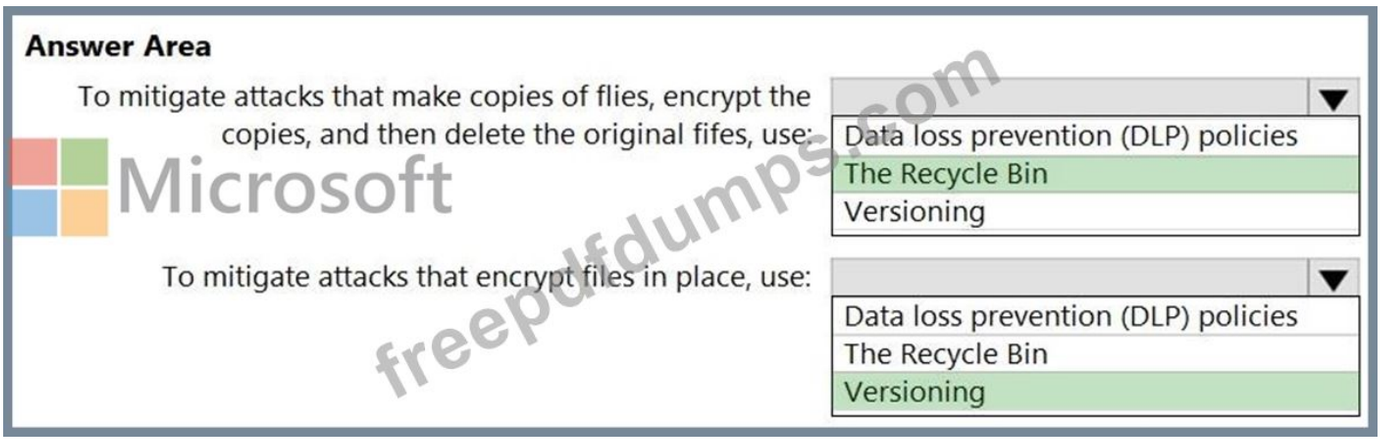
- Mitigates attacks that make copies of files, encrypt the copies, and then delete the original files
- Mitigates attacks that encrypt files in place
- Minimizes administrative effort

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:**





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

**NEW QUESTION: 99**
Your company has a main office and a branch office.
The main office contains 20 on-premises servers that run Windows Server and host apps that are published by using Microsoft Entra application proxy. The main office contains 500 on-premises computers that run Windows 11. The branch office contains 100 on-premises computers that run Windows 11.
NOT enrolled in Intune.
All the main office computers are enrolled in Microsoft Intune. The branch office computers are
You have a Microsoft 365 ES subscription.
You have a Microsoft Entra tenant. You have a third-party software as a service (SaaS) app that is registered in the Microsoft Entra tenant.
You plan to implement Global Secure Access.
You are evaluating the use of compliant network check and Conditional Access.
Which two scenarios are supported by compliant network check? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point
**A.** connections to the third-party SaaS app
**B.** connections from the branch office computers
**C.** Continuous Access Evaluation for Microsoft Exchange Online
**D.** connections to the on-premises apps
**Answer: (SHOW ANSWER)**
Global Secure Access, Enable compliant network check with Conditional Access A: Organizations who use Conditional Access along with the Global Secure Access, can prevent malicious access to Microsoft apps, third-party SaaS apps, and private line-of-business (LoB) apps using multiple conditions to provide defense-in-depth. These conditions might include device compliance, location, and more to provide protection against user identity or token theft.
Global Secure Access introduces the concept of a compliant network within Microsoft Entra ID Conditional Access. This compliant network check ensures users connect from a verified network

connectivity model for their specific tenant and are compliant with security policies enforced by administrators.
C: Compliant network check data plane enforcement (preview) with Continuous Access Evaluation is supported for SharePoint Online and Exchange Online.
Compliant network check is currently not supported for Private Access applications.
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/reference-current-known-limitations
https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-compliant-network

**NEW QUESTION: 100**
You have an Azure subscription that contains multiple network security groups (NSGs), multiple virtual machines, and an Azure Bastion host named bastion1.
Several NSGs contain rules that allow direct RDP access to the virtual machines by bypassing bastion1.
You need to ensure that the virtual machines can be accessed only by using bastion1. The solution must prevent the use of NSG rules to bypass bastion1.
What should you include in the solution?
**A.** Azure Virtual Network Manager security admin rules
**B.** Azure Virtual Network Manager connectivity configurations
**C.** Azure Firewall application rules
**D.** Azure Firewall network rules
**Answer: (SHOW ANSWER)**
How security admin rules and network security groups (NSGs) are evaluated Security admin rules and network security groups (NSGs) can be used to enforce network security policies in Azure. However, they have different scopes and priorities.# Security admin rules are intended to be used by network admins of a central governance team, thereby delegating NSG rules to individual application or service teams to further specify security as needed. Security admin rules have a higher priority than NSGs and are evaluated before NSG rules.
NSGs, on the other hand, are used to filter network traffic to and from individual subnets or network interfaces. They're intended to be used by individual application or service teams to further specify security as needed. NSGs have a lower priority than security admin rules and are evaluated after security admin rules.
Security admin rules are currently applied at the virtual network level, whereas network security groups can be associated at the subnet and NIC level.
This table shows these differences and similarities:

| Rule Type | Target Audience | Applied On | Evaluation Order | Action Types | Parameters |
|---|---|---|---|---|---|
| Security admin rules | Network admins, central governance team | Virtual networks | Higher priority | Allow, Deny, Always Allow | Priority, protocol, action, source, destination |
| Network security group rules | Individual teams | Subnets, NICs | Lower priority, after security admin rules | Allow, Deny | Priority, protocol, action, source, destination |

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network-manager/concept-security-admins

**NEW QUESTION: 101**
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.** Enable Microsoft Defender for Cosmos DB.
**B.** Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.
**C.** Disable local authentication for Azure Cosmos DB.
**D.** Enable Microsoft Defender for Identity.
**E.** Send the Azure Cosmos DB logs to a Log Analytics workspace.
**Answer: B,C (LEAVE A REPLY)**
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.
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.
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

**NEW QUESTION: 102**
Your network contains an Active Directory Domain Services (AD DS) domain named Domain1.
You have a Microsoft Entra tenant.
Domain1 syncs with the tenant by using Microsoft Entra Connect.

You need to monitor Domain1 for privilege escalation attacks.
What should you use?
**A.** Microsoft Entra ID Protection
**B.** Microsoft Defender for Servers
**C.** Microsoft Defender for Identity
**D.** Privileged Identity Management (PIM)
**Answer: C (LEAVE A REPLY)**
Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization.
Note: Detecting and preventing privilege escalation attacks leveraging Kerberos relaying (KrbRelayUp) Microsoft Defender for Identity detects activity from the early stages of the attack chain by monitoring anomalous behavior as seen by the domain controller.
Reference:
https://learn.microsoft.com/en-us/defender-for-identity/what-is
https://www.microsoft.com/en-us/security/blog/2022/05/25/detecting-and-preventing-privilege-escalation-attacks-leveraging-kerberos-relaying- krbrelayup/

**NEW QUESTION: 103**
Hotspot Question
You have a Microsoft Entra tenant that is linked to a Microsoft 365 subscription and an Azure subscription. The tenant contains service principals that are used to access applications in the Azure subscription.
You need to recommend a solution to detect risky sign-ins and other risky activities performed by the service principals in the tenant. The solution must minimize costs.
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:**


Explanation:

Box 1: Microsoft Entra ID Protection

Service

Microsoft Entra ID Protection, Investigate risk

Microsoft Entra ID Protection provides organizations with reporting they can use to investigate identity risks in their environment. These reports includerisky users,risky sign-ins,risky workload identities, andrisk detections.

Box 2: Microsoft Entra ID P2

License type

Microsoft Entra ID and Microsoft Entra Suite


Reference:
https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk
https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing

**NEW QUESTION: 104**
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
**Answer: A (LEAVE A REPLY)**
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

**NEW QUESTION: 105**
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 Storage Analytics
**B.** Azure Network Watcher
**C.** Microsoft Sentinel
**D.** Azure Policy
**Answer: (SHOW ANSWER)**
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

**NEW QUESTION: 106**

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 attach surface.
What should you include in the recommendation?
**A.** Azure Firewall Premium
**B.** Azure Application Gateway Web Application Firewall (WAF)
**C.** network security groups (NSGs)
**D.** Azure Traffic Manager and application security groups
**Answer: B (LEAVE A REPLY)**
Roughly 20% of all Internet traffic comes from bad bots. They do things like scraping, scanning, and looking for vulnerabilities in your web application. When these bots are stopped at the Web Application Firewall (WAF), they can't attack you. They also can't use up your resources and services, such as your backends and other underlying infrastructure.
You can enable a managed bot protection rule set for your WAF to block or log requests from known malicious IP addresses. The IP addresses are sourced from the Microsoft Threat Intelligence feed. Intelligent Security Graph powers Microsoft threat intelligence and is used by multiple services including Microsoft Defender for Cloud.
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection-overview



**NEW QUESTION: 107**
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the 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 configurations 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 configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

**A.** Configure Azure Active Directory (Azure AD) Conditional Access policies.

**B.** Create a custom collector that uses the Log Analytics agent.

**C.** Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.

**D.** Use the Azure Monitor agent with the multi-homing configuration.

**Answer: (SHOW ANSWER)**

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.

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.

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

**NEW QUESTION: 108**

Hotspot Question

You have an Azure subscription that contains three Azure App Service web apps.

You need to secure the apps by using Azure Web Application Firewall (WAF) on Azure Front Door. The solution must meet the following requirements:

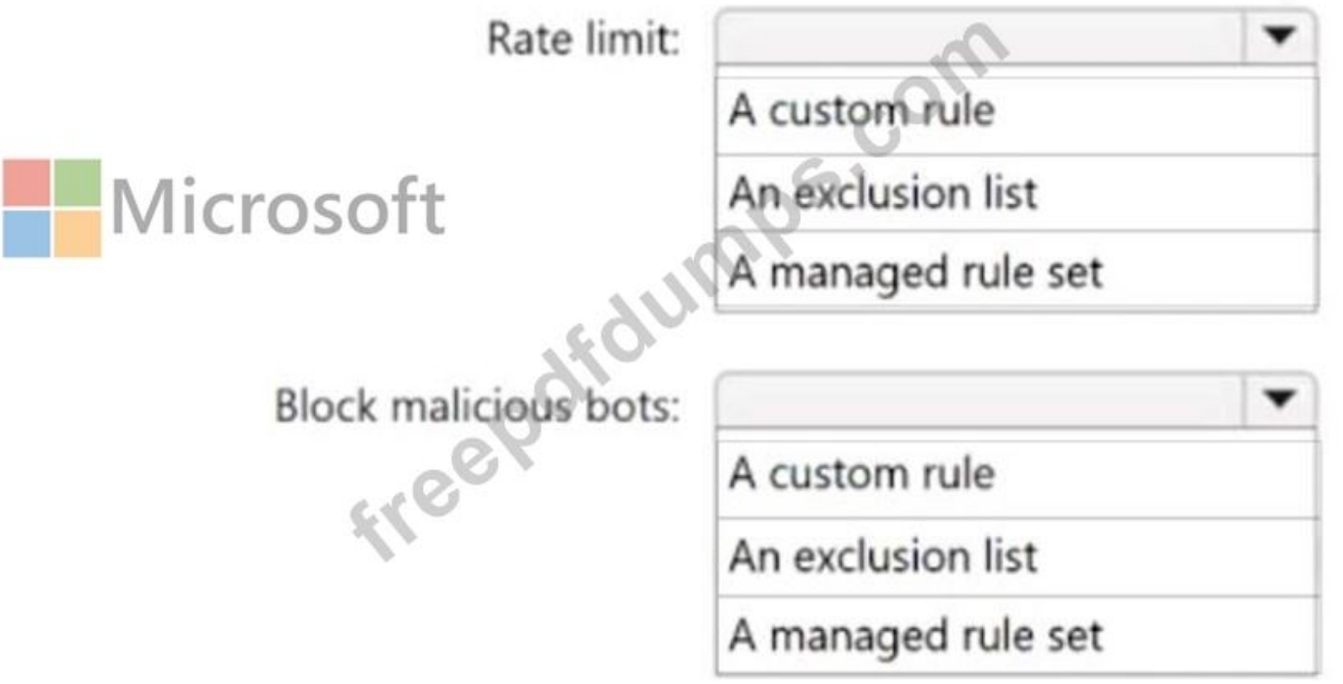
- Block attempts to access the apps from malicious bots.
- Rate limit incoming connections to the apps.

The solution must minimize administrative effort.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

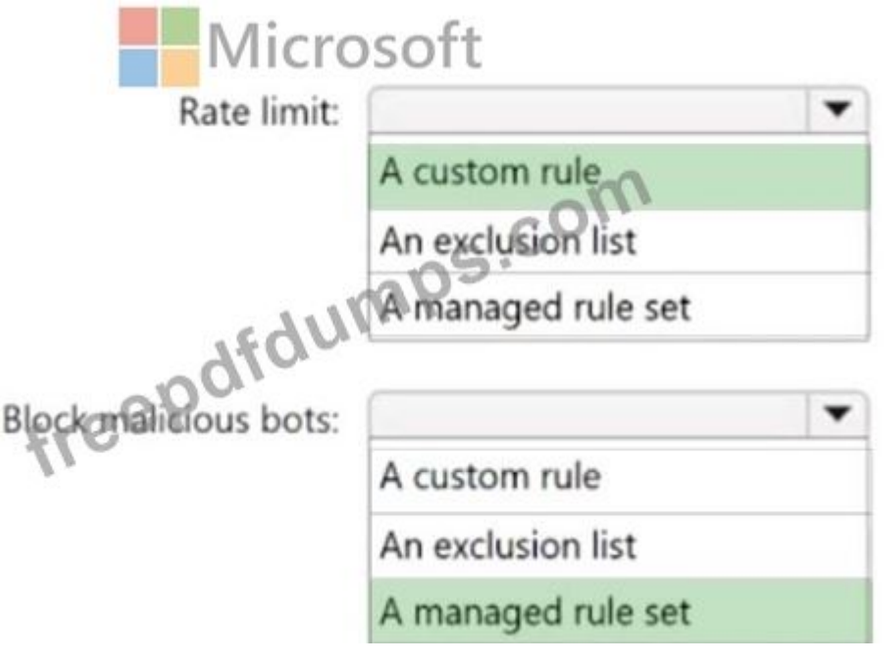
NOTE: Each correct selection is worth one point.

Answer Area




**Answer:**

Answer Area




Explanation:

Box 1: A custom rule

To rate limit incoming connections to Azure App Services using Azure Web Application Firewall (WAF) with Azure Front Door, you need to configure a custom WAF rule within your Front Door WAF policy. This rule will specify a rate limit threshold and a match condition that determines when the rate limiting should be applied.

Box 2: A managed rule set

Block attempts to access the apps from malicious bots.

To block malicious bots with Azure Web Application Firewall (WAF) on Azure Front Door and Azure App Service, you can enable bot protection rules within the WAF policy. Specifically, you'll want to enable the Bot Manager rule set, which helps identify and manage bot traffic, distinguishing between good bots and malicious ones.
Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

**NEW QUESTION: 109**
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.
Which Microsoft Purview feature should you include in the recommendation?
**A.** content explorer
**B.** data loss prevention (DLP)
**C.** eDiscovery
**D.** data lifecycle management
**Answer: B (LEAVE A REPLY)**
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.
For this question the incorrect answers include:
* 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.
* data classification 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.
* data lifecycle management
* eDiscovery
* Information Governance
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

**NEW QUESTION: 110**

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft 365 subscription that uses Microsoft Defender XDR. The subscription contains 500 devices that are enrolled in Microsoft Intune. The subscription contains 500 users that connect to external software as a service (SaaS) apps by using the devices.
You need to implement a solution that meets the following requirements:
- Allows user access to SaaS apps that Microsoft has identified as low
risk
- Blocks user access to Saas apps that Microsoft has identified as high risk Solution: From Microsoft Defender for Cloud Apps, you configure SaaS security posture management (SSPM) and create an access policy.
Does this meet the goal?
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
To allow access to only low-risk external SaaS apps in a Microsoft 365 environment with Defender XDR and Intune, you can use Microsoft Entra Conditional Access policies. These policies can leverage Learn Microsoft's Defender for Endpoint data to restrict access based on device compliance and threat level. Specifically, you can create policies that require a device to be compliant or have an app protection policy applied before allowing access to specific SaaS apps.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/posture-overview
https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

**NEW QUESTION: 111**
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
**Answer: B (LEAVE A REPLY)**

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

**NEW QUESTION: 112**
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.** adaptive application controls in Defender for Cloud
**C.** Azure Security Benchmark compliance controls in Defender for Cloud
**D.** app protection policies in Microsoft Endpoint Manager
**Answer: (SHOW ANSWER)**
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.
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

**NEW QUESTION: 113**
You are an Azure solution architect; your organization has an on-premises Microsoft SQL server. You recently deployed an Azure App Service with a web app; the web app is required to securely connect to the Microsoft SQL Server in your on-premises environment.
The intention is to establish an ExpressRoute to connect to Azure in the future, but as it stands today, there is no direct connection to Azure.
The development team is inquiring if there is a secure way to connect the Microsoft SQL Server to the Azure App Service for testing purposes without needing the ExpressRoute connection.

What would be the recommended solution

**A.** Virtual network NAT gateway integration

**B.** Hybrid connections

**C.** Virtual network integration

**D.** A private endpoint

**Answer: B (LEAVE A REPLY)**

Option A is incorrect because virtual network NAT gateway integration outbound Internet connectivity; in this scenario, we would need an inbound connection.

Option B is correct, as hybrid connections can be created directly in Azure app services to connect to your on-premises resources. It uses static TCP ports.

Option C is incorrect because You can set up a vnet integration with Azure vnet or an on-premise network, but you would need a site-to-site VPN, which is unavailable.

Option D is incorrect because a private endpoint provides connections to Azure services, not on-premises resources.

Reference:

https://docs.microsoft.com/en-us/answers/questions/701793/connecting-to-azure-app-to-onprem-datbase.html

**NEW QUESTION: 114**

Drag and Drop Question

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1.

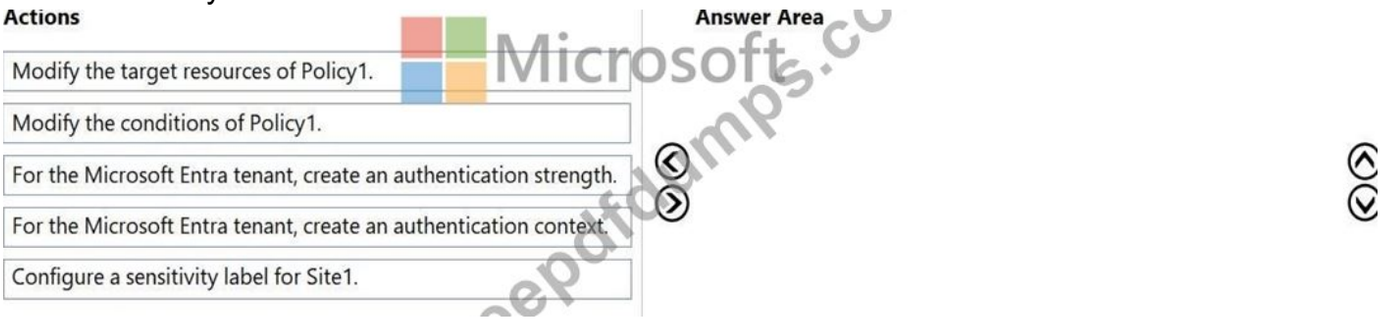
You have a Conditional Access policy named Policy1 that only allows workload identities from trusted locations to access SharePoint Online.

You plan to move all business-sensitive information to Site1.

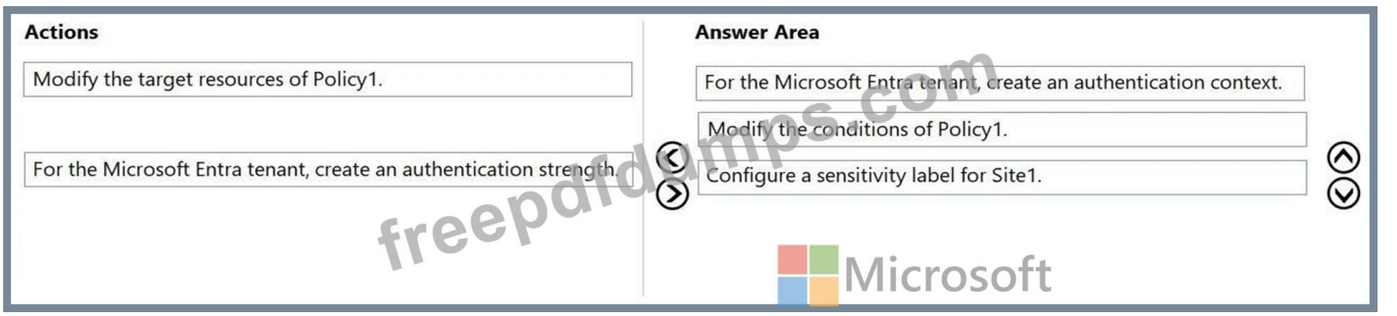
You need to ensure that CAPolicy1 applies to Site1 only.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.




**Answer:**



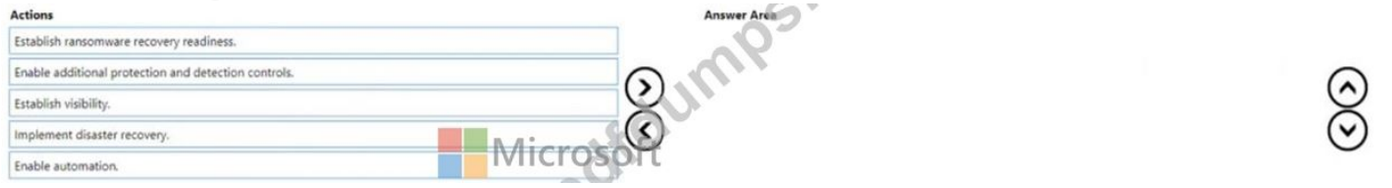


Explanation:
Reference:
https://learn.microsoft.com/en-us/sharepoint/authentication-context-example

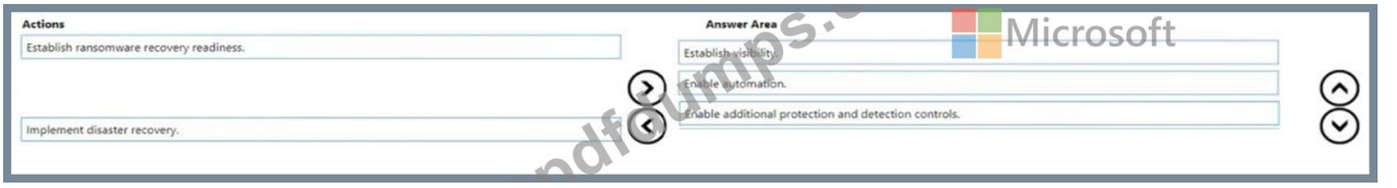
**NEW QUESTION: 115**
You have a Microsoft Entra tenant named contoso.com and use Microsoft Intune. Each user in contoso.com has a Microsoft Entra ID P1 license and a Windows 11 device that has the Global Secure Access client deployed.
You plan to deploy the following configuration of Microsoft Entra Internet Access:
- Enable a baseline profile.
- Create a security profile named Profile1 that has a priority of 300
and contains a single web content filtering policy named
WCFPolicy1.Configure WCFPolicy1 as follows:
- Set Action to allow.
- Include a single rule that has a fully qualified domain name (FQDN)
destination of *.adatum.com. Link Profile1 to a Conditional Access
policy named CAPolicy1, apply CAPolicy1 to all users, and grant access
unless a user's device is noncompliant.
You need to evaluate the impact of the planned deployment on traffic to the following resources:
- https://www.adatum.com:8433
- https://www.fabrikam.com
Which two traffic scenarios will occur? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
**A.** Traffic to https://www.fabrikam.com will be allowed from all the devices.
**B.** Traffic to https://www.adatum.com:8433 will be blocked from all the devices.
**C.** Traffic to https://www.adatum.com:8433 will be allowed from all the devices.
**D.** Traffic to https://www.fabrikam.com will be allowed from compliant devices only.
**E.** Traffic to https://www.adatum.com:8433 will be allowed from compliant devices only.
**F.** Traffic to https://www.fabrikam.com will be blocked from noncompliant devices only.
**Answer: B,D (LEAVE A REPLY)**
Traffic to https://www.adatum.com:8433:
In WCFPolicy1, the only rule specifies *.adatum.com as the allowed domain but without specifying a particular port.
Typically, web content filtering applies only to standard HTTP/HTTPS traffic (ports 80 and 443).

Since this traffic is over port 8433, which is nonstandard, it would not match the allow rule in WCFPolicy1. Thus, it will be blocked from all devices.
Traffic to https://www.fabrikam.com:
Since there is no rule in WCFPolicy1 to specifically allow or block traffic to fabrikam.com, the Conditional Access policy CAPolicy1 will govern access.
CAPolicy1 is configured to grant access only if a user's device is compliant. Therefore, traffic to https://www.fabrikam.com will be allowed only from compliant devices

**NEW QUESTION: 116**
Drag and Drop Question
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.




**Answer:**




**NEW QUESTION: 117**
You have a Microsoft 365 subscription and an Azure subscription. Microsoft Defender XDR 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 the Microsoft Entra tenant
**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
**Answer: D (LEAVE A REPLY)**

Microsoft Defender for Endpoint includes application control policies that allow you to define which applications are authorized to run on a machine.
This can help block any unauthorized applications and provide an approval mechanism, ensuring that only approved software is allowed to run.
The solution aligns with the requirement to block unauthorized applications from running on the virtual machines automatically until approved by an administrator.

**NEW QUESTION: 118**
You are a cloud security administrator, and you have been tasked with providing a security solution for an Azure App Service, a web app named web-App0. Web-App0 has the following requirements:
Users will request access to web-App0 through the organization portal, and an internal stakeholder will approve.
Authentication for users must be provided by Azure AD.
What would be your recommended approach to enable AD authentication to web-app0?
**A.** Azure AD application
**B.** Azure AD application proxy
**C.** Microsoft Defender for 365
**D.** Application Gateway
**Answer: A (LEAVE A REPLY)**
Option A is correct because you can use application management in Azure AD, which is a process of creating and configuring applications in the cloud; when an application is registered in a Azure AD tenant, you can assign users to access the application securely.
Option B is incorrect because Azure AD Application Proxy provides secure remote access to on-premises web applications; this is not part of the objective.
Option C is incorrect because Microsoft Defender for Office 365 protects your organization against malicious risks posed by email messages, links (URLs), and collaboration tools; the objective of your task is to provide access using Azure AD.
Option D is incorrect because Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications, the function of this solution is not required.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management

**NEW QUESTION: 119**
Hotspot Question
Your network contains an Active Directory Domain Services (AD DS) domain named Domain1.
You have a Microsoft Entra tenant.
Domain1 syncs with the tenant by using Microsoft Entra Connect.

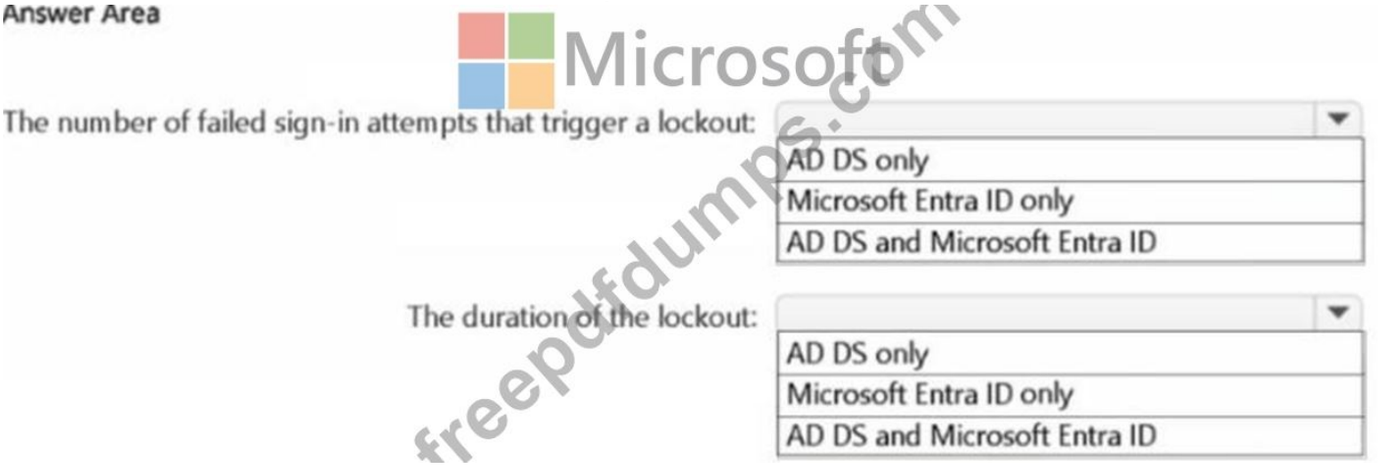
You need to evaluate Microsoft Entra smart lockout by testing the following account lockout considerations:

- The number of failed sign-in attempts that trigger a lockout
- The duration of the lockout

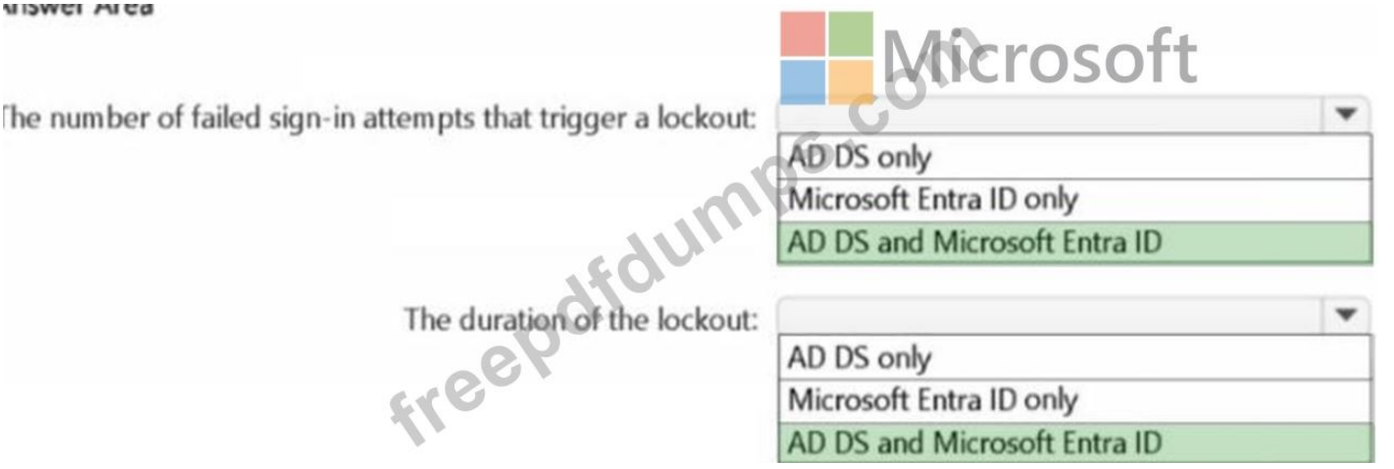
What should you use to test each consideration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area




**Answer:**




Explanation:

Box 1: AD DS and Microsoft Entra ID

The number of failed sign-in attempts that trigger a 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. By setting smart lockout policies in Microsoft Entra ID appropriately, attacks can be filtered out before they reach on-premises AD DS.

When using pass-through authentication, the following considerations apply:

* The Microsoft Entra lockout threshold must be less than the AD DS account lockout threshold. Set the values so that the AD DS account lockout threshold is at least two or three times greater than the Microsoft Entra lockout threshold.
* The Microsoft Entra lockout duration must be longer than the AD DS account lockout duration. The Microsoft Entra duration is set in seconds, while the AD DS duration is set in minutes.

Tip
This configuration ensures Microsoft Entra smart lockout stops your on-premises AD DS accounts from being locked out by brute force attacks, like password spray attacks on your Microsoft Entra accounts.
Box 2: AD DS and Microsoft Entra ID
The duration of the lockout.
Reference:
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout

**NEW QUESTION: 120**
Your company has a main office and 10 branch offices. Each branch office contains an on-premises file server that runs Windows Server and multiple devices that run either Windows 11 or macOS. The devices are enrolled in Microsoft Intune.
You have a Microsoft Entra tenant.
You need to deploy Global Secure Access to implement web filtering for device traffic to the internet. The solution must ensure that all the web traffic from the devices in the branch offices is controlled by using Global Secure Access.
What should you do first in each branch office?
**A.** Configure an Intune policy to onboard Microsoft Defender for Endpoint to each device.
**B.** Configure an IPsec tunnel on the router.
**C.** Install the Microsoft Entra private network connector on the file server.
**D.** Configure an Intune policy to deploy the Global Secure Access client to each device.
**Answer: C (LEAVE A REPLY)**
Configure private network connectors for Microsoft Entra Private Access and Microsoft Entra application proxy Connectors are lightweight agents that sit on a server in a private network and facilitate the outbound connection to the Global Secure Access service.
Connectors must be installed on a Windows Server that has access to the backend resources and applications. You can organize connectors into connector groups, with each group handling traffic to specific applications.
Reference:
https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors

**NEW QUESTION: 121**
You have 50 Azure subscriptions.
You need to monitor 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.
NOTE: Each correct selection is worth one point.
**A.** Assign an initiative to a management group.
**B.** Assign a blueprint to each subscription.

**C.** Assign a policy to each subscription.
**D.** Assign a blueprint to a management group.
**E.** Assign an initiative to each subscription.
**F.** Assign a policy to a management group.
**Answer: A,D (LEAVE A REPLY)**
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.
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.
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.
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

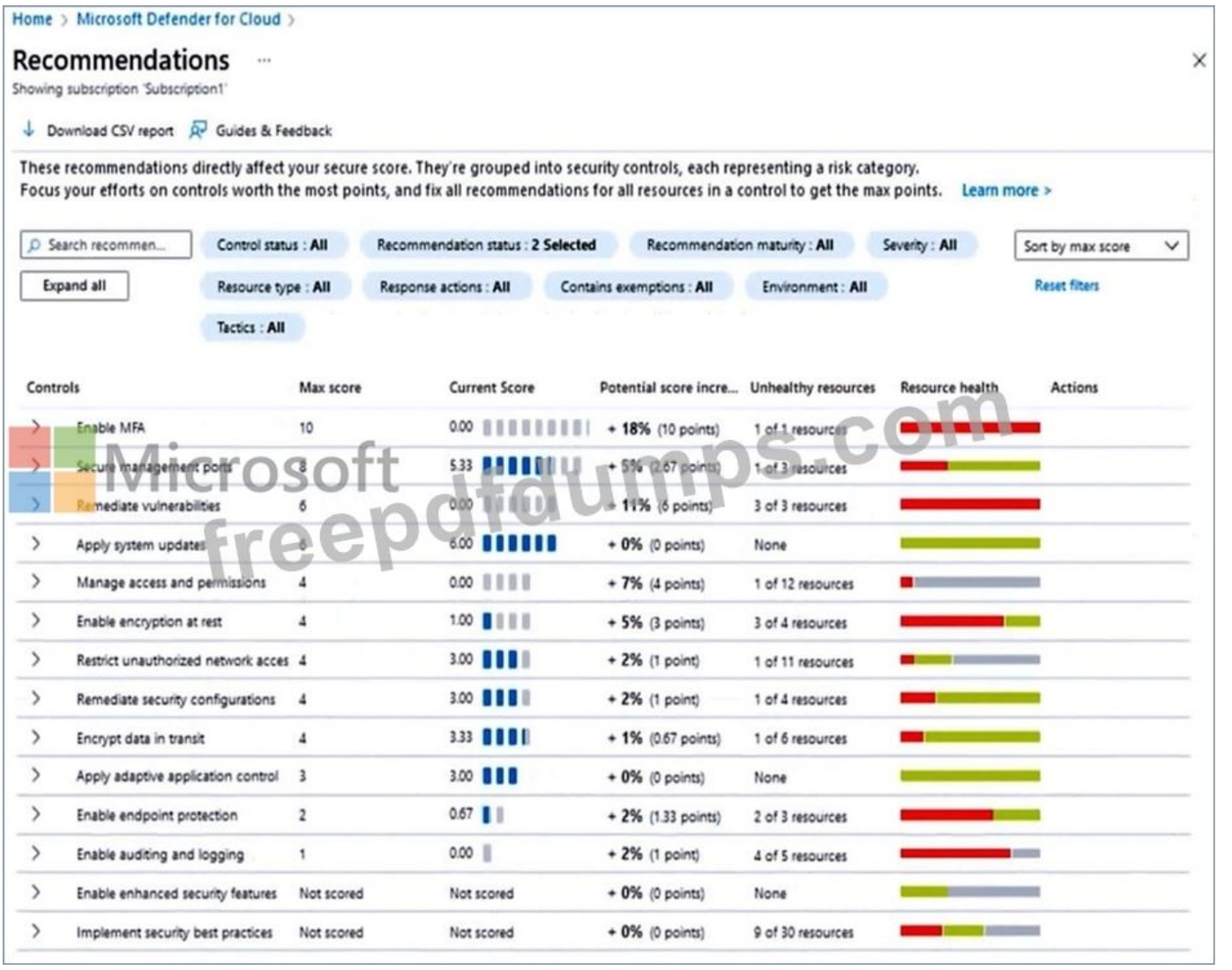
**NEW QUESTION: 122**
Your company is exploring migrating data into Azure; they would like to have a central authentication solution when accessing the data; they have chosen Azure Active Directory.
Which two storage types natively support Active Directory authentication?
**A.** Azure Data Box
**B.** Azure Data Lake Storage Gen2
**C.** Azure File Share
**D.** Azure Storage blob containers
**Answer: B,D (LEAVE A REPLY)**
Option D is correct Because Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data.
Option B is correct Because Azure Data Lake Storage Gen2 (ADLS Gen2) accounts support using OAuth 2.0 with an Azure Active Directory (Azure AD).
Option C is incorrect because To support AD DS authentication over SMB for Azure File Share; you need to register your storage account with AD DS.
Option A is incorrect because Azure Data Box is a device used to move large amounts of data to Azure; this process is known as seeding.
References:
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

**NEW QUESTION: 123**
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and hunt for potential threats across all deployed services.
You need to recommend a solution for the customer.
The solution must minimize costs.
What should you include in the recommendation?
**A.** Microsoft 365 Defender
**B.** Microsoft Defender for Cloud
**C.** Microsoft Defender for Cloud Apps
**D.** Microsoft Sentinel
**Answer: D (LEAVE A REPLY)**
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

**NEW QUESTION: 124**
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 Microsoft Entra credentials.
You need to recommend a solution to enable users to authenticate to App1 by using their Microsoft Entra credentials.
What should you include in the recommendation?
**A.** a relying party trust in Active Directory Federation Services (AD FS)
**B.** a Microsoft Entra enterprise application
**C.** Microsoft Entra Application Proxy
**D.** Microsoft Entra External ID
**Answer: B (LEAVE A REPLY)**
Note: Users in Microsoft 365 can use their Microsoft Entra credentials to authenticate to third-party SaaS applications through the Microsoft Entra enterprise application feature. This is achieved by configuring the SaaS application to use Microsoft Entra ID as its identity provider and enabling single sign-on (SSO).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/integrated-apps-and-azure-ads

**NEW QUESTION: 125**
Hotspot Question
You open Microsoft Defender for Cloud as shown in the following exhibit.




Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

**Answer Area**

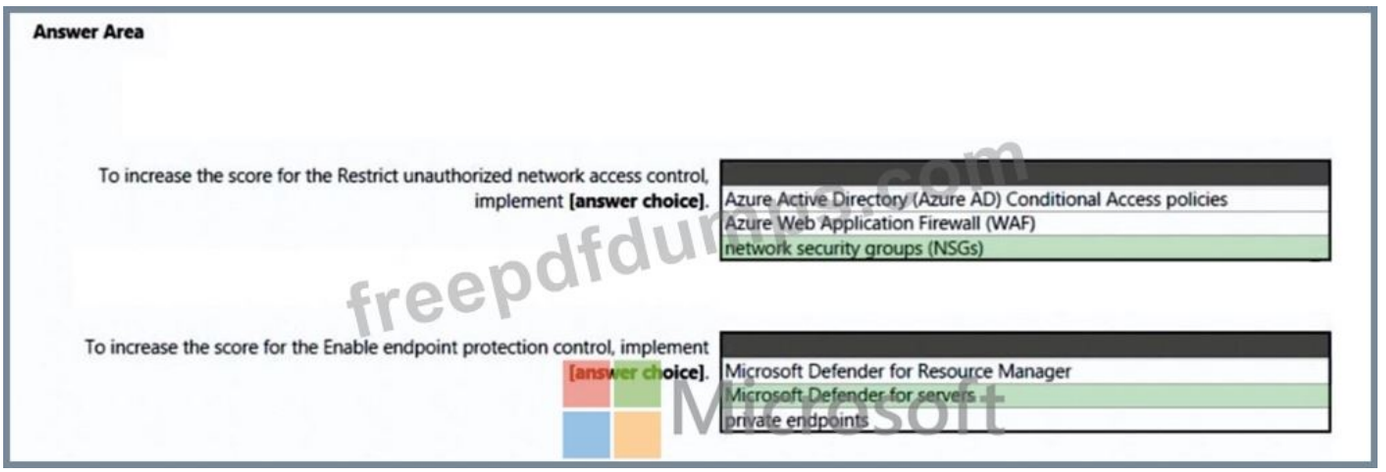
To increase the score for the Restrict unauthorized network access control, implement **[answer choice]**.

| |
|---|
| 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 |

**Answer:**




Explanation:
Box 1: network security groups (NSGs)
https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833 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).
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls#security-controls-and-their-recommendations

**NEW QUESTION: 126**
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.** Policy Analyzer
**C.** Local Group Policy Object (LGPO)
**D.** Windows Autopilot
**Answer: B (LEAVE A REPLY)**
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 -
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

**NEW QUESTION: 127**
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.
**Answer: (SHOW ANSWER)**
https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v2-identity-management

**NEW QUESTION: 128**
You have an Azure subscription and a Microsoft 365 subscription.
Your company uses several software as a service (SaaS) applications.
To align with Microsoft cloud security benchmark (MCSB) and Microsoft Cybersecurity Reference Architectures (MCRA), you plan to design a solution to provide visibility into user activity across the applications and detect potentially risky behavior in real time.

Which service should you recommend?

**A.** Microsoft Defender for Cloud Apps

**B.** Microsoft Purview Information Protection

**C.** Microsoft Sentinel

**D.** Microsoft Defender for Endpoint

**Answer: A (LEAVE A REPLY)**

Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) can be used to monitor user activity across SaaS applications in Azure and Microsoft 365, detect risky behavior in real-time, and align with Microsoft's security benchmarks and architectures. It acts as a comprehensive SaaS security solution, going beyond traditional CASB capabilities to provide full visibility and control over your SaaS environment.

In essence, Microsoft Defender for Cloud Apps provides a comprehensive solution for securing SaaS applications in Azure and Microsoft 365, aligning with Microsoft's security benchmarks and reference architectures by offering real-time threat detection, data protection, and access control capabilities.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

**NEW QUESTION: 129**

You have an on-premises app named App1.

Remote users access App1 by using VPN connections.

You have a third-party software as a service (SaaS) app named App2.

You need to deploy Global Secure Access to manage access to App1 and App2.

What should you use for each app?

**A.** Microsoft Entra Private Access for App2 and Microsoft Entra Internet Access for App1

**B.** Microsoft Entra Private Access for App1 and Microsoft Entra Internet Access for App2

**C.** Microsoft Entra Internet Access for App1 and App2

**D.** Microsoft Entra Private Access for App1 and App2

**Answer: A (LEAVE A REPLY)**

* App1

The features of Microsoft Entra Private Access provide a quick and easy way to replace your VPN to allow secure access to your internal resources with an easy-one time configuration, using the secure capabilities of Conditional Access.

* App2

Microsoft Entra Internet Access is an identity-centric Secure Web Gateway (SWG) for SaaS apps and internet traffic that protects against malicious internet traffic, unsafe or non-compliant content, and other threats from the open internet. Working alongside Microsoft Entra Private Access and the rest of Microsoft Entra identity stack it unifies your access policies across all internet resources and SaaS apps, including Microsoft 365 with Microsoft Entra Conditional Access.

Reference:

https://learn.microsoft.com/en-us/entra/global-secure-access/concept-private-access

https://techcommunity.microsoft.com/t5/microsoft-entra-blog/microsoft-entra-internet-access-an-identity-centric-secure-web/ba-p/3922548

**NEW QUESTION: 130**

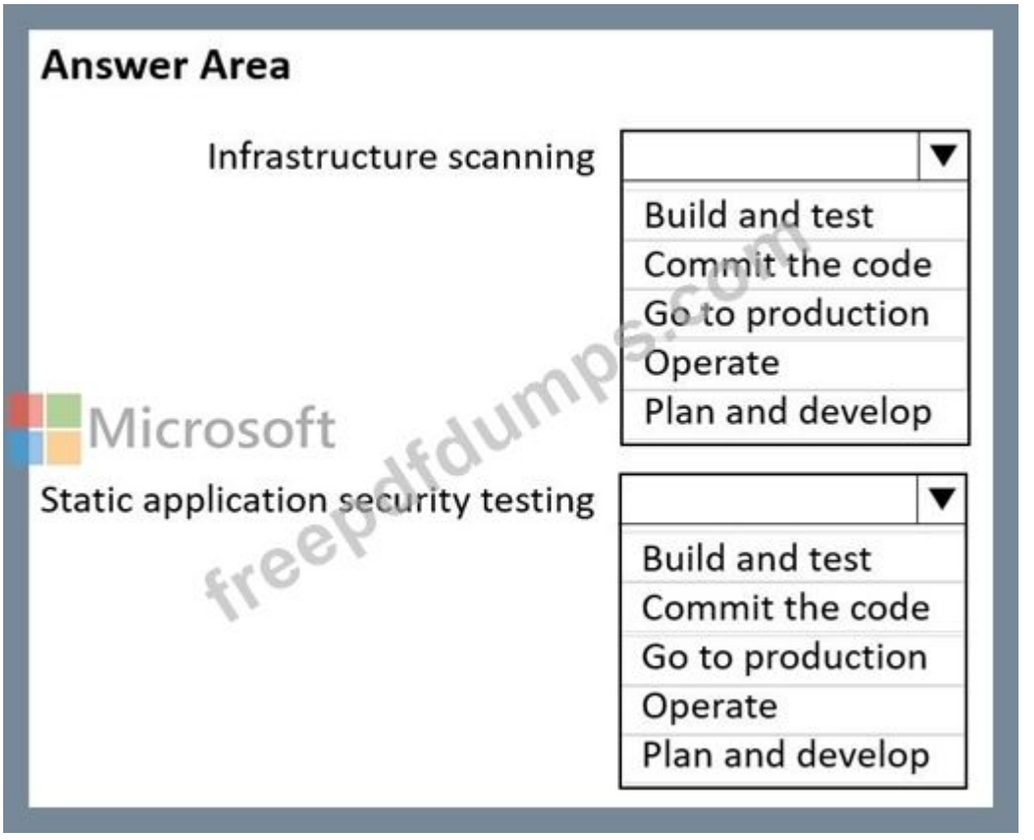
Hotspot Question

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.

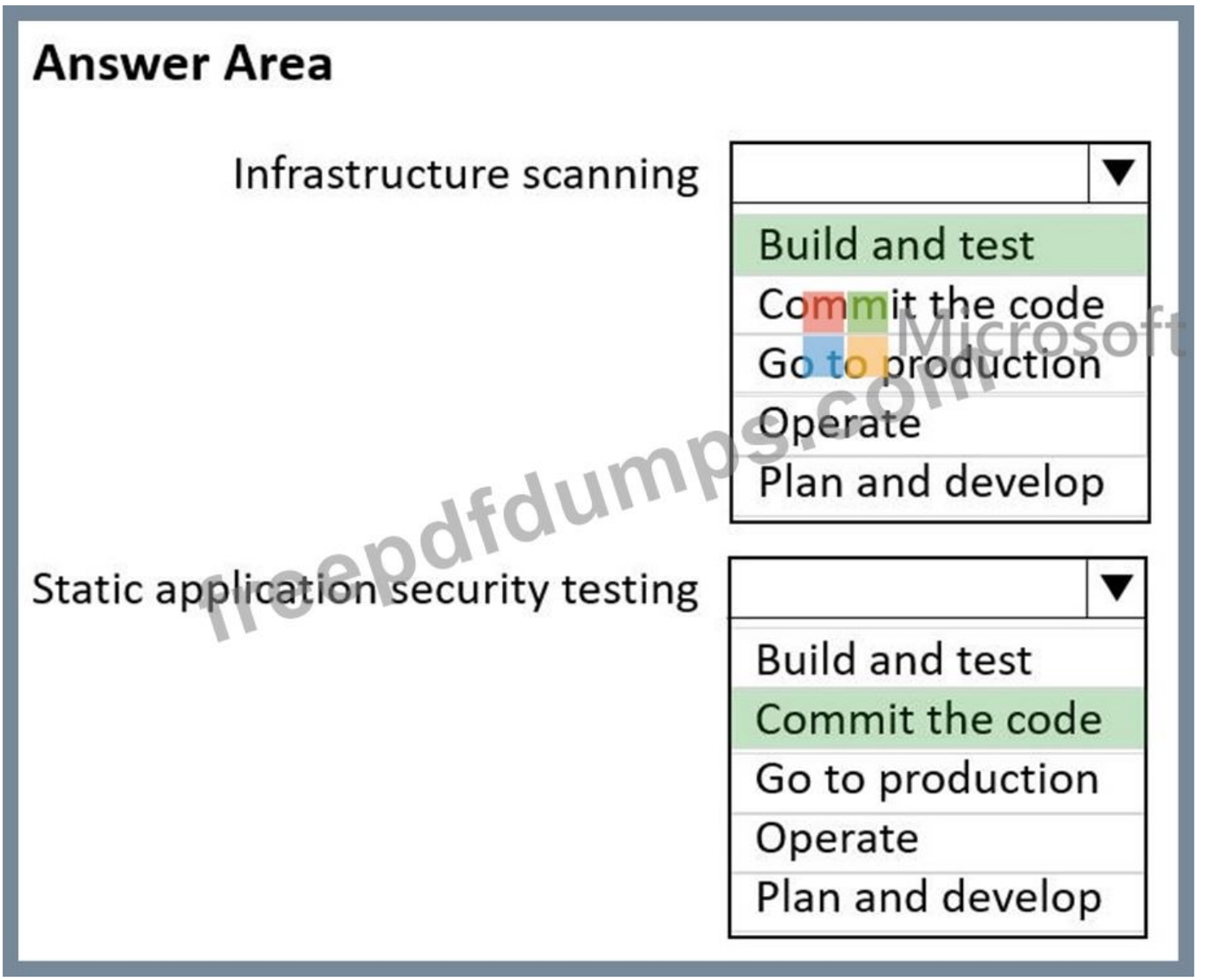
You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines.

What should recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

**NEW QUESTION: 131**
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.** sensitivity label policies
**C.** retention label policies
**D.** eDiscovery cases
**Answer: A,B (LEAVE A REPLY)**

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.
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.
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

**NEW QUESTION: 132**
You have a Microsoft Entra tenant. The tenant contains 500 Windows devices that have the Global Secure Access client deployed.
You have a third-party software as a service (SaaS) app named App1.
You plan to implement Global Secure Access to manage access to App1.
You need to recommend a solution to manage connections to App1. The solution must ensure that users authenticate by using their Microsoft Entra credentials before they can connect to App1.
What should you include the recommendation?
**A.** a Global Secure Access app
**B.** a private access traffic forwarding profile
**C.** an internet access traffic forwarding profile
**D.** a Quick Access app
**Answer: A (LEAVE A REPLY)**
Global Secure Access app is the best solution to manage access to a third-party SaaS application, such as App1. By configuring this app within A Microsoft Entra, you can enforce authentication policies that require users to log in with their Microsoft Entra credentials before accessing the SaaS application. This setup provides centralized access management, secure access controls, and ensures consistent user authentication for App1.

**NEW QUESTION: 133**
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
**Answer: B (LEAVE A REPLY)**
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.
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

**NEW QUESTION: 134**
Case Study 1 - Fabrikam, Inc
OverView
Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.
Existing Environment
On-premises Environment
The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.
Azure Environment
Fabrikam has the following Azure resources:
- A Microsoft Entra tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com
- A single Azure subscription named Sub1
- A virtual network named Vnet1 in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled

- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts
- All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure:

- An Microsoft Entra named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications.

The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1. The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

- Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation. Machines should have a vulnerability assessment solution. All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

- ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.
- Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- Azure DevTest labs will be used by developers for testing.
- All the application code must be stored in GitHub Enterprise.
- Azure Pipelines will be used to manage application deployments.

- All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- Internet-accessible applications must prevent connections that originate in North Korea.
- Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
- Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers:

- Every month, the membership of the ContosoDevelopers group must be verified.
- The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

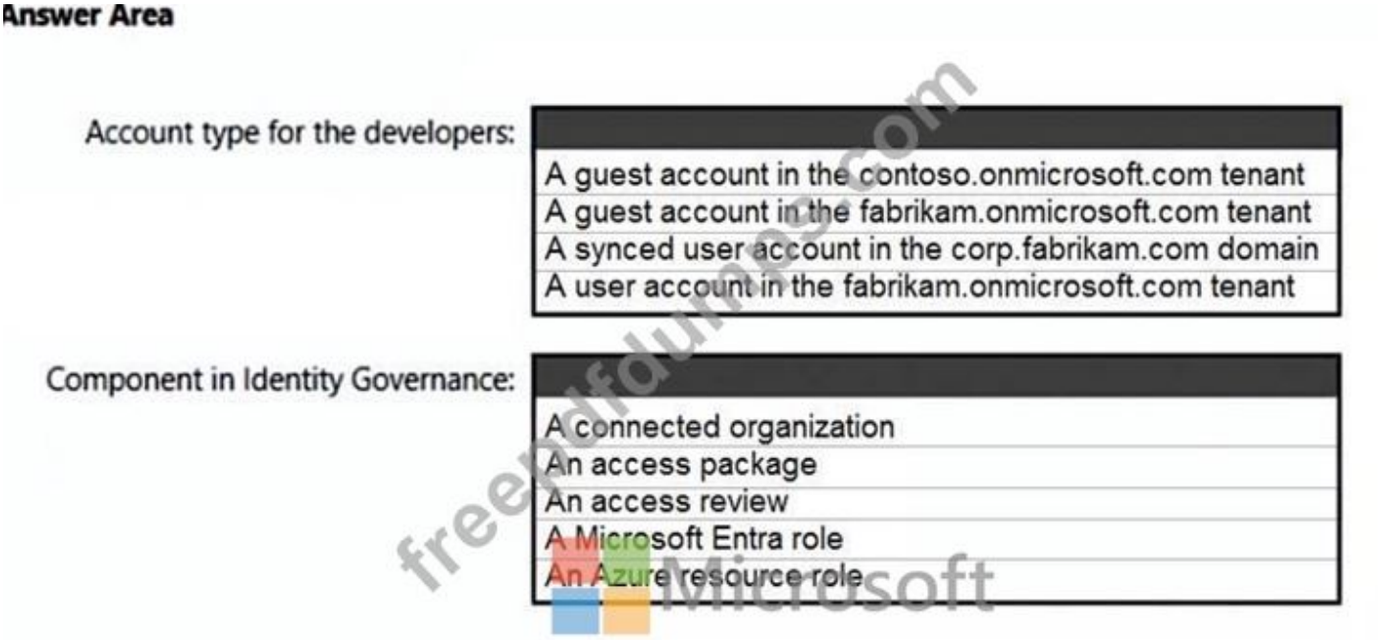
Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

Hotspot Question

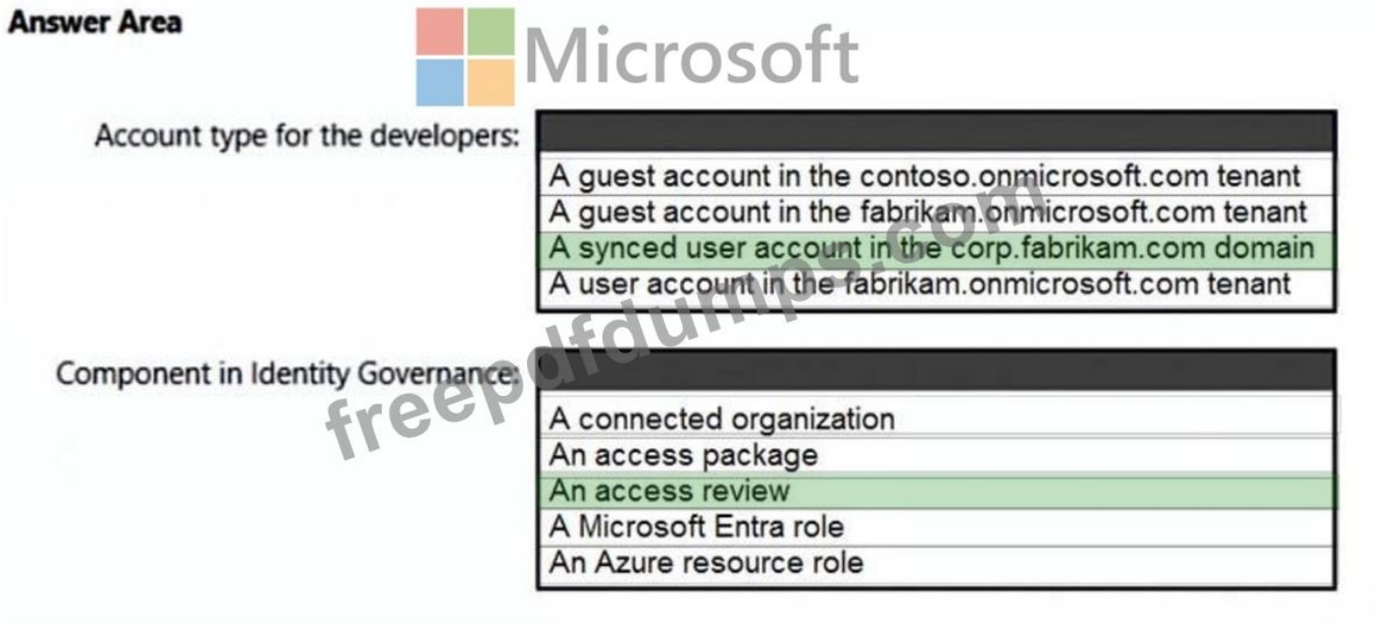
What should you create in Microsoft Entra ID to meet the Contoso developer requirements?

**Answer Area**




**Answer:**

**Answer Area**




Explanation:

Box 1: A guest account in the fabrikham.onmicrosoft.com tenant

The Contoso devlopers must use their existing contoso.onmicrosoft.com credentials.

Box 2: An access review

Scenario: Every month, the membership of the ContosoDevelopers group must be verified.

Microsoft Entra ID access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Access review is part of Microsoft Entra ID governance.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

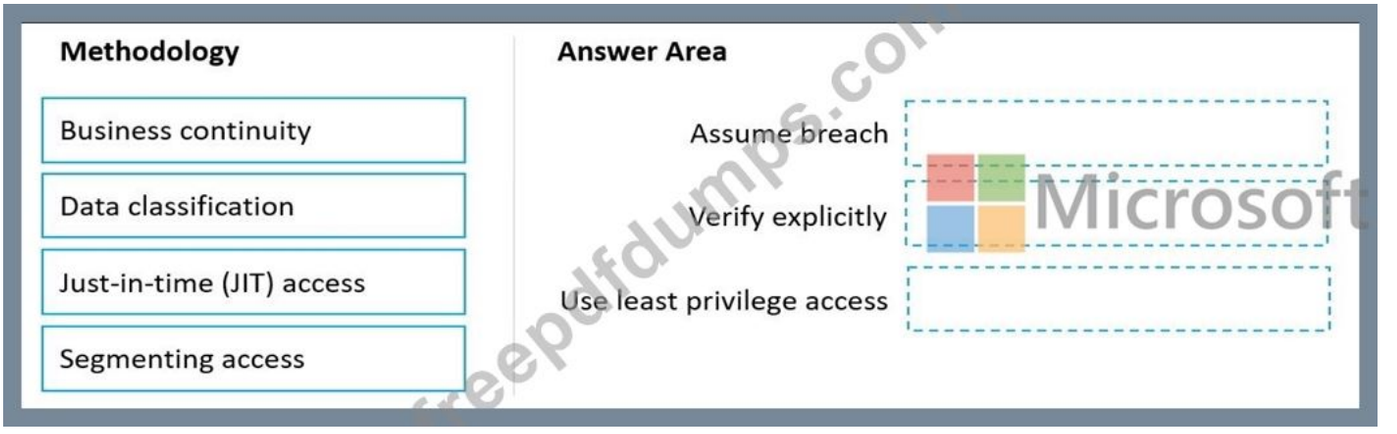
**NEW QUESTION: 135**

Drag and Drop Question

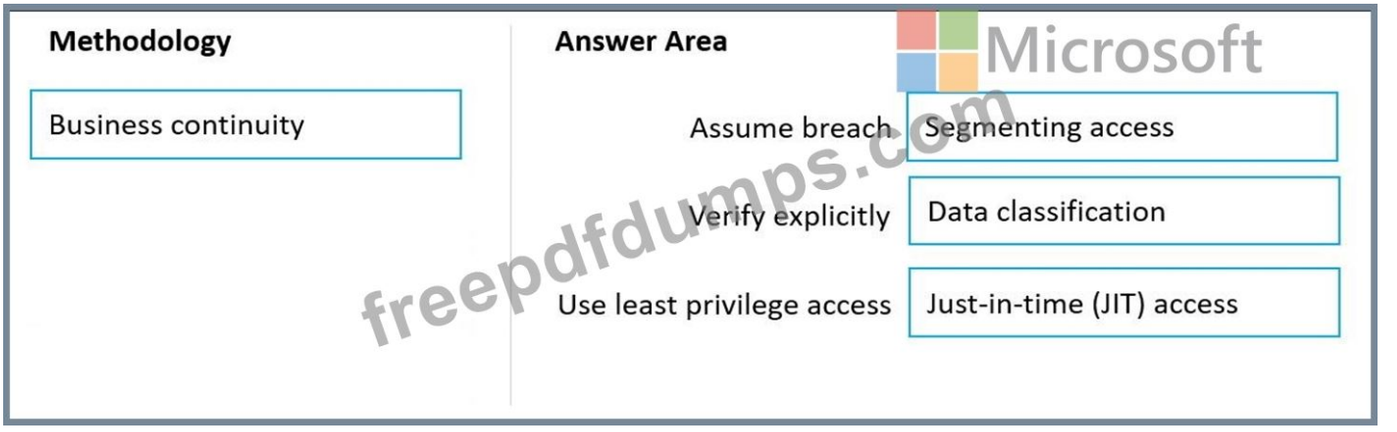
For a Microsoft cloud environment, you need to recommend a security architecture that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

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.




**Answer:**




Explanation:

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 and 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.

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

**NEW QUESTION: 136**
You have an Azure subscription.
You plan to deploy Azure Kubernetes Service (AKS) clusters that will be used to host web services.
You need to recommend an ingress controller solution that will protect the hosted web services.
What should you include in the recommendation?
**A.** Azure Load Balancer
**B.** Azure Application Gateway
**C.** Azure Front Door
**D.** Azure Firewall
**Answer: B (LEAVE A REPLY)**
Use Application Gateway Ingress Controller (AGIC) with a multitenant Azure Kubernetes Service.
In this solution, Azure Web Application Firewall (WAF) provides centralized protection for web applications deployed on a multi-tenant Azure Kubernetes Service (AKS) cluster from common exploits and vulnerabilities.
Web applications running on Azure Kubernetes Service (AKS) cluster and exposed via the Application Gateway Ingress Controller (AGIC) can be protected from malicious attacks, such as SQL injection and cross-site scripting, by using a WAF Policy on Azure Application Gateway.
WAF policy on Azure Application Gateway comes pre-configured with Open Worldwide Application Security Project (OWASP) core rule sets and can be changed to other supported OWASP Core Rule Set (CRS) versions.
Reference:
https://learn.microsoft.com/en-us/azure/architecture/example-scenario/aks-agic/aks-agic



**NEW QUESTION: 137**
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

**Answer: (SHOW ANSWER)**

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

**NEW QUESTION: 138**

Hotspot Question

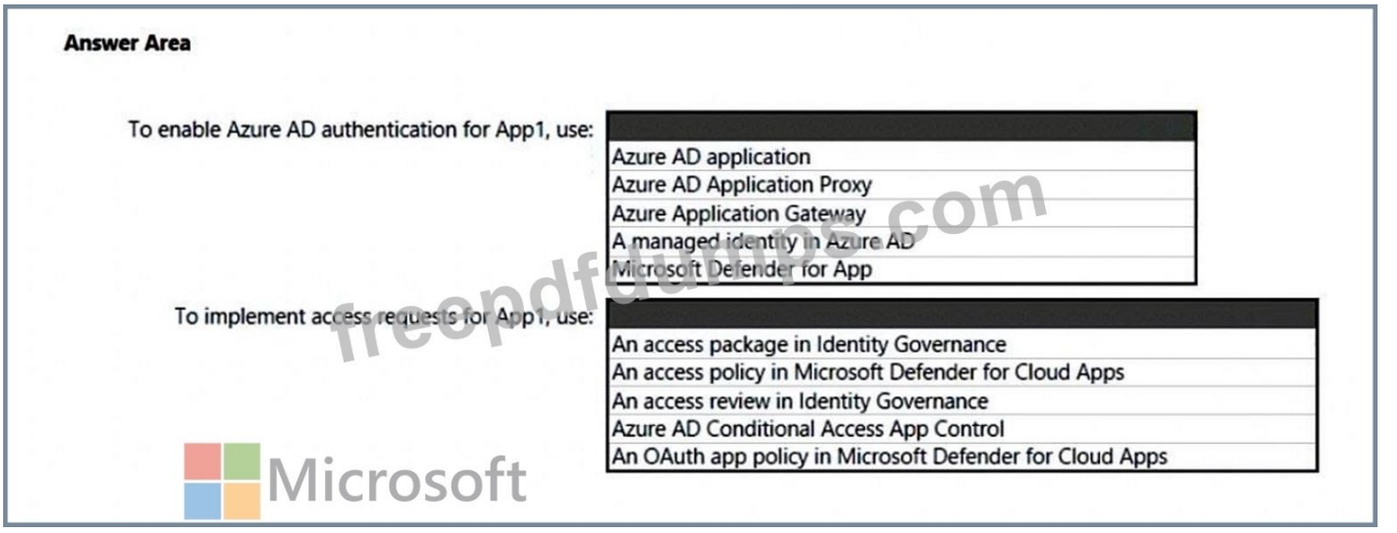
You are creating the security recommendations for an Azure App Service web app named App1.

App1 has the following specifications:

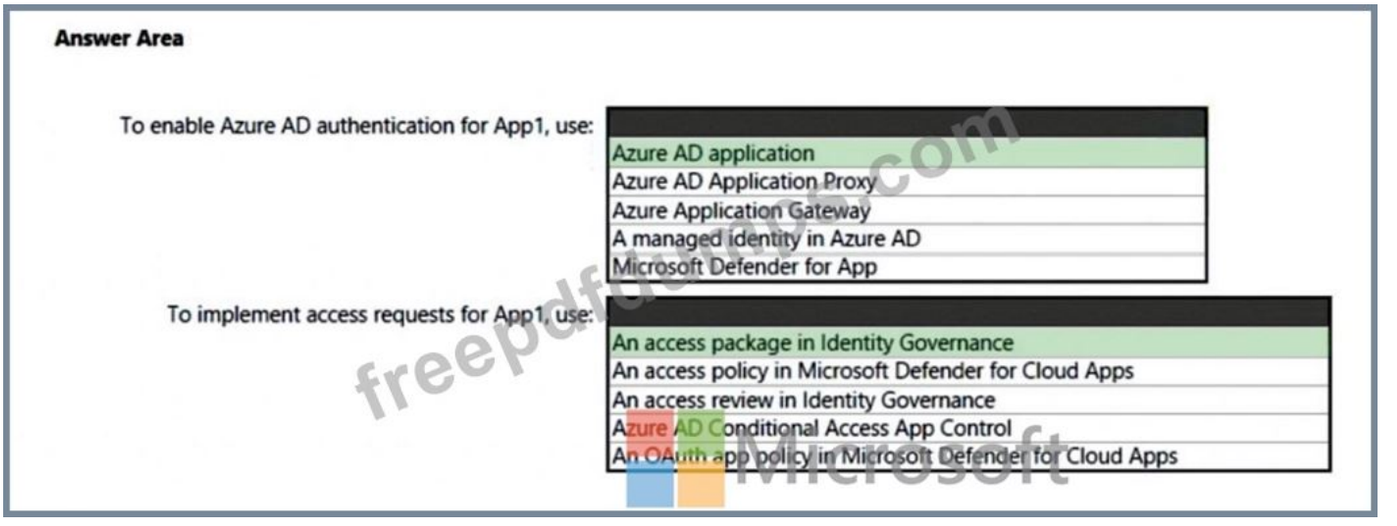
- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

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.




**Answer:**




Explanation:

Box 1: Azure AD application

You need first to register your app in AAD, then add users or group to this app so they can used it.
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app Box 2: An access package in identity governance Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

**NEW QUESTION: 139**
What measures the percentage of loss of an asset when doing a risk analysis?
**A.** Exposure factor
**B.** Single loss expectancy
**C.** Annualized loss expectancy
**D.** The annualized rate of occurrence
**Answer: (SHOW ANSWER)**
The exposure factor measures the percentage of loss of an asset when doing a risk analysis.

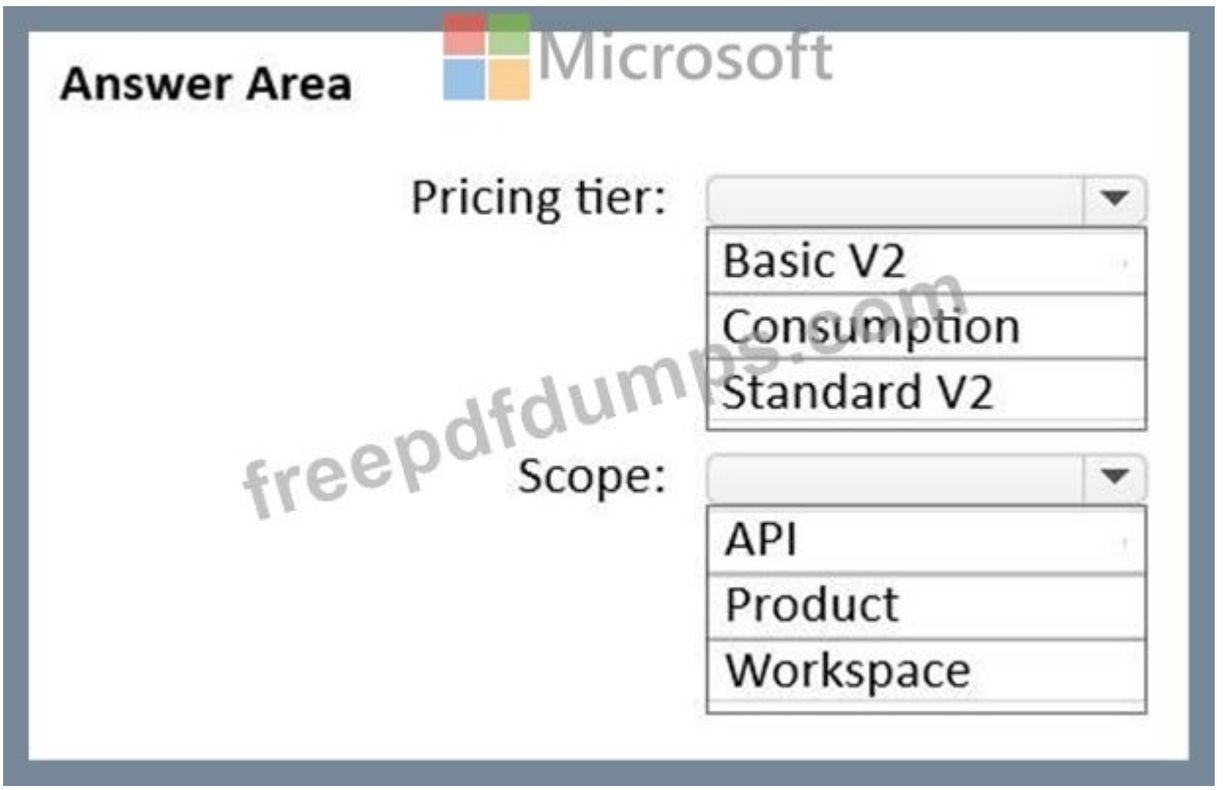
**NEW QUESTION: 140**
Hotspot Question
You have a Microsoft 365 E5 subscription.
You need to mitigate ransomware attacks against messages posted to Microsoft Teams channels and files stored in Teams channels.
What should you include in the solution for each type of content? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.


**Answer:**

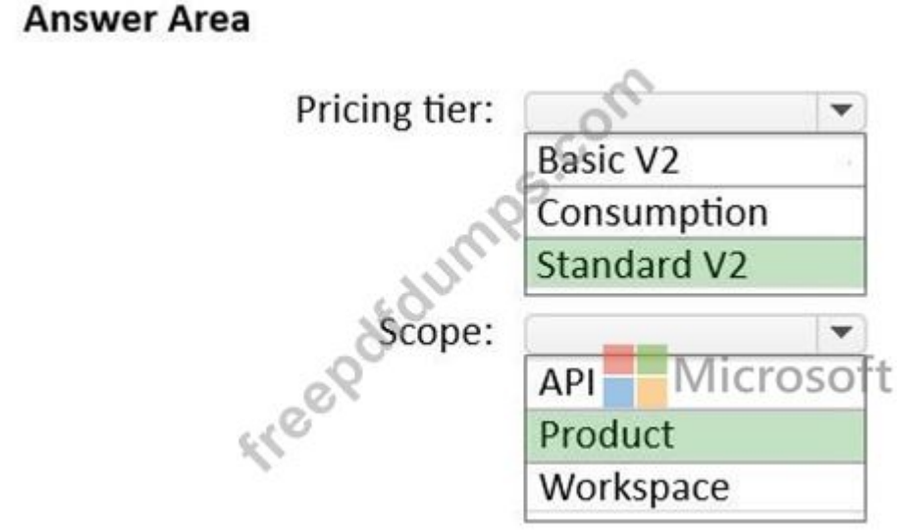
Answer Area


Explanation:
Box 1: Exchange Online Protection (EOP)
Ransomware protection in Microsoft 365
Teams
Teams chats are stored within Exchange Online user mailboxes and files are stored in either SharePoint or OneDrive. Microsoft Teams data is protected by the controls and recovery mechanisms available in these services.
Box 2: The Preservation Hold library
Preservation Hold library: Files stored in SharePoint or OneDrive sites can be retained by applying retention settings. When a document with versions is subject to retention settings, versions get copied to the Preservation Hold library and exist as a separate item. If a user suspects their files have been compromised, they can investigate file changes by reviewing the retained copy. File Restore can then be used to recover files within the last 30 days.
Reference:
https://learn.microsoft.com/en-us/compliance/assurance/assurance-shared-ransomware-protection

**NEW QUESTION: 141**
Hotspot Question
You plan to deploy an Azure API Management solution that will enable different groups of developers to access different sets of APIs at random times and rates.
You need to recommend the pricing tier that should be purchased and the scope at which the rate limit policies should be applied. The solution must meet the following requirements:
- Ensure that each group of developers can access only specific sets of APIs.
- Ensure that each set of APIs can be configured with specific rate
limits.
- Minimize development and administrative effort and costs.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




**Answer:**




Explanation:

Box 1: Standard V2

Standard v2 - Standard v2 is a production-ready tier with support for network-isolated backends.

Box 2: Product

API Management allows you to define policies at the following scopes, from most broad to most narrow:

Global (all APIs)

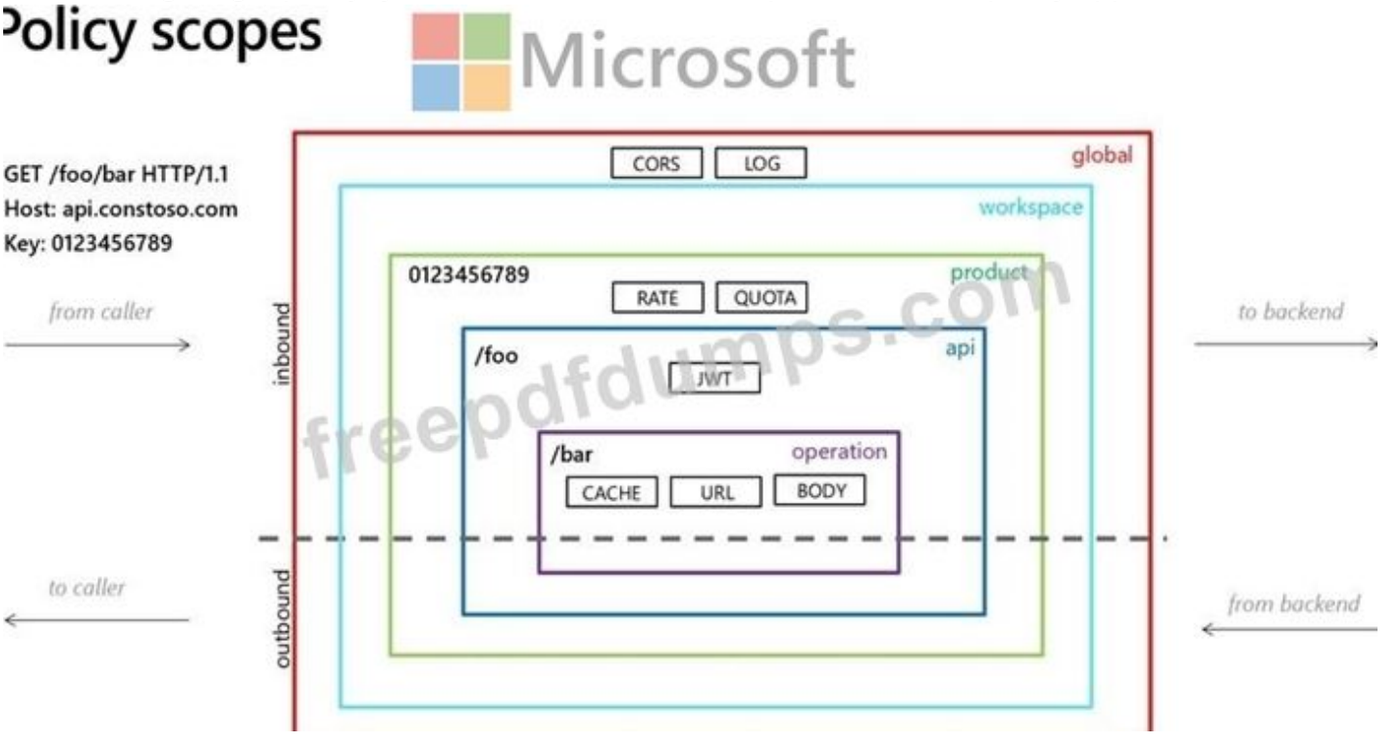
Workspace (all APIs associated with a selected workspace)

*-> Product (all APIs associated with a selected product)

API (all operations in an API)

Operation (single operation in an API)

When configuring a policy, you must first select the scope at which the policy applies.




Reference:
https://learn.microsoft.com/en-us/azure/api-management/api-management-features
https://learn.microsoft.com/en-us/azure/api-management/api-management-howto-policies