SC-100$^{Q\&As}$

Microsoft Cybersecurity Architect

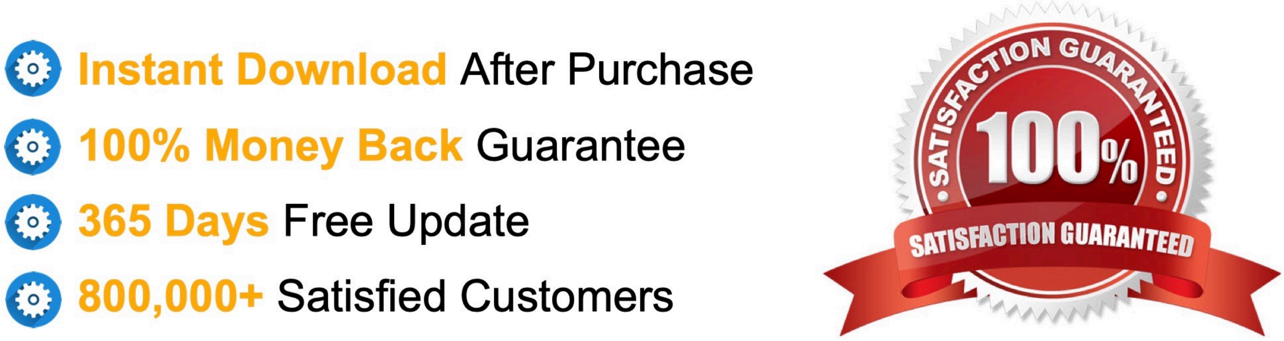
Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

HOTSPOT

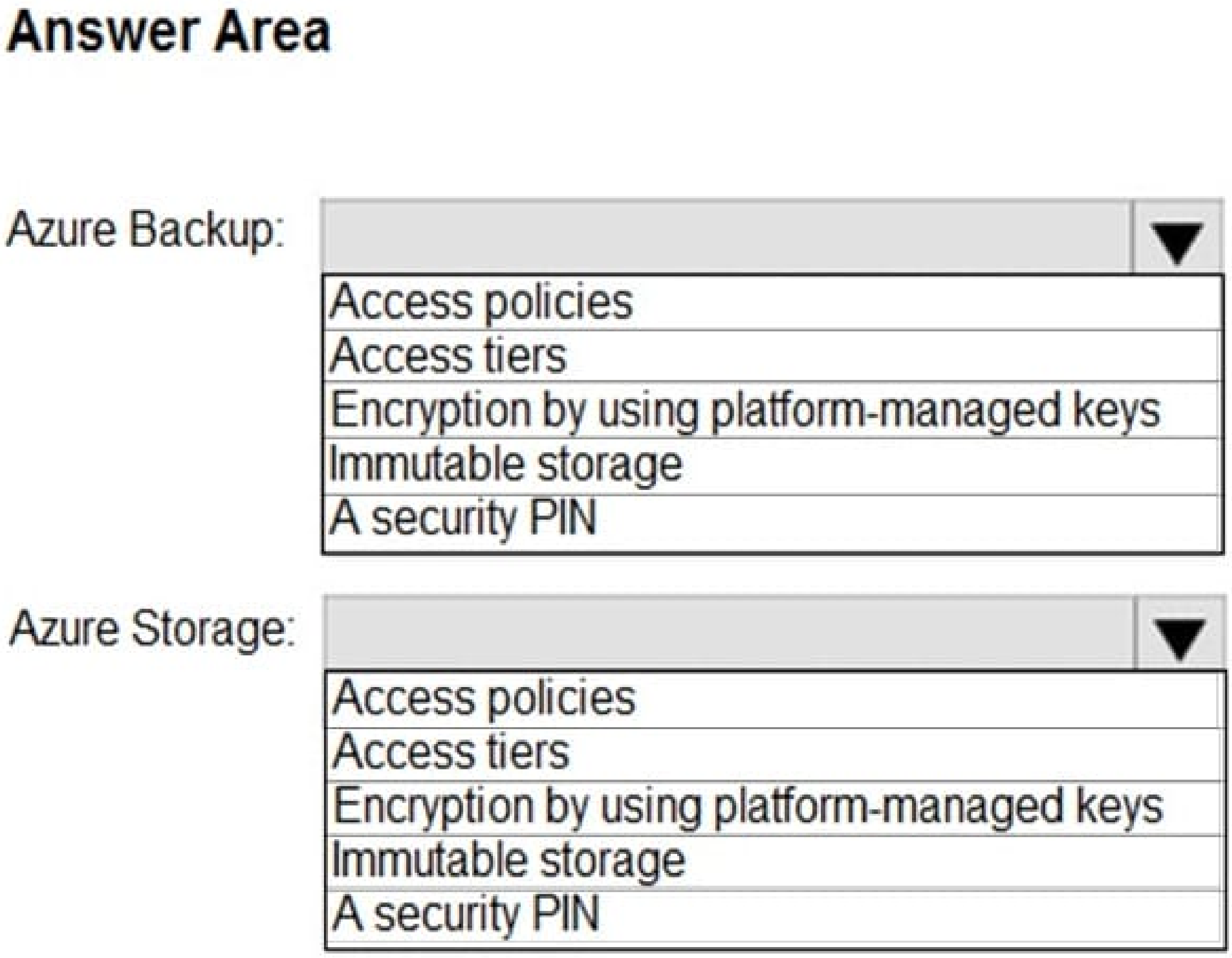
Your company wants to optimize using Azure to protect its resources from ransomware.

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

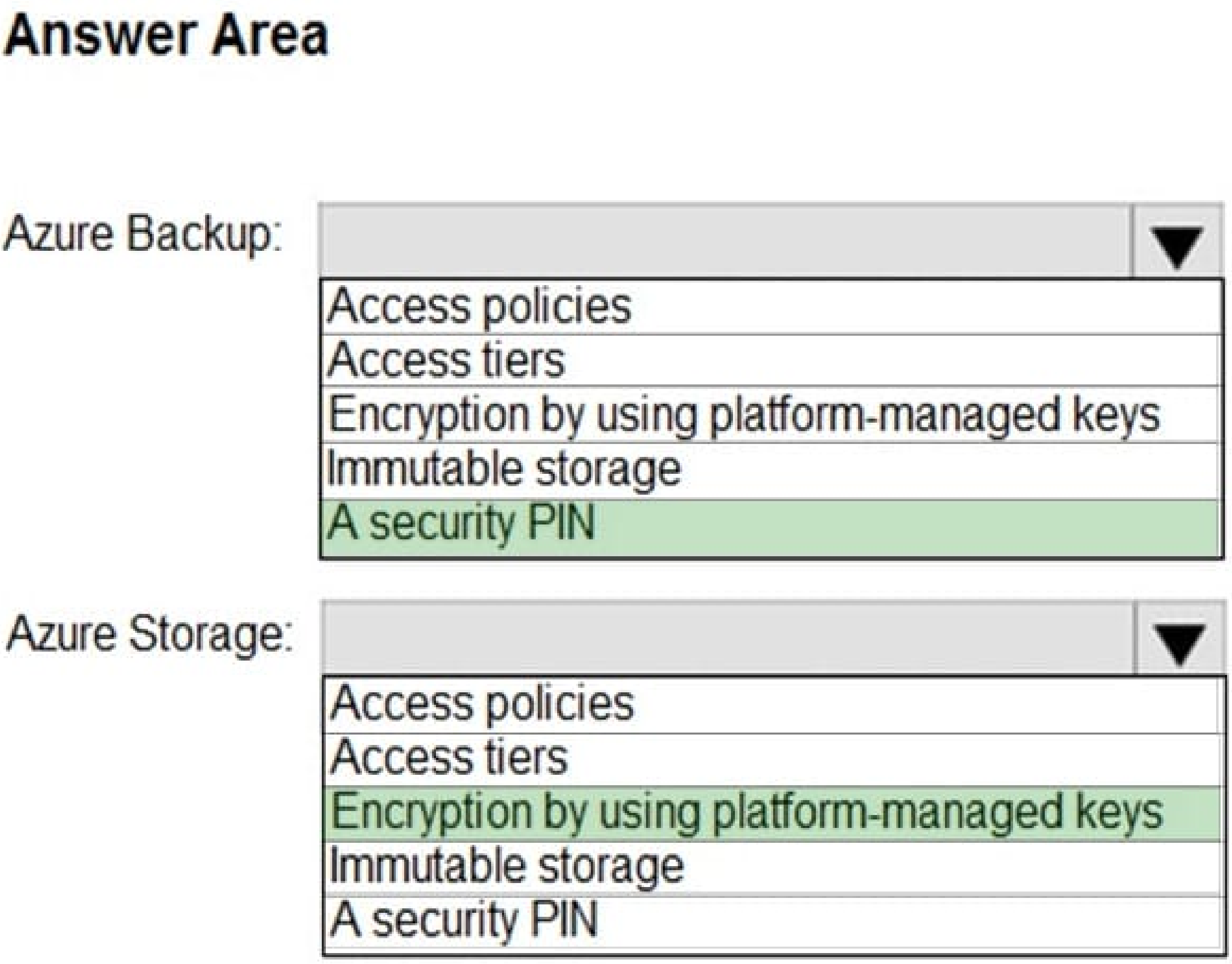
Azure Backup:

- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Azure Storage:

- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Correct Answer:



Answer Area

Azure Backup:

- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- [✓ A security PIN]

Azure Storage:

- Access policies
- Access tiers
- [✓ Encryption by using platform-managed keys]
- Immutable storage
- A security PIN

Box 1: A security PIN

Azure Backup

The best way to prevent falling victim to ransomware is to implement preventive measures and have tools that protect your organization from every step that attackers take to infiltrate your systems.

You can reduce your on-premises exposure by moving your organization to a cloud service.

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a

security PIN before modifying online backups.

Box 2: Encryption by using platform-managed keys

Ensure backup data is encrypted.

By default, backup data at rest is encrypted using platform-managed keys (PMK). For vaulted backups, you can choose to use customer-managed keys (CMK) to own and manage the encryption keys yourself. Additionally, you can configure

encryption on the storage infrastructure using infrastructure-level encryption, which along with CMK encryption provides double encryption of data at rest.

Reference:

https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

QUESTION 2

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.

Does this meet the goal?

A. Yes

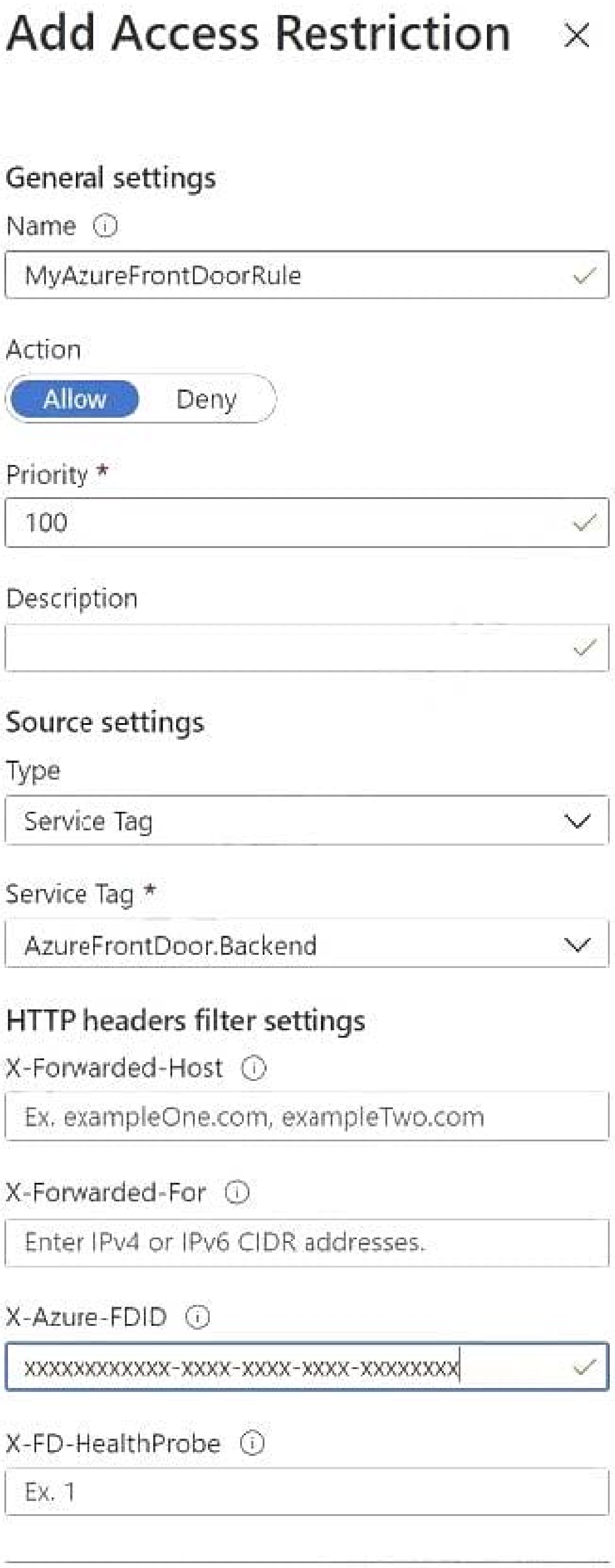
B. No

Correct Answer: A

Restrict access to a specific Azure Front Door instance.

Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front

Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.



Add Access Restriction ×

General settings

Name ⓘ

MyAzureFrontDoorRule ✓

Action

Priority *

100 ✓

Description

✓

Source settings

Type

Service Tag

Service Tag *

AzureFrontDoor.Backend

HTTP headers filter settings

X-Forwarded-Host ⓘ

Ex. exampleOne.com, exampleTwo.com

X-Forwarded-For ⓘ

Enter IPv4 or IPv6 CIDR addresses.

X-Azure-FDID ⓘ

xxxxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx ✓

X-FD-HealthProbe ⓘ

Ex. 1

Reference: https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

QUESTION 3

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two solutions should you include in the design to ensure that preventative controls are implemented to increase the secure score? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Web Application Firewall (WAF)

B. Azure AD Privileged Identity Management (PIM)

C. Microsoft Sentinel

D. Azure Firewall

E. Microsoft Defender for Cloud alerts

Correct Answer: BC

B: Azure identity and access for landing zones, Privileged Identity Management (PIM)

Use Azure AD Privileged Identity Management (PIM) to establish zero-trust and least privilege access. Map your organization\\'s roles to the minimum access levels needed. Azure AD PIM can use Azure native tools, extend current tools and

processes, or use both current and native tools as needed.

Azure identity and access for landing zones, Design recommendations include:

*

(B) Use Azure AD managed identities for Azure resources to avoid credential-based authentication. Many security breaches of public cloud resources originate with credential theft embedded in code or other text. Enforcing managed identities for programmatic access greatly reduces the risk of credential theft.

*

Etc.

C: Improve landing zone security, onboard Microsoft Sentinel You can enable Microsoft Sentinel, and then set up data connectors to monitor and protect your environment. After you connect your data sources using data connectors, you choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.

Note: Landing zone security best practices

The following list of reference architectures and best practices provides examples of ways to improve landing zone security:

Microsoft Defender for Cloud: Onboard a subscription to Defender for Cloud.

Microsoft Sentinel: Onboard to Microsoft Sentinel to provide a security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Secure network architecture: Reference architecture for implementing a perimeter network and secure network architecture.

Identity management and access control: Series of best practices for implementing identity and access to secure a landing zone in Azure.

Network security practices: Provides additional best practices for securing the network.

Operational security provides best practices for increasing operational security in Azure.

The Security Baseline discipline: Example of developing a governance-driven security baseline to enforce security requirements.

Incorrect:

Not E: Implementing alerts is not a preventive measure.

Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-area/identity-access-landing-zones

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

QUESTION 4

You are designing the security standards for containerized applications onboarded to Azure.

You are evaluating the use of Microsoft Defender for Containers.

In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Instances

B. Windows containers deployed to Azure Kubernetes Service (AKS)

C. Windows containers deployed to Azure Container Registry

D. Linux containers deployed to Azure Container Registry

E. Linux containers deployed to Azure Kubernetes Service (AKS)

Correct Answer: DE

https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=azure-aks#registries-and-images Windows is on preview.

OS Packages Supported

- Alpine Linux 3.12-3.15
- Red Hat Enterprise Linux 6, 7, 8
- CentOS 6, 7
- Oracle Linux 6,6,7,8
- Amazon Linux 1,2 • openSUSE Leap 42, 15
- SUSE Enterprise Linux 11,12, 15
- Debian GNU/Linux wheezy, jessie, stretch, buster, bullseye
- Ubuntu 10.10-22.04
- FreeBSD 11.1-13.1
- Fedora 32, 33, 34, 35

QUESTION 5

You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.

B. Obtain Azure AD Premium Plan 2 licenses.

C. Add Microsoft Sentinel data connectors.

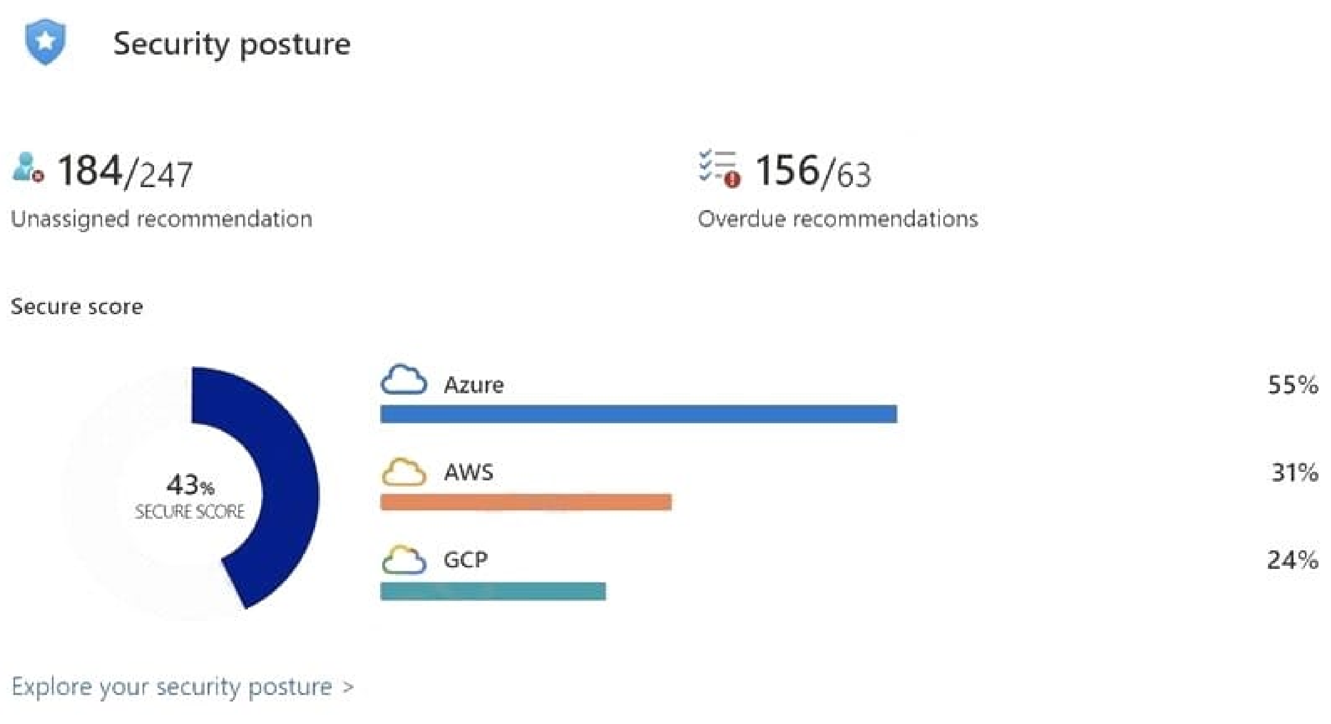
D. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.

Correct Answer: D

You can evaluate security postures by using Microsoft Defender for Cloud.

Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the

score, the lower the identified risk level.


Security posture

184/247
Unassigned recommendation

156/63
Overdue recommendations

Secure score

Explore your security posture >

Note: Security in the Azure landing zone accelerator

Security is at the core of the Azure landing zone accelerator. As part of the implementation, many tools and controls are deployed to help organizations quickly achieve a security baseline.

For example, the following are included:

Tools:

Microsoft Defender for Cloud, standard or free tier

Microsoft Sentinel

Azure DDoS standard protection plan (optional)

Azure Firewall

Web Application Firewall (WAF)

Privileged Identity Management (PIM)

Incorrect:

Not C: Microsoft Sentinel uses data from Microsoft Defender for Cloud, so would need setup Defender for Cloud first.

Reference: https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/3-postures-use-microsoft-defender-for-cloud https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone

QUESTION 6

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:

1.

A user account is disabled or deleted.

2.

The password of a user is changed or reset.

3.

All the refresh tokens for a user are revoked.

4.

Multi-factor authentication (MFA) is enabled for a user.

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

NOTE: Each correct selection is worth one point.

A. continuous access evaluation

B. Azure AD Application Proxy

C. a sign-in risk policy

D. Azure AD Privileged Identity Management (PIM)

E. Conditional Access

Correct Answer: AE

Continuous access evaluation

Key benefits

User termination or password change/reset: User session revocation will be enforced in near real time.

Network location change: Conditional Access location policies will be enforced in near real time.

Token export to a machine outside of a trusted network can be prevented with Conditional Access location policies.

Scenarios

There are two scenarios that make up continuous access evaluation, critical event evaluation and Conditional Access policy evaluation.

*

Critical event evaluation Continuous access evaluation is implemented by enabling services, like Exchange Online, SharePoint Online, and Teams, to subscribe to critical Azure AD events. Those events can then be evaluated and enforced near real time. Critical event evaluation doesn\\'t rely on Conditional Access policies so it\\'s available in any tenant. The following events are currently evaluated:

User Account is deleted or disabled Password for a user is changed or reset Multi-factor authentication is enabled for the user Administrator explicitly revokes all refresh tokens for a user High user risk detected by Azure AD Identity Protection

*

Conditional Access policy evaluation

Exchange Online, SharePoint Online, Teams, and MS Graph can synchronize key Conditional Access policies for evaluation within the service itself.

This process enables the scenario where users lose access to organizational files, email, calendar, or tasks from Microsoft 365 client apps or SharePoint Online immediately after network location changes.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

QUESTION 7

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

Correct Answer: C

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide like for example 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.

QUESTION 8

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing the encryption standards for data at rest for an Azure resource.

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

We need to use customer-managed keys.

Azure Storage encryption for data at rest.

Azure Storage uses service-side encryption (SSE) to automatically encrypt your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance

commitments.

Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.

Data in a new storage account is encrypted with Microsoft-managed keys by default. You can continue to rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. If you choose to

manage encryption with your own keys, you have two options. You can use either type of key management, or both:

*

You can specify a customer-managed key to use for encrypting and decrypting data in Blob Storage and in Azure Files.

*

You can specify a customer-provided key on Blob Storage operations. A client making a read or write request against Blob Storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.

Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices.

This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers endto-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

QUESTION 9

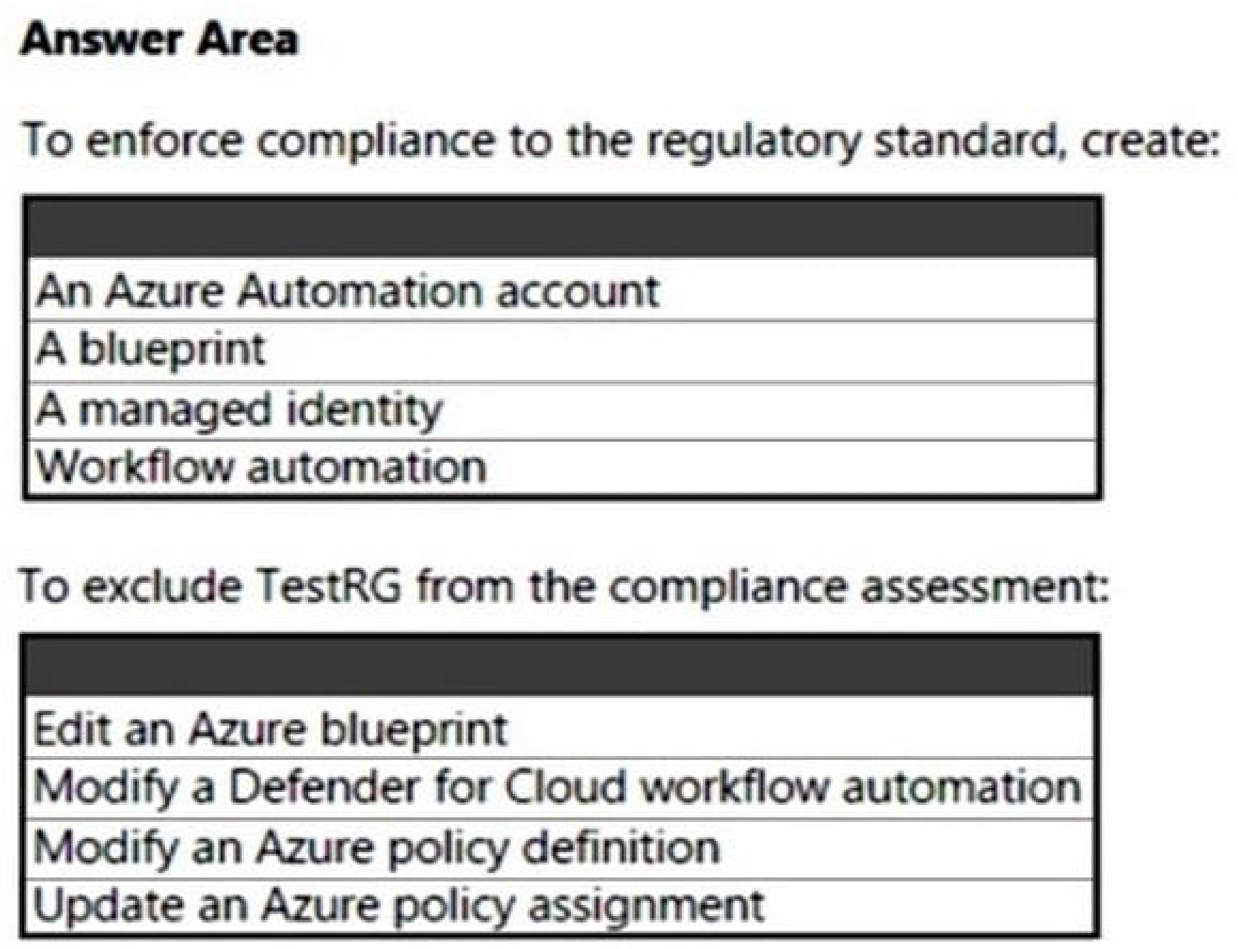
HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

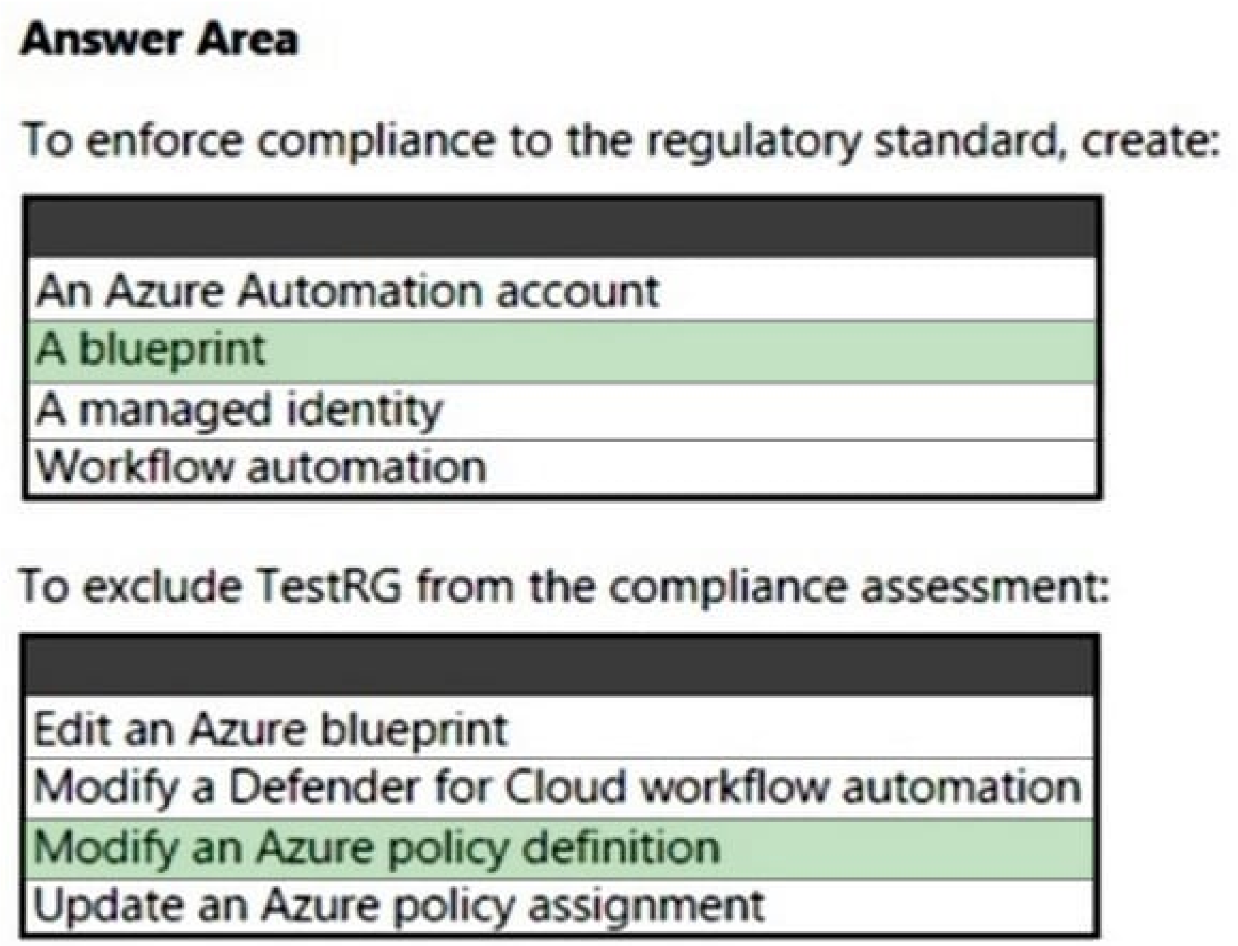
To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

Correct Answer:



Answer Area

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- [✓ A blueprint]
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- [✓ Modify an Azure policy definition]
- Update an Azure policy assignment

Box 1: A blueprint Scenario: Requirements. Compliance Requirements Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPAA HITRUST standard.

Microsoft releases automation for HIPAA/HITRUST compliance I am excited to share our new Azure Security and Compliance Blueprint for HIPAA/HITRUST

QUESTION 10

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.

All resources are backed up multiple times a day by using Azure Backup.

You are developing a strategy to protect against ransomware attacks.

You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.

Which two controls should you include in the recommendation? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Enable soft delete for backups.

B. Require PINs for critical operations.

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

D. Perform offline backups to Azure Data Box.

E. Use Azure Monitor notifications when backup configurations change.

Correct Answer: BE

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a security PIN before modifying online backups.

Your backups need to be protected from sophisticated bot and malware attacks. Permanent loss of data can have significant cost and time implications to your business. To help protect against this, Azure Backup guards against malicious attacks through deeper security, faster notifications, and extended recoverability.

For deeper security, only users with valid Azure credentials will receive a security PIN generated by the Azure portal to allow them to backup data. If a critical backup operation is authorized, such as “delete backup data,” a notification is immediately sent so you can engage and minimize the impact to your business. If a hacker does delete backup data, Azure Backup will store the deleted backup data for up to 14 days after deletion.

E: Key benefits of Azure Monitor alerts include:

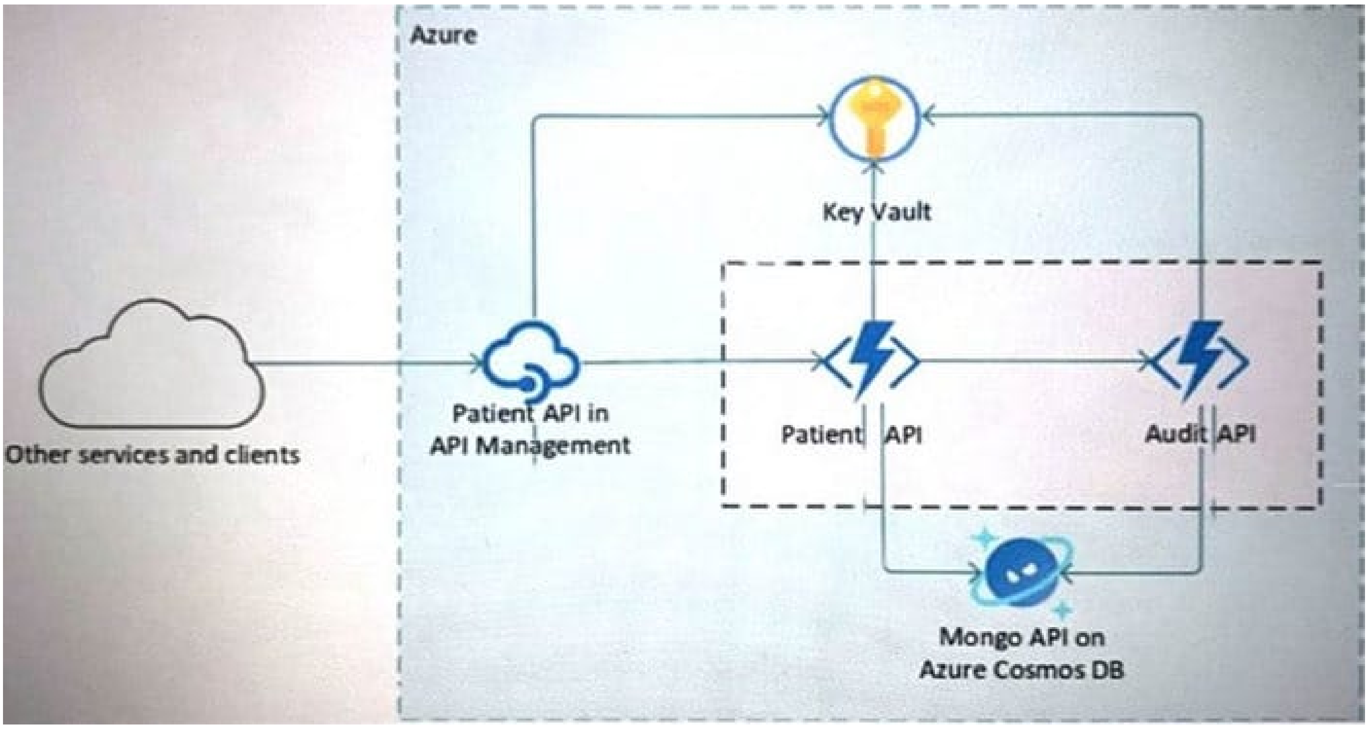
Monitor alerts at-scale via Backup center: In addition to enabling you to manage the alerts from Azure Monitor dashboard, Azure Backup also provides an alert management experience tailored to backups via Backup center. This allows you

to filter alerts by backup specific properties, such as workload type, vault location, and so on, and a way to get quick visibility into the active backup security alerts that need attention.

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
https://www.microsoft.com/security/blog/2017/01/05/azure-backup-protects-against-ransomware/
https://docs.microsoft.com/en-us/azure/backup/move-to-azure-monitor-alerts

QUESTION 11

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



You need to recommend a solution to isolate the compute components on an Azure virtual network. What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications

B. an Azure App Service Environment (ASE)

C. Azure service endpoints

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

Correct Answer: B

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

1.

Windows web apps

2.

Linux web apps

3.

Docker containers

4.

Mobile apps

5.

Functions

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

Very high scale.

Isolation and secure network access.

High memory utilization.

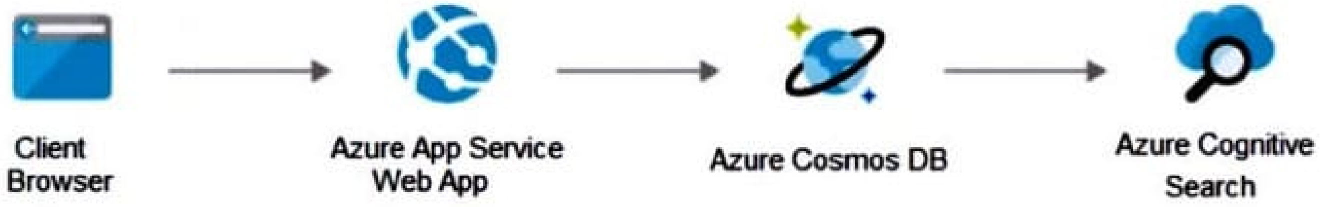
Customers can create multiple ASEs within a single Azure region or across multiple Azure regions. This flexibility makes ASEs ideal for horizontally scaling stateless application tiers in support of high requests per second (RPS) workloads.

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

QUESTION 12

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend creating private endpoints for the web app and the database layer.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: “How can we safely deploy internal business applications to Azure App Services?”

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private

Endpoint is a read-only network interface service associated with the Azure PAAS Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources. They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App,

your own / partner owned services, Azure Backups, Event Grids, Azure Service Bus, or Azure Automations.

Reference: https://www.varonis.com/blog/securing-access-azure-webapps

QUESTION 13

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation?(Choose Two)

A. Onboard the virtual machines to Microsoft Defender for Endpoint.

B. Onboard the virtual machines to Azure Arc.

C. Create a device compliance policy in Microsoft Endpoint Manager.

D. Enable the Qualys scanner in Defender for Cloud.

Correct Answer: AD

Scenario: 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud.

Existing Environment. 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.

Note: Deploying Microsoft Defender for Endpoint is a two-step process.

Onboard devices to the service

Configure capabilities of the service

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm https://docs.microsoft.com/en-us/microsoft-365/security/defenderendpoint/switch-to-mde-phase-3?view=o365-worldwide

QUESTION 14

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft 365 subscription, and an Azure subscription.

The company\\'s on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

1.

Prevent the remote users from accessing any other resources on the network.

2.

Support Azure Active Directory (Azure AD) Conditional Access.

3.

Simplify the end-user experience. What should you include in the recommendation?

A. Azure AD Application Proxy

B. web content filtering in Microsoft Defender for Endpoint

C. Microsoft Tunnel

D. Azure Virtual WAN

Correct Answer: A

Azure Active Directory\\'s Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal

application portal.

Azure AD Application Proxy is:

Secure. On-premises applications can use Azure\\'s authorization controls and security analytics. For example, on-premises applications can use Conditional Access and two-step verification. Application Proxy doesn\\'t require you to open

inbound connections through your firewall.

Simple to use. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don\\'t need to change or update your applications to work with Application Proxy.

Incorrect:

Not D: Azure Virtual WAN

Azure Virtual WAN is for end users, not for applications.

Note: Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:

Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).

Site-to-site VPN connectivity.

Remote user VPN connectivity (point-to-site).

Private connectivity (ExpressRoute).

Intra-cloud connectivity (transitive connectivity for virtual networks).

VPN ExpressRoute inter-connectivity.

Routing, Azure Firewall, and encryption for private connectivity.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

QUESTION 15

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

What are three best practices for identity management based on the Azure Security Benchmark? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Manage application identities securely and automatically.

B. Manage the lifecycle of identities and entitlements

C. Protect identity and authentication systems.

D. Enable threat detection for identity and access management.

E. Use a centralized identity and authentication system.

Correct Answer: ACE