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.pass4itsure.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

QUESTION 1

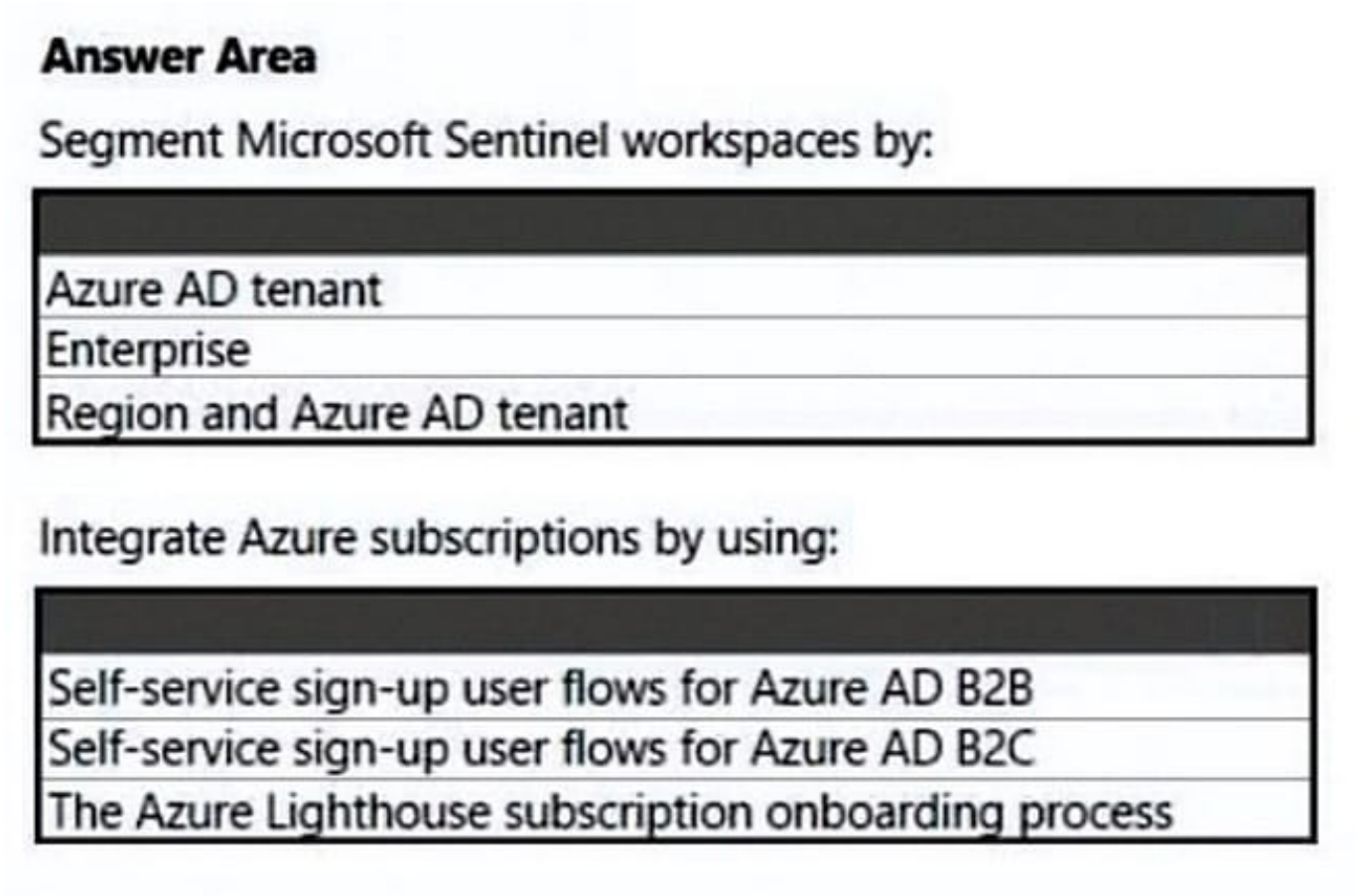
HOTSPOT

You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.

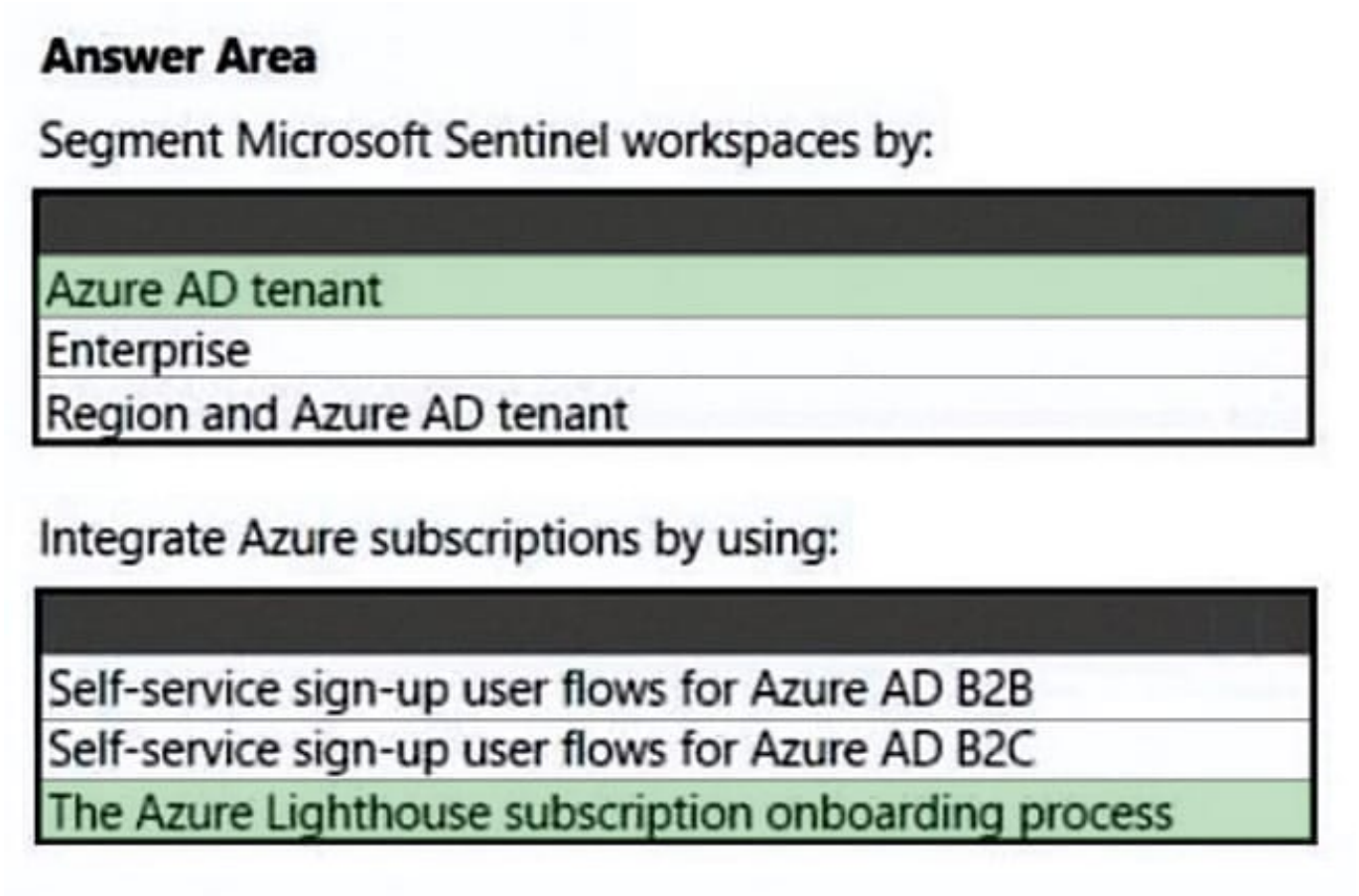
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Azure tenant

Microsoft Sentinel multiple workspace architecture

There are cases where a single SOC (Security Operations Center) needs to centrally manage and monitor multiple Microsoft Sentinel workspaces, potentially across Azure Active Directory (Azure AD) tenants.

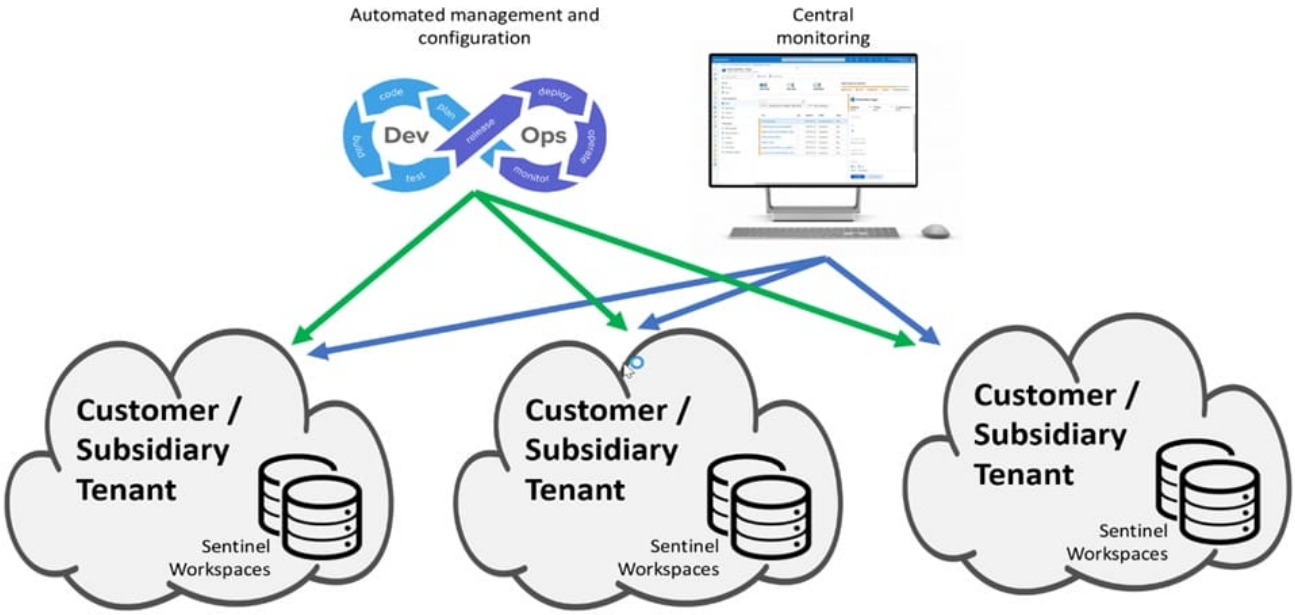
An MSSP Microsoft Sentinel Service.

A global SOC serving multiple subsidiaries, each having its own local SOC.

A SOC monitoring multiple Azure AD tenants within an organization.

To address these cases, Microsoft Sentinel offers multiple-workspace capabilities that enable central monitoring, configuration, and management, providing a single pane of glass across everything covered by the SOC. This diagram shows

an example architecture for such use cases.



This model offers significant advantages over a fully centralized model in which all data is copied to a single workspace.

Scenario:

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.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Box 2: Azure Lighthouse subscription onboarding process

You can use Azure Lighthouse to extend all cross-workspace activities across tenant boundaries, allowing users in your managing tenant to work on Microsoft Sentinel workspaces across all tenants.

Azure Lighthouse enables you to see and manage Azure resources from different tenancies, in the one place, with the power of delegated administration. That tenancy may be a customer (for example, if you\\'re a managed services provider

with a support contract arrangement in place), or a separate Azure environment for legal or financial reasons (like franchisee groups or Enterprises with large brand groups).

Incorrect:

* not Azure AD B2B

Azure AD B2B uses guest account, which goes against the requirements in this scenario,

Note: Azure Active Directory (Azure AD) B2B collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants
https://docs.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture
https://techcommunity.microsoft.com/t5/itops-talk-blog/onboarding-to-azure-lighthouse-using-a-template/ba-p/1091786
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

QUESTION 2

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

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

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

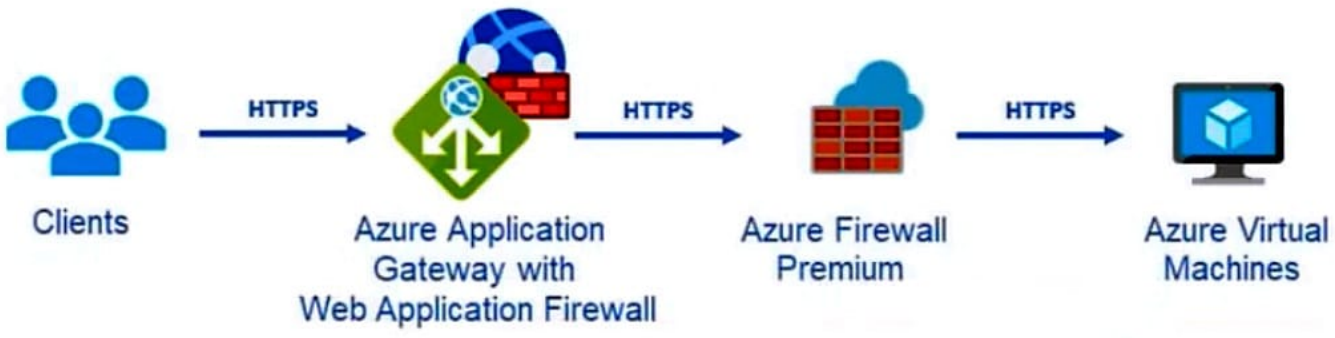
Correct Answer: B

QUESTION 3

HOTSPOT

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel.

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



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

1.

Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.

2.

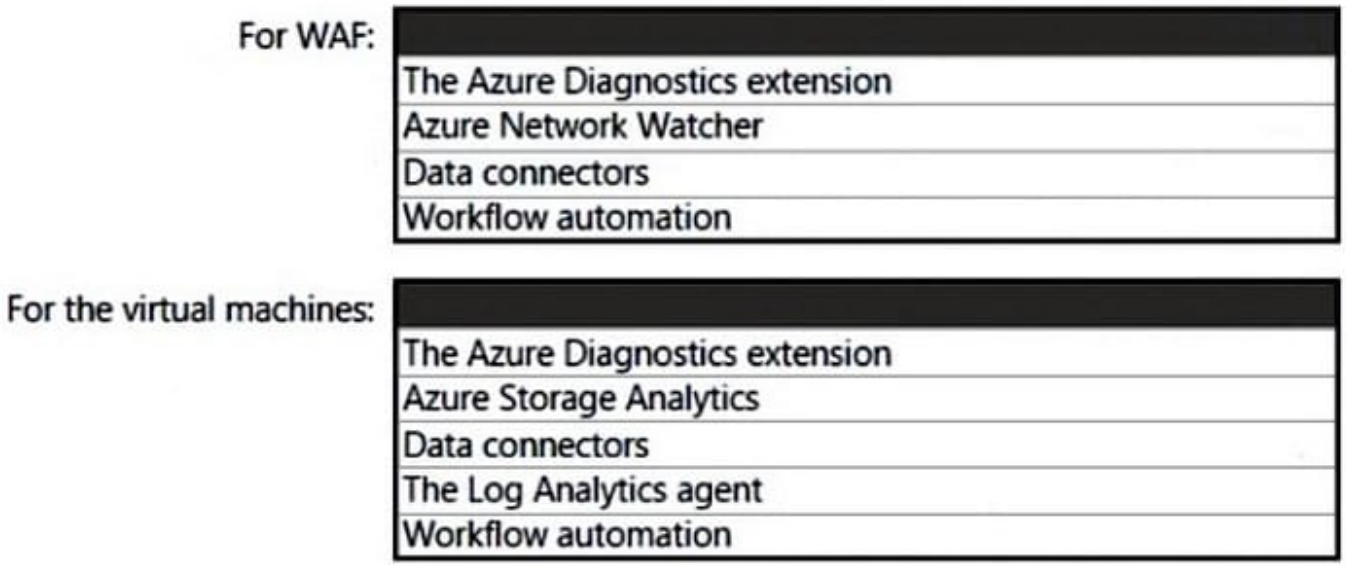
Use Defender for Cloud to review alerts from the virtual machines.

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

NOTE: Each correct selection is worth one point.

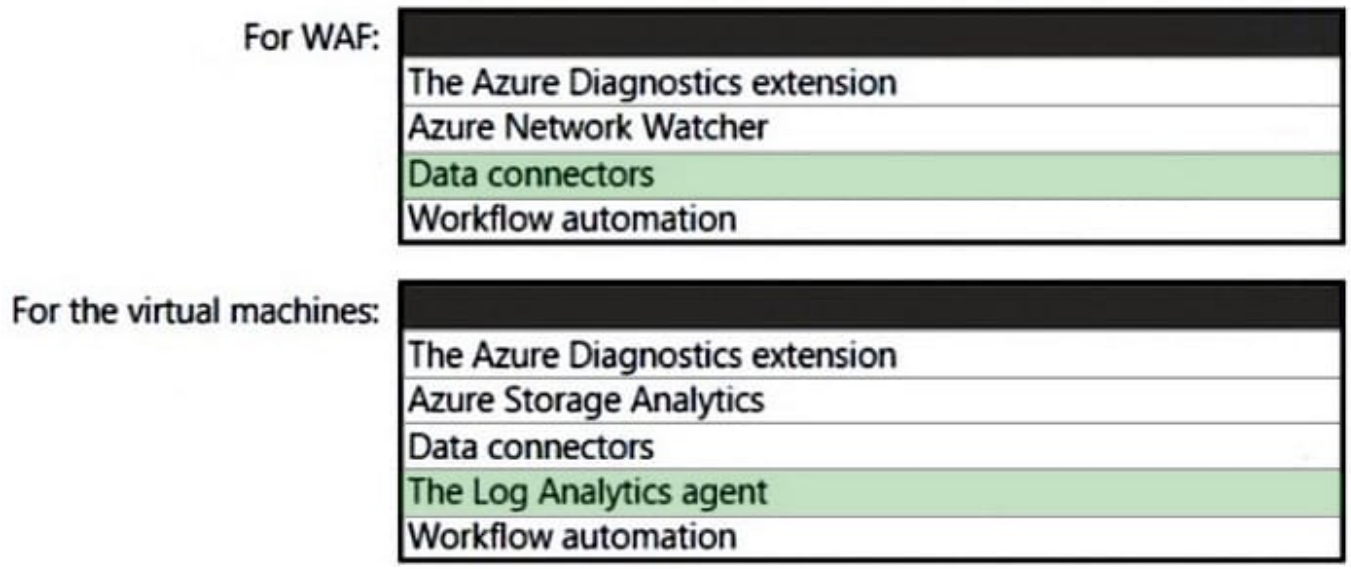
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Data connectors

Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel.

Launch a WAF workbook (see step 7 below)

The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource.

To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:

1.

Select Diagnostic settings.

2.

Select + Add diagnostic setting.

3.

In the Diagnostic setting page (details skipped)

4.

On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.

5.

Select an already active workspace or create a new workspace.

6.

On the left side panel under Configuration select Data Connectors.

7.

Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.

8.

Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven\\'t done so previously.

9.

Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent

Use the Log Analytics agent to integrate with Microsoft Defender for cloud.

Windows agents

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

QUESTION 4

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 5

You design cloud-based software as a service (SaaS) solutions.

You need to recommend a recovery solution for ransomware attacks. The solution must follow Microsoft Security Best Practices.

What should you recommend doing first?

A. Develop a privileged identity strategy.

B. Implement data protection.

C. Develop a privileged access strategy.

D. Prepare a recovery plan.

Correct Answer: D

Recommend a ransomware strategy by using Microsoft Security Best Practices The three important phases of ransomware protection are:

*

create a recovery plan

*

limit the scope of damage

*

harden key infrastructure elements

Plan for ransomware protection and extortion-based attacks Phase 1 of ransomware protection is to develop a recovery plan. The first thing you should do for these attacks is prepare your organization so that it has a viable alternative to paying the ransom. While attackers in control of your organization have a variety of ways to pressure you into paying, the demands

primarily focus on two categories:

Pay to regain access

Pay to avoid disclosure

Reference:

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/

https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/2-plan-for-ransomware-protection-extortion-based-attacks