SC-100Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

https://www.pass2lead.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

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator

authorizes the application.

Which security control should you recommend?

A. Azure AD Conditional Access App Control policies

B. Azure Security Benchmark compliance controls in Defender for Cloud

C. app protection policies in Microsoft Endpoint Manager

D. application control policies in Microsoft Defender for Endpoint

Correct Answer: D

Explanation:

Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

Note: Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC.

Incorrect:

Not C: App protection policies (APP) are rules that ensure an organization\\'s data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of

actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.

Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization\\'s data within an application. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy

QUESTION 2

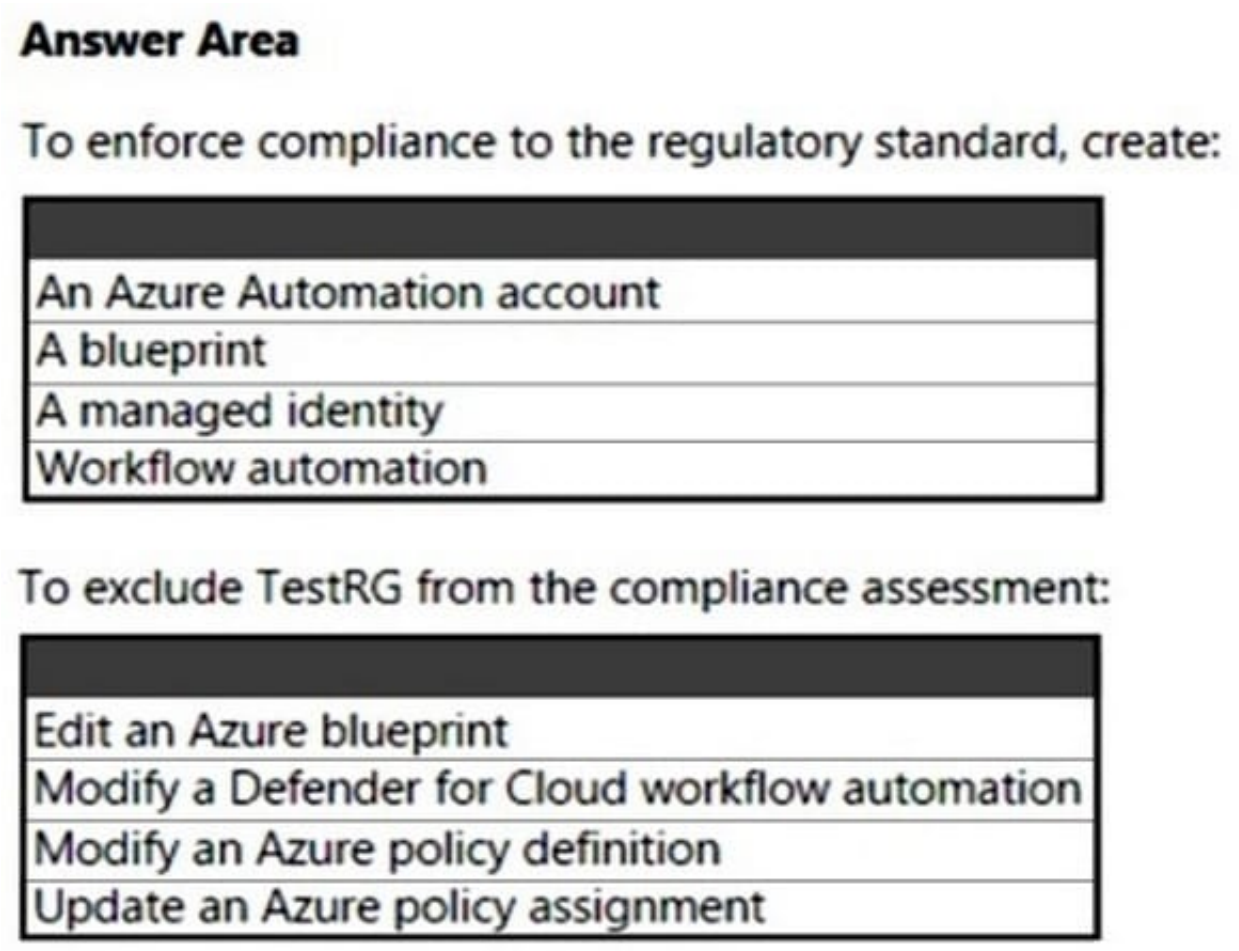
HOTSPOT

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

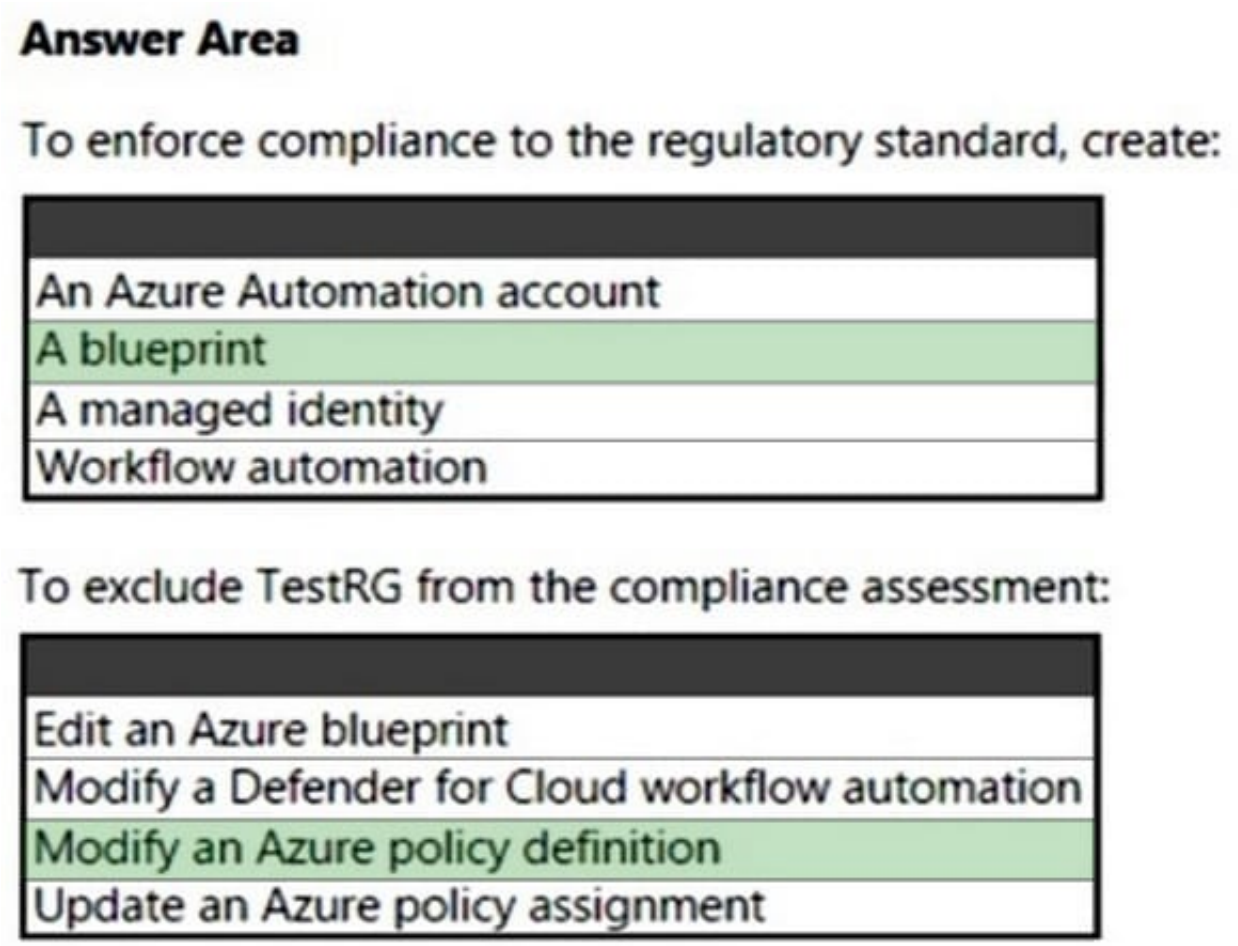
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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 3

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices.

You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

A. controlled folder access

B. application isolation

C. memory scanning

D. machine isolation

E. user isolation

Correct Answer: D

Explanation:

If a ransomware attack is detected the affected entity should immediately activate its security incident response plan, which should include measures to isolate the infected computer systems in order to halt propagation of the attack.

Note: Isolate devices from the network

Depending on the severity of the attack and the sensitivity of the device, you might want to isolate the device from the network. This action can help prevent the attacker from controlling the compromised device and performing further activities

such as data exfiltration and lateral movement.

Reference:

https://csrc.nist.gov/CSRC/media/Presentations/Ransomware-and-Breach/images-media/ransomware_guidance.pdf

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide#isolate-devices-from-the-network

---

QUESTION 4

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

You have an Amazon Web Services (AWS) implementation.

You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc.

Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Containers

B. Microsoft Defender for servers

C. Azure Active Directory (Azure AD) Conditional Access

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

E. Azure Policy

Correct Answer: ACE

Environment settings page (in preview) (recommended) - This preview page provides a greatly improved, simpler, onboarding experience (including auto provisioning). This mechanism also extends Defender for Cloud\\'s enhanced security features to your AWS resources:

*(A) Microsoft Defender for Containers brings threat detection and advanced defenses to your Amazon EKS clusters. This plan includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control

recommendations and more.

* Microsoft Defender for Servers, though it requires Arc.

C: AWS installations can benefit from Conditional Access. Defender for Cloud Apps integrates with Azure AD Conditional Access to enforce additional restrictions, and monitors and protects sessions after sign-in. Defender for Cloud Apps

uses user behavior analytics (UBA) and other AWS APIs to monitor sessions and users and to support information protection.

E: Kubernetes data plane hardening.

For a bundle of recommendations to protect the workloads of your Kubernetes containers, install the Azure Policy for Kubernetes. You can also auto deploy this component as explained in enable auto provisioning of agents and extensions.

With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure to enforce the best practices and

mandate them for future workloads.

Incorrect:

Not B: To enable the Defender for Servers plan you need Azure Arc for servers installed on your EC2 instances.

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

https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-security-solutions

QUESTION 5

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 6

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.

You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

A. Azure Monitor webhooks

B. Azure Logics Apps

C. Azure Event Hubs

D. Azure Functions apps

Correct Answer: B

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

QUESTION 7

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

---

QUESTION 8

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 9

HOTSPOT

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

You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

1.

A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers

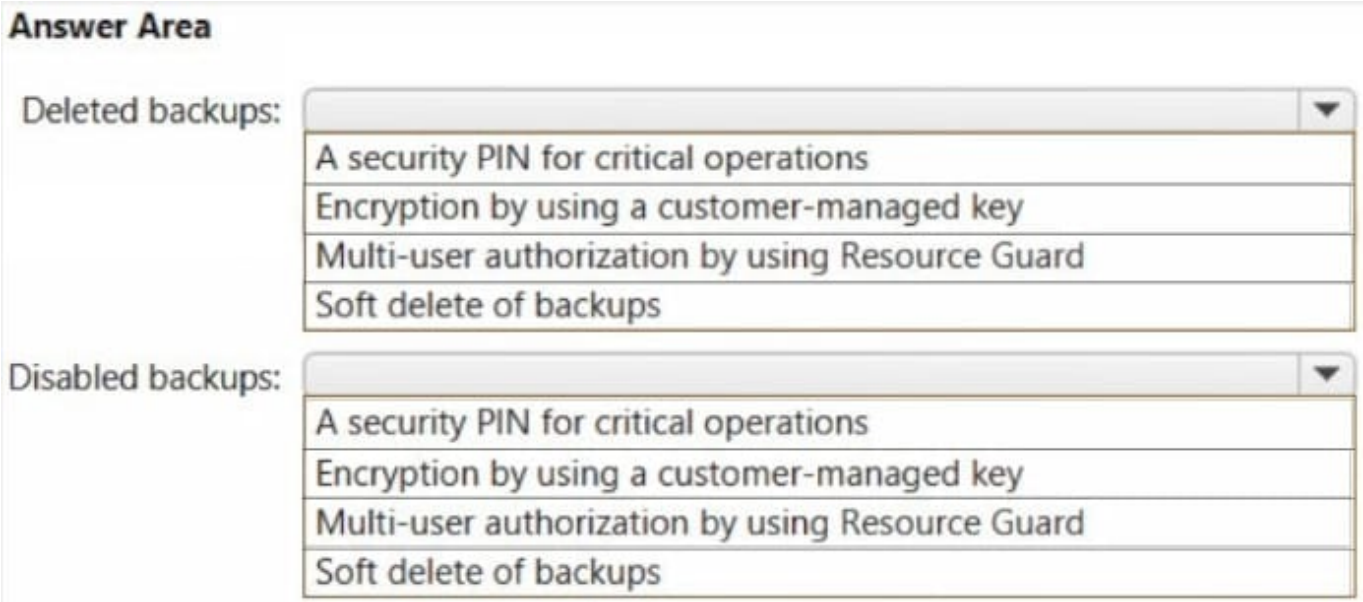
2.

A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

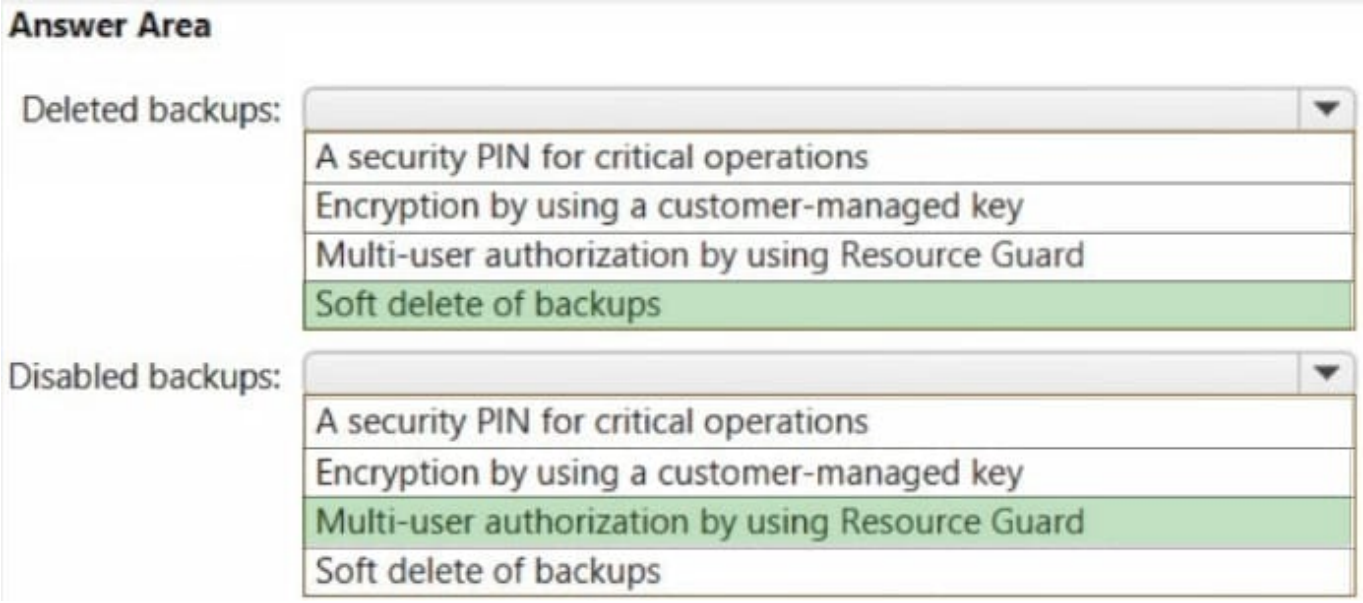
What should you use for each risk? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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

---

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

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

A. From Microsoft Defender for Endpoint, perform a security scan.

B. Recover files to a cleaned computer or device.

C. Contact law enforcement.

D. Disable Microsoft OneDrive sync and Exchange ActiveSync.

Correct Answer: D

The following containment steps can be done concurrently as new threat vectors are discovered.

Step 1: Assess the scope of the situation

Which user accounts were compromised?

Which devices are affected? Which applications are affected? Step 2: Preserve existing systems

*

Disable all privileged user accounts except for a small number of accounts used by your admins to assist in resetting the integrity of your AD DS infrastructure. If a user account is believed to be compromised, disable it immediately.

*

Isolate compromised systems from the network, but do not shut them off.

*

Etc.

Note:

With OneDrive, you can sync files between your computer and the cloud, so you can get to your files from anywhere - your computer, your mobile device, and even through the OneDrive website at OneDrive.com.

ActiveSync is a client protocol that lets users synchronize their Exchange mailbox with a mobile device.

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

QUESTION 12

Your company has an Azure subscription that uses Azure Storage.

The company plans to share specific blobs with vendors.

You need to recommend a solution to provide the vendors with secure access to specific blobs without exposing the blobs publicly. The access must be time-limited.

What should you include in the recommendation?

A. Configure private link connections.

B. Configure encryption by using customer-managed keys (CMKs).

C. Share the connection string of the access key.

D. Create shared access signatures (SAS).

Correct Answer: D

A shared access signature (SAS) provides secure delegated access to resources in your storage account. With a SAS, you have granular control over how a client can access your data. For example:

What resources the client may access.

What permissions they have to those resources.

How long the SAS is valid.

Types of shared access signatures

Azure Storage supports three types of shared access signatures:

User delegation SAS

Service SAS

Account SAS

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

QUESTION 13

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD)

The customer plans to obtain an Azure subscription and provision several Azure resources.

You need to evaluate the customer\\'s security environment.

What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

A. Azure AD Privileged Identity Management (PIM)

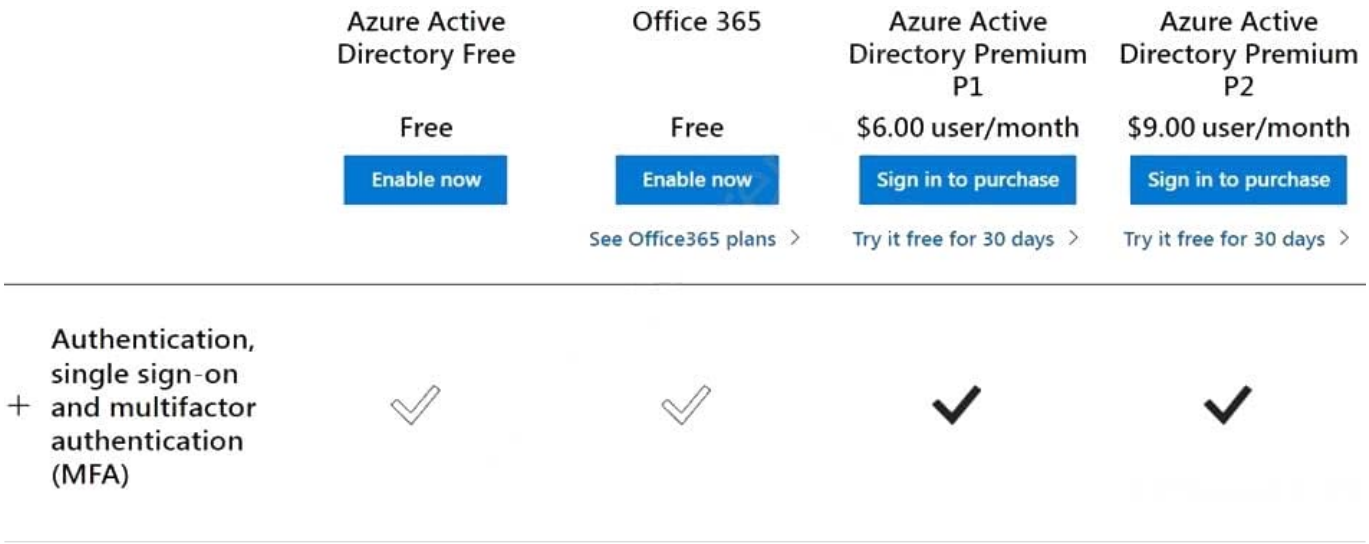
B. role-based authorization

C. resource-based authorization

D. Azure AD Multi-Factor Authentication

Correct Answer: D

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



QUESTION 14

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

Correct Answer: D

Microsoft Sentinel is a scalable, cloud-native solution that provides:

Security information and event management (SIEM)

Security orchestration, automation, and response (SOAR)

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, you get a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Microsoft Sentinel is your bird\\'s-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously undetected threats, and minimize false positives using Microsoft\\'s analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Microsoft Sentinel natively incorporates proven Azure services, like Log Analytics and Logic Apps. Microsoft Sentinel enriches your investigation and detection with AI. It provides Microsoft\\'s threat intelligence stream and enables you to bring

your own threat intelligence.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/overview

QUESTION 15

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

Correct Answer: D

ExpressRoute provides direct connectivity to Azure cloud services and connecting Microsoft\\'s global network. All transferred data is not encrypted, and do not go over the public Internet. VPN Gateway provides secured connectivity to Azure

cloud services over public Internet.

Note:

Litware identifies the following landing zone requirements:

1.

Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

2.

Provide a secure score scoped to the landing zone.

3.

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.

4.

Minimize the possibility of data exfiltration.

5.

Maximize network bandwidth.

Litware identifies the following business requirements:

1.

Minimize any additional on-premises infrastructure.

2.

Minimize the operational costs associated with administrative overhead.

Reference: https://medium.com/awesome-azure/azure-difference-between-azure-expressroute-and-azure-vpn-gateway-comparison-azure-hybrid-connectivity-5f7ce02044f3