Vendor: Microsoft

Exam Code:SC-100

Exam Name: Microsoft Cybersecurity Architect

Version: Demo

QUESTION 1

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.

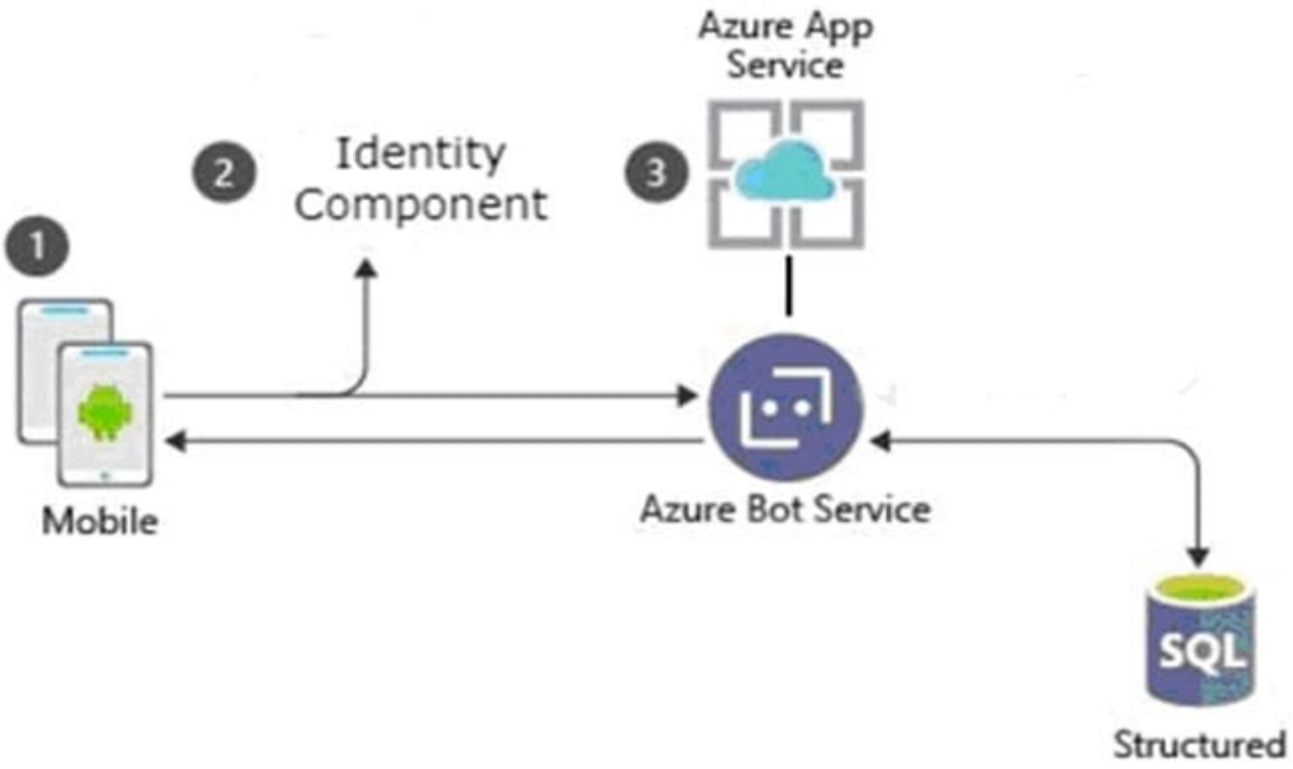
OS Packages Supported

- 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 2

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:

1.

Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.

2.

Be managed separately from the identity store of the customer.

3.

Support fully customizable branding for each app. Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2B

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD) B2C

D. Azure AD Connect

Correct Answer: C

Azure Active Directory B2C (Azure AD B2C), an identity store, is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page

(SPA), and other applications.

You can set up sign-up and sign-in with a Facebook/Google account using Azure Active Directory B2C.

Branding

Branding and customizing the user interface that Azure Active Directory B2C (Azure AD B2C) displays to your customers helps provide a seamless user experience in your application. These experiences include signing up, signing in, profile

editing, and password resetting. This article introduces the methods of user interface (UI) customization.

Incorrect:

Not D: Azure AD Connect is a tool for connecting on-premises identity infrastructure to Microsoft Azure AD.

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

https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow

https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

---

QUESTION 3

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

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

You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Note: Secure management ports - Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups. Recommendations:

-Internet-facing virtual machines should be protected with network security groups

-

Management ports of virtual machines should be protected with just-in-time network access control

-

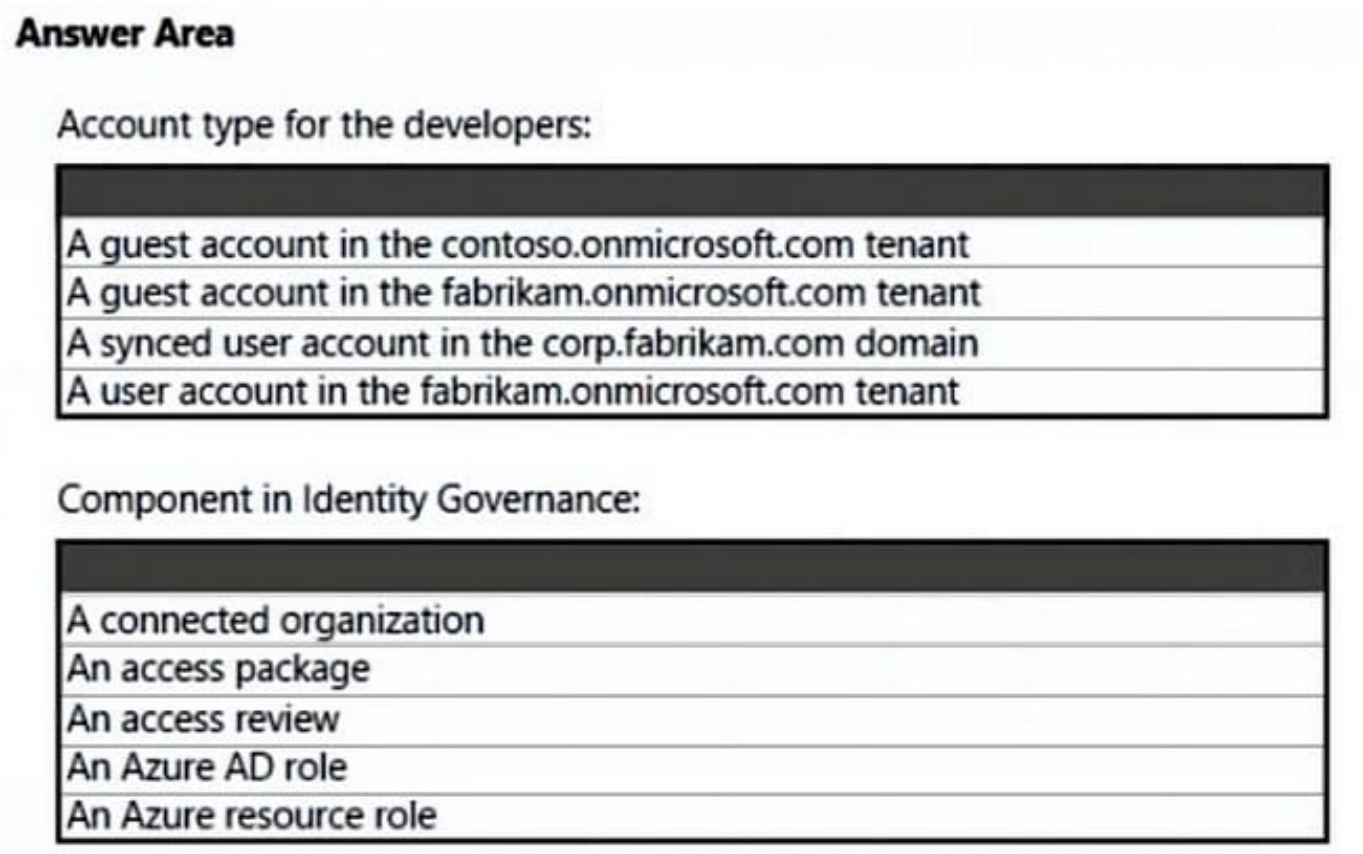
Management ports should be closed on your virtual machines Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

---

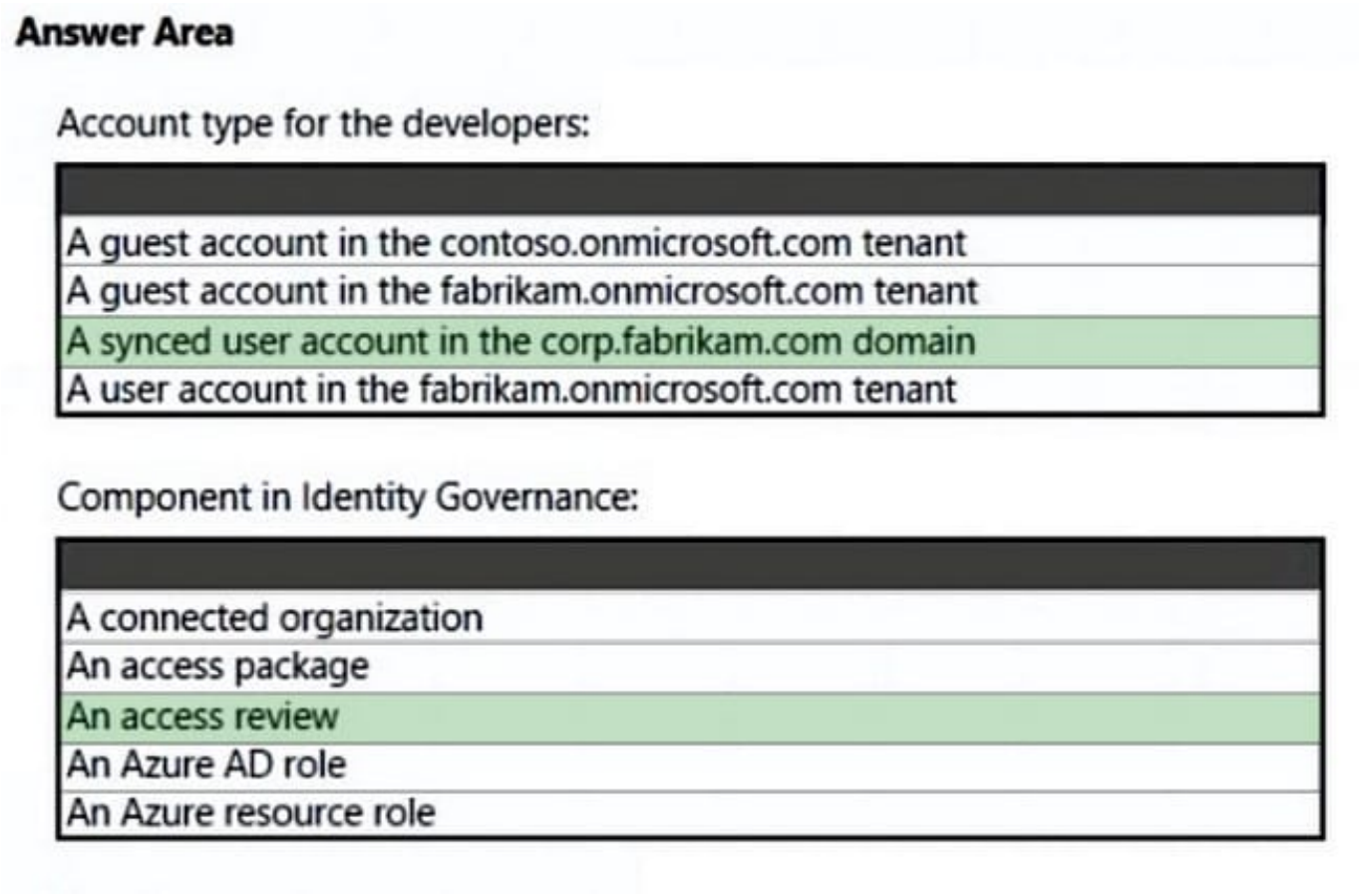
QUESTION 4

What should you create in Azure AD to meet the Contoso developer requirements?

Hot Area:



Correct Answer:



Box 1: A synced user account

Need to use a synched user account.

Incorrect:

*

Not A user account in the fabrikam.onmicrosoft.com tenant

The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.

*

Guest accounts would not meet the requirements.

Note: 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 ContosoDevelopers 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.

Contoso Developers 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 Contoso developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Box 2: An access review

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

Azure Active Directory (Azure AD) 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 Azure AD Identity 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

---

QUESTION 5

You have Microsoft Defender for Cloud assigned to Azure management groups.

You have a Microsoft Sentinel deployment.

During the triage of alerts, you require additional information about the security events, including suggestions for remediation.

Which two components can you use to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel threat intelligence workbooks

B. Microsoft Sentinel notebooks

C. threat intelligence reports in Defender for Cloud

D. workload protections in Defender for Cloud

Correct Answer: AC

A: Workbooks provide insights about your threat intelligence

Workbooks provide powerful interactive dashboards that give you insights into all aspects of Microsoft Sentinel, and threat intelligence is no exception. You can use the built-in Threat Intelligence workbook to visualize key information about

your threat intelligence, and you can easily customize the workbook according to your business needs. You can even create new dashboards combining many different data sources so you can visualize your data in unique ways. Since

Microsoft Sentinel workbooks are based on Azure Monitor workbooks, there is already extensive documentation available, and many more templates.

C: What is a threat intelligence report?

Defender for Cloud\\'s threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to

identify threats.

Defender for Cloud has three types of threat reports, which can vary according to the attack. The reports available are:

Activity Group Report: provides deep dives into attackers, their objectives, and tactics.

Campaign Report: focuses on details of specific attack campaigns.

Threat Summary Report: covers all of the items in the previous two reports.

This type of information is useful during the incident response process, where there\\'s an ongoing investigation to understand the source of the attack, the attacker\\'s motivations, and what to do to mitigate this issue in the future.

Incorrect:

Not B: When to use Jupyter notebooks

While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data.

For example, use notebooks to:

Perform analytics that aren\\'t provided out-of-the box in Microsoft Sentinel, such as some Python machine learning features

Create data visualizations that aren\\'t provided out-of-the box in Microsoft Sentinel, such as custom timelines and process trees

Integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

Not D: Defender for Cloud offers security alerts that are powered by Microsoft Threat Intelligence. It also includes a range of advanced, intelligent, protections for your workloads. The workload protections are provided through Microsoft

Defender plans specific to the types of resources in your subscriptions. For example, you can enable Microsoft Defender for Storage to get alerted about suspicious activities related to your Azure Storage accounts.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports https://docs.microsoft.com/en-us/azure/sentinel/notebooks

---

QUESTION 6

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

A. Azure Firewall

B. Azure Web Application Firewall (WAF)

C. Microsoft Defender for Cloud alerts

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

E. Microsoft Sentinel

Correct Answer: AB

This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secure score. Sentinel and PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.

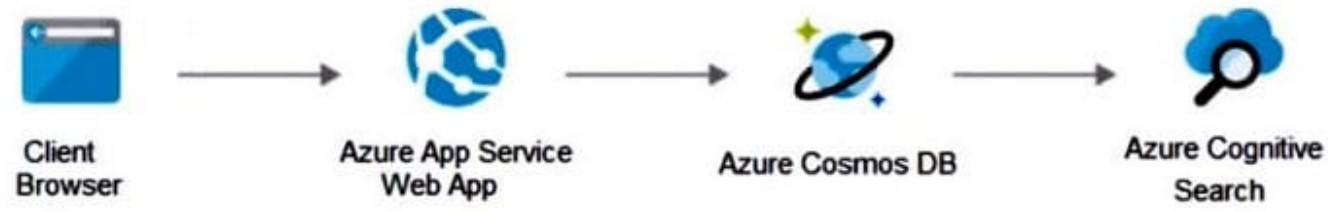
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

---

QUESTION 7

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

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



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

Solution: You recommend implementing Azure Key Vault to store credentials.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead use solution: You recommend creating private endpoints for the web app and the database layer.

Note:

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

As an Azure administrator or architect, you are sometimes asked the question: “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 8

Your company has a Microsoft 365 ES subscription.

The Chief Compliance Officer plans to enhance privacy management in the working environment.

You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:

1.

Identify unused personal data and empower users to make smart data handling decisions.

2.

Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.

3.

Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

Correct Answer: C

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

guides and can help you:

Detect overexposed personal data so that users can secure it.

Spot and limit transfers of personal data across departments or regional borders.

Help users identify and reduce the amount of unused personal data that you store.

Incorrect:

Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the

day for uninterrupted, individual work.

Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export

content that\\'s responsive to your organization\\'s internal and external investigations.

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

---

QUESTION 9

HOTSPOT

You open Microsoft Defender for Cloud as shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Azure AD Conditional Access policies
Azure Web Application Firewall (WAF)
network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement **[answer choice]**.

Microsoft Defender for Resource Manager
Microsoft Defender for servers
private endpoints

Correct Answer:

Answer Area

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

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

Box 1: Azure Web Application Firewall (WAF)

Restrict unauthorized network access control: 1 resource out of 11 needs to be addresses.

Restrict unauthorized network access - Azure offers a suite of tools designed to ensure accesses across your network meet the highest security standards.

Use these recommendations to manage Defender for Cloud\\'s adaptive network hardening settings, ensure you configured Azure Private Link for all relevant PaaS services, enable Azure Firewall on your virtual networks, and more.

Note: Azure Web Application Firewall (WAF) is an optional addition to Azure Application Gateway.

Azure WAF protects inbound traffic to the web workloads, and the Azure Firewall inspects inbound traffic for the other applications. The Azure Firewall will cover outbound flows from both workload types.

Incorrect:

Not network security groups (NSGs).

Box 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization\\'s endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn\\'t found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).

Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they\\'re performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity. Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

---

QUESTION 10

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 11

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.

You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

A. unit testing

B. penetration testing

C. dependency checks

D. threat modeling

Correct Answer: B

Dynamic application security testing (DAST)

In a classical waterfall development model, security was typically introduced at the last step, right before going to production. One of the most popular security approaches is penetration testing or pen testing. Penetration testing lets a team

look at the application from a black-box security perspective, as in, closest to an attacker mindset.

Reference:

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

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

---

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.

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

Allow | Deny

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