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.passapply.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: B

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

QUESTION 2

DRAG DROP

You have a Microsoft 365 subscription.

You need to recommend a security solution to monitor the following activities:

1.

User accounts that were potentially compromised

2.

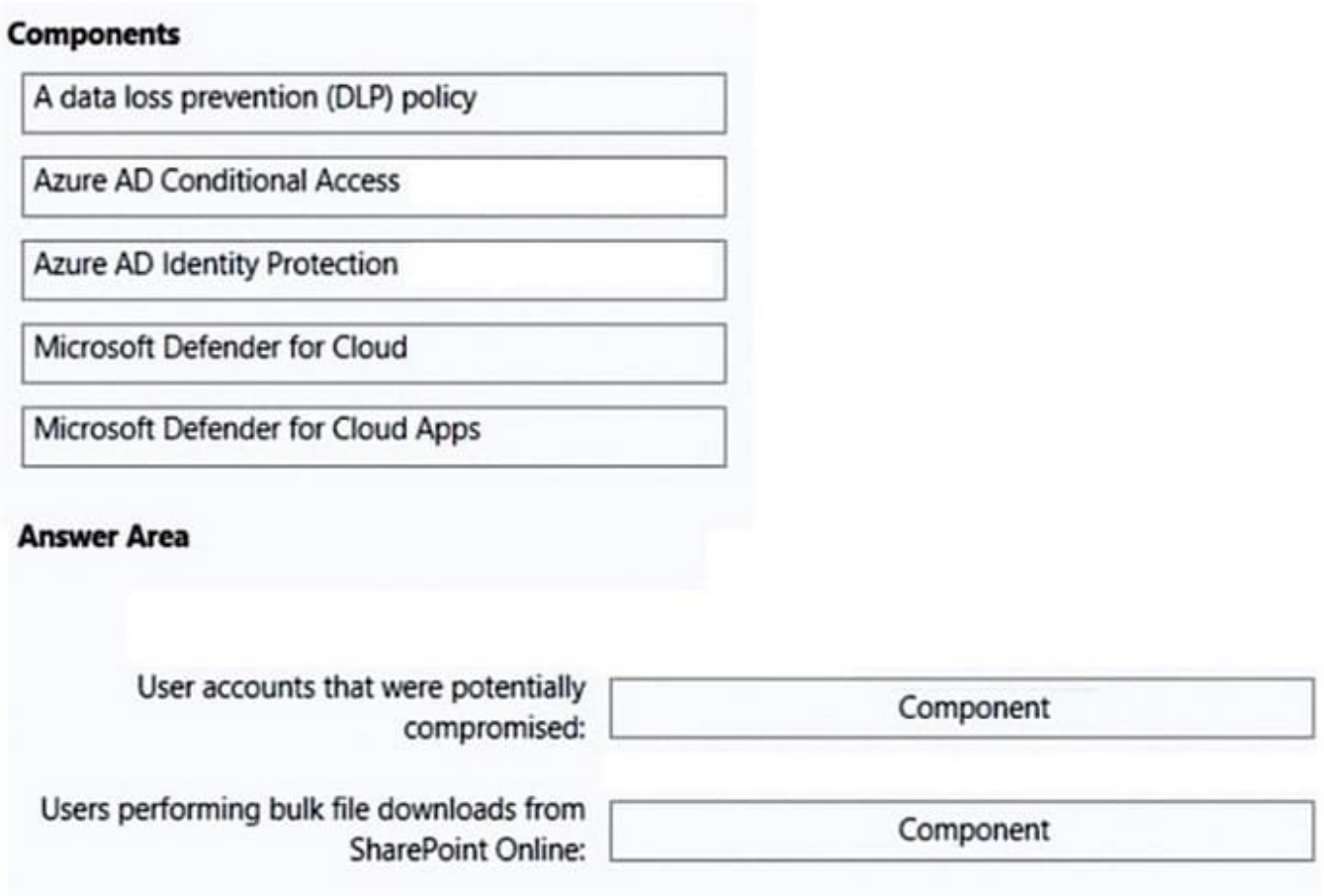
Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component may be used once, more than once, or not at all. You may need to drag the split bar

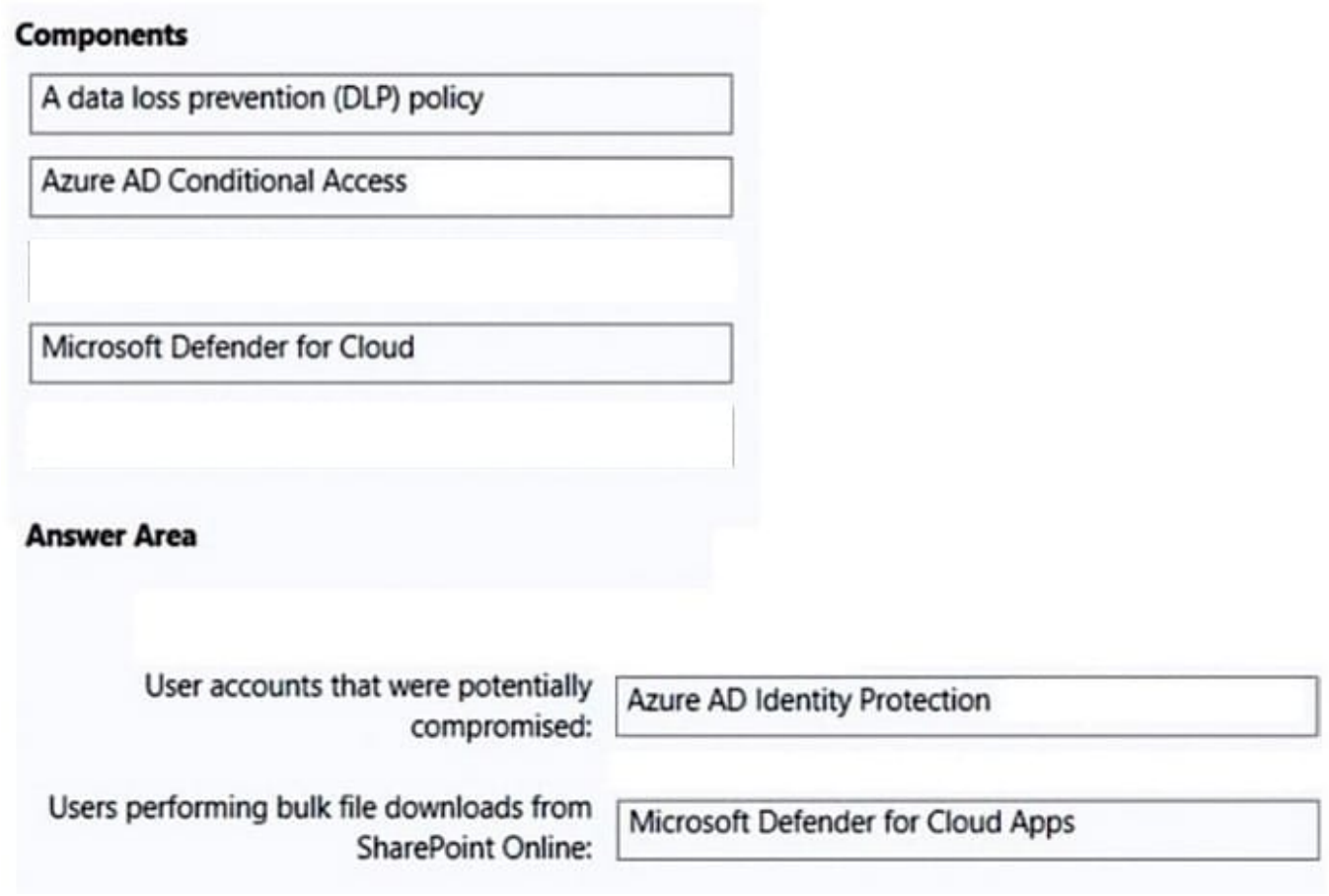
between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Azure Active Directory (Azure AD) Identity Protection

Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory. Risk detections (both user and sign-in linked) contribute to the overall user risk score that is found in the Risky

Users report.

Identity Protection provides organizations access to powerful resources to see and respond quickly to these suspicious actions.

Note:

Premium sign-in risk detections include:

*

Token Issuer Anomaly - This risk detection indicates the SAML token issuer for the associated SAML token is potentially compromised. The claims included in the token are unusual or match known attacker patterns.

*

Suspicious inbox manipulation rules - This detection is discovered by Microsoft Defender for Cloud Apps. This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user\\'s inbox. This detection may indicate that the user\\'s account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.

*

Etc.

Incorrect:

Not: Microsoft 365 Defender for Cloud

Part of your incident investigation can include user accounts. You can see the details of user accounts identified in the alerts of an incident in the Microsoft 365 Defender portal from Incidents and alerts > incident > Users.

Box 2: Microsoft 365 Defender for App

Defender for Cloud apps detect mass download (data exfiltration) policy

Detect when a certain user accesses or downloads a massive number of files in a short period of time.

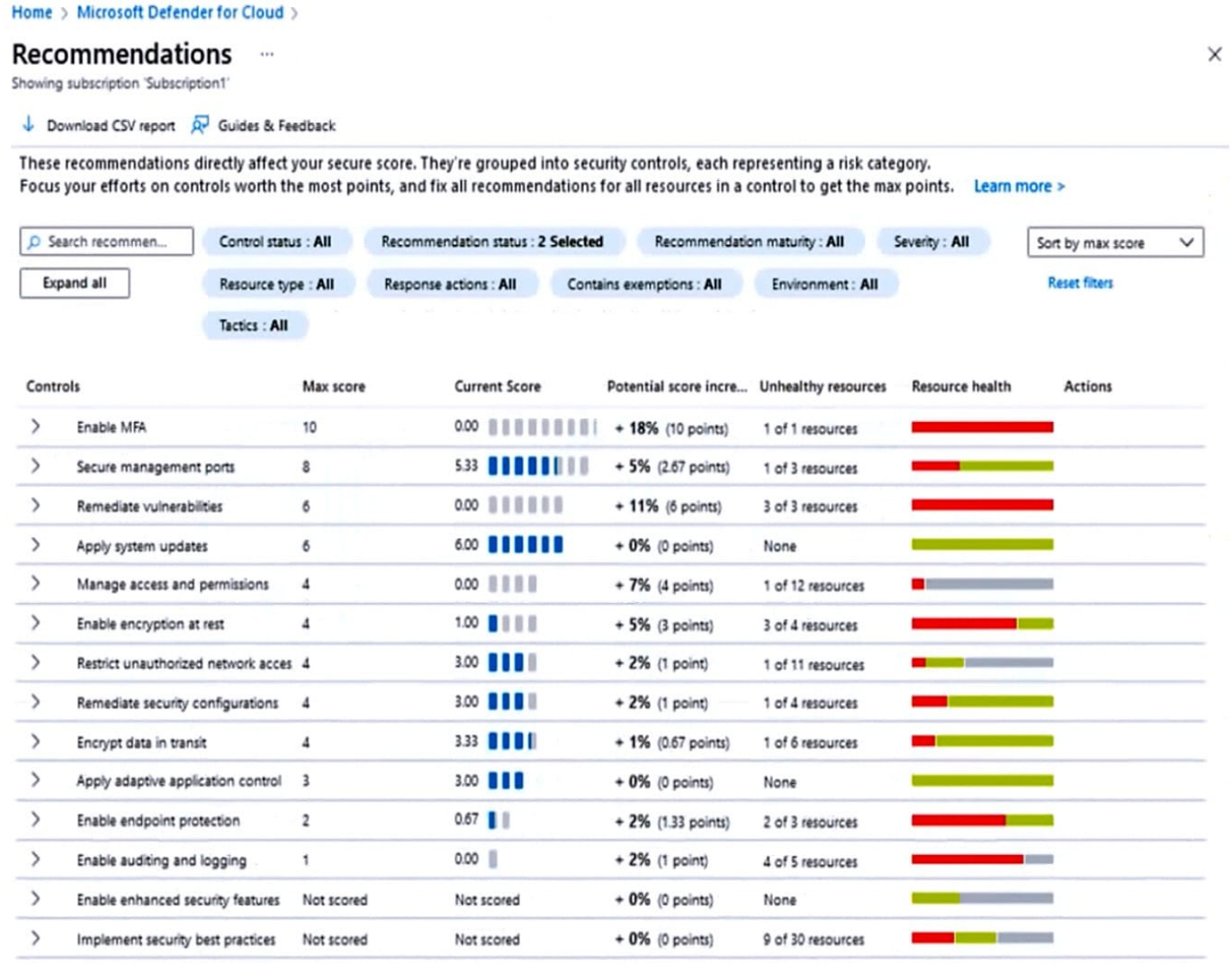
Reference: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exfiltration
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

---

QUESTION 3

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]**.

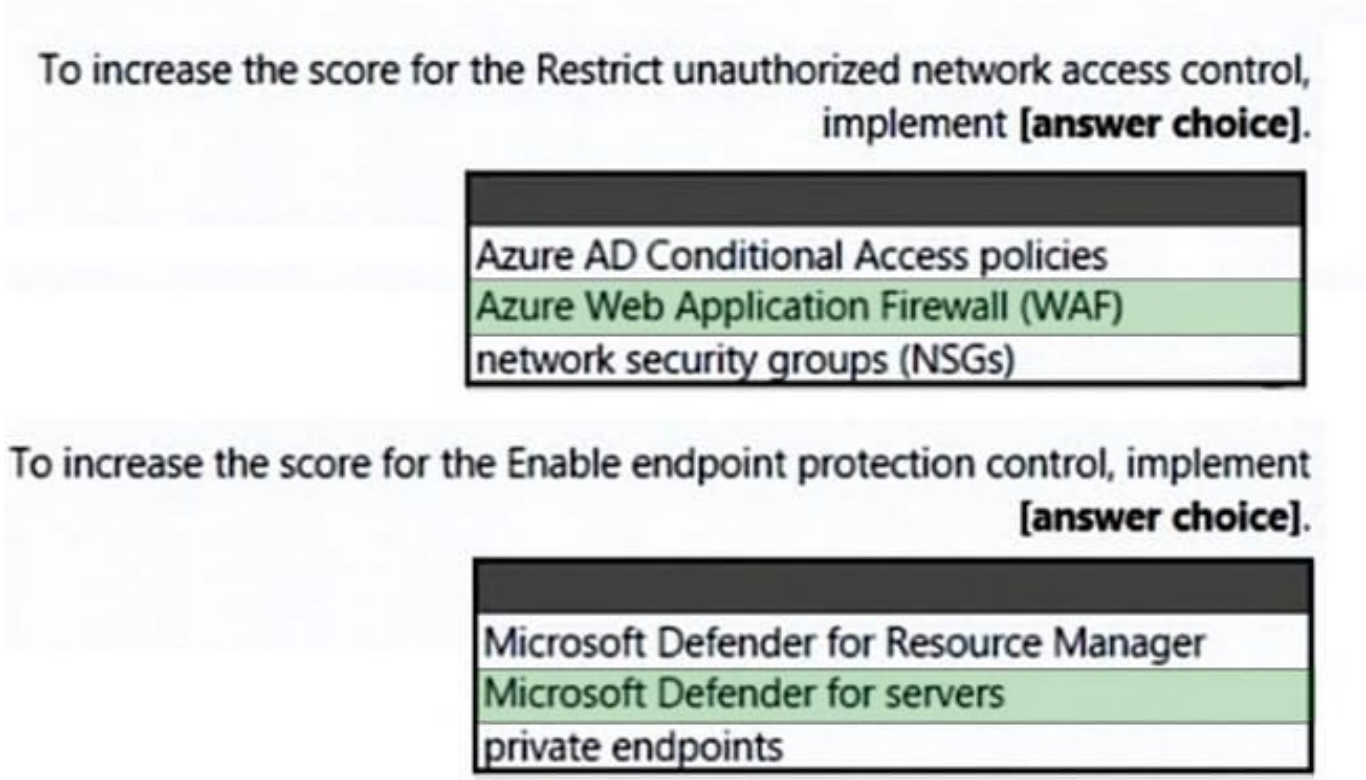
Azure AD Conditional Access policies
Azure Web Application Firewall (WAF)
network security groups (NSGs)

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



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 4

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel.

You plan to integrate Microsoft Sentinel with Splunk.

You need to recommend a solution to send security events from Microsoft Sentinel to Splunk.

What should you include in the recommendation?

A. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

Correct Answer: A

Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP Data Collector API. Reference: https://splunkbase.splunk.com/app/5312/

QUESTION 5

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials.

You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials.

What should you include in the recommendation?

A. Azure AD Application Proxy

B. Azure AD B2C

C. an Azure AD enterprise application

D. a relying party trust in Active Directory Federation Services (AD FS)

Correct Answer: A

SC-100 VCE Dumps SC-100 Exam Questions SC-100 Braindumps