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

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

QUESTION 1

Your company is developing a modern application that will un as an Azure App Service web app.

You plan to perform threat modeling to identity potential security issues by using the Microsoft Threat Modeling Tool.

Which type of diagram should you create?

A. data flow

B. system flow

C. process flow

D. network flow

Correct Answer: A

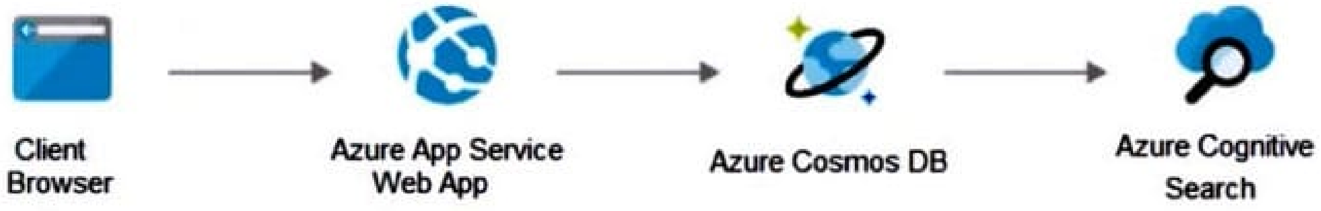
A data-flow diagram is a way of representing a flow of data through a process or a system (usually an information system). The DFD also provides information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow — there are no decision rules and no loops. Specific operations based on the data can be represented by a flowchart.[1]

Data flow diagram with data storage, data flows, function and interface

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.

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 3

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware.

The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. The client access tokens are refreshed.

B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. Microsoft Defender for Endpoint reports the endpoints as compliant.

Correct Answer: AC

A: When a client acquires an access token to access a protected resource, the client also receives a refresh token. The refresh token is used to obtain new access/refresh token pairs when the current access token expires. Refresh tokens

are also used to acquire extra access tokens for other resources.

Refresh token expiration

Refresh tokens can be revoked at any time, because of timeouts and revocations.

C: Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. It uses a combination of endpoint behavioral sensors, cloud

security analytics, and threat intelligence.

The interviewees said that “by implementing Zero Trust architecture, their organizations improved employee experience (EX) and increased productivity.” They also noted, “increased device performance and stability by managing all of their endpoints with Microsoft Endpoint Manager.” This had a bonus effect of reducing the number of agents installed on a user\\'s device, thereby increasing device stability and performance. “For some organizations, this can reduce boot times from 30 minutes to less than a minute,” the study states. Moreover, shifting to Zero Trust moved the burden of security away from users. Implementing single sign-on (SSO), multifactor authentication (MFA), leveraging passwordless authentication, and eliminating VPN clients all further reduced friction and improved user productivity.

Note: Azure AD at the heart of your Zero Trust strategy Azure AD provides critical functionality for your Zero Trust strategy. It enables strong authentication, a point of integration for device security, and the core of your user-centric policies to guarantee least-privileged access. Azure AD\\'s Conditional Access capabilities are the policy decision point for access to resource

Reference: https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/ https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

QUESTION 4

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. Azure SQL Managed Instance

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

D. SQL Server on Azure Virtual Machines

Correct Answer: C

Azure SQL Database is a general-purpose relational database, provided as a managed service. Categorized as a platform as a service (PaaS), Azure SQL Databases are built on standardized hardware and software that is owned, hosted, and maintained by Microsoft. When using Azure SQL Database, you pay-as-you-go, with the option to scale up or out with no service interruption.

Within Azure SQL Database, you have the option to deploy a managed instance. Azure SQL Database Managed Instance is a collection of system and user databases with a shared set of resources. In addition to all the PaaS benefits of Azure SQL Database, this option provides a native virtual network (VNet) and near 100 percent compatibility with on-premises SQL Server. Azure SQL Database Managed Instance provides you with full SQL Server access and feature compatibility for migrating SQL Servers to Azure.

Recommendation: Choose Azure SQL Database for your modern cloud applications, or when you have time constraints in development and marketing.

QUESTION 5

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.

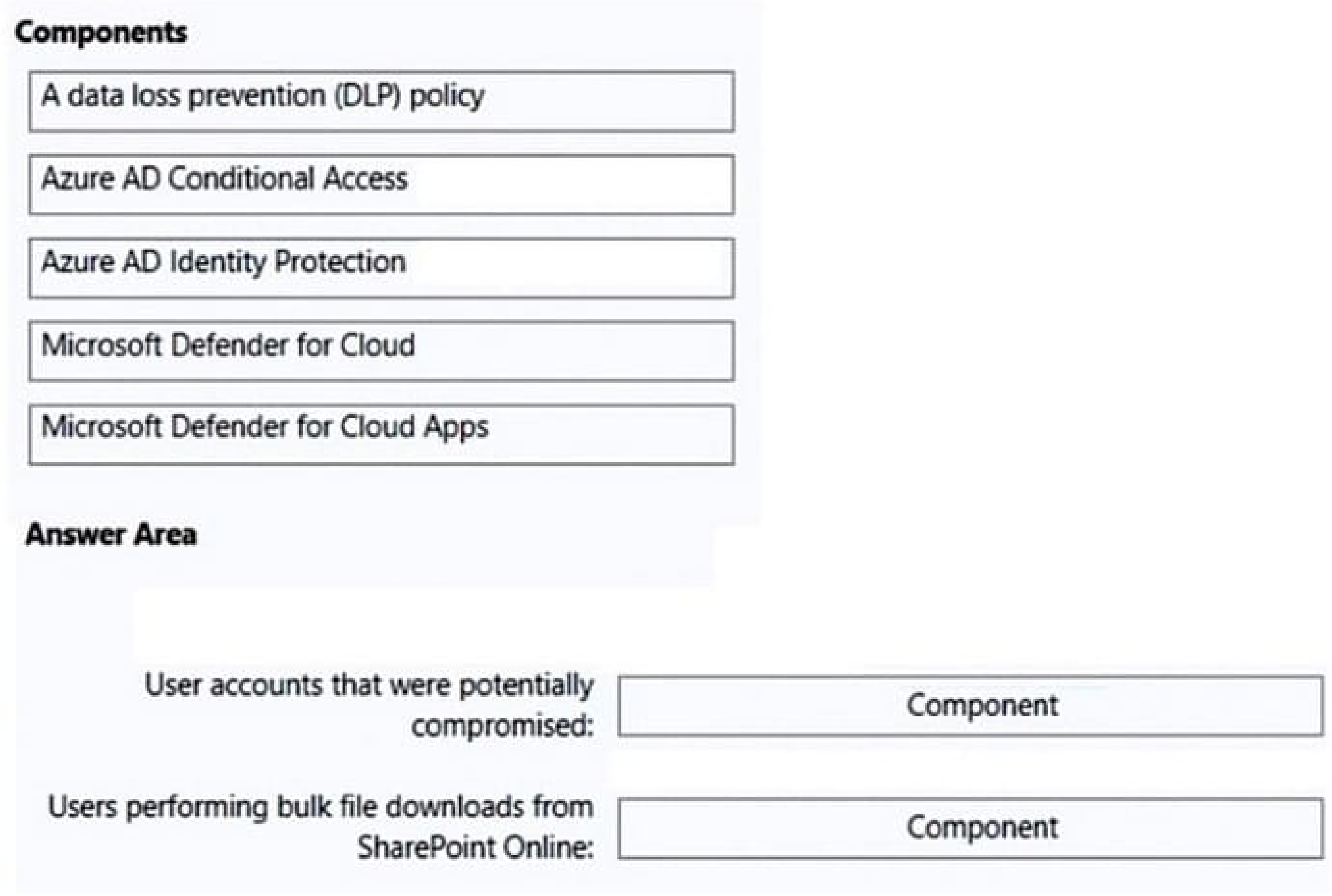
Users performing bulk file downloads from Microsoft SharePoint Online

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:



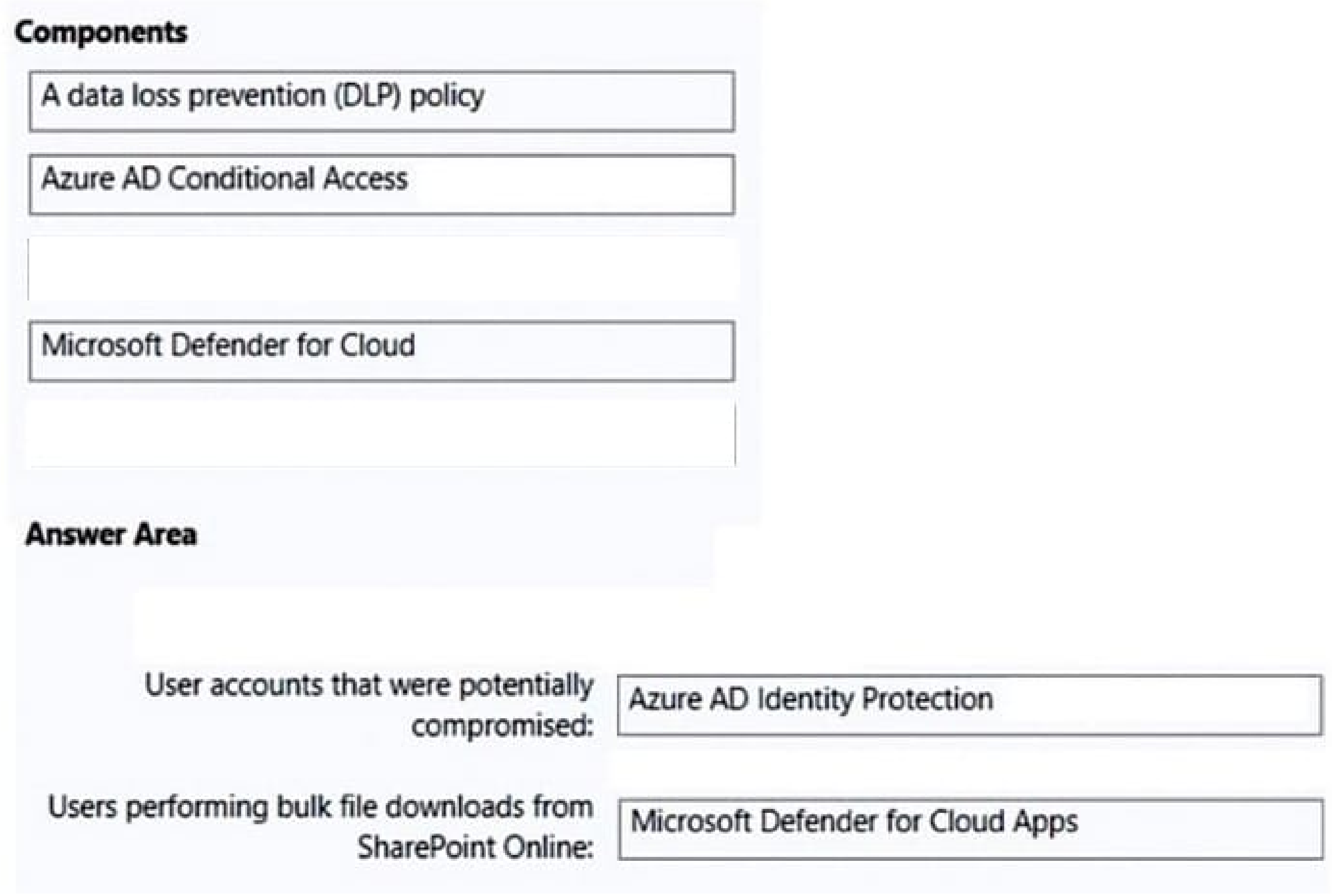
Components

- A data loss prevention (DLP) policy
- Azure AD Conditional Access
- Azure AD Identity Protection
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer Area

User accounts that were potentially compromised:	Component
Users performing bulk file downloads from SharePoint Online:	Component

Correct Answer:



Components

A data loss prevention (DLP) policy

Azure AD Conditional Access

Microsoft Defender for Cloud

Answer Area

User accounts that were potentially compromised: Azure AD Identity Protection

Users performing bulk file downloads from SharePoint Online: Microsoft Defender for Cloud Apps

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