QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Microsoft

SC-100

Microsoft Cybersecurity Architect

Question: 19

HOTSPOT

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation.

You need to recommend a security posture management solution for the following components:

• Azure loT Edge devices

• AWS EC2 instances

Which services should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

For the IoT Edge devices:

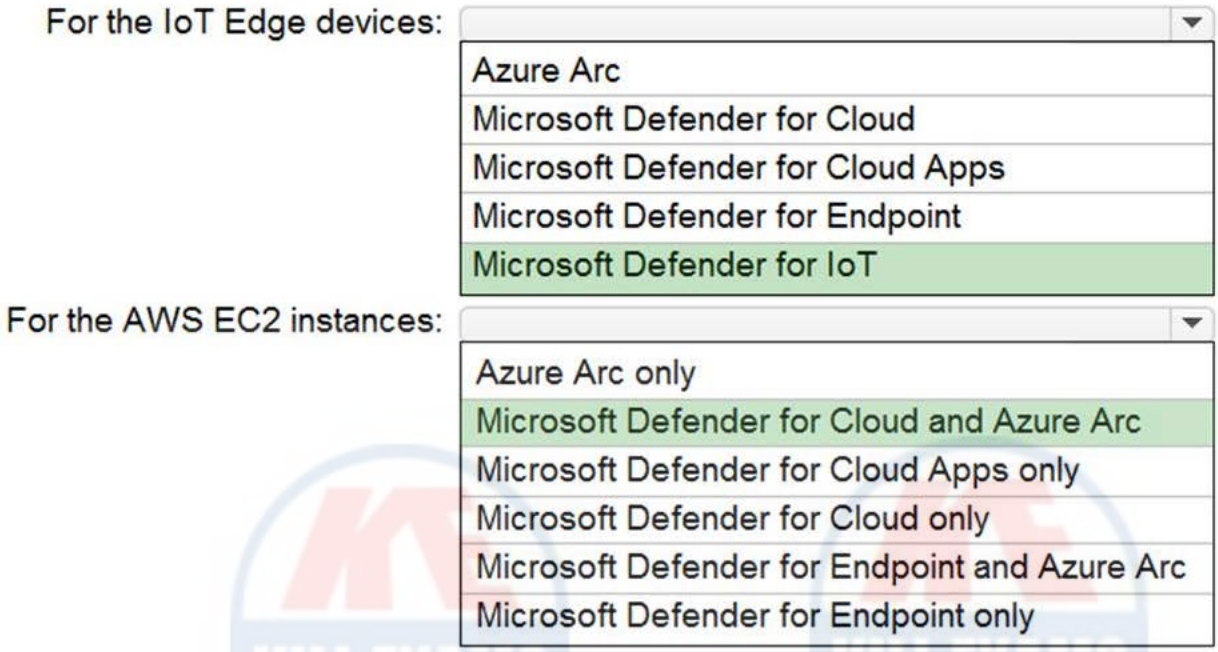
- Azure Arc
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for IoT

For the AWS EC2 instances:

- Azure Arc only
- Microsoft Defender for Cloud and Azure Arc
- Microsoft Defender for Cloud Apps only
- Microsoft Defender for Cloud only
- Microsoft Defender for Endpoint and Azure Arc
- Microsoft Defender for Endpoint only

Answer:

Answer Area



Question: 20

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

You have a Microsoft Sentinel deployment.

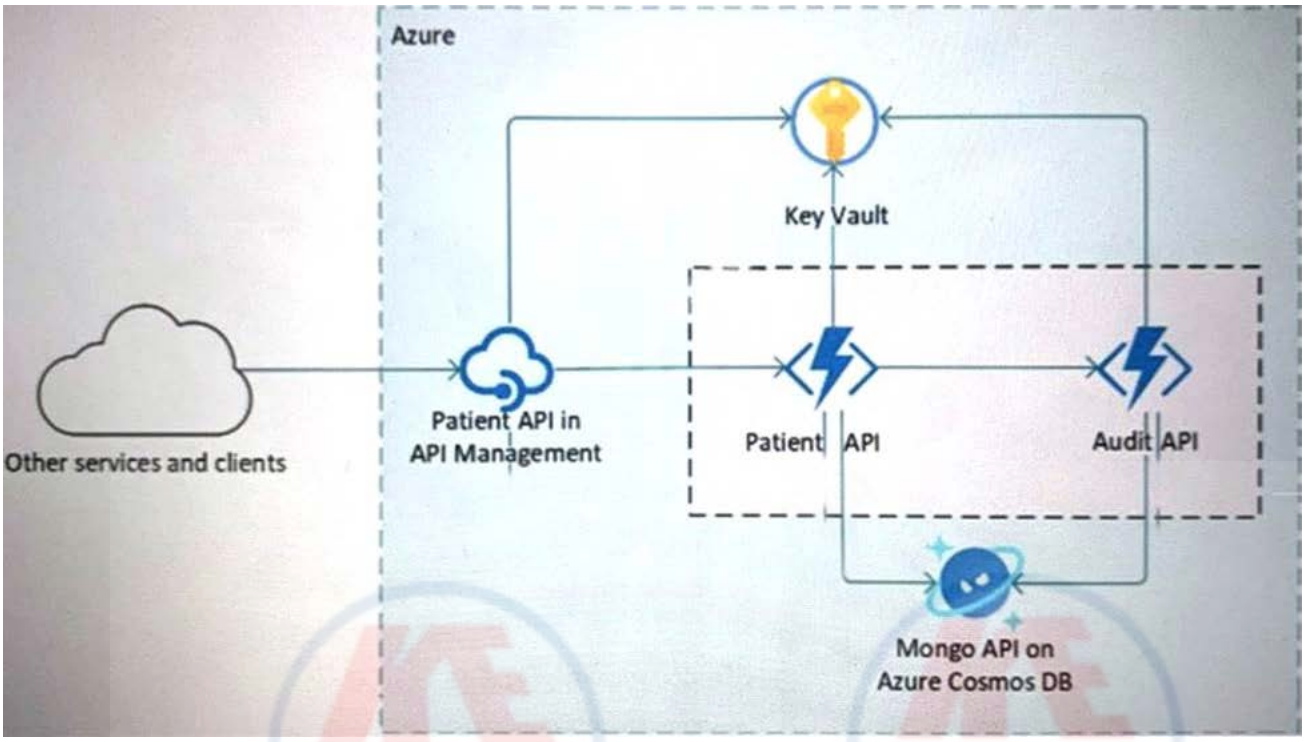
During the triage of alerts, you require additional information about the security events, including suggestions for remediation.

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. workload protections in Defender for Cloud
B. threat intelligence reports in Defender for Cloud
C. Microsoft Sentinel notebooks
D. Microsoft Sentinel threat intelligence workbooks

Answer: B D

Question: 21

Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.



You need to recommend a solution to isolate the compute components on an Azure virtual network.

What should you include in the recommendation?
A. Azure Active Directory (Azure AD) enterprise applications
B. an Azure App Service Environment (ASE)
C. Azure service endpoints
D. an Azure Active Directory (Azure AD) application proxy

Answer: B

Question: 22

You need to recommend a solution to scan the application code. The solution must meet the application development requirements.

What should you include in the recommendation?
A. Azure Key Vault
B. GitHub Advanced Security
C. Application Insights in Azure Monitor
D. Azure DevTest Labs

Answer: B

Question: 23

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

Answer: B

Question: 24

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription.

The company uses the following devices:

• Computers that run either Windows 10 or Windows 11

• Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored.

What should you include in the recommendation?
A. eDiscovery
B. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Answer: D

Question: 25

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

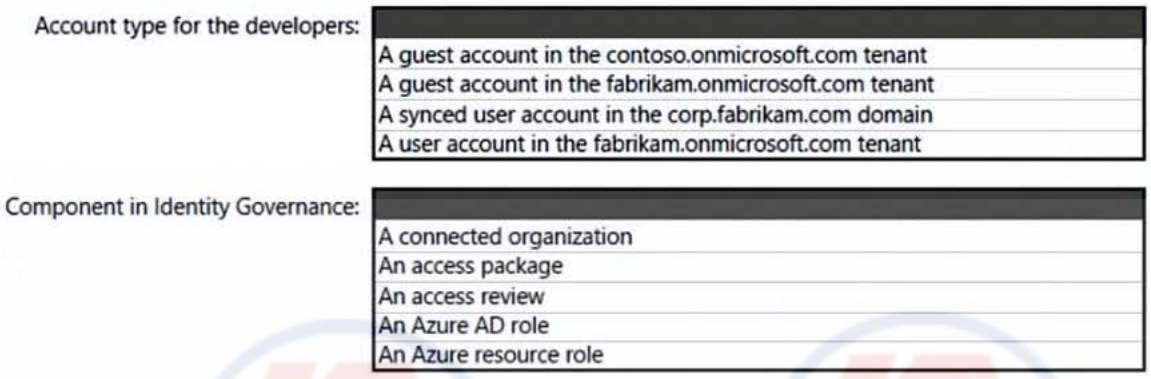
Answer: C

Question: 26

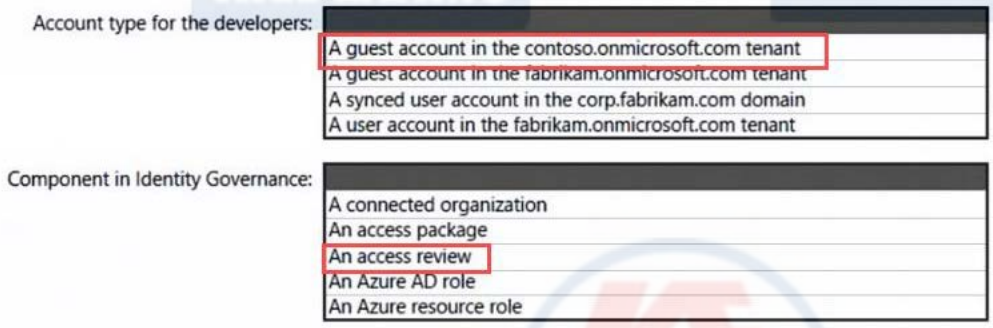
HOTSPOT

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

Answer Area



Answer:



Question: 27

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. Security Assertion Markup Language (SAML)
B. NTLMv2
C. certificate-based authentication
D. Kerberos

Answer: A,D

Question: 28

You need to recommend a solution to meet the security requirements for the InfraSec group.

What should you use to delegate the access?
A. a subscription
B. a custom role-based access control (RBAC) role

C. a resource group
D. a management group

Answer: B

Question: 29

You have Windows 11 devices and Microsoft 365 E5 licenses.

You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites.

What should you include in the recommendation?
A. Microsoft Endpoint Manager
B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Answer: D

Question: 30

HOTSPOT

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

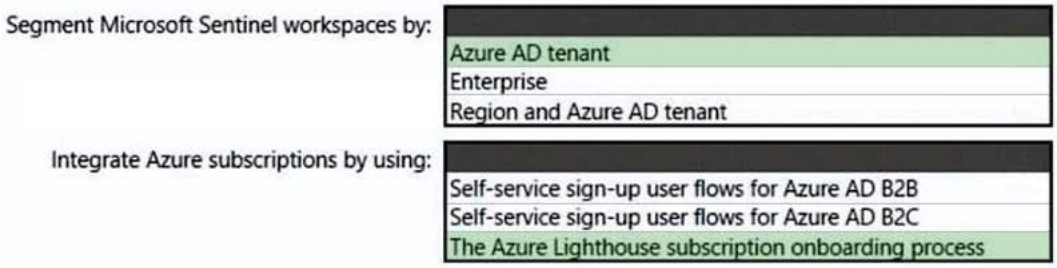
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Segment Microsoft Sentinel workspaces by:	Azure AD tenant Enterprise Region and Azure AD tenant
Integrate Azure subscriptions by using:	Self-service sign-up user flows for Azure AD B2B Self-service sign-up user flows for Azure AD B2C The Azure Lighthouse subscription onboarding process

Answer:

Answer Area



Question: 31

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.

The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps.

The solution must meet the following requirements:

• Prevent the remote users from accessing any other resources on the network.

• Support Azure Active Directory (Azure AD) Conditional Access.

• Simplify the end-user experience.

What should you include in the recommendation?
A. Azure AD Application Proxy
B. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Answer: A

Question: 32

Topic 2, Litware, inc. Case Study 2

Overview

Litware, inc. is a financial services company that has main offices in New York and San Francisco. litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions.

The acquisitions include several companies based in France.

Existing Environment

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD D%) forest named Utvvare.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses.

The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Planned Changes

Litware plans to implement the following changes:

• Create a management group hierarchy for each Azure AD tenant.

• Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

• Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Business Requirements

Litware identifies the following business requirements:

• Minimize any additional on-premises infrastructure.

• Minimize the operational costs associated with administrative overhead.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

• Enable the management of on-premises resources from Azure, including the following: •Use Azure Policy for enforcement and compliance evaluation.

• Provide change tracking and asset inventory.

• Implement patch management.

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

Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAK) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOQ by using Microsoft Sentinel.

Identity Requirements

Litware identifies the following identity requirements:

• Detect brute force attacks that directly target AD DS user accounts.

• Implement leaked credential detection in the Azure AD tenant of Litware.

• Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

• Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for.

• The management of group properties, membership, and licensing « The management of user properties, passwords, and licensing

• The delegation of user management based on business units.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

• insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.

• Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.

• Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

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

• Provide a secure score scoped to the landing zone.

• 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.

• Minimize the possibility of data exfiltration.

• Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity.

Each landing zone will have the following characteristics:

• Be created in a dedicated subscription.

• Use a DNS namespace of litware.com.

Application Security Requirements

Litware identifies the following application security requirements:

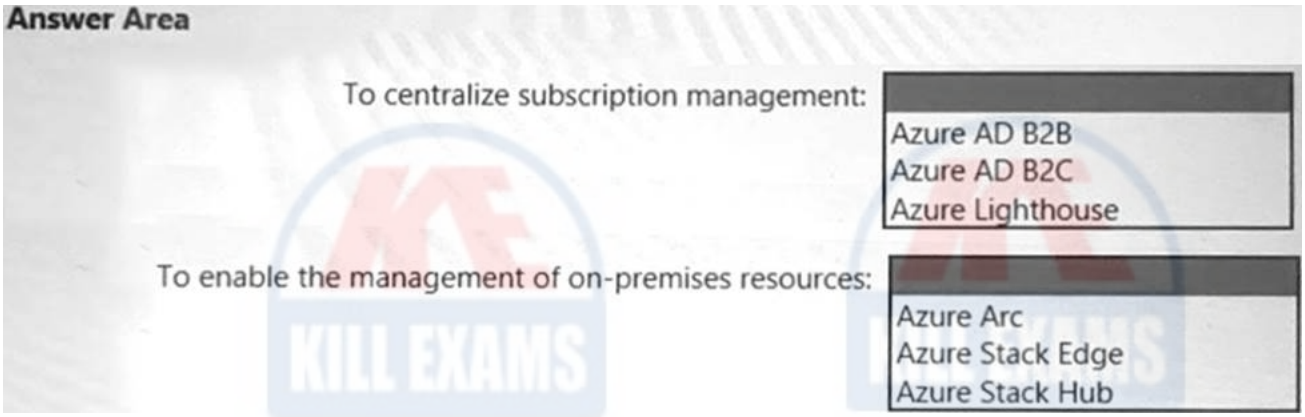
• Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

• Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

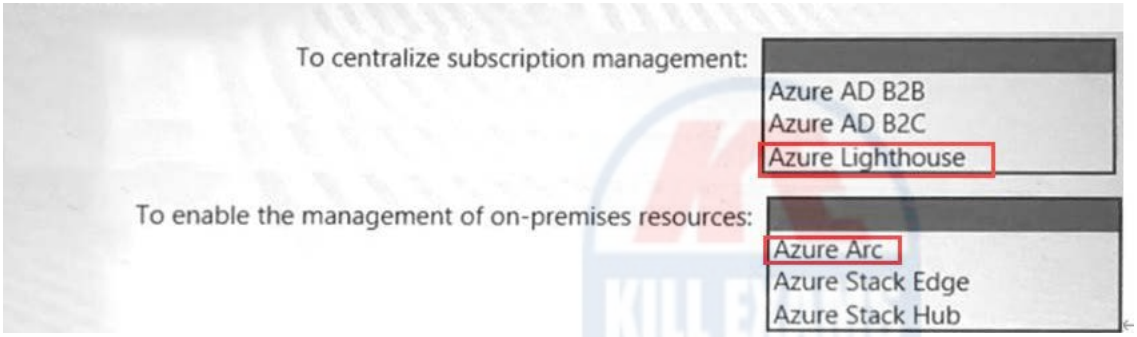
HOTSPOT

You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:

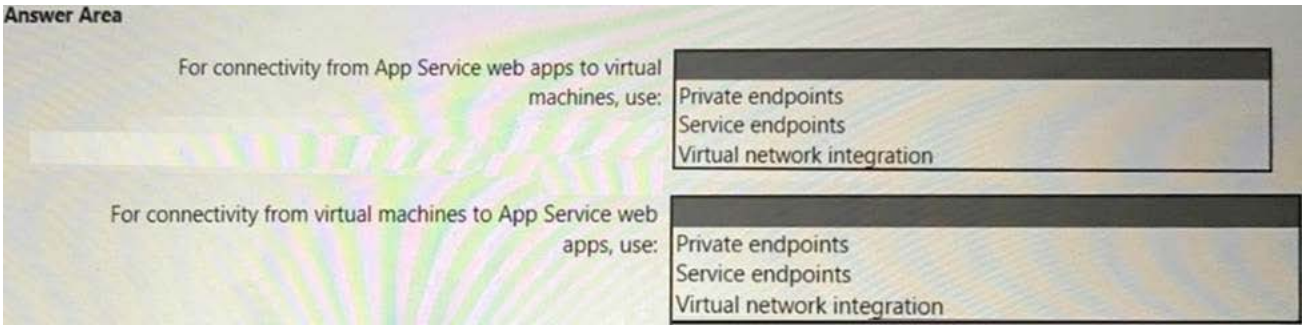


Question: 33

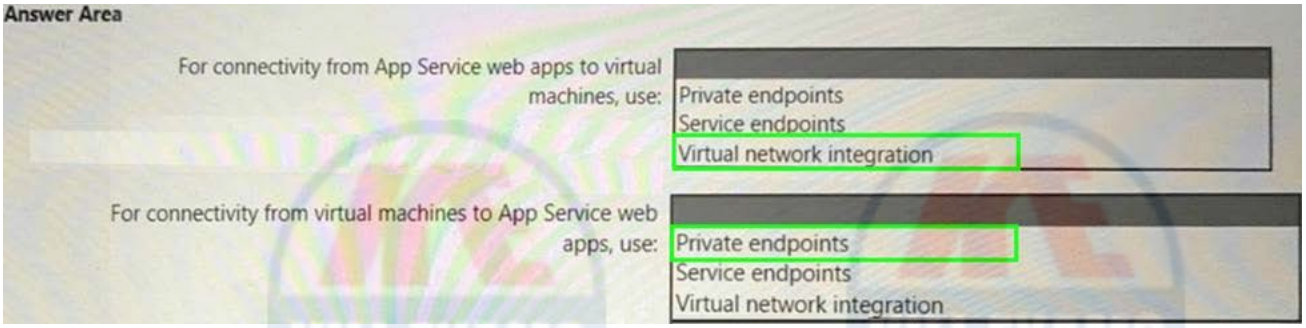
HOTSPOT

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



Answer:



Question: 34

Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD). You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications.

What should you include in the recommendation?
A. activity policies in Microsoft Defender for Cloud Apps
B. sign-in risk policies in Azure AD Identity Protection
C. device compliance policies in Microsoft Endpoint Manager
D. Azure AD Conditional Access policies
E. user risk policies in Azure AD Identity Protection

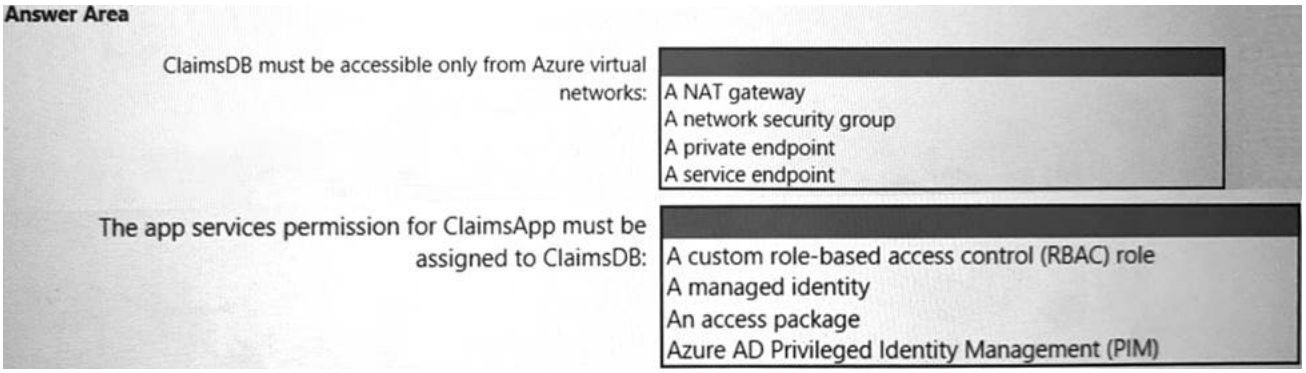
Answer: D

Question: 35

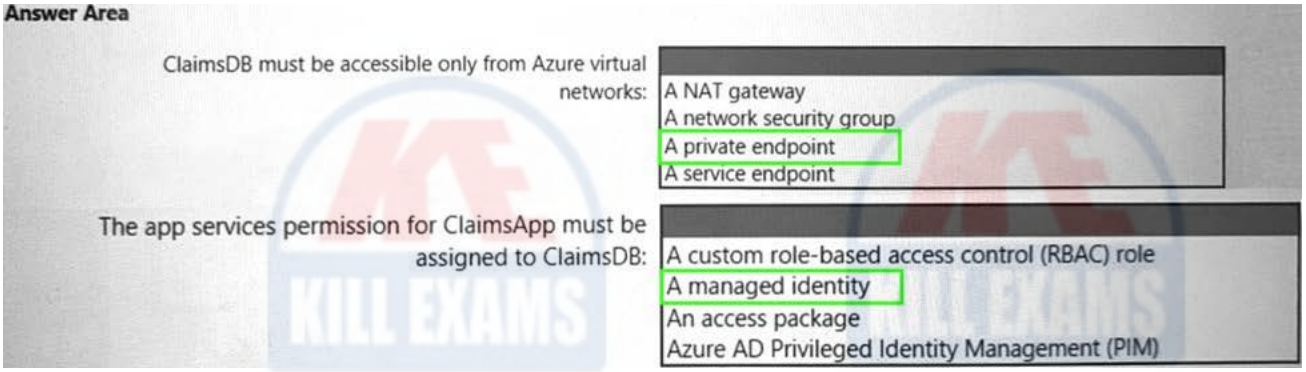
HOTSPOT

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

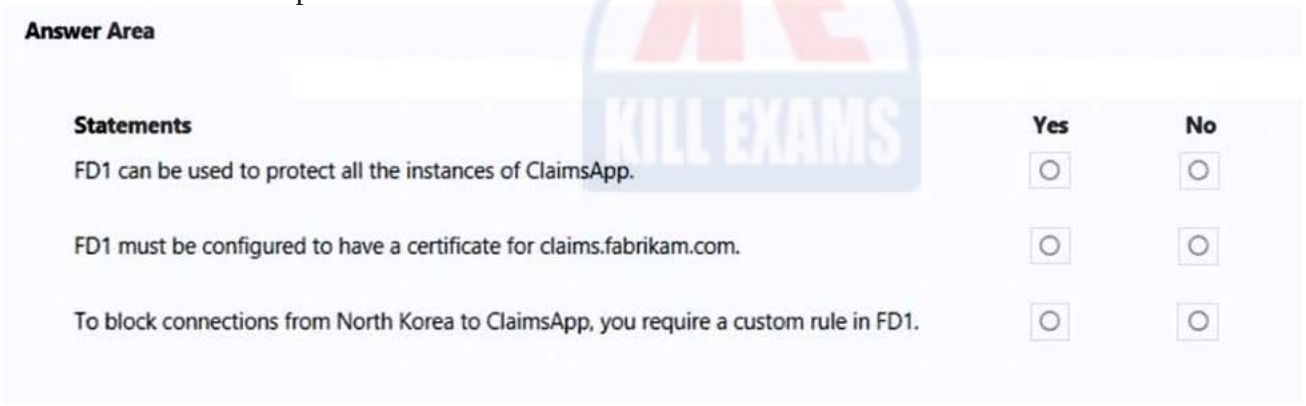


Question: 36

HOTSPOT

You are evaluating the security of ClaimsApp.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.NOTE; Each correct selection is worth one point.



Answer:

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	○	○
FD1 must be configured to have a certificate for claims.fabrikam.com.	○	○
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	○	○