QUESTION 56
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription. Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.
Which three actions should you recommend? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Implement Azure Firewall to restrict host pool outbound access.
C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
E. Deploy a Remote Desktop server to an Azure region located in France.

Answer: BCD
Explanation:
Organizations can use this location for common tasks like:
Requiring multi-factor authentication for users accessing a service when they're off the corporate network.
Blocking access for users accessing a service from specific countries or regions.
The location is determined by the public IP address a client provides to Azure Active Directory or GPS coordinates provided by the Microsoft Authenticator app.
Conditional Access policies by default apply to all IPv4 and IPv6 addresses.
Use Azure Firewall to protect Azure Virtual Desktop deployments.
Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. When an end user connects to an Azure Virtual Desktop environment, their session is run by a host pool. A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts. These virtual machines run in your virtual network and are subject to the virtual network security controls. They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users. Azure Firewall can help you lock down your environment and filter outbound traffic.
Reference:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

QUESTION 57
Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

- Minimizes manual intervention by security operation analysts
- Supports Waging alerts within Microsoft Teams channels

What should you include in the strategy?

A. data connectors
B. playbooks
C. workbooks
D. KQL

Answer: B
Explanation:
Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.
A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

QUESTION 58
Your company plans to provision blob storage by using an Azure Storage account. The blob storage will be accessible from 20 application sewers on the internet.
You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

A. service tags in network security groups (NSGs)
B. managed rule sets in Azure Web Application Firewall (WAF) policies
C. inbound rules in network security groups (NSGs)
D. firewall rules for the storage account
E. inbound rules in Azure Firewall

Answer: D
Explanation:
Configure Azure Storage firewalls and virtual networks.
To secure your storage account, you should first configure a rule to deny access to traffic from all networks (including internet traffic) on the public endpoint, by default. Then, you should configure rules that grant access to traffic from specific VNets. You can also configure rules to grant access to traffic from selected public internet IP address ranges, enabling connections from specific internet or on-premises clients. This configuration enables you to build a secure network boundary for your applications.
Storage firewall rules apply to the public endpoint of a storage account. You don't need any firewall access rules to allow traffic for private endpoints of a storage account. The process of approving the creation of a private endpoint grants implicit access to traffic from the subnet that hosts the private endpoint.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

QUESTION 59
Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10.
You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
- Ensure that only authorized applications can run on the kiosks.
- Regularly harden the kiosks against new threats.

Which two actions should you include in the recommendations? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Onboard the kiosks to Azure Monitor.
B. Implement Privileged Access Workstation (PAW) for the kiosks.

C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Answer: DE
Explanation:
Vuln management sits on top of defender for endpoint.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide

QUESTION 60
Your company has an office in Seattle.
The company has two Azure virtual machine scale sets hosted on different virtual networks.
The company plans to contract developers in India.
You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:
- Prevent exposing the public IP addresses of the virtual machines.
- Provide the ability to connect without using a VPN.
- Minimize costs.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Deploy Azure Bastion to one virtual network.
B. Deploy Azure Bastion to each virtual network.
C. Enable just-in-time VM access on the virtual machines.
D. Create a hub and spoke network by using virtual network peering.
E. Create NAT rules and network rules in Azure Firewall.

Answer: AD
Explanation:
Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.
Note: Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.
Reference:
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

QUESTION 61
Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify 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

Answer: A
Explanation:
https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/1b-elements

QUESTION 62
Your company is moving a big data solution to Azure. The company plans to use the following storage workloads:

- Azure Storage blob containers
- Azure Data Lake Storage Gen2
- Azure Storage file shares
- Azure Disk Storage

Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Disk Storage
B. Azure Storage blob containers
C. Azure Storage file shares
D. Azure Data Lake Storage Gen2

Answer: BD
Explanation:
B: Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against the Blob service.
You can scope access to Azure blob resources at the following levels, beginning with the narrowest scope:
* An individual container. At this scope, a role assignment applies to all of the blobs in the container, as well as container properties and metadata.
* The storage account.
* The resource group.
* The subscription.
* A management group.
D: You can securely access data in an Azure Data Lake Storage Gen2 (ADLS Gen2) account using OAuth 2.0 with an Azure Active Directory (Azure AD) application service principal for authentication. Using a service principal for authentication provides two options for accessing data in your storage account:
A mount point to a specific file or path
Direct access to data
Incorrect:
Not C: To enable AD DS authentication over SMB for Azure file shares, you need to register your storage account with AD DS and then set the required domain properties on the storage account. To register your storage account with AD DS, create an account representing it in your AD DS.
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory
https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

QUESTION 63
You are evaluating an Azure environment for compliance. You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.
Which effect should you use in Azure Policy?

A. Deny
B. Disabled
C. Modify
D. Append

Answer: B
Explanation:
It has to be disabled since deny will send the compliance report as non-complaint.
This effect is useful for testing situations or for when the policy definition has parameterized the effect. This flexibility makes it possible to disable a single assignment instead of disabling all of that policy's assignments.
An alternative to the Disabled effect is enforcementMode, which is set on the policy assignment. When enforcementMode is Disabled, resources are still evaluated.
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#disabled

QUESTION 64
Your company has a Microsoft 365 E5 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:
- Identify unused personal data and empower users to make smart data handling decisions.
- Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
- Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?

A. Microsoft Viva Insights
B. Advanced eDiscovery
C. Privacy Risk Management in Microsoft Priva
D. communication compliance in insider risk management

Answer: C
Explanation:
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.
Reference:
https://docs.microsoft.com/en-us/privacy/priva/risk-management
https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management

QUESTION 65
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.

You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows.
Which compliance control should you evaluate?

A. Data Protection
B. Incident Response
C. Posture and Vulnerability Management
D. Asset Management
E. Endpoint Security

Answer: E
Explanation:
Microsoft Defender for servers compliance control installed on Windows
Defender for clout "Endpoint Security" azure security benchmark v3
Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.
Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.
Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.
Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.
Reference:

https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

QUESTION 66
A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions. You are evaluating the security posture of the customer.
You discover that the AKS resources are excluded from the secure score recommendations.
You need to produce accurate recommendations and update the secure score.
Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure auto provisioning.
B. Assign regulatory compliance policies.
C. Review the inventory.
D. Add a workflow automation.
E. Enable Defender plans.

Answer: AE
Explanation:
Enable the defender for containers plan - then ensure it deploys to your container resources with auto provision.

QUESTION 67
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: BD
Explanation:
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.
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.
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 68
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?

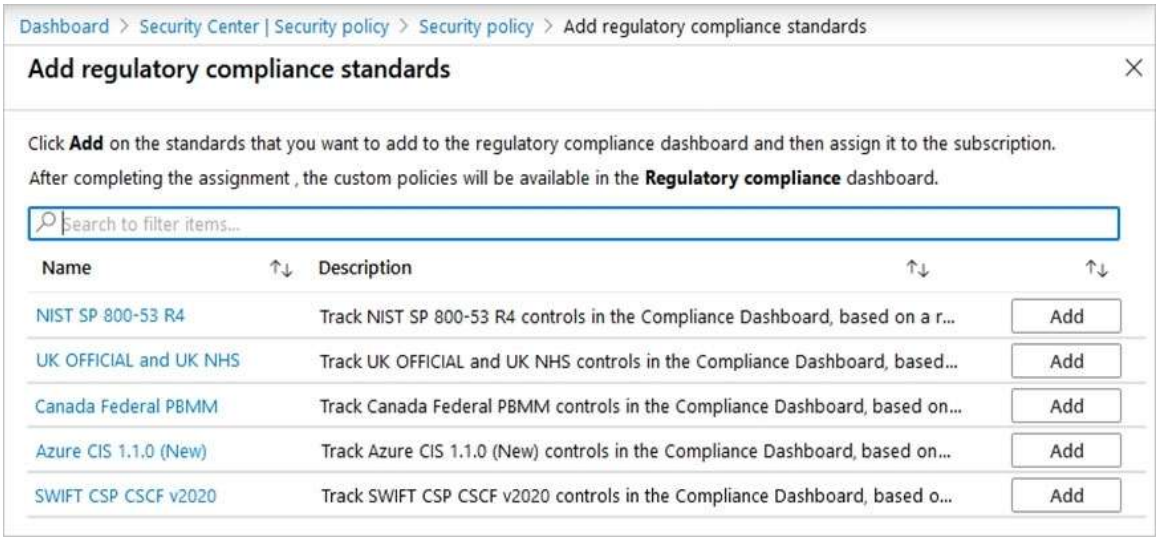
A. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Answer: D
Explanation:
Adaptive application controls are an intelligent and automated solution for defining allowlists of known-safe applications for your machines.
Often, organizations have collections of machines that routinely run the same processes. Microsoft Defender for Cloud uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allowlists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.
When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy
https://docs.microsoft.com/en-us/defender-cloud-apps/cloud-discovery-anomaly-detection-policy
https://docs.microsoft.com/en-us/security/benchmark/azure/overview

QUESTION 69
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance.
What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, add a regulatory compliance standard.
C. From Defender for Cloud, enable Defender for Cloud plans.
D. From Defender for Cloud, review the secure score recommendations.

Answer: B
Explanation:
Add a regulatory standard to your dashboard
The following steps explain how to add a package to monitor your compliance with one of the supported regulatory standards.
Add a standard to your Azure resources
1. From Defender for Cloud's menu, select Regulatory compliance to open the regulatory compliance dashboard. Here you can see the compliance standards currently assigned to the currently selected subscriptions.
2. From the top of the page, select Manage compliance policies. The Policy Management page appears.
3. Select the subscription or management group for which you want to manage the regulatory compliance posture.
4. To add the standards relevant to your organization, expand the Industry & regulatory standards section and select Add more standards.
5. From the Add regulatory compliance standards page, you can search for any of the available standards:



6. Select Add and enter all the necessary details for the specific initiative such as scope, parameters, and remediation.
7. From Defender for Cloud's menu, select Regulatory compliance again to go back to the regulatory compliance dashboard.

Your new standard appears in your list of Industry & regulatory standards.
Note: Customize the set of standards in your regulatory compliance dashboard.
Microsoft Defender for Cloud continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

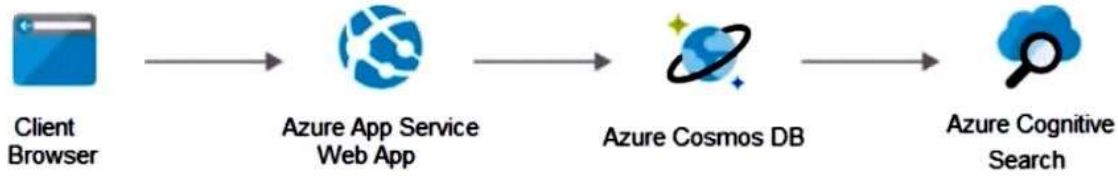
QUESTION 70
You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard. You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution 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

Answer: B
Explanation:
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.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

QUESTION 71
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 Application Gateway with Azure Web Application Firewall (WAF).
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

QUESTION 72
Case Study 2 - Litware, inc.
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.

You need to recommend a strategy for routing internet-bound traffic from the landing zones.
The solution must meet the landing zone requirements.
What should you recommend as part of the landing zone deployment?

A. service chaining
B. local network gateways
C. forced tunneling
D. a VNet-to-VNet connection

Answer: A

Explanation:

Service chaining enables you to direct traffic from one virtual network to a virtual appliance or gateway in a peered network through user-defined routes.
You can deploy hub-and-spoke networks, where the hub virtual network hosts infrastructure components such as a network virtual appliance or VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic flows through network virtual appliances or VPN gateways in the hub virtual network.
Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway.
You can't route between virtual networks with a user-defined route that specifies an Azure ExpressRoute gateway as the next hop type.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview#service-chaining
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

QUESTION 73
Case Study 2 - Litware, inc.
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.

You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access
B. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. Microsoft Defender for Endpoint
E. access reviews in Azure AD

Answer: AB
Explanation:
Access Reviews are not relevant here.
Monitor real-time needs Conditional Access & Defender for Cloud Apps.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#conditional-access-application-control
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cloud-application-security

QUESTION 74
Your company has devices that run either Windows 10, Windows 11, or Windows Server.
You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune
B. Policy Analyzer
C. Local Group Policy Object (LGPO)
D. Windows Autopilot

Answer: B
Explanation:
Microsoft Security Compliance Toolkit 1.0, Policy Analyzer.
The Policy Analyzer is a utility for analyzing and comparing sets of Group Policy Objects (GPOs). Its main features include:
- Highlight when a set of Group Policies has redundant settings or internal inconsistencies.
- Highlight the differences between versions or sets of Group Policies.
- Compare GPOs against current local policy and local registry settings
- Export results to a Microsoft Excel spreadsheet

Policy Analyzer lets you treat a set of GPOs as a single unit. This treatment makes it easy to determine whether particular settings are duplicated across the GPOs or are set to conflicting values. Policy Analyzer also lets you capture a baseline and then compare it to a snapshot taken at a later time to identify changes anywhere across the set.
Note: The Security Compliance Toolkit (SCT) is a set of tools that allows enterprise security administrators to download, analyze, test, edit, and store Microsoft- recommended security configuration baselines for Windows and other Microsoft products.

The SCT enables administrators to effectively manage their enterprise's Group Policy Objects (GPOs). Using the toolkit, administrators can compare their current
GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, store them in GPO backup file format, and apply them broadly through Active Directory or individually through local policy.
Security Compliance Toolkit Tools:
Policy Analyzer -
Local Group Policy Object (LGPO)
Set Object Security -
GPO to Policy Rules -
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

QUESTION 75
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. Microsoft Defender for Endpoint reports the endpoints as compliant.
B. Microsoft Intune reports the endpoints as compliant.
C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
D. The client access tokens are refreshed.

Answer: BD
Explanation:
Mobile device management (MDM) solutions like Intune can help protect organizational data by requiring users and devices to meet some requirements. In Intune, this feature is called compliance policies.
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

QUESTION 76
Hotspot Question
You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CO) workflows.
You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.
What should you include in the recommendation for each stage? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Answer Area

QUESTION 77
Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.
You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.
What should you include in the recommendation?

A. Use geo-redundant storage (GRS).
B. Use customer-managed keys (CMKs) for encryption.
C. Require PINs to disable backups.
D. Implement Azure Site Recovery replication.

Answer: C
Explanation:
Azure Backup
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.
Authentication to perform critical operations
As part of adding an extra layer of authentication for critical operations, you're prompted to enter a security PIN when you perform Stop Protection with Delete data and Change Passphrase operations.
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
https://docs.microsoft.com/en-us/azure/backup/backup-azure-security-feature#prevent-attacks

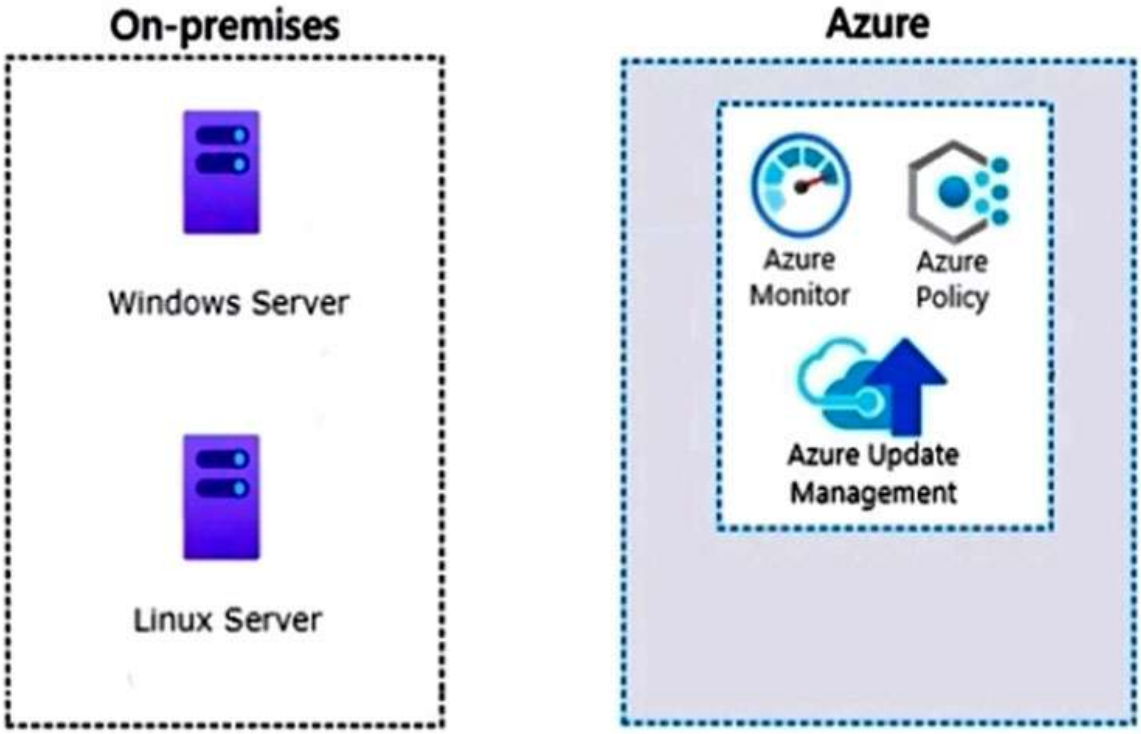
QUESTION 78
You have a customer that has a Microsoft 365 subscription and an Azure subscription. The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules.
What should you include in the solution?

A. Microsoft Information Protection
B. Microsoft Defender for Endpoint
C. Microsoft Sentinel
D. Microsoft Endpoint Manager

Answer: D
Explanation:
Microsoft Endpoint Manager includes Microsoft Intune.
Device compliance policies are a key feature when using Intune to protect your organization's resources. In Intune, you can create rules and settings that devices must meet to be considered compliant, such as a minimum OS version.

Microsoft Endpoint Manager helps deliver the modern workplace and modern management to keep your data secure, in the cloud and on-premises. Endpoint
Manager includes the services and tools you use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.
Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co- management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk.
Note: Microsoft Defender for Endpoint Plan 2 protects your Windows and Linux machines whether they're hosted in Azure, hybrid clouds (on-premises), or multicloud.
Microsoft Defender for Endpoint on iOS offers protection against phishing and unsafe network connections from websites, emails, and apps.
Microsoft Defender for Endpoint on Android supports installation on both modes of enrolled devices - the legacy Device Administrator and Android Enterprise modes. Currently, Personally-owned devices with work profile and Corporate-owned fully managed user device enrollments are supported in Android Enterprise.
Reference:
https://docs.microsoft.com/en-us/mem/endpoint-manager-overview
https://docs.microsoft.com/en-us/azure/defender-for-cloud/integration-defender-for-endpoint

QUESTION 79
Your company has a hybrid cloud infrastructure.
Data and applications are moved regularly between cloud environments.
The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:
- Govern virtual machines and servers across multiple environments.
- Enforce standards for all the resources across all the environments by using Azure Policy.
Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Azure VPN Gateway
B. guest configuration in Azure Policy
C. on-premises data gateway

D. Azure Bastion
E. Azure Arc

Answer: BE
Explanation:
B: Azure Policy's guest configuration feature provides native capability to audit or configure operating system settings as code, both for machines running in Azure and hybrid Arc-enabled machines. The feature can be used directly per-machine, or at-scale orchestrated by Azure Policy.
Configuration resources in Azure are designed as an extension resource. You can imagine each configuration as an additional set of properties for the machine.
E: Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.
Microsoft recently [2019/2020] released Azure Arc, which unlocks new hybrid scenarios for organizations by bringing new Azure services and management features to any infrastructure.
Reference:
https://techcommunity.microsoft.com/t5/azure-developer-community-blog/azure-arc-for-servers-getting-started/ba-p/1262062
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/guest-configuration

QUESTION 80
You are designing the security standards for a new Azure environment.
You need to design a privileged identity strategy based on the Zero Trust model.
Which framework should you follow to create the design?

A. Enhanced Security Admin Environment (ESAE)
B. Microsoft Security Development Lifecycle (SDL)
C. Rapid Modernization Plan (RaMP)
D. Microsoft Operational Security Assurance (OSA)

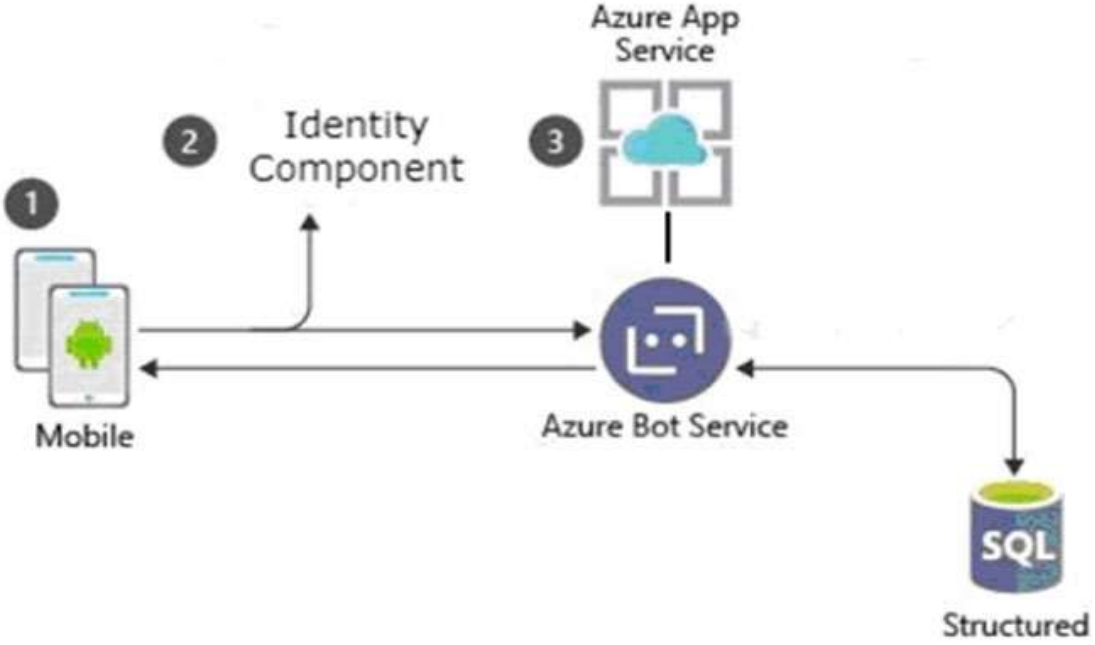
Answer: C
Explanation:
This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.
https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan

QUESTION 81
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. role-based authorization
B. Azure AD Privileged Identity Management (PIM)
C. resource-based authorization
D. Azure AD Multi-Factor Authentication

Answer: B
Explanation:
Default security feature give the option to turn on MFA for all users even in Free AAD tenants.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

QUESTION 82
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:
- Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.
- Be managed separately from the identity store of the customer.
- Support fully customizable branding for each app.

Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2C
B. Azure Active Directory (Azure AD) B2B
C. Azure AD Connect
D. Azure Active Directory Domain Services (Azure AD DS)

Answer: A
Explanation:
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.
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 83
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

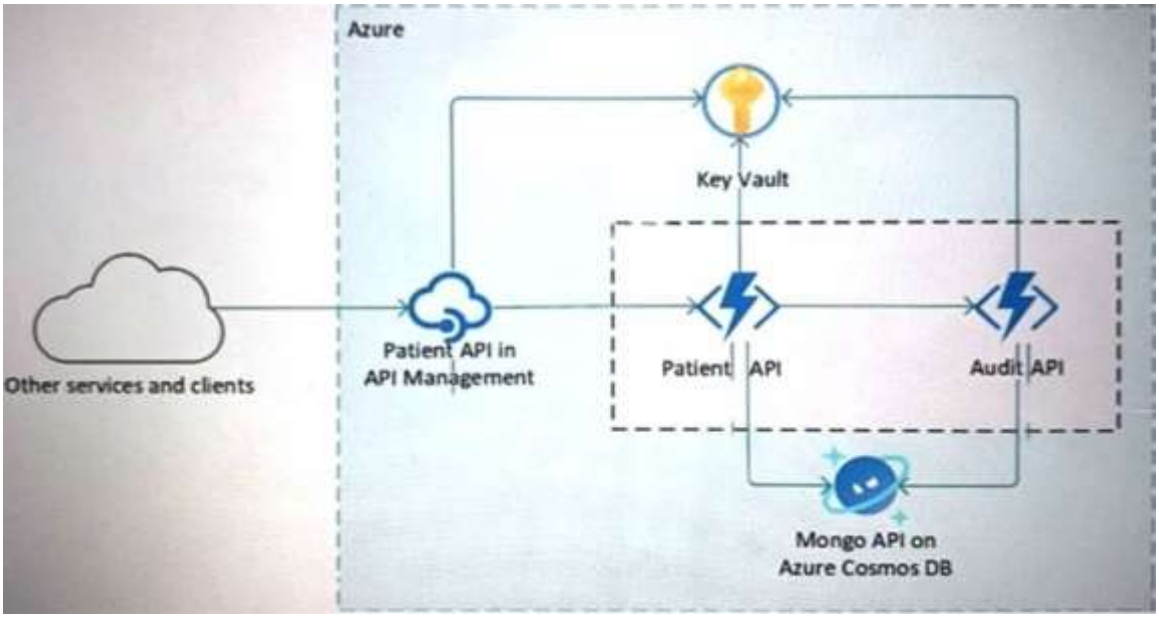
Answer: D
Explanation:
Microsoft Sentinel is a scalable, cloud-native solution that provides:
Security information and event management (SIEM)
Security orchestration, automation, and response (SOAR)
Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. 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 84
You have an Azure subscription that is used as an Azure landing zone for an application.
You need to evaluate the security posture of all the workloads in the landing zone.
What should you do first?

A. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Answer: C
Explanation:
https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone

QUESTION 85
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
Explanation:
The Azure App Service Environment (ASE) is a Premium feature offering of the Azure App Service. It gives a single-tenant instance of the Azure App Service that runs right in your own Azure virtual network (VNet), providing network isolation and improved scaling capabilities.
https://docs.microsoft.com/en-us/archive/msdn-magazine/2017/april/azure-the-new-azure-app-service-environment

QUESTION 86
You have a Microsoft 365 E5 subscription.
You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.
You need to recommend a solution to prevent Personally Identifiable Information (Pll) from being shared.
Which two components should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies
B. sensitivity label policies
C. retention label policies
D. eDiscovery cases

Answer: AB
Explanation:
Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate.

Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.
Reference:
https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/
https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

QUESTION 87
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?

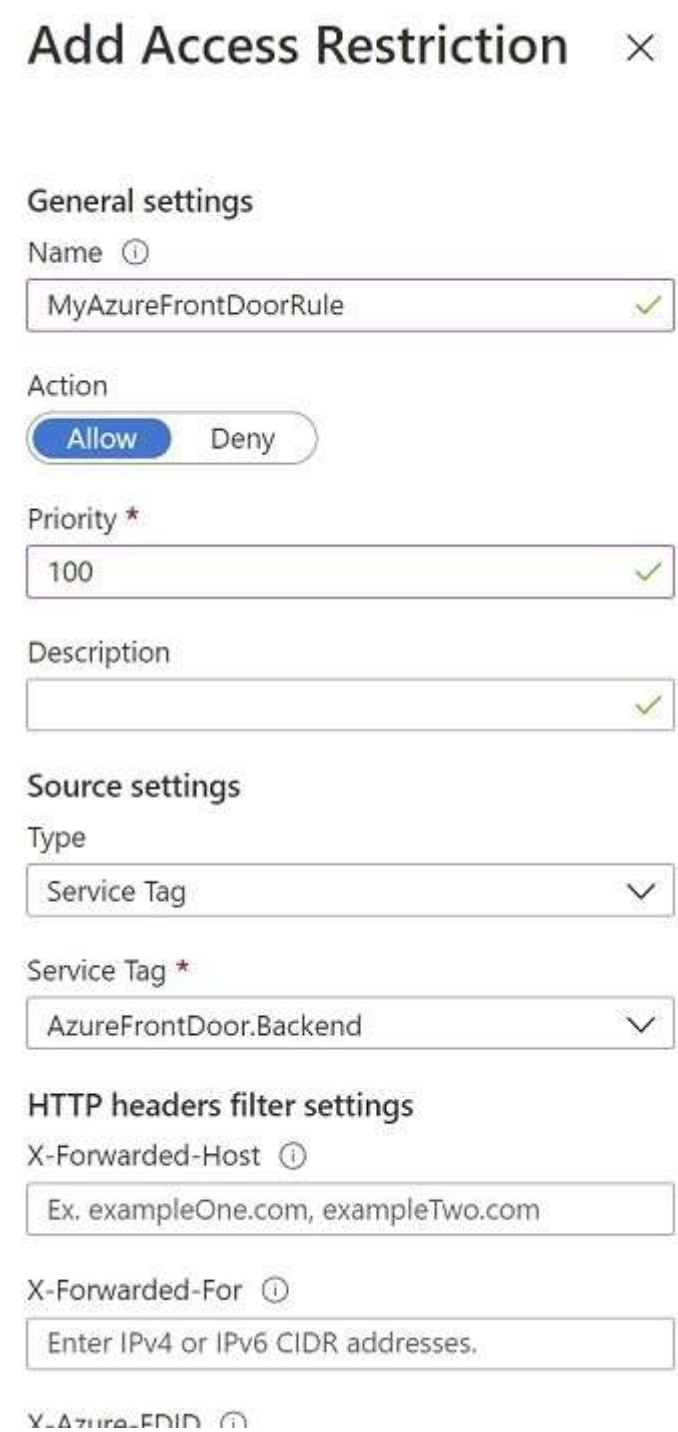
A. eDiscovery
B. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Answer: D
Explanation:
Protect your sensitive data with Microsoft Purview.
Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.
Note: You can use Microsoft Information Protection: Microsoft Purview for Auditing and Analytics in Outlook for iOS, Android, and Mac (DoD).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection
https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

QUESTION 88
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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

Answer: A
Explanation:
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.



Reference:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

QUESTION 89
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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

Answer: A
Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

QUESTION 90
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 enabling just-in-time (JIT) VM access on all virtual machines.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
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