AZ-500T00: Microsoft Azure Security Technologies

Course Duration: 32 Hours (4 Days)

Overview

The AZ-500: Microsoft Azure Security Technologies course is a comprehensive training program designed to equip learners with the knowledge and skills required to Implement security controls, maintain the security posture, manage identity and access, and Protect data, applications, and networks in Azure environments. Participants who undertake this course can expect to gain a deeper understanding of Azure security services and features, enabling them to effectively secure their Azure workloads and subscriptions. Module 1 focuses on identity and access management, including Azure Active Directory and Azure AD Privileged Identity Management. Module 2 covers platform protection strategies, from network security to host and Subscription security. Module 3 delves into security operations, teaching how to Configure security services, manage alerts, and respond to security incidents. Finally, Module 4 addresses data and application security, including Encryption, Application lifecycle security, and Azure Key Vault management. By mastering these areas, learners will be well-prepared to tackle Azure security challenges and enhance their careers in cloud security.

Audience Profile

As the Azure security engineer, you implement, manage, and monitor security for resources in Azure, multi-cloud, and hybrid environments as part of an end-to-end infrastructure. You recommend security components and configurations to protect the following:

- Identity and access
- Data
- Applications
- Networks

Your responsibilities as an Azure security engineer include:

- Managing the security posture.
- Identifying and remediating vulnerabilities.
- Performing threat modelling.
- Implementing threat protection.

You may also participate in responding to security incidents. As an Azure security engineer, you work with architects, administrators, and developers to plan and implement solutions that meet security and compliance requirements.

You should have:

- Practical experience in administration of Microsoft Azure and hybrid environments.
- Strong familiarity with computer, network, and storage in Azure and Microsoft Entra ID.

Course Syllabus

Module 1: Manage identity and access (25–30%)

Manage Microsoft Entra identities

- Secure Microsoft Entra users
- Secure Microsoft Entra groups
- Recommend when to use external identities
- Secure external identities
- Implement Microsoft Entra ID Protection

Manage Microsoft Entra authentication

- Implement multi-factor authentication (MFA)
- Configure Microsoft Entra Verified ID
- Implement passwordless authentication
- Implement password protection
- Implement single sign-on (SSO)
- Integrate single sign on (SSO) and identity providers
- Recommend and enforce modern authentication methods

Manage Microsoft Entra authorization

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Assign Microsoft Entra built-in roles
- Assign Azure built-in roles
- Create and assign custom roles, including Azure roles and Microsoft Entra roles
- Implement and manage Microsoft Entra Permissions Management
- Configure Microsoft Entra Privileged Identity Management
- Configure role management and access reviews in Microsoft Entra
- Implement Conditional Access policies

Manage Microsoft Entra application access

- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants
- Manage Microsoft Entra app registrations
- Configure app registration permission scopes
- Manage app registration permission consent

- Manage and use service principals
- Manage managed identities for Azure resources
- Recommend when to use and configure a Microsoft Entra Application Proxy, including authentication

Module 1: Manage identity and access (25–30%)

Manage Microsoft Entra identities

- Secure Microsoft Entra users
- Secure Microsoft Entra groups
- Recommend when to use external identities
- Secure external identities
- Implement Microsoft Entra ID Protection

Manage Microsoft Entra authentication

- Implement multi-factor authentication (MFA)
- Configure Microsoft Entra Verified ID
- Implement password less authentication
- Implement password protection
- Implement single sign-on (SSO)
- Integrate single sign on (SSO) and identity providers
- Recommend and enforce modern authentication methods

Manage Microsoft Entra authorization

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Assign Microsoft Entra built-in roles
- Assign Azure built-in roles
- Create and assign custom roles, including Azure roles and Microsoft Entra roles
- Implement and manage Microsoft Entra Permissions Management
- Configure Microsoft Entra Privileged Identity Management
- Configure role management and access reviews in Microsoft Entra
- Implement Conditional Access policies

Manage Microsoft Entra application access

- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants
- Manage Microsoft Entra app registrations
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage and use service principals

- Manage managed identities for Azure resources
- Recommend when to use and configure a Microsoft Entra Application Proxy, including authentication

Module 2: Secure Networking (20–25%)

Plan and implement security for virtual networks

- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Plan and implement user-defined routes (UDRs)
- Plan and implement Virtual Network peering or VPN gateway
- Plan and implement Virtual WAN, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Implement encryption over ExpressRoute
- Configure firewall settings on PaaS resources
- Monitor network security by using Network Watcher, including NSG flow logging

Plan and implement security for private access to Azure resources

- Plan and implement virtual network Service Endpoints
- Plan and implement Private Endpoints
- Plan and implement Private Link services
- Plan and implement network integration for Azure App Service and Azure Functions
- Plan and implement network security configurations for an App Service Environment (ASE)
- Plan and implement network security configurations for an Azure SQL Managed Instance

Plan and implement security for public access to Azure resources

- Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
- Plan and implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Plan and implement a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Module 3: Secure compute, storage, and databases (20–25%)

Plan and implement advanced security for compute

- Plan and implement remote access to public endpoints, including Azure
- Bastion and just-in-time (JIT) virtual machine (VM) access
- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor AKS
- Configure authentication for AKS
- Configure security monitoring for Azure Container Instances (ACIs)
- Configure security monitoring for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR)
- Configure disk encryption, including Azure Disk Encryption (ADE), encryption at host, and confidential disk encryption
- Recommend security configurations for Azure API Management

Plan and implement security for storage

- Configure access control for storage accounts
- Manage life cycle for storage account access keys
- Select and configure an appropriate method for access to Azure Files
- Select and configure an appropriate method for access to Azure Blob Storage
- Select and configure an appropriate method for access to Azure Tables
- Select and configure an appropriate method for access to Azure Queues
- Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
- Configure Bring your own key (BYOK)
- Enable double encryption at the Azure Storage infrastructure level

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Enable Microsoft Entra database authentication
- Enable database auditing
- Identify use cases for the Microsoft Purview governance portal
- Implement data classification of sensitive information by using the Microsoft Purview governance portal
- Plan and implement dynamic masking
- Implement Transparent Data Encryption (TDE)
- Recommend when to use Azure SQL Database Always Encrypted

Module 4: Manage security operations (25–30%)

Plan, implement, and manage governance for security

- Create, assign, and interpret security policies and initiatives in Azure Policy
- Configure security settings by using Azure Blueprints
- Deploy secure infrastructures by using a landing zone

- Create and configure an Azure Key Vault
- Recommend when to use a dedicated Hardware Security Module (HSM)
- Configure access to Key Vault, including vault access policies and Azure Role Based Access Control
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys

Manage security posture by using Microsoft Defender for Cloud

- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Add industry and regulatory standards to Microsoft Defender for Cloud
- Add custom initiatives to Microsoft Defender for Cloud
- Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud
- Identify and monitor external assets by using Microsoft Defender External Attack Surface Management

Configure and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud, including Microsoft Defender for Storage, Databases, Containers, App Service, Key Vault, and Resource Manager
- Configure Microsoft Defender for Servers
- Configure Microsoft Defender for Azure SQL Database
- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Evaluate vulnerability scans from Microsoft Defender for Server

Configure and manage security monitoring and automation solutions

- Monitor security events by using Azure Monitor
- Configure data connectors in Microsoft Sentinel
- Create and customize analytics rules in Microsoft Sentinel
- Evaluate alerts and incidents in Microsoft Sentinel
- Configure automation in Microsoft Sentinel