AZ-500T00: Microsoft Azure Security Technologies

Course Code: AZ-500T00
Duration: 4 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Level up with Microsoft Certified: Azure Security Engineer Associate

Reduce costs and complexity with a highly secure cloud foundation managed by Microsoft. Use multilayered, built-in security controls and unique threat intelligence from Azure to help identify and protect against rapidly evolving threats.

This **Azure Security Engineer** course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities on Microsoft Azure. This course includes security for identity and access, platform protection, data and applications, and security operations.

Are you currently retrenched? If yes, check out our PERKESO EIS: Get Back into the Workforce through Upskilling program.

SKILLS COVERED

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.
- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.
- Implement Azure Key Vault including certificates, keys, and secretes.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.
- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

WHO SHOULD ATTEND?

This course is for **Azure Security Engineers** who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

This **Microsoft Official Course** prepares students for the **Microsoft Certified: Azure Security Engineer Associate** certification. The AZ-500 exam measures your ability to accomplish the following technical tasks: manage identity and access; implement platform protection; manage security operations; and secure data and applications.

PREREQUISITES

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model.
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Have experience with Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.

Prerequisite courses (or equivalent knowledge and hands-on experience):

- AZ-900T00: Microsoft Azure Fundamentals
- AZ-104T00: Microsoft Azure Administrator

MODULES

Module 1: Secure Azure solutions with Azure Active Directory
Explore how to securely configure and administer your Azure Active Directory instance.

Learning objectives

By the end of this module, you will be able to:

- Configure Azure AD and Azure AD Domain Services for security
- Create users and groups that enable secure usage of your tenant
- Use MFA to protect user's identities
- Configure passwordless security options

Prerequisites

- None

Module 2: Implement Hybrid identity
Explore how to deploy and configure Azure AD Connect to create a hybrid identity solution for your company.

Learning objectives

By the end of this module, you will be able to:

- Deploy Azure AD Connect

- Pick and configure that best authentication option for your security needs
- Configure password writeback

Prerequisites

- None

Module 3: Deploy Azure AD identity protection
Protect identities in Azure AD using Conditional Access, MFA, access reviews, and other capabilities.

Learning objectives

By the end of this module, you will be able to:

- Deploy and configure Identity Protection
- Configure MFA for users, groups, and applications
- Create Conditional Access policies to ensure your security
- Create and follow an access review process

Prerequisites

- None

Module 4: Configure Azure AD privileged identity management
Ensure that your privileged identities have extra protection and are accessed only with the least amount of access needed to do the job.

Learning objectives

By the end of this module, you'll be able to:

- Describe Zero Trust and how it impacts security
- Configure and deploy roles using Privileged Identity Management (PIM)
- Evaluate the usefulness of each PIM setting as it relates to your security goals

Prerequisites

- None

Module 5: Design an enterprise governance strategy
Learn to use RBAC and Azure Policy to limit access to your Azure solutions, and determine which method is right for your security goals.

Learning objectives

By the end of this module, you will be able to:

- Explain the shared responsibility model and how it impacts your security configuration
- Create Azure policies to protect your solutions
- Configure and deploy access to services using RBAC

Prerequisites

- None

Module 6: Implement perimeter security
Prevent attacks before they get to your Azure solutions. Use the concepts of defense in depth and zero trust to secure Azure perimeter.

Learning objectives

By the end of this module, you will be able to:

- Define defense in depth
- Protect your environment from denial-of-service attacks
- Secure your solutions using firewalls and VPNs

- Explore your end-to-end perimeter security configuration based on your security posture

Prerequisites

- None

Module 7: Configure network security
Use Azure network capabilities to secure your network and applications from external and internal attacks.

Learning objectives

By the end of this module, you will be able to:

- Deploy and configure network security groups to protect your Azure solutions
- Configure and lockdown service endpoints and private links
- Secure your applications with Application Gateway, Web App Firewall, and Front Door
- Configure ExpressRoute to help protect your network traffic

Prerequisites

- None

Module 8: Configure and manage host security
Learn to lock down the devices, virtual machines, and other components that run your applications in Azure.

Learning objectives

By the end of this module, you will be able to:

- Configure and deploy Endpoint Protection
- Deploy a privileged access strategy for devices and privileged workstations
- Secure your virtual machines and access to them
- Deploy Windows Defender
- Practice layered security by reviewing and implementing Security Center and Security Benchmarks

Prerequisites

- None

Module 9: Enable Containers security
Explore how to secure your applications running within containers and how to securely connect to them.

Learning objectives

By the end of this module, you will be able to:

- Define the available security tools for containers in Azure
- Configure security settings for containers and Kubernetes services
- Lock down network, storage, and identity resources connected to your containers
- Deploy RBAC to control access to containers

Prerequisites

- None

Module 10: Deploy and secure Azure Key Vault
Protect your keys, certificates, and secrets in Azure Key Vault. Learn to configure key vault for the most secure deployment.

Learning objectives

By the end of this module, you will be able to:

- Define what a key vault is and how it protects certificates and secrets

- Deploy and configure Azure Key Vault
- Secure access and administration of your key vault
- Store keys and secrets in your key vault
- Explore key security considers like key rotation and backup / recovery

Prerequisites

- None

Module 11: Configure application security features
Register your company applications then use Azure security features to configure and monitor secure access to the application.

Learning objectives

By the end of this module, you will be able to:

- Register an application in Azure using app registration
- Select and configure which Azure AD users can access each application
- Configure and deploy web app certificates

Prerequisites

- None

Module 12: Implement storage security
Ensure your data is stored, transferred, and accessed in a secure way using Azure storage and file security features.

Learning objectives

By the end of this module, you will be able to:

- Define data sovereignty and how that is achieved in Azure
- Configure Azure Storage access in a secure and managed way
- Encrypt your data while it is at rest and in transit
- Apply rules for data retention

Prerequisites

- None

Module 13: Configure and manage SQL database security
Configure and lock down your SQL database on Azure to protect your corporate data while it is stored.

Learning objectives

By the end of this module, you will be able to:

- Configure which users and applications have access to your SQL databases
- Block access to your servers using firewalls
- Discover, classify, and audit the use of your data
- Encrypt and protect your data while is it stored in the database.

Prerequisites

- None

Module 14: Configure and manage Azure Monitor 1 hr 3 min Module 10 Units
Use Azure Monitor, Log Analytics, and other Azure tools to monitor the secure operation of your Azure solutions.

Learning objectives

By the end of this module, you will be able to:

- Configure and monitor Azure Monitor
- Define metrics and logs you want to track for your Azure applications

- Connect data sources to and configure Log Analytics
- Create and monitor alerts associated with your solutions security

Prerequisites

- None

Module 15: Enable and manage Microsoft Defender for Cloud
Use Azure Security Center, Azure Defender, and Secure Score to track and improve your security posture in Azure.

Learning objectives

By the end of this module, you will be able to:

- Define the most common types of cyber-attacks
- Configure Azure Security Center based on your security posture
- Review Secure Score and raise it
- Lock down your solutions using Security Center and Defender
- Enable Just-in-Time access and other security features

Prerequisites

- None

Module 16: Configure and monitor Microsoft Sentinel
Use Azure Sentinel to discover, track, and respond to security breaches within your Azure environment.

Learning objectives

By the end of this module, you will be able to:

- Explain what Azure Sentinel is and how it is used
- Deploy Azure Sentinel
- Connect data to Azure Sentinel, like Azure Logs, Azure AD, and others
- Track incidents using workbooks, playbooks, and hunting techniques

Prerequisites

- None

END OF PAGE