Tech Data | ExitCertified®

Gold
Microsoft Partner
Microsoft

Microsoft Azure Security Technologies

Code:	AZ-500T00
Length:	4 days
URL:	View Online

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organizations security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

Skills Gained

After completing this course, students will be able to:

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 Can Benefit

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.

Prerequisites

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defense indepth, 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), InternetSecurity Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have some experience deploying Azure workloads. This course does not cover the basicsof Azure administration, instead the course content builds on that knowledge by addingsecurity specific information.
- Have experience with Windows and Linux operating systems and scripting languages.Course labsmay use PowerShell and the CLI.

Prerequisite courses (or equivalent knowledge and hands-on experience):
This free online training will give you the experience you need to be successful in this course.

- AZ-104: Manage identities and governance in Azure - Learn | Microsoft Docs
- AZ-104: Implement and manage storage in Azure - Learn | Microsoft Docs
- AZ-104: Configure and manage virtual networks for Azure administrators - Learn | Microsoft Docs
- AZ-104: Monitor and back up Azure resources - Learn | Microsoft Docs
- AZ-104: Deploy and manage Azure compute resources - Learn | Microsoft Docs

Course Details

Outline

Module 1: Manage Identity and Access
This module covers Azure Active Directory, Azure Identity Protection, Enterprise Governance, Azure AD PIM, and Hybrid Identity.
Lesson

- Azure Active Directory
- Hybrid Identity
- Azure Identity Protection
- Azure AD Privileged Identity Management
- Enterprise Governance

Lab : Role-Based Access Control
Lab : Azure Policy
Lab : Resource Manager Locks
Lab : MFA, Conditional Access and AAD Identity Protection

Lab : Azure AD Privileged Identity Management
Lab : Implement Directory Synchronization
After completing this module, students will be able to:

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.

Module 2: Implement Platform Protection
This module covers perimeter, network, host, and container security.
Lesson

- Perimeter Security
- Network Security
- Host Security
- Container Security

Lab : Network Security Groups and Application Security Groups
Lab : Azure Firewall
Lab : Configuring and Securing ACR and AKS
After completing this module, students will be able to:

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.

Module 3: Secure Data and Applications
This module covers Azure Key Vault, application security, storage security, and SQL database security.
Lesson

- Azure Key Vault
- Application Security
- Storage Security
- SQL Database Security

Lab : Key Vault (Implementing Secure Data by setting up Always Encrypted)
Lab : Securing Azure SQL Database
Lab : Service Endpoints and Securing Storage
After completing this module, students will be able to:

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.

Module 4: Manage Security Operations
This module covers Azure Monitor, Azure Security Center, and Azure Sentinel.
Lesson

- Azure Monitor
- Azure Security Center
- Azure Sentinel

Lab : Azure Monitor
Lab : Azure Security Center
Lab : Azure Sentinel
After completing this module, students will be able to:

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.

Related Certifications

Authorized training from ExitCertified is created and maintained by the vendor who also creates the certification exams. While it may not be a requirement of certification to attend a vendor-authorized training class, doing so will put you in the best position to successfully complete the related exams. Start training and begin working towards one of the following certifications today.

AZURE APPS AND INFRASTRUCTURE
Microsoft Azure Security Engineer Associate
View Certification arrow_forward
View All Certifications arrow_forward