

**Microsoft Azure Security Technologies (AZ-500)**

**Course Number:** MOC-AZ-500
**Duration:** 4 days

**Overview**

This Microsoft Azure Security Technologies training (AZ-500) teaches attendees how to implement security controls, maintain an organization’s security posture, and identify and remediate security vulnerabilities. In addition, students learn how to set up security for identity and access, platform protection, data and applications, and security operations.  This Azure training prepares students for the [AZ-500 exam](https://docs.microsoft.com/en-us/learn/certifications/exams/AZ-500) for which every attendee receives a voucher.

**Prerequisites**

Students must have knowledge 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.
* Security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
* 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.
* Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.

**Materials**

All Microsoft training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computer for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will be fine.

**Objectives**

* Configure Azure AD and Azure AD Domain Services for security
* Deploy Azure AD Connect
* Deploy and configure Identity Protection
* Describe Zero Trust and how it impacts security
* Create Azure policies to protect your solutions
* Secure your solutions using firewalls and VPNs
* Deploy and configure network security groups to protect your Azure solutions
* Practice layered security by reviewing and implementing Security Center and Security Benchmarks
* Configure security settings for containers and Kubernetes services
* Deploy and configure Azure Key Vault
* Register an application in Azure using app registration
* Configure Azure Storage access in a secure and managed way
* Encrypt and protect your data while it is stored in the database
* Configure and monitor Azure Monitor
* Configure Azure Security Center based on your security posture
* Connect data to Azure Sentinel, like Azure Logs, Azure AD, and others

**Outline**

* Introduction
* Secure Azure Solutions with Azure Active Directory
* Implement Hybrid Identity
* Deploy Azure AD Identity Protection
* Configure Azure AD Privileged Identity Management
* Design an Enterprise Governance Strategy
* Implement Perimeter Security
* Configure Network Security
* Configure and Manage Host Security
* Enable Containers Security
* Deploy and Secure Azure Key Vault
* Configure Application Security Features
* Implement Storage Security
* Configure and Manage SQL Database Security
* Configure and Manage Azure Monitor
* Enable and Manage Microsoft Defender for Cloud
* Configure and Monitor Microsoft Sentinel
* Conclusion