Implement end-to-end security controls for cloud and AI workloads Training

Duration: **4 Day**

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

Overview

The **Implement End-to-End Security Controls for Cloud and AI Workloads Training** course provides practical knowledge and skills for implementing and managing security controls across Microsoft Azure, Microsoft 365, and AI-enabled environments.

Through this training, participants will:

- Learn to implement security measures that protect **identities, data, infrastructure, and applications** across cloud, hybrid, and multicloud environments.
- Develop practical experience with **Microsoft Entra ID, Azure Key Vault, Microsoft Defender for Cloud, and Microsoft Sentinel**.
- Explore approaches to securing **AI applications, autonomous agents, identities, data access paths, gateways, and supporting infrastructure**.
- Strengthen their ability to **reduce unauthorised access, enforce secure configurations, and manage security risks**.
- Build technical knowledge and practical competencies to support preparation for the **SC-500 certification exam**.

This **four-day training course** equips security professionals with the practical capabilities required to implement and manage end-to-end security controls across **Microsoft Azure, Microsoft 365, and AI-enabled workloads**.

The course focuses on protecting **identities, data, infrastructure, applications, and AI solutions** operating in cloud, hybrid, and multicloud environments. Participants will examine how Microsoft security technologies can be used to prevent unauthorised access, reduce security exposure, apply secure configurations, and improve an organisation's overall security posture.

Through **instructor-led sessions, hands-on labs, knowledge checks, demonstrations, and technical discussions**, participants will gain experience working with Microsoft Entra ID, Azure Key Vault, Azure Policy, Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Purview, Microsoft Security Copilot, and other Microsoft security capabilities.

As artificial intelligence becomes more widely integrated into modern cloud solutions, the course also addresses the protection of **AI agents, identities, data access paths, gateways, guardrails, and the infrastructure supporting AI workloads**.

By exploring how different security technologies operate together, participants will develop a broader understanding of cloud and AI security controls and how to apply them to practical security engineering tasks.

Exams and Assessments

Implement end-to-end security controls for cloud and AI workloads Training

Duration: **4 Day**

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

This course supports preparation for the **SC-500 certification exam**.

The associated study areas include **identity, access, and governance management; storage, database, and network security; compute security; and security posture management and monitoring**.

Prerequisites

To benefit fully from this course, participants should have foundational knowledge and experience in the following areas:

- **Microsoft Azure fundamentals:** Subscriptions, resource groups, virtual networks, storage accounts, virtual machines, and Azure role-based access control (RBAC).
- **Identity and access management:** Microsoft Entra ID, authentication, authorisation, multifactor authentication (MFA), Conditional Access, and application or service identities.
- **Core security principles:** Least privilege, defence in depth, Zero Trust, encryption, auditing, threat protection, and secure configuration.
- **Cloud networking:** Virtual networks, subnets, private endpoints, firewalls, VPN connections, and network security rules.
- **Azure workloads:** Storage services, SQL databases, virtual machines, containers, App Services, and APIs.
- **Microsoft security technologies:** Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender XDR, Microsoft Purview, or Microsoft Security Copilot.
- **AI fundamentals:** Copilots, AI agents, prompts, models, and data grounding.
- **Practical experience:** Navigating the Azure portal and performing basic configuration changes in a lab environment.

Implement end-to-end security controls for cloud and AI workloads Training

Duration: **4 Day**

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is intended for **security engineers responsible for protecting organisational systems and information across cloud, hybrid, and AI-enabled environments**.

It is especially relevant to professionals working in:

- **Cloud security and cybersecurity engineering**
- **Identity and access management**
- **Network, infrastructure, and application security**
- **Security operations and threat management**
- **DevOps and cloud platform engineering**
- **AI solution security**
- **Data security and governance**

The course is also appropriate for professionals collaborating with architects, administrators, developers, security analysts, database specialists, and network teams.

It supports learners preparing for responsibilities involving **identity, access, governance, data protection, networking, compute, application platforms, AI workloads, and cloud security posture management**.

Implement end-to-end security controls for cloud and AI workloads Training

Duration: **4 Day**

BILGINÇ
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, participants will be able to:

- Secure **users, applications, and AI agent identities** with Microsoft Entra ID by implementing authentication controls, privileged access management, and appropriate identity configurations.
- Protect **secrets, cryptographic keys, certificates, storage services, databases, and sensitive resources** using Azure Key Vault and related security controls.
- Apply **governance, compliance, and least-privilege controls** through Azure Policy, RBAC, resource management capabilities, and security recommendations.
- Strengthen **Azure network and resource access security** using network segmentation, traffic inspection, private connectivity, firewalls, and other network protection measures.
- Assess and protect **AI workloads, agents, identities, data access paths, gateways, guardrails, and supporting infrastructure**.
- Implement security controls for **virtual machines, hybrid servers, containers, application platforms, APIs, and other cloud workloads**.
- Manage and monitor security posture across **Azure, hybrid, and multicloud environments** using Microsoft Defender for Cloud and related security technologies.
- Configure foundational security operations capabilities with **Microsoft Sentinel**, including event collection, log management, and security monitoring.
- Use **Microsoft Security Copilot** to support security operations by managing workspaces, plugins, agents, and access controls.
- Apply **end-to-end security controls for cloud and AI environments** to practical security engineering scenarios.

Outline

1. Securing Access with Microsoft Entra ID

Explore the importance of **identity security** in protecting cloud and AI workloads. This module examines authentication methods, Conditional Access, privileged access, application registrations, and application identity protection.

Key Topics:

- Implementing and managing authentication methods
- Configuring **Privileged Identity Management (PIM)**
- Enforcing **multifactor authentication (MFA)** through Conditional Access

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Protecting application and service identities
- Authenticating API plugins for declarative agents using secured APIs

2. Protecting Secrets and Keys with Azure Key Vault

Learn how to secure sensitive credentials and cryptographic assets used by cloud workloads. The module covers secure access, secrets management, certificates, managed identities, and workload protection.

Key Topics:

- Configuring and securing **Azure Key Vault**
- Managing cryptographic keys and secrets
- Managing certificates and monitoring Key Vault activity
- Accessing protected resources through **Managed Identities**
- Protecting Azure Key Vault with Microsoft Defender for Cloud

3. Implementing Governance and Security Controls

Examine how **governance and least-privilege principles** contribute to maintaining secure and compliant cloud environments.

Key Topics:

- Enforcing governance through **Azure Policy** and resource locks
- Managing **Role-Based Access Control (RBAC)** assignments
- Supporting appropriate access permissions through access reviews
- Configuring security controls and addressing security recommendations
- Assessing regulatory compliance
- Protecting backup data using Azure security capabilities
- Implementing security controls through **Infrastructure as Code (IaC)**

4. Securing Storage, Databases, and Networking

Explore security measures for protecting cloud data services and controlling network access to Azure resources.

Key Topics:

- Managing access permissions and network security for Azure Storage
- Configuring firewalls, **private endpoints**, and **Shared Access Signatures (SAS)**

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Using Microsoft Defender for Storage
- Securing **Azure SQL Database**
- Configuring SQL auditing and Microsoft Defender for SQL
- Examining data masking and ledger capabilities
- Implementing workload segmentation and isolation
- Centralising network traffic inspection with **Azure Firewall**
- Securing remote and hybrid connections
- Minimising public network exposure for platform services

5. Securing Servers, Virtual Machines, and Hybrid Infrastructure

Learn to implement security measures that protect Azure virtual machines and hybrid server environments.

Key Topics:

- Implementing disk encryption
- Configuring **Trusted Launch** security capabilities
- Providing secure access through **Azure Bastion**
- Managing security for Azure Arc-enabled hybrid servers
- Implementing **Microsoft Defender for Servers**
- Enforcing **Just-in-Time (JIT)** virtual machine access
- Applying virtual machine security configuration controls
- Exploring agentless security capabilities

6. Implementing Security for AI Workloads

Examine emerging security risks associated with artificial intelligence applications and autonomous agents. Learn how **identity protection, data security, platform guardrails, gateways, and workload protection** can work together to reduce AI-related risks.

Key Topics:

- Securing **Microsoft Entra Agent Identity**
- Analysing AI identity risks with Microsoft Defender XDR
- Protecting **Copilot Studio agents**

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Configuring AI gateway security in **Microsoft Foundry**
- Configuring and managing **AI guardrails**
- Securing AI workloads with Microsoft Defender for Cloud
- Enabling workload protection for AI services
- Managing agents through **Microsoft Agent 365**
- Identifying AI data risks using Microsoft Purview**Data Security Posture Management**

7. Securing Containers and Application Platforms

Develop an understanding of security controls for modern application platforms, containers, APIs, and web services.

Key Topics:

- Identifying container risks with Microsoft Defender for Containers
- Securing **Azure Kubernetes Service (AKS)**
- Protecting Azure Container Registry, Container Instances, and Container Apps
- Securing **Azure Functions** and Logic Apps
- Implementing security controls for Azure App Services
- Using **Web Application Firewall (WAF)** capabilities
- Protecting API back-end services with Azure API Management

8. Managing Cloud Security Posture

Build the skills required to identify security risks, improve security posture, and manage protection across cloud, hybrid, and multicloud environments.

Key Topics:

- Connecting hybrid and multicloud environments to**Microsoft Defender for Cloud**
- Identifying risks through **Cloud Security Posture Management (CSPM)**
- Discovering unprotected assets and security vulnerabilities
- Exploring **External Attack Surface Management**
- Assessing regulatory compliance
- Enabling and configuring workload protection plans
- Managing vulnerability settings for Azure virtual machines

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Using **Secure Score**, security recommendations, secret scanning, and governance controls

9. Collecting and Managing Security Events with Microsoft Sentinel

Explore essential security operations capabilities using **Microsoft Sentinel**, including event collection, automation, log management, and security data analysis.

Key Topics:

- Creating and managing Microsoft Sentinel workspaces
- Managing security content
- Connecting Microsoft and third-party data sources
- Collecting **Syslog, Common Event Format (CEF)**, and Windows host data
- Implementing automation rules and **playbooks**
- Managing data storage
- Querying and auditing collected security logs

10. Implementing Microsoft Security Copilot

Discover how **Microsoft Security Copilot** supports security operations through configured workspaces, plugins, agents, and access management capabilities.

Key Topics:

- Understanding Microsoft Security Copilot features and capabilities
- Configuring **Security Copilot workspaces**
- Managing plugins and agents
- Understanding the **Security Compute Unit (SCU)** consumption model
- Managing relevant roles and access permissions