

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

**Courses Code:** SC\_500T00

**Duration:** 4 Days

**Delivery Mode:** Instructor-led Training (ILT) | Virtual Instructor led Training (VILT)

### Overview

This course prepares you to design, implement, and manage end-to-end security controls across Microsoft Azure and Microsoft 365 environments — including the emerging landscape of AI workloads and autonomous agents. Through a combination of instructor-led sessions and hands-on labs, you build practical skills in identity security, cloud infrastructure protection, threat detection, and posture management. This course is intended for security engineers who are responsible for planning and implementing security controls across cloud, hybrid, and multi-cloud environments using Microsoft security technologies.

### Skills Covered

- Design and implement end-to-end security controls across Microsoft Azure and Microsoft 365 environments.
- Secure identities and access using Microsoft Entra ID, Conditional Access, Privileged Identity Management (PIM), and Zero Trust principles.
- Protect secrets, keys, and certificates by implementing security best practices for Azure Key Vault.
- Enforce security governance and regulatory compliance using Azure Policy, resource locks, RBAC, and Microsoft Defender for Cloud.
- Secure Azure Storage, Azure SQL Database, and SQL Managed Instance with encryption, identity-based access, and threat protection.
- Implement network security controls using Network Security Groups (NSGs), Azure Firewall, Azure Private Link, Private Endpoints, and Microsoft Entra Private Access.
- Protect AI workloads by implementing layered security controls for AI platforms, identities, data, and runtime environments.
- Secure Azure virtual machines, Azure Arc-enabled servers, and hybrid environments using Trusted Launch, Azure Bastion, Just-in-Time VM access, and Microsoft Defender for Servers.
- Implement security for Azure application platform services, including Azure Kubernetes Service (AKS), Azure Container Registry (ACR), Azure App Service, Azure Functions, Logic Apps, Azure API Management, and Web Application Firewall (WAF).



- Monitor and strengthen cloud security posture using Microsoft Defender for Cloud, Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Defender External Attack Surface Management (EASM), and Microsoft Defender Vulnerability Management.
- Configure security monitoring, event collection, automated response, and compliance reporting using Microsoft Sentinel.
- Deploy, configure, and manage Microsoft Security Copilot, including workspace planning, governance, plugin management, and AI security operations.
- Apply security best practices across cloud, hybrid, and multi-cloud environments to detect threats, reduce risk, and maintain regulatory compliance.

### Who Should Attend

As a candidate for this course, you're a security engineer who protects organizational systems and data across cloud and hybrid environments by implementing comprehensive security controls that prevent unauthorized access and mitigate risks proactively. This role spans multiple security domains including identity, network, application, data, and compute. This role also ensures that platforms, data, identities, and infrastructure used by AI workloads are securely implemented and monitored. You work closely with architects, administrators, engineers, analysts, and developers responsible for Azure, Microsoft 365, identity and access, information protection, security operations, devops, application development, database platforms, and networks. You should have practical experience in administration of Microsoft Azure and hybrid environments, including compute, network, and storage. You should have strong familiarity with Microsoft Entra ID and familiarity with Microsoft 365 administration. Your responsibilities for this role include:

- Securing access to resources by using Microsoft Entra ID and Azure Key Vault
- Enforcing security and regulatory compliance
- Securing storage, databases, and networking
- Securing compute
- Securing AI solutions
- Managing and monitoring security posture

### Prerequisites

- A basic understanding of business operations and supply chain management concepts.
- Familiarity with procurement, inventory, warehousing, manufacturing, or sales business processes is beneficial.
- Basic computer skills and experience using Microsoft Windows and Microsoft 365 applications.
- An interest in learning enterprise resource planning (ERP) solutions and how they support end-to-end business operations.
- No prior experience with Microsoft Dynamics 365 is required; however, a general understanding of business applications and cloud-based solutions is helpful.



## Course Modules

### Module 1: Secure access to resources by using Microsoft Entra

Controlling who can access what, and under what conditions, is one of the most consequential responsibilities in cloud security. A misconfigured authentication policy, an overprivileged account left unreviewed, or a poorly secured AI agent can each become the foothold an attacker needs to move laterally through your environment.

### Module 2: Secure Azure Key Vault with defense in depth for the cloud and AI workloads

Implement a defense-in-depth security strategy for Azure Key Vault. In this learning path, you apply security-hardened vault configuration, enforce least-privilege access with just-in-time activation, manage the full lifecycle of keys, secrets, and certificates, and use Microsoft Defender for Cloud to detect exposed credentials and malicious access patterns targeting your vaults.

### Module 3: Enforce security governance and regulatory compliance

Enforce security governance and regulatory compliance across Azure environments. Configure Azure Policy and resource locks to block noncompliant deployments. Then manage security standards and remediate recommendations in Defender for Cloud, evaluate regulatory compliance posture, govern RBAC role assignments at scale, protect backup data against ransomware and deletion, and embed security controls into Bicep pipelines before resources reach production.

### Module 4: Implement security for Azure Storage for the cloud and AI security engineer

Implement a defense-in-depth security strategy for Azure Storage. In this learning path, you harden storage accounts against common attack vectors, and govern access with Microsoft Entra ID managed identities and stored access policies. Next you configure network perimeter controls using firewall rules and private endpoints, and enable Microsoft Defender for Storage to detect threats including malicious file uploads and compromised AI agent credentials.

### Module 5: Implement security for Azure SQL databases

Implement end-to-end security for Azure SQL Database and SQL Managed Instance. Configure Entra ID authentication with managed identity access, deploy private endpoints, and apply encryption and access controls to protect sensitive financial data. Establish compliant audit trails and enable Microsoft Defender for Databases to detect SQL injection, anomalous access, and vulnerability exposures.

### Module 6: Implement network security controls in Azure

Implement defense-in-depth network security controls in Azure. Segment workloads and enforce least-privilege access using NSGs, ASGs, and Azure Virtual Network Manager. Inspect and control traffic centrally with Azure Firewall. Harden remote and hybrid connectivity and replace broad VPN access with Zero Trust application-level access using Microsoft Entra Private Access. Eliminate public exposure of PaaS and AI services using private endpoints and Azure Private Link.



### **Module 7: Implement security for AI**

AI workloads introduce new attack surfaces across identity, data, and runtime layers that traditional security controls don't fully address. In this learning path, you implement layered AI security controls across the Microsoft security platform.

### **Module 8: Implement security for servers and virtual machines**

Implement layered security controls across Azure virtual machines and Arc-enabled hybrid servers. Configure disk encryption options including encryption at host with customer-managed keys and confidential disk encryption. Enable Trusted Launch security features—Secure Boot, vTPM, and integrity monitoring—to protect against boot-level threats. Eliminate public RDP and SSH exposure with Azure Bastion. Extend Azure security governance to on-premises and multicloud servers using Azure Arc. Deploy Microsoft Defender for Servers for vulnerability scanning, endpoint detection, agentless machine scanning, and File Integrity Monitoring. Enforce just-in-time VM access to eliminate permanently open management ports. Apply Azure Machine Configuration to audit and enforce OS security baselines across your entire server estate.

### **Module 9: Secure Azure application platform services for the cloud and AI security engineer**

Implement security controls across Azure application platform services—from container workloads to the API layer. Configure Microsoft Defender for Containers to detect risks in AKS and ACR, enforce AKS security baselines, harden container registries and runtime environments. Then apply authentication, network access, and policy controls across Azure Function apps, Logic apps, App Services, Web Application Firewall, and Azure API Management.

### **Module 10: Manage security posture by using Microsoft Defender for Cloud**

Learn to build and maintain a strong security posture across your hybrid and multicloud estate using Microsoft Defender for Cloud. You start by connecting on-premises, AWS, and GCP environments to establish unified visibility. You then identify and prioritize security risks using Cloud Security Posture Management (CSPM)—including Secure Score, attack path analysis, and Cloud Security Explorer. You extend that posture view outside-in with Microsoft Defender External Attack Surface Management (EASM) to discover unknown internet-facing assets and surface exploitable exposure. You assess your organization's compliance posture against regulatory frameworks and generate audit-ready reports. Finally, you enable Cloud Workload Protection Platform (CWPP) plans to defend servers, storage, databases, and AI workloads against active threats. Then configure Microsoft Defender Vulnerability Management to scan and remediate vulnerabilities on Azure VMs.

### **Module 11: Implement activity and event collection in Microsoft Sentinel**

Build a complete event collection and response architecture in Microsoft Sentinel. In this learning path, you set up and secure a Microsoft Sentinel workspace, deploy Content Hub solutions, and connect Azure resource data. Then you collect Linux and Windows security events with data collection rules,



and implement automated response workflows with Logic Apps playbooks. The final stage is to manage data retention and audit log access to meet compliance requirements.

### **Module 12: Deploy and operate Microsoft Security Copilot**

In this learning path, you build a working foundation with Microsoft Security Copilot and advance to enterprise-grade deployment and day-to-day operations. You start by exploring core concepts, how Security Copilot processes natural language prompts, the elements of an effective prompt, and the steps to enable the solution for your organization. You then plan and configure workspaces with the right Security Compute Units, data residency settings, and role assignments to support enterprise segmentation requirements. Finally, you govern plugin access and manage the full lifecycle of both Microsoft-built and partner-built agents to keep your deployment running smoothly and securely.

Ref: <https://trainocate.com/courses/microsoft/sc-500t00-implement-end-to-end-security-controls-for-cloud-and-ai-workloads-training>

**END OF THE PAGE**

