Microsoft Azure IaaS Security Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today?ÇÖs accelerated world of digital transformation and cloud adoption, organizations are rapidly shifting mission-critical Infrastructure as a Service (IaaS) workloads to Microsoft Azure. This migration introduces a complex layer of shared responsibility where securing the operating systems, applications, and data falls squarely on the customer. A significant gap exists between standard Azure deployment and a truly secure cloud posture, often leading to critical security misconfigurations and exposure to advanced persistent threats. This course is the essential, deep-dive training that bridges that gap.

Microsoft Azure IaaS Security Training Course focuses on implementing a Zero Trust Architecture across your Azure IaaS environment. You'll master the deployment and configuration of key native security controls including Azure Network Security Groups, Azure Key Vault, Microsoft Defender for Cloud, and Microsoft Entra ID to establish robust identity and access management and strong network microsegmentation. Equip yourself with the skills to mitigate common IaaS risks, ensure regulatory compliance, and become a central figure in your organization's Cloud Security Posture Management strategy.

Programme Curriculum

Microsoft Azure IaaS Security Training Course

Introduction

In today?ÇÖs accelerated world of digital transformation and cloud adoption, organizations are rapidly shifting mission-critical Infrastructure as a Service (IaaS) workloads to Microsoft Azure. This migration introduces a complex layer of shared responsibility where securing the operating systems, applications, and data falls squarely on the customer. A significant gap exists between standard Azure deployment and a truly secure cloud posture, often leading to critical security misconfigurations and exposure to advanced persistent threats. This course is the essential, deep-dive training that bridges that gap.

Microsoft Azure IaaS Security Training Course focuses on implementing a Zero Trust Architecture across your Azure IaaS environment. You'll master the deployment and configuration of key native security controls including Azure Network Security Groups, Azure Key Vault, Microsoft Defender for Cloud, and Microsoft Entra ID to establish robust identity and access management and strong network microsegmentation. Equip yourself with the skills to mitigate common IaaS risks, ensure regulatory compliance, and become a central figure in your organization's Cloud Security Posture Management strategy.

Course Duration

5 days

Course Objectives

1. Master the Azure Shared Responsibility Model to clearly define customer security scope in IaaS.
2. Design and implement a robust Zero Trust Architecture for Azure Virtual Machines (VMs) and networks.
3. Configure Network Security Groups (NSGs) and Azure Firewall for advanced network microsegmentation.
4. Implement and manage Microsoft Defender for Cloud (MDfC) for Cloud Workload Protection (CWP) and CSPM.
5. Establish powerful Identity and Access Management (IAM) using Microsoft Entra ID and Conditional Access.
6. Securely manage application secrets, keys, and certificates using Azure Key Vault with Hardware Security Module (HSM) integration.
7. Apply and enforce Azure Policy and Azure Blueprints to automate security governance and compliance.
8. Implement Azure Disk Encryption and manage the keys to ensure data at rest is protected.
9. Configure Just-in-Time (JIT) VM Access to minimize the attack surface for administrative endpoints.
10. Integrate Azure Sentinel (SIEM/SOAR) for advanced threat detection, proactive hunting, and automated incident response.
11. Develop and execute a continuous vulnerability management and patch management strategy for VMs.
12. Leverage Azure Backup and Azure Site Recovery to ensure IaaS disaster recovery and business continuity.
13. Integrate IaaS security controls into a modern DevSecOps pipeline using Infrastructure as Code (IaC).

Target Audience

1. Cloud Security Engineers
2. Azure Administrators/Engineers
3. Security Operations (SecOps) Analysts
4. Security Architects
5. DevSecOps Practitioners
6. IT Risk and Compliance Officers
7. Cloud Migration Specialists
8. Information Security Managers

Course Modules

Module 1: Foundations of Azure IaaS Security & Zero Trust

- Reviewing the Shared Responsibility Model and customer security obligations for IaaS.
- Implementing the Zero Trust principle in an IaaS context.
- Securing the Azure Management Plane using Microsoft Entra ID and PIM.

- Hardening the Azure Subscription and Resource Group access with RBAC.
- Case Study: Analyzing a breach scenario where unmanaged credentials led to lateral movement via a compromised service principal.

Module 2: Network Security and Microsegmentation

- Designing secure Virtual Networks and subnets for IaaS workloads.
- Deep-dive configuration of Network Security Groups and Application Security Groups.
- Deploying and managing Azure Firewall and Web Application Firewall on Azure Application Gateway.
- Enforcing JIT VM Access and Bastion Host deployment to eliminate RDP/SSH exposure.
- Case Study: Implementing Network Microsegmentation to isolate a multi-tier web application using NSGs, preventing a single server compromise from reaching the backend database.

Module 3: Identity, Access, and Credential Protection

- Enforcing strong Multi-Factor Authentication and Conditional Access Policies for all administrators.
- Implementing Privileged Identity Management for JIT role activation.
- Using Microsoft Entra ID to authenticate Linux/Windows VMs.
- Storing and rotating application secrets, keys, and certificates in Azure Key Vault.
- Case Study: The SolarWinds-style breach scenario focusing on compromised identities and how PIM and Conditional Access would have limited the blast radius.

Module 4: Virtual Machine (VM) and Host Hardening

- Implementing a robust patch management strategy for Windows and Linux guest OS
- Configuring and verifying Azure Disk Encryption for OS and Data Disks.
- Installing and integrating a next-generation antimalware solution
- Securing VM images using Azure Image Builder and ensuring no default secrets exist.
- Case Study: Mitigating a Ransomware attack on an unpatched VM by leveraging ADE and Azure Backup?ÇÖs immutability features.

Module 5: Security Posture Management and Governance

- Onboarding and utilizing Microsoft Defender for Cloud for CSPM scores and recommendations.
- Configuring Azure Policy to prevent misconfigurations and enforce security baselines
- Deploying standard security environments using Azure Blueprints or Terraform IaC.
- Implementing regulatory compliance controls within MDfC.
- Case Study: Automating compliance for 100+ new VMs by enforcing a custom Azure Policy that mandates network logging and anti-malware at deployment.

Module 6: Threat Detection and Incident Response (SecOps)

- Integrating Activity Logs and Resource Logs with Azure Monitor and Log Analytics Workspace.
- Deploying and customizing Azure Sentinel for SIEM/SOAR functionality.
- Creating custom Kusto Query Language queries for proactive threat hunting.
- Automating incident response using Sentinel Playbooks
- Case Study: Developing a Sentinel Analytic Rule and Playbook to automatically isolate a VM after detecting a brute-force attack on an administrative account.

Module 7: Data Protection and Storage Security

- Securing Azure Storage Accounts used by IaaS with fine-grained SAS tokens and Access Tiers.

- Enabling encryption at rest for all managed disks and storage accounts.
- Implementing Azure Backup for IaaS VMs with immutability and long-term retention policies.
- Configuring network access control for Storage Accounts using Service Endpoints or Private Link.
- Case Study: A data leak scenario where a misconfigured storage account public access was exploited, and the subsequent remediation using Private Link and MDfC storage protection.

Module 8: Advanced Security and DevSecOps Integration

- Integrating security scanning into a DevOps/DevSecOps pipeline for VM images and IaC.
- Securing containerized workloads using Defender for Containers.
- Reviewing security best practices for specialized IaaS workloads
- Future-proofing IaaS security with concepts like Confidential Computing and eBPF-based runtime security.
- Case Study: Transforming a manual VM deployment process into a secure, automated IaC pipeline that includes security checks

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com