

SC-500: Cloud and AI Security Engineer

Protect Azure workloads and the AI services built on them, from identity to posture management — and prepare for SC-500.

DURATION

4 days · 32 hours

LEVEL

Intermediate

CURRICULUM

13 modules · 10 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

Cloud security work has widened. Engineers who once focused on network rules and role assignments now also need to secure model endpoints, prompt data, AI search indexes and the identities that applications use to reach them. This four-day course prepares you for that broader role by securing a realistic Azure workload one layer at a time.

Day one establishes identity and access: Microsoft Entra ID, Conditional Access, Privileged Identity Management, managed identities and Azure role-based access control. Day two hardens the network and platform with network security groups, Azure Firewall, private endpoints, Key Vault and encryption choices for storage and databases.

Day three is dedicated to AI workloads. You will lock down access to AI services, apply network isolation and keyless authentication, configure content safety, protect sensitive data used for grounding and review the threats specific to generative AI applications, such as prompt injection and data leakage. Day four covers security operations: Microsoft Defender for Cloud, regulatory compliance dashboards, workload protection plans and sending signals to Microsoft Sentinel.

Labs build on each other, so you finish with a sample application whose identity, network, data and AI layers you have secured yourself, together with a checklist you can reuse at work.

This course is aligned to the SC-500 exam, reported as the successor to AZ-500, which retired on 31 August 2026. As the exam is new, verify the current skills outline on Microsoft Learn before booking; we revise the course as Microsoft publishes changes.

Highlights

- 32 hours of live, lab-focused sessions
- Secures a sample workload layer by layer across four days
- Dedicated day on securing AI and model endpoints
- Defender for Cloud posture and threat protection in practice
- Successor path for learners who planned to take AZ-500

What's included

- Layer-by-layer hardening of one sample workload
- Dedicated AI workload security day
- Privileged Identity Management and Conditional Access labs
- Private endpoints, Azure Firewall and Key Vault in practice
- Defender for Cloud recommendations and secure score
- Reusable security review checklist
- 30 days of post-training doubt support

Who this course is for

Who should attend

- Azure security engineers and cloud security specialists
- Azure administrators taking on security responsibilities
- Learners who were preparing for the retired AZ-500 exam
- Engineers deploying AI services in regulated environments
- Security architects reviewing cloud and AI designs

Prerequisites

- Hands-on Azure administration experience (AZ-104 level recommended)
- Understanding of networking and identity concepts
- Familiarity with security fundamentals (SC-900 level helps)

Detailed curriculum — 4 days, 32 hours, 13 modules, 10 hands-on labs

Day 1 Identity and Access Security

8 hours

1.1 Microsoft Entra ID protection

- Conditional Access policy design
- Identity Protection risk policies
- Phishing-resistant MFA
- Emergency access accounts

LAB Build Conditional Access policies with report-only testing · 50 min

1.2 Privileged access

- Privileged Identity Management for Entra and Azure roles
- Least privilege with Azure RBAC and custom roles
- Access reviews
- Just-enough administration

LAB Configure PIM activation with approval for an Azure role · 45 min

1.3 Application and workload identities

- Managed identities
- Workload identity federation
- Service principals and credential hygiene
- App consent and permissions

LAB Replace stored credentials with a managed identity · 35 min

Day 2 Network, Data and Compute Security

8 hours

2.1 Network security

- NSGs and application security groups
- Private endpoints and service endpoints
- DDoS protection
- Azure Firewall and firewall policies
- Web Application Firewall

LAB Isolate a workload with private endpoints and Azure Firewall · 60 min

2.2 Data protection

- Azure Key Vault access models
- Storage account hardening
- Encryption at rest with customer-managed keys
- Azure SQL security features

LAB Encrypt storage with a customer-managed key from Key Vault · 40 min

2.3 Compute security

- VM hardening and Azure Bastion
- Container registry and AKS security basics
- Just-in-time VM access
- App Service authentication and access restrictions

Day 3 Securing AI Workloads

8 hours

3.1 AI service access

- Keyless authentication to AI services
- Network isolation for model endpoints
- RBAC roles for AI resources
- Quotas and abuse controls

LAB Lock down an AI service with private networking and keyless access · 55 min

3.2 Generative AI threats

- Prompt injection and jailbreak attempts
- Content safety and filtering configuration
- Data leakage through grounding data
- Threat modelling an AI application

LAB Configure content filters and test with adversarial prompts · 45 min

3.3 Protecting AI data

- Securing AI Search indexes and data sources
- Logging and auditing AI usage
- Sensitivity labels and Microsoft Purview for AI

LAB Restrict a search index with role-based access · 35 min

Day 4 Security Posture, Operations and Exam Readiness

8 hours

4.1 Microsoft Defender for Cloud

- Secure score and recommendations
- Regulatory compliance dashboards
- Defender plans for servers, storage, databases and AI
- Attack path analysis

LAB Remediate recommendations and raise secure score · 50 min

4.2 Governance for security

- Azure Policy for security baselines
- Multi-subscription posture management
- Security benchmarks

LAB Assign a security initiative and review compliance · 35 min

4.3 Monitoring and response

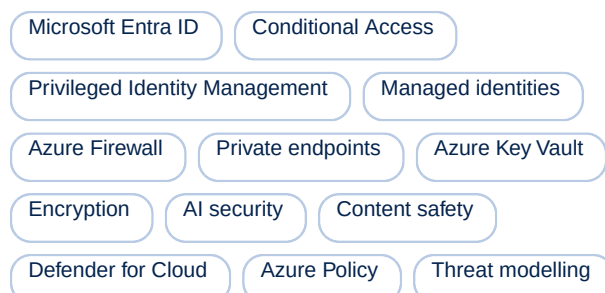
- Diagnostic settings and log collection
- Investigating security alerts
- Connecting Defender for Cloud to Microsoft Sentinel

4.4 Exam readiness

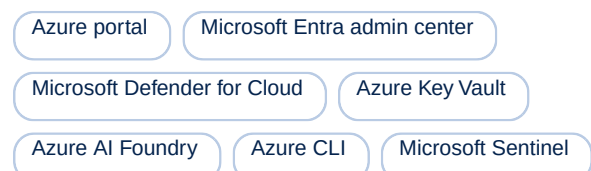
- Exam format and scenario questions
- Practice questions with review
- Common distractors in security questions

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	Cloud and AI Security Engineer (SC-500)
Exam code	SC-500
Delivery	Online proctored, Test centre
Validity	1 year (free online renewal assessment)
Official page	https://learn.microsoft.com/credentials/

Exam skill areas covered

Secure network access
Secure network storage and databases

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

I was preparing for AZ-500. Should I switch to this course?

Yes. AZ-500 retired on 31 August 2026, and SC-500 is the reported successor; most AZ-500 topics carry over, with added depth on AI workloads.

Do I need AI experience?

No. We explain how AI services are deployed and used before securing them, so a general Azure background is enough.

How much of the course is hands-on?

Every day has two or three guided labs, and together they harden a single sample workload from identity through to posture management.

What happens if Microsoft updates the SC-500 exam?

We map the curriculum to the current published skills outline and revise it when Microsoft changes the exam. Always check the latest outline on Microsoft Learn before booking.

Do you run weekend batches?

Yes. Weekend batches cover the same 32 hours across consecutive Saturdays and Sundays, with timings in IST that also suit learners in the Gulf.

Can you run a private batch for our team?

Yes. We run private online or onsite batches for corporate teams, and we can weight the labs towards your security baseline and compliance needs. Request a corporate quote with your team size and preferred dates.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/sc-500-cloud-and-ai-security-engineer · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

Microsoft, Azure, Microsoft 365, Power BI and Microsoft Entra are trademarks of the Microsoft group of companies. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.