

Microsoft 365 Security Architecture

ARC501

Design, justify, implement, and defend a Zero Trust security architecture for Microsoft 365 that protects every user, device, app, and data across Entra ID, Defender XDR, Purview, Intune, and hybrid environments.

Modules	23
Lessons	253
Phases	4
Free preview	Course Orientation (8 lessons)

The method

Architecture is the discipline of making decisions that later decisions depend on. This course runs the same loop for every layer it designs, and the layers are deliberately in dependency order.

1. Decide, and write down why. An architecture is a set of decisions with reasons attached. Without the reason, the next person reverses it and nobody knows what broke.
2. Design against the attack, not the feature list. Each layer is built from what it has to stop rather than from what the product can do.
3. Check the layer against the one beneath it. Conditional Access rests on authentication methods, detection rests on workspace design, and a strong layer on a weak one is a weak layer.
4. Make the failure mode explicit. Every control blocks somebody, every log has a retention, every design has a cost. An architecture that hides these gets overruled in an incident.
5. Produce something that outlives you. Decision records, not diagrams. The diagram shows the state; the record explains why it is that state.

The capstone assembles the complete architecture from every layer designed along the way.

What this course assumes

No minimum experience and no prerequisite course. Each service is introduced from what it does architecturally rather than from how it is administered.

What makes it go faster: an estate you are responsible for, because every design decision in the course has a real counterpart in it. Not required.

What this course does not cover: hands-on administration of each service, incident response process and forensics. This course decides what should exist; the operational courses run it.

Full syllabus

Phase 1: Identity Foundation

Course Orientation FREE PREVIEW

What Microsoft 365 Security Architecture teaches: design, justify, and defend one Zero Trust architecture across identity, devices, apps, and data, with detection, response, and governance, and walk away with a portfolio-grade package of ADRs, decision matrices, a risk register, diagrams, and an...

1. MSA0.1 What Security Architecture Actually Is
2. MSA0.2 The M365 Security Stack as Architecture
3. MSA0.3 Architecture Decision Records
4. MSA0.4 Threat-Informed Architecture
5. MSA0.5 Your Tenant Baseline Assessment
6. MSA0.6 Lab Setup and Cost Management
7. MSA0.7 Your Architecture Package
8. Module Summary

Entra ID Identity Architecture

The foundation. Every authentication, every authorization, every access decision in M365 flows through Entra ID. This module teaches you to design the identity layer, tenant architecture, identity types and their attack surfaces, hybrid identity, directory structure, the identity lifecycle...

1. MSA1.1 Tenant Architecture. The Boundary That Constrains Everything
2. MSA1.2 Identity Types in Entra ID
3. MSA1.3 The Attack Surface of Each Identity Type
4. MSA1.4 Hybrid Identity Architecture
5. MSA1.5 Hybrid Identity. What Breaks and What's Legacy
6. MSA1.6 Directory Structure and Administrative Units
7. MSA1.7 The Identity Lifecycle. Joiner, Mover, Leaver
8. MSA1.8 Stale Identities and Access Accumulation
9. MSA1.9 Naming Conventions and Governance Foundations
10. MSA1.10 Group Architecture
11. MSA1.11 NE Identity Assessment
12. MSA1.12 Module Lab. Identity Baseline
13. MSA1.13 Guided Walkthrough. The Identity Layer as a System
14. Module Summary
15. Check My Knowledge

Authentication Architecture

Design an authentication architecture that stops real attacks, beyond enabling MFA.

1. MSA2.1 Authentication Methods. The Security Analysis
2. MSA2.2 How AiTM Attacks Work. Why Phishing Resistance Matters
3. MSA2.3 Phishing-Resistant Authentication Design
4. MSA2.4 The Passwordless Roadmap
5. MSA2.5 Legacy Authentication. Kill It or Manage It
6. MSA2.6 Service Account and Workload Authentication
7. MSA2.7 Authentication Strength Policies
8. MSA2.8 SSPR Architecture
9. MSA2.9 Token Protection and Session Security
10. MSA2.10 Authentication Architecture Assessment
11. MSA2.11 Module Lab. Authentication Implementation
12. MSA2.12 Guided Walkthrough. The Authentication Architecture as a System
13. Module Summary
14. Check My Knowledge

Conditional Access Architecture

Design a systematic CA framework that's maintainable, auditable, and resilient to bypass.

1. MSA3.1 Conditional Access as the Policy Engine
2. MSA3.2 Policy Design Methodology
3. MSA3.3 The Baseline Policy Set
4. MSA3.4 Tiered Access Policies
5. MSA3.5 Device-Based Conditional Access Policies
6. MSA3.6 Application-Specific Conditional Access Policies
7. MSA3.7 Named Locations and Network Controls
8. MSA3.8 Break-Glass Accounts and Emergency Access
9. MSA3.9 Policy Lifecycle and Change Management
10. MSA3.10 Exception Management
11. MSA3.11 CA Policy Audit and Compliance Evidence
12. MSA3.12 Hybrid Conditional Access
13. MSA3.13 The Complete Conditional Access Architecture
14. MSA3 Module Lab. CA Framework Deployment
15. MSA3 Guided Walkthrough. The CA Framework as a System
16. Module Summary
17. Check My Knowledge

Phase 2: Protection Stack

Privileged Access Architecture

Design a privilege model where administrative access is earned temporarily, not granted permanently.

1. MSA4.1 The Privilege Problem in M365
2. MSA4.2 Entra ID Role Architecture
3. MSA4.3 PIM Design and Deployment
4. MSA4.4 Privileged Access Workstations
5. MSA4.5 Service Principal and Managed Identity Governance
6. MSA4.6 Cross-Tenant and B2B Privilege
7. MSA4.7 Emergency Access Architecture
8. MSA4.8 Securing Microsoft Copilot and AI Workloads
9. MSA4.9 The Complete Privileged Access Architecture
10. MSA4 Module Lab. Privileged Access Deployment
11. MSA4 Guided Walkthrough. The Privilege Architecture as a System
12. Module Summary
13. Check My Knowledge

Data Protection Architecture

Design a data protection framework that controls what happens to sensitive data after a legitimate user has access to it.

1. MSA5.1 Data Classification Strategy
2. MSA5.2 Sensitivity Label Architecture
3. MSA5.3 DLP Policy Architecture
4. MSA5.4 Information Barriers
5. MSA5.5 DLP Channels
6. MSA5.6 Retention Architecture
7. MSA5.7 Insider Risk Management
8. MSA5.8 Complete Architecture
9. MSA5 Module Lab. Data Protection Deployment
10. MSA5 Guided Walkthrough. Data Protection as a System
11. Module Summary
12. Check My Knowledge

Endpoint Security Architecture

Design device trust as an architectural pillar, compliance policies that evaluate real security properties across four platforms, configuration baselines that prevent drift, custom compliance scripts for settings built-in rules can't check, BYOD strategy with app protection, MDE as a real-time...

1. MSA6.1 Endpoint Trust as an Architectural Pillar
2. MSA6.2 Windows Compliance Policy Design
3. MSA6.3 iOS, macOS, and Android Compliance
4. MSA6.4 The Compliance Tier Model
5. MSA6.5 Configuration Baseline Design
6. MSA6.6 Configuration Drift and Baseline Lifecycle
7. MSA6.7 App Protection Without Device Enrollment
8. MSA6.8 MDE as the Risk Signal
9. MSA6.9 Attack Surface Reduction Architecture
10. MSA6.10 Automated Investigation and Endpoint Privilege Management
11. MSA6.11 Autopilot and Device Lifecycle
12. MSA6.12 Your Endpoint Architecture
13. MSA6 Module Lab. Endpoint Security Deployment
14. MSA6 Guided Walkthrough. Connecting the Endpoint Architecture
15. Module Summary
16. Check My Knowledge

Email and Collaboration Security Architecture

Design the protection architecture for the attack surface where most breaches begin, email and collaboration.

1. MSA7.1 Email Threat Surface Audit
2. MSA7.2 EOP Baseline Protection
3. MSA7.3 Safe Links Architecture
4. MSA7.4 Safe Attachments Architecture
5. MSA7.5 Anti-Phishing and Impersonation Protection
6. MSA7.6 Attack Simulation and User Resilience
7. MSA7.7 SPF and DKIM. Domain Authentication
8. MSA7.8 DMARC and ARC. Policy Enforcement
9. MSA7.9 Teams Security Architecture
10. MSA7.10 SharePoint and OneDrive External Sharing
11. MSA7.11 Post-Delivery Response Architecture
12. MSA7.12 Complete Email and Collaboration Architecture
13. MSA7 Module Lab. Email and Collaboration Security Deployment
14. Guided Walkthrough. Email and Collaboration Security
15. Module Summary
16. Check My Knowledge

Phase 3: Detection & Response

Sentinel Workspace Architecture

Design the detection and investigation infrastructure, workspace topology, data connectors, log tiering, RBAC, and content deployment for Microsoft Sentinel.

1. MSA8.1 Workspace Design Decisions
2. MSA8.2 Workspace Cost Modeling
3. MSA8.3 M365 Data Connectors
4. MSA8.4 Azure and Third-Party Connectors
5. MSA8.5 Log Tier Architecture
6. MSA8.6 Data Collection Rules and Transformation
7. MSA8.7 Workspace RBAC Architecture
8. MSA8.8 Table-Level and Resource-Context Access
9. MSA8.9 Content Hub and Solution Deployment
10. MSA8.10 Workbook and Hunting Architecture
11. MSA8.11 Workspace Health and Cost Monitoring
12. MSA8.12 Complete Sentinel Architecture
13. MSA8 Module Lab. Sentinel Workspace Deployment
14. Guided Walkthrough. Sentinel Workspace Architecture
15. Module Summary
16. Check My Knowledge

Detection Architecture

Design the detection rule framework, analytics rule architecture, identity and email detection patterns, privileged activity monitoring, data exfiltration detection, alert tuning, and detection coverage measurement.

1. MSA9.1 Detection Philosophy. What to Detect and Why
2. MSA9.2 Analytics Rule Types and Architecture
3. MSA9.3 Identity-Based Detection. Credential Compromise
4. MSA9.4 Identity-Based Detection. Privilege Abuse and Lateral Movement
5. MSA9.5 Email-Based Detection Patterns
6. MSA9.6 Endpoint Detection Architecture
7. MSA9.7 Data Exfiltration Detection
8. MSA9.8 Cloud App and OAuth Detection
9. MSA9.9 Alert Tuning and False Positive Management
10. MSA9.10 Detection Coverage Measurement
11. MSA9.11 Detection-as-Code and Rule Lifecycle
12. MSA9.12 Complete Detection Architecture
13. MSA9 Module Lab. Detection Architecture Deployment
14. Guided Walkthrough. Detection Architecture
15. Module Summary
16. Check My Knowledge

Incident Response Architecture

Design the incident response architecture, automation rules, containment playbooks, evidence preservation, incident workflows, communication procedures, and post-incident review.

1. MSA10.1 IR Architecture vs IR Execution
2. MSA10.2 Automation Rules and Playbook Architecture
3. MSA10.3 Automated Investigation and Response (AIR)
4. MSA10.4 Containment Architecture. Identity Actions
5. MSA10.5 Containment Architecture. Endpoint and Network
6. MSA10.6 Evidence Preservation and Forensic Readiness
7. MSA10.7 Incident Classification and Severity Framework
8. MSA10.8 Incident Workflow and Assignment Architecture
9. MSA10.9 Communication and Escalation Architecture
10. MSA10.10 Post-Incident Review and Lessons Learned
11. MSA10.11 IR Playbook Library
12. MSA10.12 Complete Response Architecture
13. MSA10 Module Lab. Response Architecture Deployment
14. Guided Walkthrough. Response Architecture
15. Module Summary
16. Check My Knowledge

Defender XDR as the Security Operations Fabric

Design the XDR operations architecture, unified schema, cross-domain correlation, attack disruption, custom detection rules, incident orchestration, Sentinel coexistence, and unified RBAC.

1. MSA11.1 The Unified Advanced Hunting Schema
2. MSA11.2 Signal Correlation Architecture
3. MSA11.3 Cross-Domain Incident Correlation
4. MSA11.4 Attack Disruption Architecture
5. MSA11.5 AIR in the Unified Fabric
6. MSA11.6 Advanced Hunting Across Domains
7. MSA11.7 Custom Detection Rules in Defender XDR
8. MSA11.8 Incident Orchestration in the Unified Portal
9. MSA11.9 Sentinel-XDR Coexistence Architecture
10. MSA11.10 Data Flow and Duplication Management
11. MSA11.11 Unified RBAC Architecture
12. MSA11.12 Complete XDR Operations Architecture
13. MSA11 Module Lab. XDR Operations Deployment
14. MSA11 Guided Walkthrough. XDR as an Integrated System
15. Module Summary
16. Check My Knowledge

Phase 4: Governance & Capstone

Identity Governance Architecture

Design the identity governance architecture, access reviews, entitlement management, lifecycle workflows, HR-driven provisioning, workload identity governance, agent identity governance, and PIM integration.

1. MSA12.1 The Governance Problem
2. MSA12.2 Access Reviews. Scope and Design
3. MSA12.3 Access Reviews. Automation and Decisions
4. MSA12.4 Entitlement Management. Access Packages
5. MSA12.5 Entitlement Management. Auto-Assignment and Lifecycle
6. MSA12.6 Lifecycle Workflows. Joiner
7. MSA12.7 Lifecycle Workflows. Mover and Leaver
8. MSA12.8 HR-Driven Provisioning Architecture
9. MSA12.9 Workload Identity Governance
10. MSA12.10 Agent Identity Governance
11. MSA12.11 PIM Governance Integration
12. MSA12.12 Complete Governance Architecture
13. MSA12 Module Lab. Governance Deployment
14. MSA12 Guided Walkthrough. Governance as a System
15. Module Summary
16. Check My Knowledge

Security Posture and Compliance Architecture

Design the security posture measurement and compliance architecture, Secure Score interpretation, Compliance Manager assessments, framework mapping across ISO 27001, SOC 2, NIST CSF, and UK frameworks, maturity roadmaps, and executive communication.

1. MSA13.1 The Posture Problem
2. MSA13.2 Secure Score. Honest Interpretation
3. MSA13.3 Compliance Manager. Assessment Architecture
4. MSA13.4 Compliance Manager. Evidence and Automation
5. MSA13.5 Mapping Controls to ISO 27001
6. MSA13.6 Mapping Controls to SOC 2 and NIST CSF
7. MSA13.7 Mapping Controls to UK Frameworks
8. MSA13.8 Maturity Roadmaps and Gap Analysis
9. MSA13.9 Communicating Security Architecture to Leadership
10. MSA13.10 The NE Posture Assessment
11. MSA13.11 Continuous Posture Monitoring
12. MSA13.12 Complete Posture and Compliance Architecture
13. Module Lab. Posture and Compliance Baseline
14. Guided Walkthrough
15. Module Summary
16. Check My Knowledge

Capstone: The Complete Architecture

Assemble, defend, threat-model, and present the complete M365 security architecture built across Modules 0–13, producing the portfolio-grade deliverable that survives your departure.

1. MSA14.1 Architecture Package Assembly
2. MSA14.2 Architecture Review Simulation
3. MSA14.3 Threat Model Walkthrough
4. MSA14.4 Executive Presentation
5. MSA14.5 What Changes Next Quarter
6. Module Summary

Phase 0: Course Resources

Cheatsheets

The commands, queries and decision criteria behind every architecture domain in the course, with what each answer settles and what it leaves open.

1. Identity Architecture
2. Authentication Architecture
3. Conditional Access
4. Privileged Access
5. Data Protection
6. Endpoint Security
7. Email and Collaboration
8. Sentinel Workspace
9. Detection Architecture
10. Incident Response
11. Defender XDR
12. Identity Governance
13. Posture and Compliance
14. Cadences and Graph Reference

Cookbooks

Ordered procedures for the architecture work that recurs: deploying a policy without an outage, reducing standing privilege, assessing a tenant, and retiring a control.

1. Deploying a Conditional Access Policy
2. Reducing Standing Privilege
3. Assessing an Unfamiliar Tenant
4. Retiring a Control
5. Onboarding an Acquired Tenant
6. Verifying Emergency Access
7. Reviewing a Proposed Design

Lab Setup

Building a tenant where you can deploy architecture, break it, and see what the controls actually do, without touching anything anyone depends on.

1. The Tenant and What It Costs
2. Building a Population Worth Testing
3. Deploying the First Controls
4. Breaking It on Purpose
5. Verify, and What the Lab Cannot Teach

Walkthroughs

Architecture decisions worked end to end, including the ones where the correct answer was to deploy nothing and the ones where the design was right and still failed.

1. The Control That Was Already There
2. The Privilege That Was Not a Role
3. The Design That Should Not Ship
4. The Question the Tenant Cannot Answer
5. The Tenant Nobody Documented
6. The Saving That Would Have Cost More

Playbooks

What to do when a decision is forced on you: a merger, an audit finding, a regulator, a breach elsewhere, a budget cut, or a product retirement.

1. A Merger Adds a Tenant
2. An Audit Finding Lands
3. A Regulator Changes the Requirement
4. A Breach Elsewhere Forces a Review
5. The Budget Is Cut
6. A Product You Depend On Is Retired
7. A Control You Deployed Causes an Outage

Playground

Every practice surface available for this course, what each one actually gives you, and where the gaps are.

References & Further Reading

Microsoft documentation, security frameworks, compliance standards, threat intelligence, and vendor references used throughout the MSA course.

Course Completion

Course Exam

Microsoft 365 Security Architecture end-of-course exam: a three-phase simulation testing whether you can apply the method to a situation the course did not walk through.

1. Course Completion. Microsoft 365 Security Architecture

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/m365-security-architecture/