

Endpoint Security Engineering

ARC402

Harden endpoints, stop advanced attacks, and maintain a resilient security posture across your entire fleet. Master Microsoft Defender for Endpoint, Intune security policies, attack surface reduction, and endpoint hardening techniques to detect, block, and respond to threats targeting Windows, macOS, Linux, and mobile devices.

Modules	23
Lessons	246
Phases	4
Free preview	Course Orientation (13 lessons)

The method

This course builds an endpoint security capability in the order it has to be built, because each layer depends on the one under it. The loop repeats through every control it deploys.

1. Understand what the operating system is doing. Endpoint controls intercept OS behavior. Configuring them without knowing what they intercept produces settings nobody can explain.
2. Deploy so the telemetry is trustworthy. Onboarding, device health and compliance first. A control on a device that stopped reporting is a control you believe you have.
3. Configure for what it must stop, then measure the cost. Attack surface reduction, application control and device control each block something legitimate. Knowing what, before enforcement, is the whole job.
4. Detect what the controls let through. No preventive layer is complete, and the detections exist for the gap rather than as a duplicate of the block.
5. Practice the response before you need it. Triage, containment and artifact collection, on the same endpoints you configured.

The course closes on a complete endpoint security architecture assembled from every layer built along the way.

What this course assumes

No minimum experience and no prerequisite course. OS internals, the Defender architecture and every control surface are introduced from the beginning.

What makes it go faster: a tenant with Defender for Endpoint and a device to onboard. Not required, and every configuration is shown with the portal path and the policy behind it.

What this course does not cover: deep Windows forensics, malware reverse engineering and network security. This is engineering and operating the endpoint layer.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What Endpoint Security Engineering teaches: engineer layered endpoint defense across a Windows, macOS, Linux, and mobile fleet using Defender for Endpoint, Intune, ASR, and EDR to stop advanced attacks.

1. ES0.1 Why Traditional AV Fails
2. ES0.2 Modern Attack Chains on Endpoints
3. ES0.3 The Endpoint Security Stack
4. ES0.4 Key Metrics: MTTD, MTTR, and What Actually Matters
5. ES0.5 The Microsoft Ecosystem View
6. ES0.6 The NE Endpoint Landscape
7. ES0.7 The Deployment Sequence That Matters
8. ES0.8 The Blast Radius Problem
9. ES0.9 The Endpoint Security Maturity Model
10. ES0.10 Attacker Perspective: What the Adversary Sees
11. ES0.11 Interactive Lab: Endpoint Security Assessment
12. Module Summary
13. Check My Knowledge

Endpoint Architecture and OS Internals

The operating system internals that attackers target and defenders must understand.

1. ES1.1 Windows Process Model for Security Practitioners
2. ES1.2 LSASS and Credential Storage
3. ES1.3 Windows Registry as an Attack Surface
4. ES1.4 Event Tracing for Windows (ETW)
5. ES1.5 Windows Security Subsystem Architecture
6. ES1.6 Linux Kernel and eBPF for Security
7. ES1.7 Linux Authentication and Privilege Model
8. ES1.8 macOS Security Architecture
9. ES1.9 What Attackers Actually Target
10. ES1.10 From Internals to Controls
11. ES1.11 Interactive Lab: OS Internals Exploration
12. Module Summary
13. Check My Knowledge

Phase 2: Protection Engineering

ES2, MDE Architecture, Onboarding & Device Health

How the MDE sensor works, how to achieve 100% onboarding across endpoints, servers, and Linux, and how to build the device health monitoring that detects silent coverage gaps.

1. ES2.1 MDE Sensor Architecture
2. ES2.2 Cloud-Side Processing and Data Flow
3. ES2.3 Licensing Tiers: Operational Reality
4. ES2.4 Onboarding Methods Compared
5. ES2.5 Intune-Based Onboarding at Scale
6. ES2.6 Server and Linux Onboarding
7. ES2.7 Onboarding Validation and Troubleshooting
8. ES2.8 Device Health Monitoring
9. ES2.9 Device Groups, Tags, and RBAC
10. ES2.10 Mobile and Non-Traditional Endpoints
11. ES2.11 Interactive Lab: Onboarding Health Audit
12. Module Summary
13. Check My Knowledge

ES3, Production Deployment, Compliance & Conditional Access

Connect endpoint compliance to zero-trust access decisions.

1. ES3.1 Zero-Trust Onboarding Playbook
2. ES3.2 Tamper Protection
3. ES3.3 GPO vs Intune vs MDE Settings Conflicts
4. ES3.4 Compliance Policies That Actually Work
5. ES3.5 Windows Compliance Baseline
6. ES3.6 macOS, iOS, and Android Compliance
7. ES3.7 Compliance + Conditional Access Enforcement
8. ES3.8 Security Baselines vs Custom Policies
9. ES3.9 Non-Compliant Device Remediation and Exception Management
10. ES3.10 Performance Impact Testing
11. ES3.11 Interactive Lab: Compliance and CA Stack
12. Module Summary
13. Check My Knowledge

ES4, Attack Surface Reduction Rules Mastery

Deploy, tune, and enforce all 18+ ASR rules using audit-first methodology.

1. ES4.1 ASR Rules: What They Actually Block
2. ES4.2 The Audit-First Deployment
3. ES4.3 Analyzing ASR Audit Data
4. ES4.4 ASR Deployment: The Safe Set
5. ES4.5 ASR Deployment: The Careful Set
6. ES4.6 ASR Deployment: The High-Risk Set
7. ES4.7 Block vs Audit vs Warn Modes
8. ES4.8 Custom Exclusions for Line-of-Business Applications
9. ES4.9 Controlled Folder Access and Ransomware Protection
10. ES4.10 ASR Monitoring, Drift Detection, and Continuous Tuning
11. ES4.11 Interactive Lab: ASR Deployment Simulation
12. Module Summary
13. Check My Knowledge

ES5, Antivirus Engineering & Behavioral Protection

Tune Defender AV beyond defaults, cloud protection, behavioral monitoring, AMSI, scan optimization, exclusion management, and the ransomware defense stack that MDE provides when properly configured.

1. ES5.1 Beyond Default AV: What To Actually Configure
2. ES5.2 Cloud-Delivered Protection and Machine Learning Models
3. ES5.3 Behavioral Monitoring and In-Memory Detection
4. ES5.4 Ransomware Protection Deep Dive
5. ES5.5 Network Protection
6. ES5.6 Scan Configuration for Production
7. ES5.7 AV Exclusions: The Necessary Evil
8. ES5.8 PUA Protection and Unwanted Software
9. ES5.9 AV Health Monitoring and Signature Management
10. ES5.10 Server-Specific AV Configuration
11. ES5.11 Interactive Lab: AV Policy Engineering
12. Module Summary
13. Check My Knowledge

ES6, Device Control, Application Control & Exploit Guard

Control which devices connect, which applications execute, and which exploit techniques are mitigated.

1. ES6.1 Device Control: The USB and Removable Media Problem
2. ES6.2 Printer and Bluetooth Control
3. ES6.3 AppLocker: When and Why
4. ES6.4 Windows Defender Application Control Deep Dive
5. ES6.5 WDAC at Scale
6. ES6.6 Exploit Protection
7. ES6.7 Web Content Filtering
8. ES6.8 Endpoint DLP Integration
9. ES6.9 Device Control Monitoring and Reporting
10. ES6.10 Building the Device Control Policy
11. ES6.11 Interactive Lab: Defense-in-Depth Deployment
12. Module Summary
13. Check My Knowledge

Phase 3: Detection & Response

ES7, EDR Configuration & Automated Response

Configure MDE's EDR capabilities beyond default, automated investigation, live response, device isolation, indicator management, and alert tuning for operational efficiency.

1. ES7.1 EDR Beyond Default: What To Configure
2. ES7.2 Automated Investigation and Response (AIR)
3. ES7.3 AIR Tuning: The Confidence Decision
4. ES7.4 Live Response: Configuration and Operational Workflow
5. ES7.5 Live Response Scripting
6. ES7.6 Device Isolation and Containment
7. ES7.7 Indicator Management
8. ES7.8 Alert Tuning and Suppression
9. ES7.9 Threat Analytics
10. ES7.10 EDR Telemetry Optimization
11. ES7.11 Interactive Lab: EDR Engineering
12. Module Summary
13. Check My Knowledge

ES8, Detection Engineering for Endpoints

Build custom detection rules in MDE using KQL, credential access, lateral movement, persistence, defense evasion.

1. ES8.1 Custom Detections in MDE vs Sentinel
2. ES8.2 MDE Advanced Hunting Tables
3. ES8.3 Building Effective Detection KQL
4. ES8.4 Custom Detection: Credential Access
5. ES8.5 Custom Detection: Lateral Movement
6. ES8.6 Custom Detection: Persistence and Defense Evasion
7. ES8.7 Threat Intelligence Integration
8. ES8.8 Automated Actions on Detection
9. ES8.9 Detection Testing and Validation
10. ES8.10 Detection Lifecycle and Version Control
11. ES8.11 Interactive Lab: Build Endpoint Detections
12. Module Summary
13. Check My Knowledge

ES9, KQL for Endpoint Hunting

Proactive threat hunting across MDE endpoint tables.

1. ES9.1 Endpoint Hunting Philosophy
2. ES9.2 DeviceProcessEvents Deep Dive
3. ES9.3 DeviceNetworkEvents Deep Dive
4. ES9.4 DeviceFileEvents and DeviceRegistryEvents
5. ES9.5 DeviceLogonEvents and DeviceImageLoadEvents
6. ES9.6 Essential Joins and Time-Window Queries
7. ES9.7 Advanced Techniques: JSON Parsing and Nested Data
8. ES9.8 LOLBAS Tracking and Living-off-the-Land Detection
9. ES9.9 Parent-Child Process Anomalies
10. ES9.10 Building the Endpoint Hunting Query Library
11. ES9.11 Interactive Lab: Endpoint Hunting Exercise
12. Module Summary
13. Check My Knowledge

ES10, Alert Triage, Investigation & Containment

Operationalize the detection layer. Triage MDE alerts in 60 minutes, investigate using device timeline and process tree analysis, execute containment at scale, and apply incident-type-specific playbooks for ransomware, commodity malware, and living-off-the-land attacks.

1. ES10.1 MDE Alert → Sentinel Incident
2. ES10.2 The 60-Minute Endpoint Triage Rule
3. ES10.3 Device Timeline Exploration
4. ES10.4 Process Tree Analysis
5. ES10.5 Investigation Playbook: Ransomware on Endpoint
6. ES10.6 Investigation Playbook: Commodity Malware
7. ES10.7 Investigation Playbook: Living-off-the-Land
8. ES10.8 Evidence Collection Without Breaking Chain of Custody
9. ES10.9 Containment at Scale
10. ES10.10 Decision Trees: Ransomware vs Commodity vs APT
11. ES10.11 Interactive Lab: Endpoint Investigation and Containment
12. Module Summary
13. Check My Knowledge

Phase 4: Advanced & Operations

ES11, Forensic Readiness & Artifact Collection

Configure the telemetry layer that ensures evidence exists when the incident happens.

1. ES11.1 Forensic Readiness: Designing for Investigation
2. ES11.2 Windows Audit Policy Configuration
3. ES11.3 PowerShell Logging
4. ES11.4 Sysmon Deployment and Configuration
5. ES11.5 Windows Event Forwarding Architecture
6. ES11.6 KAPE for Endpoint Collection
7. ES11.7 Memory Acquisition Readiness
8. ES11.8 Velociraptor for Endpoint Collection at Scale
9. ES11.9 OSQuery for Endpoint State Inspection
10. ES11.10 Windows LAPS Configuration
11. ES11.11 Interactive Lab: Forensic Readiness Deployment
12. Module Summary
13. Check My Knowledge

ES12, Advanced Evasion, Anti-Forensics & Threat Intelligence

Understand what attackers do to bypass the endpoint security stack, process injection, AMSI bypass, ETW tampering, EDR evasion, anti-forensics, from the defender's perspective.

1. ES12.1 Why Defenders Need to Understand Evasion
2. ES12.2 Process Injection Techniques
3. ES12.3 AMSI Bypass and Script-Level Evasion
4. ES12.4 ETW Tampering and Blind Spots
5. ES12.5 EDR Evasion: What Attackers Actually Do
6. ES12.6 Anti-Forensics on Endpoints
7. ES12.7 Defense Evasion: Living-off-the-Land at Scale
8. ES12.8 Validation: Red Team and Purple Team Exercises
9. ES12.9 Threat Intelligence-Driven Defense
10. ES12.10 Building Resilient Detections
11. ES12.11 Interactive Lab: Evasion-Aware Defense
12. Module Summary
13. Check My Knowledge

ES13, Servers, Linux & Cross-Platform Endpoint Security

Extend the endpoint security architecture to servers, Linux, macOS, and VDI.

1. ES13.1 Server Security Architecture
2. ES13.2 Domain Controller Protection
3. ES13.3 SQL Server, IIS, and File Server Protection
4. ES13.4 CIS Benchmarks for Server Hardening
5. ES13.5 Defender for Linux: Deployment and Configuration
6. ES13.6 eBPF-Based Detection on Linux
7. ES13.7 Sysmon for Linux
8. ES13.8 macOS Endpoint Security
9. ES13.9 Unified Hunting Across Platforms
10. ES13.10 VDI and Multi-Session Environments
11. ES13.11 Interactive Lab: Cross-Platform Configuration
12. Module Summary
13. Check My Knowledge

ES14, Zero Trust, Integration & Automation

Connect the endpoint security architecture to the broader security ecosystem.

1. ES14.1 Zero Trust for Endpoints
2. ES14.2 MDE + Sentinel Integration
3. ES14.3 MDE + Entra ID + Conditional Access
4. ES14.4 MDE + Defender for Cloud
5. ES14.5 MDE + MDO + MDI
6. ES14.6 Endpoint Security Automation with Logic Apps
7. ES14.7 Cross-Workload Automation
8. ES14.8 MDE API for Engineering and Operations
9. ES14.9 Third-Party SIEM and MSSP Integration
10. ES14.10 Building the Integrated Security Architecture
11. ES14.11 Interactive Lab: Integration and Automation
12. Module Summary
13. Check My Knowledge

ES15, Capstone: Complete Endpoint Security Architecture

Synthesize every module into a single deliverable: the complete endpoint security architecture for NE, designed, deployed, validated, and documented across a 90-day project plan.

1. ES15.1 Capstone Briefing
2. ES15.2 Phase 1: Assessment and Planning
3. ES15.3 Phase 2: Onboarding and Compliance
4. ES15.4 Phase 3: Attack Surface Reduction
5. ES15.5 Phase 4: AV and EDR Optimization
6. ES15.6 Phase 5: Custom Detections and Hunting
7. ES15.7 Phase 6: Forensic Readiness
8. ES15.8 Phase 7: Servers and Cross-Platform
9. ES15.9 Phase 8: Vulnerability Management
10. ES15.10 Phase 9: Monitoring, Governance & Validation
11. ES15.11 The Complete Architecture Document
12. Module Summary
13. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Subject-area sheets for endpoint work: the query, where the control lives in the portal, what the fields mean, and what the answer does not prove.

1. Which Device Table, and Reading Process Events
2. Onboarding and Device Health
3. Attack Surface Reduction Rules
4. Antivirus and Behavioral Protection
5. Device, Application and Exploit Control
6. EDR Configuration and Automated Response
7. Endpoint Detection Engineering
8. Alert Triage and Containment
9. Forensic Collection
10. Servers, Linux and Cross-Platform
11. Tables, ActionTypes and Limits

Cookbooks

Seven procedures an endpoint engineer repeats: deploying a control from audit to enforce, onboarding a population, triaging an alert, and collecting from a live host.

1. Deploying a Protection Control
2. Onboarding a Device Population
3. Building an Exclusion Set
4. The Sixty-Minute Endpoint Triage
5. Collecting From a Live Host
6. Deploying Application Control
7. Recovering a Compromised Endpoint

Lab Setup

A complete endpoint lab: tenant, licensing, virtual machines, onboarding, safe test activity, and the checks that prove it works.

1. Tenant and Licensing
2. Building the Endpoints
3. Onboarding and Telemetry
4. Generating Test Activity
5. Verify and Limits

Walkthroughs

Worked endpoint investigations end to end, including the wrong turns, the queries that looked right and were not, and what would have changed each answer.

1. The Rule That Was Never Enforcing
2. The Device That Was Not Reporting
3. The Exclusion That Hid It
4. The Block That Was Not the End
5. The Administrator Who Looked Wrong
6. The Movement Nobody Was Watching
7. The Rule That Went Quiet

Playbooks

Seven endpoint events with a procedure each: prerequisites, a pre-flight that validates the sources, a numbered sequence, tiered disposition and a worked handoff.

1. A Device Stopped Reporting
2. Defender Was Tampered With
3. A Credential Access Alert Fired
4. Ransomware Preparation on a Host
5. A Control Started Blocking at Volume
6. Malware Detected and Not Remediated
7. An Unmanaged Device Appeared

Playground

Where to practice the endpoint work in this course against real data and real machines.

Course Completion

Course Exam

Endpoint Security Engineering 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. Endpoint Security Engineering

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