Endpoint Protection Platforms

EPP and EDR Solutions for OT Environments

OT Security Learning Series

Document 835 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Endpoint Protection Platforms (EPP) have evolved significantly from traditional antivirus solutions. Modern EPP integrates multiple security capabilities into unified platforms, while Endpoint Detection and Response (EDR) adds advanced threat detection and investigation capabilities. Deploying these technologies in Operational Technology (OT) environments requires careful consideration of operational constraints.

Information

This document covers Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) concepts for OT environments. It addresses deployment considerations, architecture options, and the unique challenges of protecting industrial endpoints while maintaining system availability.

2 EPP vs EDR vs XDR

2.1 Technology Evolution

Endpoint security has evolved through several generations:

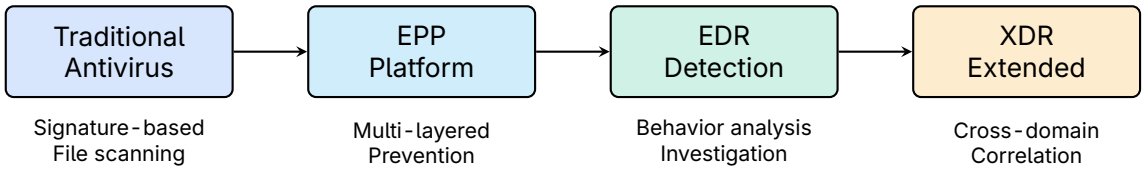

Figure 1: Evolution of endpoint security technologies

2.2 Capability Comparison

Capability	AV	EPP	EDR	XDR
Signature detection	✓	✓	✓	✓
Behavior analysis	–	✓	✓	✓
Machine learning	–	✓	✓	✓
Threat hunting	–	–	✓	✓
Forensic investigation	–	–	✓	✓
Network correlation	–	–	–	✓
Automated response	–	Limited	✓	✓

Table 1: Endpoint security capability comparison

3 EPP Core Components

3.1 Prevention Technologies

Modern EPP platforms combine multiple prevention layers:

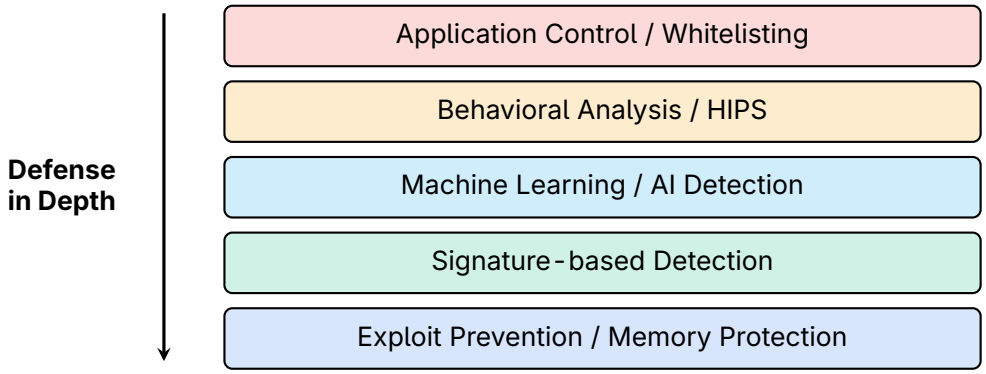

Figure 2: EPP defense-in-depth layers

3.2 Key EPP Features

- **Anti-malware:** Signature and heuristic detection of known threats
- **Application Control:** Whitelist/blacklist enforcement
- **Device Control:** USB and removable media policies
- **Host Firewall:** Local network traffic filtering
- **Exploit Prevention:** Memory protection and anti-exploit
- **Web Protection:** URL filtering and download scanning

4 EDR Capabilities

4.1 Detection and Response

EDR extends EPP with advanced detection and investigation:

Capability	Description
Continuous monitoring	Records endpoint activity including process execution, file changes, network connections, and registry modifications
Threat detection	Behavioral rules and analytics identify suspicious activity patterns
Alert triage	Prioritizes alerts based on severity and context
Investigation tools	Timeline analysis, process trees, and artifact collection
Threat hunting	Proactive search for indicators of compromise (IOCs)
Response actions	Isolate host, kill process, quarantine file, collect forensics

Table 2: EDR core capabilities

4.2 Telemetry Collection

EDR agents collect extensive telemetry:

- Process creation and termination events
- Network connections and DNS queries
- File system operations
- Registry modifications (Windows)
- User authentication events
- Loaded modules and drivers

Warning

EDR telemetry collection can impact system performance and generate significant network traffic. In OT environments, carefully evaluate resource requirements and consider limiting telemetry scope on constrained systems.

5 OT Deployment Considerations

5.1 Operational Constraints

OT environments present unique challenges for endpoint protection:

Constraint	Impact on EPP/EDR
Legacy operating systems	May not support modern agents; limited protection options
Real-time requirements	Agent overhead must not impact process timing
Change management	Agent updates require testing and approval cycles
Network isolation	Cloud-based management may not be feasible
Vendor support	Security software may void OT system warranties
Limited resources	Embedded systems lack CPU/memory for full agents

Table 3: OT constraints affecting EPP/EDR deployment

5.2 System Classification

Not all OT systems can support the same protection level:

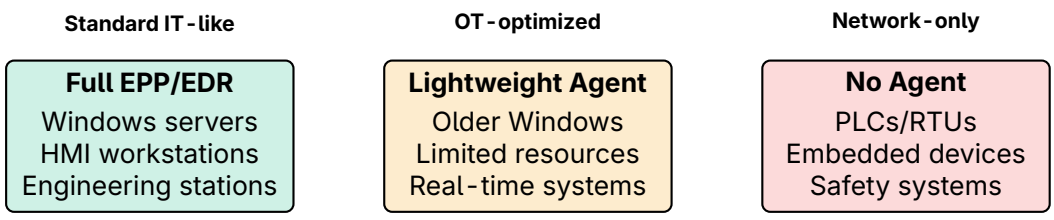

Figure 3: Endpoint protection tiers based on system capability

5.3 Agent Deployment Modes

- **Full Protection:** All EPP/EDR features enabled
- **Detection Only:** Monitor and alert without blocking
- **Audit Mode:** Log what would be blocked for tuning
- **Passive:** Minimal footprint, scheduled scans only

Key Point

Recommendation: Start with detection-only or audit mode in OT environments. Analyze alerts and tune policies before enabling blocking to prevent operational disruptions.

6 Architecture Options

6.1 Management Infrastructure

EPP/EDR platforms require management infrastructure:

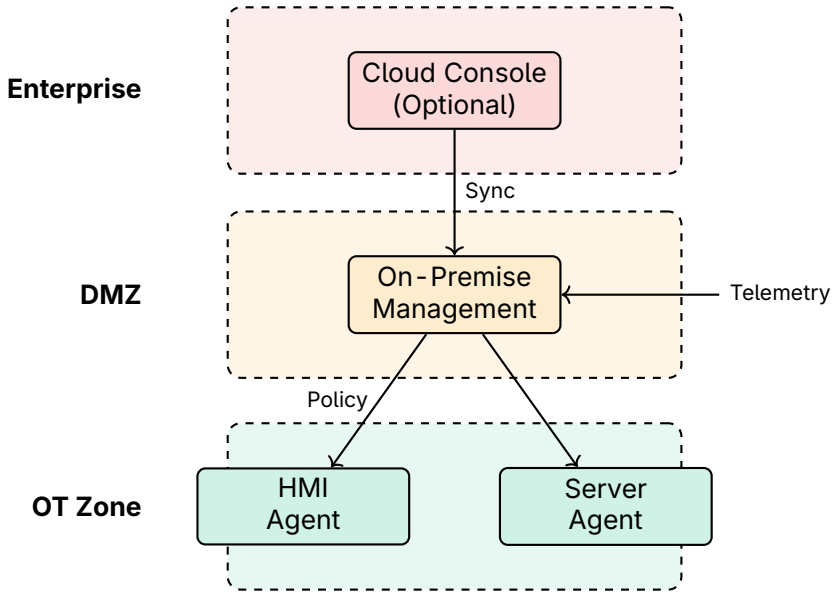

Figure 4: EPP/EDR management architecture for OT

6.2 Cloud vs On-Premise

Aspect	Cloud-Managed	On-Premise
Deployment	Quick, no infrastructure	Requires server infrastructure
Updates	Automatic, always current	Manual update cycles
Connectivity	Requires internet access	Air-gap compatible
Data residency	Data leaves network	Data stays on-site
Scalability	Unlimited	Capacity planning needed
Cost model	Subscription (OpEx)	License + infrastructure (CapEx)

Table 4: Cloud vs on-premise management comparison

Critical

Cloud-managed EPP/EDR sends telemetry outside the OT network. For air-gapped or highly sensitive environments, on-premise management is required. Evaluate data sensitivity and regulatory requirements before choosing cloud management.

7 Policy Configuration

7.1 OT-Specific Tuning

EPP policies require OT-specific adjustments:

- **Exclusions:** Whitelist OT application paths and processes
- **Scan Scheduling:** Avoid scans during critical operations
- **Update Windows:** Control signature updates to maintenance periods
- **Response Actions:** Disable automatic quarantine; alert only
- **Resource Limits:** Cap CPU and memory usage

7.2 Application Whitelisting Integration

Tip

Combine EPP with application whitelisting for defense in depth. Whitelisting prevents unauthorized executables while EPP detects threats within allowed applications. This layered approach is particularly effective in static OT environments.

8 Response Procedures

8.1 Alert Handling in OT

Response to EPP/EDR alerts in OT requires modified procedures:

1. **Assess Impact:** Determine if alert affects critical process
2. **Validate Alert:** Confirm true positive vs false positive
3. **Coordinate Response:** Involve OT operations before action
4. **Controlled Isolation:** If needed, follow safe shutdown procedures
5. **Investigate:** Use EDR tools to understand scope
6. **Remediate:** Plan remediation during maintenance window

Warning

Never automatically isolate or shut down OT endpoints without operational coordination. Abrupt disconnection of control systems can cause safety incidents or process disruptions more severe than the security threat.

9 Summary

Key Takeaways

- **Layered Protection:** EPP provides multiple prevention layers; EDR adds detection and response capabilities for advanced threats
- **Tiered Deployment:** Classify OT systems by capability and deploy appropriate protection levels—full agents, lightweight agents, or network-only monitoring
- **OT-Specific Configuration:** Tune policies for OT requirements including exclusions, scan scheduling, and disabled automatic responses
- **On-Premise Management:** Consider on-premise management servers for air-gapped or sensitive OT environments
- **Coordinated Response:** Integrate security response with OT operations to prevent disruptions from automated or hasty containment actions

10 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-2-1** – Security Program Requirements for IACS Asset Owners
  https://webstore.iec.ch/publication/7030
- **CISA** – Industrial Control Systems Security
  https://www.cisa.gov/topics/industrial-control-systems

Resources

- **MITRE ATT&CK for ICS** – Adversary Tactics and Techniques
  https://attack.mitre.org/techniques/ics/
- **SANS ICS** – Industrial Control Systems Security
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

Books

- Knapp, Eric D. – *Industrial Network Security* (Syngress)
- Hadnagy, Christopher – *Social Engineering: The Science of Human Hacking* (Wiley)

Part of the OT Security Learning Series