Endpoint Protection for OT

Antivirus, EDR, and endpoint security in industrial environments

OT Security Learning Series

Document 830 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Endpoint protection in OT environments requires balancing security with operational stability. Traditional IT security tools can disrupt industrial processes, while no protection leaves systems vulnerable to malware like Stuxnet, TRITON, and Industroyer.

OT endpoints include:

- HMI workstations and operator consoles
- Engineering workstations
- Historian servers
- SCADA servers
- Windows-based PLCs and embedded systems
- Jump servers and remote access systems

Warning

Never deploy endpoint protection without thorough testing in a non-production environment. A false positive blocking a critical DLL could halt production.

2 Endpoint Protection Options

2.1 Protection Technologies

Technology	Description	OT Fit
Traditional AV	Signature-based malware detection	Limited
Next-Gen AV (NGAV)	Behavioral + signature detection	Moderate
Application Whitelisting	Only approved apps can run	Excellent
EDR	Detection, investigation, response	Moderate
XDR	Extended detection across endpoints/network	Emerging
Host-based Firewall	Control network connections	Good
Device Control	USB and removable media control	Excellent

Table 1: Endpoint Protection Technologies

2.2 Technology Comparison

Criteria	AV	Whitelisting	EDR	Device Ctrl
Stops known malware	Yes	Yes	Yes	Partial
Stops unknown malware	Limited	Yes	Moderate	Limited
Low false positives	Moderate	High*	Moderate	High
Low system impact	Moderate	High	Moderate	High
Works offline	Limited	Yes	Limited	Yes
Legacy OS support	Varies	Good	Limited	Good

Table 2: Comparison of Endpoint Protection Approaches

* After proper baselining

3 OT-Specific Challenges

Critical

Why IT endpoint security fails in OT:

- Signature updates require internet (air-gapped networks)
- Scans consume CPU during critical operations
- False positives can block control system software
- Reboots for updates are often impossible
- Legacy OS (Windows XP, Server 2003) unsupported
- Vendor support voided by third-party security software

3.1 Vendor Compatibility

Warning

Many OT vendors only support specific antivirus products. Check compatibility before deployment:

- Siemens – Publishes tested AV compatibility list
- Rockwell – Certifies specific products
- ABB, Schneider – Provide security guidelines
- GE, Honeywell – May void support for untested software

4 Recommended Approach

4.1 Layered Strategy

Key Point

OT endpoint protection stack (recommended):

1. **Application Whitelisting** – Primary control
2. **Device Control** – Block unauthorized USB/media
3. **Host Firewall** – Limit network connections
4. **AV/EDR** – Secondary, where compatible

4.2 Protection by System Type

System Type	Recommended Protection
Engineering Workstation	Full EDR + AV + Whitelisting + Device Control
HMI / Operator Station	Whitelisting + Device Control + Host Firewall
Historian Server	AV + Whitelisting + Host Firewall
SCADA Server	Whitelisting + Device Control
Jump Server	Full EDR + AV + MFA
Legacy Windows (XP)	Whitelisting + Network isolation
Embedded Windows	Whitelisting or Write Filter

Table 3: Endpoint Protection by System Type

5 Application Whitelisting

Application Whitelisting

A security approach that only allows pre-approved applications to execute. All other executables are blocked by default—the opposite of traditional AV which blocks known-bad.

5.1 Benefits for OT

- **Stops unknown malware** – Including zero-days
- **Low resource usage** – No signature scanning
- **Works offline** – No updates required
- **Stable environments** – OT systems rarely change
- **Audit trail** – Log of execution attempts

5.2 Implementation Steps

1. **Audit mode** – Monitor what executes without blocking
2. **Build baseline** – Capture all legitimate applications
3. **Create policies** – Define allowed executables/publishers
4. **Test thoroughly** – Validate all operations work
5. **Enable enforcement** – Block unauthorized execution
6. **Maintain** – Update for patches and software changes

6 Device Control

6.1 USB and Removable Media Risks

- Stuxnet spread via infected USB drives
- Contractors introducing malware
- Data exfiltration
- Unauthorized software installation

6.2 Device Control Policies

Policy	Description
Block all USB	Most restrictive, may impact operations
Read-only USB	Allow data export, prevent execution
Approved devices only	Whitelist specific USB serial numbers
Scan before access	AV scan on USB mount
Secure transfer station	Dedicated kiosk for file transfer

Table 4: USB Control Policy Options

7 EDR in OT

7.1 EDR Capabilities

- Real-time process monitoring
- Behavioral analysis
- Threat hunting queries
- Incident investigation
- Remote response actions

7.2 EDR Considerations for OT

Warning

EDR deployment cautions:

- Test “response” actions carefully—never auto-quarantine in OT
- Ensure agent doesn’t interfere with real-time processes
- Plan for offline/air-gapped operation
- Verify compatibility with control system software
- Consider network bandwidth for telemetry

7.3 Where to Deploy EDR

- Engineering workstations – Yes

- Jump servers – Yes
- HMIs with internet access – Consider
- Isolated HMIs – Whitelisting preferred
- Control servers – Test thoroughly first
- PLCs/RTUs – Not applicable (no OS agent)

8 Legacy System Protection

For unsupported operating systems (Windows XP, Server 2003):

- **Application whitelisting** – Primary defense
- **Network isolation** – Strict firewall rules
- **Disable unnecessary services** – Reduce attack surface
- **Remove internet access** – No browsing, email
- **Virtual patching** – IPS rules at network level
- **Plan migration** – Upgrade path to supported OS

9 Deployment Best Practices

1. **Test in lab** – Never deploy untested in production
2. **Check vendor compatibility** – Get written approval
3. **Start with monitoring** – Audit mode before enforcement
4. **Exclude control processes** – Whitelist critical executables
5. **Schedule scans carefully** – During maintenance windows
6. **Plan update strategy** – Offline updates for air-gapped
7. **Document exceptions** – Track all exclusions
8. **Monitor performance** – Watch for CPU/memory impact

10 Summary

Key Takeaways

- **Whitelisting first** – Best fit for stable OT environments
- **Device control** – Essential for USB/removable media
- **Test thoroughly** – Never deploy without validation
- **Vendor approval** – Check compatibility lists
- **No auto-remediation** – Disable automatic blocking/quarantine
- **Legacy protection** – Isolation + whitelisting for old OS
- **Layered approach** – Combine multiple technologies

11 Further Reading

Standards

- **IEC 62443-2-4** – Security program requirements
  https://webstore.iec.ch/publication/7031
- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA – ICS Security**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series