PORTAINER.iO

E-Book

OT SECURITY PRACTITIONER GUIDE

How to close the gaps identified in your OT Security Readiness Assessment

Jun 2026

How to use this guide

This guide is designed to be read alongside your completed OT Security Readiness Assessment from Portainer. It maps each section of the assessment to the structural gap that a low score reveals, what good architecture looks like in that area, and the specific steps that close the gap.

You don't need to read it end to end. Find the sections where you scored Developing or At Risk and start there. Each section is self-contained. A note on Not Sure responses: each one is a visibility gap. If you recorded five or more across the assessment, an internal audit of your OT security processes is a priority action regardless of your overall score.

Section 1

Patch management readiness

What a low score here means

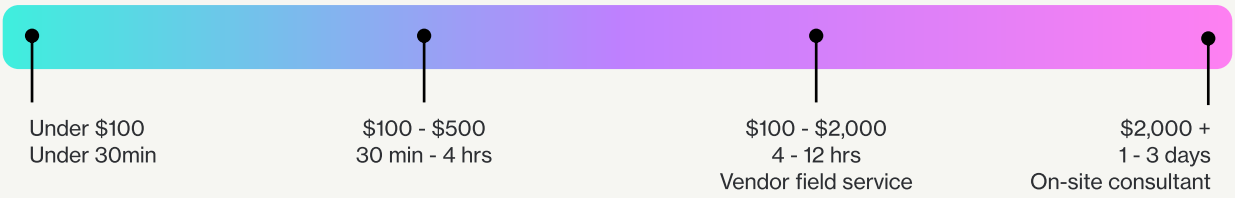
A score below 12 in the patch management readiness section means the test that every regulator will ask first (can you deploy a patch to every device in your estate within a defined window and prove it) is one you would fail today. The underlying cause is almost always structural: patching is decentralized, manual, and expensive because the management infrastructure doesn't give you a single addressable surface across the estate. Each patch event is a separate project.

At Risk scores typically indicate a lack of centralized patch process, manual CVE exposure checks, and high per-device patching costs. Developing scores often reflect partial coverage: some sites or device classes are manageable, others aren't, and rollback requires physical intervention.

What good looks like

- Automated patch deployment with fleet-level verification, not site-by-site manual confirmation
- CVE-to-asset mapping that confirms exposure within minutes of a disclosure, not via manual inventory cross-reference
- Patch cost under $100 or under 30 minutes per device, fleet-wide
- Atomic rollback to last-known-good state without requiring a site visit
- Software version inventory accessible on demand, not assembled on request

Per-device patching cost scales with access complexity between remotely manageable devices and when a site visit is required.



How to close the gap

The core enabler is a management plane that sits above the individual device layer and treats the fleet as a single addressable object. Patching, version verification, and rollback operate fleet-wide from a single interface rather than requiring direct access to each device.

Portainer IIoT provides centralized fleet management for container-based OT workloads: deploy updates, validate versions, and roll back across the estate from a single interface. For legacy devices that can't run containers, the documented pattern is a small gateway positioned adjacent to the existing hardware, managing communication on its behalf. Software version inventory is maintained as a live state, not a periodic export

Section 2

Audit and access posture

What a low score here means

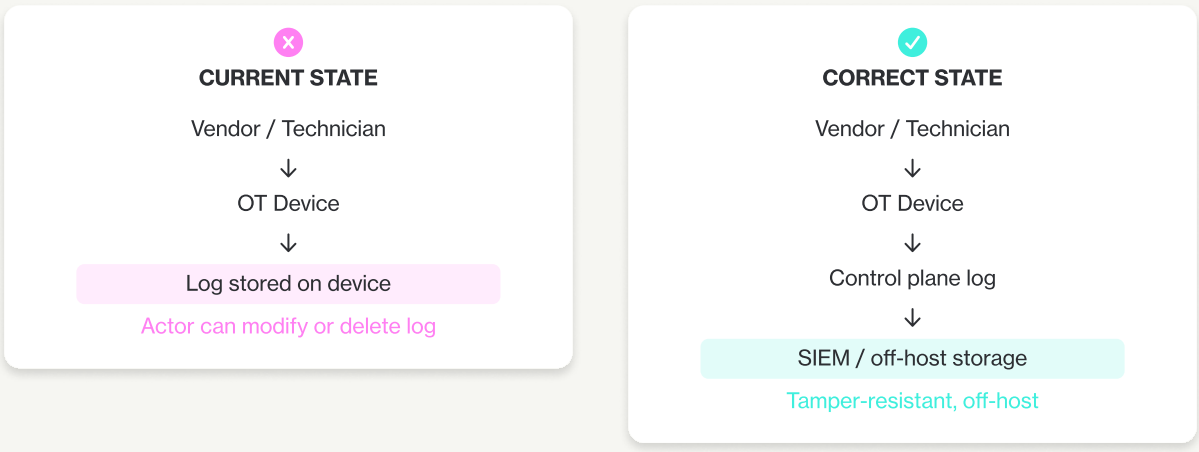
A low score in the audit and access posture section means your access control model doesn't enforce what your security policy intends and that your audit trail isn't tamper-resistant. The two most common failure modes are closely related: admin rights are too broad (shared credentials, vendor accounts that persist beyond their task), and audit logs reside on the host being accessed, meaning anyone with admin rights can alter them.

Neither is a policy failure. They're the structural default when access control was designed for IT environments and applied to OT without modification. The policy may be correct. The architecture doesn't enforce it.

What good looks like

- Defined RBAC with role-based scoping, integrated with an identity provider
- Audit logs stored off the host being recorded, not modifiable by the actor who made the change
- Vendor access granted via time-limited, process-scoped mechanisms, not persistent accounts or shared credentials
- Organization-to-permission mapping across all management infrastructure, consistently applied

When logs are stored on the host being accessed, the actor who made the change controls the record. A tamper-resistant audit trail requires the log to be written at the control plane and forwarded off-host.



How to close the gap

The audit log problem has a two-part architectural fix. First, every management action is recorded at the control plane, not on the device being accessed, so a technician or vendor working on a device cannot touch the record of what they did. Second, the audit stream is forwarded to storage outside the management plane's own administrative boundary (a SIEM or write-once storage), so platform administrators can't alter it either. Portainer records all control plane actions and streams them to any syslog-compatible SIEM.

Vendor access governance requires moving from persistent accounts to session-based provisioning. At the strong end, this means access tunnels that initiate outbound from the device, scoped to a specific process, available through Portainer's secure connectivity integration layer.

Section 3

Architectural integrity

What a low score here means

A low score in the architectural integrity section often coexists with adequate scores elsewhere, which is why it's the section operators most commonly underestimate. You may have solid patch processes and functional access controls, but if your management plane requires inbound ports, depends on a third-party cloud, or stores OT data outside operator-controlled jurisdiction, your security posture has structural vulnerabilities that policy cannot compensate for.

The three specific risks:

- Inbound-accessible management ports: OT devices discoverable at the network level are attack surface. Every open management port is an entry point.
- Cloud-hosted management plane: third-party outages affect OT operations; data residency may not meet regulatory or sovereignty requirements.
- No air-gap capability: for regulated operators, fully disconnected operation is increasingly a compliance requirement, not just a resilience preference.

What good looks like

- Device connectivity initiates outbound-only, from the device to the management plane. No inbound ports. Devices not enumerable on the public internet.
- Management plane self-hosted on operator infrastructure, in operator jurisdiction
- Full air-gap capability: OT operations and routine management continue without cloud provider availability
- OT data, audit logs, and configuration backups stored in operator-controlled jurisdiction

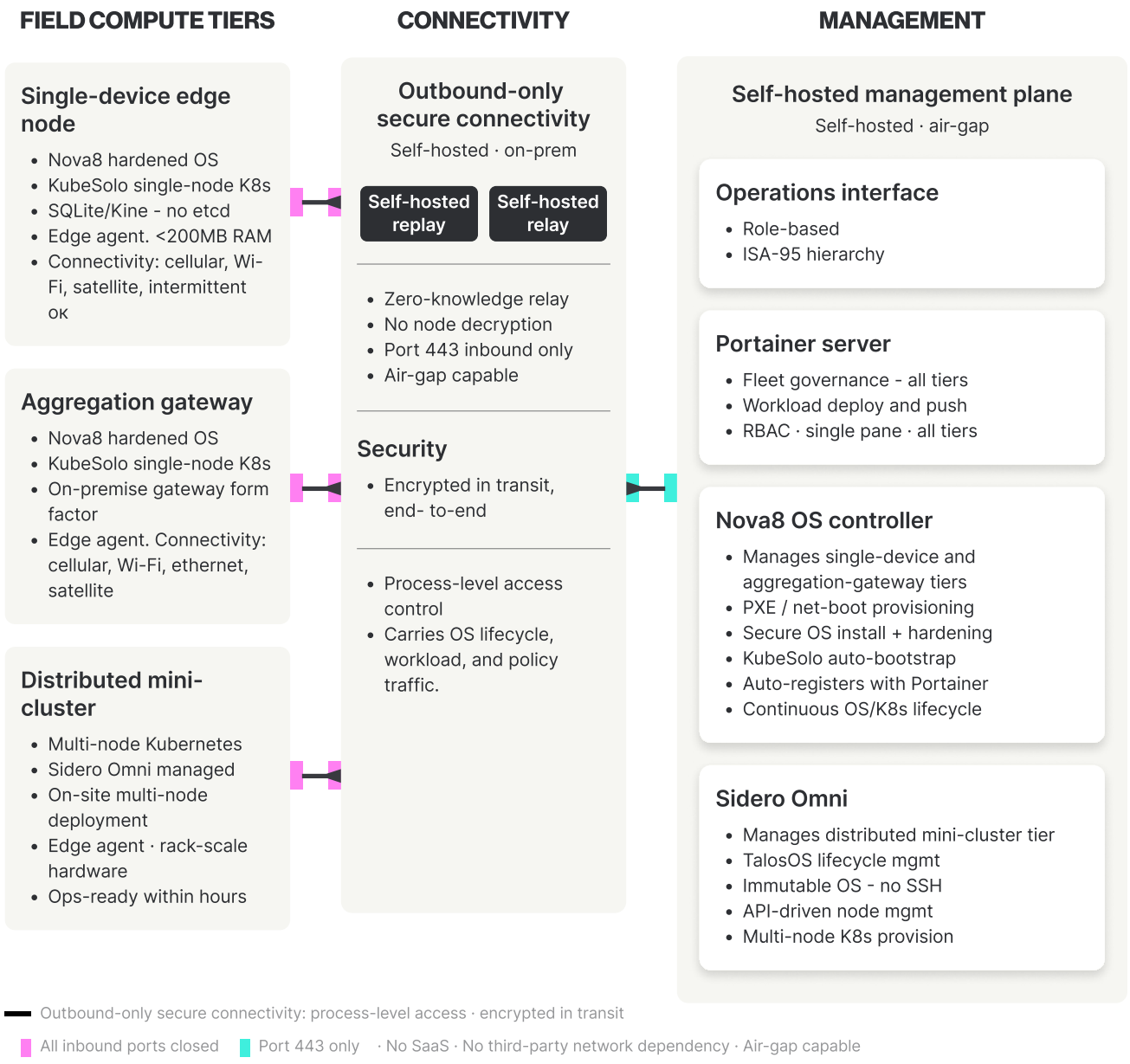
How to close the gap

Outbound-only connectivity is the architectural baseline for compliance. Portainer's Remote and Async Edge agents natively initiate outbound-only connections to the management plane, with no inbound firewall rules required. For environments that require full non-addressability, Portainer integrates with a deterministic connectivity layer that closes all inbound host firewall ports, removes any public IP presence, and binds access to the process level.

Self-hosted deployment gives operators full control of the management plane: where it runs, whose jurisdiction it falls under, and what availability profile it has. Portainer is designed for self-hosted deployment on operator infrastructure, not as a SaaS product with mandatory cloud dependency.

For operators with sovereignty requirements, data residency is a function of where the management plane is deployed. A self-hosted management plane, on operator infrastructure, in the operator's jurisdiction, means OT data does not transit or reside in a third-party cloud environment.

Outbound-only connectivity removes OT devices from the network-addressable attack surface. No inbound ports. No public IP. Management traffic flows through an encrypted tunnel initiated by the device.



Section 4

Regulatory Exposure

What a low score here means

A low regulatory exposure section score usually means one of three things: the applicable frameworks aren't clearly mapped to your environment; an upcoming audit or conformity deadline is approaching without adequate preparation; or you can't produce the evidence an assessor would ask for.

This is the only section where a high score isn't entirely within your control — regulatory frameworks are set externally and timelines are fixed. What you can control is preparedness: knowing which frameworks apply, having evidence of posture ready, and understanding what assessors will look for.

Key frameworks in the OT context

- EU Cyber Resilience Act (CRA): Applies to products with digital elements sold in the EU. For OT hardware and software, this means security-by-design requirements, vulnerability disclosure obligations, and mandatory security update support. Reporting obligations for exploited vulnerabilities and serious incidents apply from September 11, 2026. Main obligations apply from December 11, 2027.
- NIS2: Applies to operators in critical sectors including energy, manufacturing, water, and transport. Requires risk management measures, incident reporting, and supply chain security. Audits are underway across EU member states.
- IEC 62443: The dominant OT-specific security standard. Defines security levels (SL) for industrial automation and control systems. Commonly required by asset owners and integrators as a procurement condition.
- US federal EOs / FedRAMP: Executive orders on improving national cybersecurity set requirements for software used in federal and critical infrastructure contexts. FedRAMP certification applies to cloud services used by federal agencies. Portainer is FIPS 140-3 compliant and can operate in FIPS-only mode.
- Sector-specific: NERC CIP (energy/utilities), AWIA (water), HIPAA (healthcare OT), PCI DSS (payment-adjacent OT). If you identified sector-specific frameworks in the assessment, apply the framework's specific evidence requirements.

What good looks like

- Two or more applicable frameworks mapped to your environment with documented obligations
- Patch deployment evidence producible on demand for any defined date range
- A gap assessment completed within the last 12 months
- Data sovereignty documented as a formal procurement requirement

How to close the gap

The audit log problem has a two-part architectural fix. First, every management action is recorded at the control plane, not on the device being accessed, so a technician or vendor working on a device cannot touch the record of what they did. Second, the audit stream is forwarded to storage outside the management plane's own administrative boundary (a SIEM or write-once storage), so platform administrators can't alter it either. Portainer records all control plane actions and streams them to any

The applicability matrix varies by where you operate and how you sell. Verify your status before your next audit or procurement conversation.

OBLIGATION TYPE	EU	UNITED STATES	GLOBAL SUPPLY CHAIN
Procurement condition	IEC 62443	IEC 62443, CMMC	IEC 62443
Active audit / enforcement	NIS2	NERC CIP, HIPAA, AWIA	
Hard upcoming deadline	CRA Sep 2026		

Section 5

Operational reality

What a low score here means

Your operational load is how much of your team's capacity is consumed by patch and audit operations, how integrated your tools are, and how confident you'd be in an audit tomorrow. Scoring low in this section often reflects an architecture that's technically functional but operationally expensive: patching works, but takes 30+ hours per week; tools exist, but don't connect to each other; evidence is producible, but requires manual assembly from multiple systems.

This section frequently scores lower among operators who have made real progress in the first four areas, but haven't yet consolidated the workflows that support them. It's the signal that the right foundations are in place but not yet operating at full efficiency.

What good looks like

- Under 5 hours per week on patch deployment and audit operations
- Single management plane, or a tightly integrated stack with no manual handoffs
- New devices onboarded in under an hour, not a multi-day project
- Audit-ready confidence: a clean evidence package producible without advance preparation

The time cost of patching, onboarding, and evidence production isn't a staffing problem as much as an architecture one.

Workflow	Decentralized/manual	Centralized management plane
Patch one device Deploy, verify, log	**Hours to days** Requires direct or site access	**Minutes** Fleet-wide from one interface
Onboard a new site Configure, credential, connect	**Days to weeks** Bespoke per-site config	**Under and hour** Template + one-touch provisioning
Produce audit evidence For a defined date range	**Manual Assembly** Multiple systems, hours of prep	**On demand** Control plane generates it automatically

How to close the gap

The primary driver of high operational load is tool fragmentation. When patching, access control, audit logging, and fleet visibility live in separate systems with manual handoffs between them, the overhead compounds. A single management plane that addresses all four functions removes the integration overhead structurally.

Onboarding speed is the most direct measure of architectural scalability. A multi-day onboarding process has an architectural root cause: each site has a bespoke configuration, credentials are provisioned manually, and there's no reproducible process. Template-based provisioning with automated credential management and One-Touch Onboarding provisions devices via script, with no per-device manual configuration, reducing it to a fast, repeatable workflow.

Where to go from here

The gaps described in this guide have architectural solutions. The question is sequencing: which gaps carry the most regulatory exposure, and which have the most operational leverage.

The Portainer Industrial & IoT team runs structured discovery conversations with OT security leads and GRC teams. It's not a product demo as much as a working session to map your specific gaps to an architectural path forward.

Schedule a conversation: portainer.io/contact

Take a deeper dive

If you scored strongly across the assessment, your next question isn't remediation, it's whether your architecture holds at the next layer: connectivity that removes the attack surface instead of defending it. Our on-demand webinar with Xiid covers what that looks like in production OT environments.

▷ Watch on demand

PORTAINER.iO