DATA SHEET

Securing OT, SCADA, and Industrial IoT with Terniion™

The Problem: Long-Lived Systems, Growing Cyber Risk

Your OT, SCADA, and industrial IoT assets were built to run for decades. From power grids and manufacturing lines to EV chargers and building systems, these environments now sit in the blast radius of threat actors whose tactics evolve and grow more effective every week.

The constraints are brutal:

- You can't casually patch or replace PLCs, RTUs, and HMIs without risking downtime.
- Field devices live on dirty, shared networks you don't control.
- VPNs and exposed ports create standing entry points attackers can probe for years.

Traditional IT security was never designed for this world, but Xiid's Terniion is.

Terniion eliminates the attack surface for OT and industrial IoT without touching firmware or shutting down the line.

Business Outcomes

Reduced Business and Safety Risk

Process-level isolation and non-routable networks drastically cut the chance that a cyber incident turns into plant downtime, grid disruption, or a safety event executives must explain to regulators and boards.

Reduced Operational Complexity

Closing inbound ports, eliminating plant VPNs, and using one overlay for OT and industrial IoT removes layers of fragile firewall rules, jump boxes, and custom DMZs that operations teams struggle to maintain.

Lower Total Cost of Ownership

Fewer point tools for remote access, fewer emergency network workarounds, and less “hero work” to patch exposed devices reduce security spend, contractor dependence, and overtime for scarce OT talent.

Modern Security Without Downtime

Terniion wraps legacy PLCs, RTUs, HMIs, and field sensors without firmware changes or rewiring, so plants harden security in-place with no shutdown windows, no requalification cycles, and no production hit.

5 Best Practices for OT / SCADA / Industrial IoT Security

Best Practice	Key Actions	Xiid Terniion Solution
Protect Unmodifiable Legacy Systems	Avoid relying on firmware updates or hardware replacement to improve security. Support PLCs, RTUs, HMIs, and legacy controllers as they are.	Terniion overlays existing OT infrastructure without touching device firmware. Legacy systems keep running as-is, but operate behind closed inbound ports and isolated, encrypted tunnels.
Close Field Device Access	Prevent direct internet or partner access to sensors, meters, chargers, and remote controllers sitting outside plant walls.	SealedTunnelTM technology makes field devices non-routable from the internet. All inbound ports stay closed; access is only possible through outbound-only, authenticated tunnels.
Secure Remote Maintenance	Let engineers and vendors access critical systems without standing VPNs or exposed jump hosts.	Process-bound tunnels replace always-on VPNs. Maintenance sessions spin up only when needed.
Prevent Lateral Movement in Control Networks	Ensure a compromised sensor or workstation cannot serve as a pivot into safety systems, SCADA masters, or grid controls.	Terniion enforces process-level microsegmentation. A compromised device can be isolated; it cannot reach PLCs, HMIs, or central control systems over the network.
Quantum-Secure Critical Communications	Assume adversaries are capturing traffic today to decrypt later with quantum capabilities.	Triple-layer, post-quantum encryption protects SCADA commands, telemetry, and grid coordination against “harvest-now, decrypt-later” strategies across decades-long asset lifecycles.

Key Components

- **SealedTunnel**
  Executed via STLink— a lightweight software agent on either end, these are outbound-only, triple-encrypted, process-to-process tunnels that perform reliably even over unstable networks, ideal for distributed clinical sites.
- **Commander**
  The control brain coordinating secure connections across cloud, on-prem, and hybrid environments. It centralizes policy so "who can talk to what" becomes maintainable rules instead of 10,000 firewall exceptions.
- **Connector**
  Joins two outbound-only communication halves without ever decrypting traffic. It serves as a secure rendezvous where quantum-encrypted messages are dropped off and picked up by authorized STLinks, keeping critical infrastructure undiscoverable.
- **Aclave**
  Credential-less authentication that lets staff and partners access systems without usernames, passwords or long-lived credentials.

How Terniion Secures OT, SCADA, and Industrial IoT

Terniion is a secure network access control platform designed as an overlay. It does not require you to rip and replace networks, firewalls, or control systems.

What This Looks Like in OT Environments

Plants and Industrial Sites

- PLCs, RTUs, HMIs, and safety systems run with all inbound ports closed.
- Engineering workstations, OEM support, and central teams connect through outbound-only tunnels, scoped to specific processes, not entire networks.
- Malware or an attacker-compromised workstation cannot pivot into the control network.

Grid, Energy, and Utilities

- SCADA masters and control centers are no longer addressable from the broader network.
- Field devices (reclosers, meters, RTUs) talk back through encrypted outbound tunnels, even over shared carrier networks.
- Grid-management and demand-response traffic is protected against interception and manipulation.

Industrial IoT and Long-Lifecycle Devices

- EV chargers, building systems, sensors, and medical or industrial devices stay reachable for operations, but unreachable for attackers.
- No exposed VPN concentrators, jump hosts, or open ports exposed to the internet
- As assets remain in service for 10–20+ years, their communications stay protected against both current and emerging cryptographic threats.

FAQS

Will this disrupt operations or require downtime?

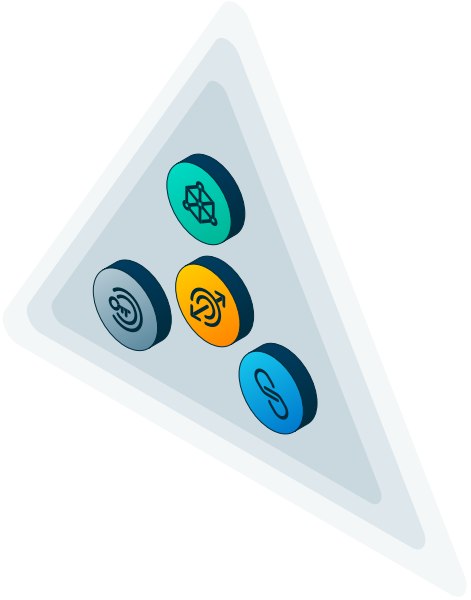
No. Terniion is designed as an overlay. It wraps existing OT and industrial IoT environments without requiring firmware changes or control system redesigns. Rollout can be phased site by site, starting with the highest-risk assets.

Do we need to replace our existing firewalls, VPNs, or identity systems?

No. Terniion reduces your reliance on VPNs for OT, but it doesn't demand a wholesale rip-and-replace. It works alongside your current firewalls and identity providers, immediately shrinking their exposed attack surface to nearly zero.

How does this help with regulators and insurers?

Regulators and insurers increasingly focus on exposure, lateral movement, and resilience. Terniion closes inbound ports, hardens remote access, and provides strong cryptographic controls, making it much easier to demonstrate reduced attack surface, containment of incidents, and alignment with modern frameworks.



The Bottom Line

Your OT, SCADA, and industrial IoT systems will be in service for decades. Your security model needs to last just as long. **Terniion gives you a way to:**

- Cut business and safety risk without shutting down production.
- Simplify a tangled OT security stack.
- Reduce long-term cost and staffing pressure.
- Bring legacy and modern assets under one, future-ready protection model.

Secure the systems that keep your business running against today's and tomorrow's attackers.

Ready to harden OT and industrial IoT without disrupting operations?
Request a briefing | See a live demo