txOne networks

TXOne Networks Product Portfolio 2026

Keep the Operation Running.

Operations-First OT Security.

Discover.
Assess.
Protect.

Industrial Cybersecurity That Runs With Operations

TXOne Networks is the operations-first OT security partner. We build prevention-first security, purpose-built for industrial environments, that now runs in 3,600+ operations with 100% operational continuity (TXOne Networks Internal Data, 2026). Every day, production teams face a coordination gap: ransomware executes in about four minutes while detection-to-enforcement coordination takes 35 to 45 minutes at best. Operations cannot afford that gap. Our job is to close it, without changing how your operation runs.

Operations-First Philosophy



Comprehensive OT Security Protection

One partner accountable across network, endpoint, inspection, and orchestration layers. No finger-pointing during incidents. No integration overhead. Single-vendor visibility and coordinated prevention across your entire OT environment.



Legacy System Life Extension

Protect legacy OT assets instead of replacing them. Coverage from Windows 2000 through Windows 11 committed through at least 2031, plus Linux support for modern control systems. Avoid $2 to $5 million in replacement cost per critical system and modernize on your schedule, not during a crisis.



Zero-Disruption OT Security

Hardware bypass keeps traffic flowing even when a security device fails. No modifications, no unscheduled downtime, no infrastructure redesign. Security that works within operational reality, not against it.

3,600+	100%	180+	70,000+
enterprise customers	operational continuity	industrial protocols	OT applications recognized (TXOne Networks Internal Data, 2026)

Discover. Assess. Protect. is our framework for every OT security outcome.

TXOne Complete: Four Approaches, One Operations-First Partner

No single security control covers an industrial operation end-to-end. TXOne Complete delivers four coordinated approaches across the OT lifecycle: validating what enters your environment, seeing what is running on every endpoint, protecting traffic on every network, and coordinating security across every site. Each approach works on its own and gains strength when combined.

The Four Approaches



Entry Point Validation

Validate devices and media before they touch production systems. Zero system modifications. Agentless. Fully air-gap capable. Designed for contractor devices, removable media, and asset-onboarding workflows in regulated environments.



Endpoint Visibility & Protection

See and protect every OT endpoint, from the newest Windows 11 engineering workstation to the oldest Windows 2000 HMI. Prevention-first architecture with automated per-device baselines, application lockdown, and OT-specific behavioral analysis.



Network Visibility & Protection

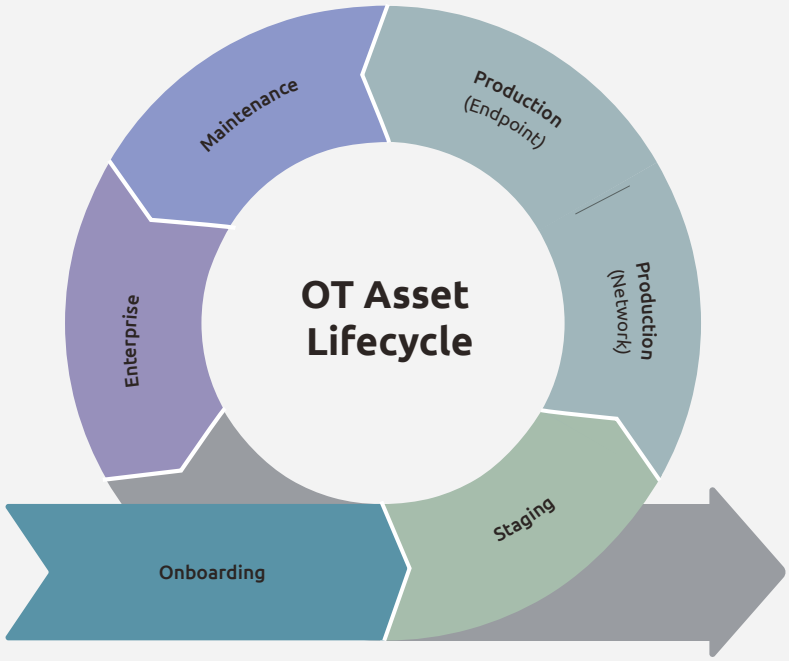
See and stop threats inline, without network redesign. Sub-second automated blocking with hardware bypass as a fail-safe. Deep packet inspection across 180+ industrial protocols with command-level enforcement for modern and legacy equipment.



Enterprise Security Orchestration

Coordinate security across sites from one console. Unified visibility, cross-product correlation, and asset-contextual risk prioritization that turns findings into production-safe remediation plans operations will approve.

Coverage Across the OT Asset Lifecycle



Lifecycle Phase	Operational Activity	How TXOne Helps
Onboarding	Validate media and portable devices before systems connect	Entry Point Validation
Staging	Understand what you have; score vulnerabilities before production	Endpoint Visibility + Enterprise Orchestration
Production (Network)	Enforce inline policies; block unauthorized commands and traffic	Network Visibility & Protection
Production (Endpoint)	Protect operating systems; prevent unauthorized process execution	Endpoint Visibility & Protection
Maintenance	Protect legacy-constrained endpoints; scan maintenance media	Endpoint Visibility + Entry Point Validation
Enterprise	Correlate events and coordinate policy across all sites	Enterprise Security Orchestration

One operations-first partner. Four coordinated approaches.
Every phase of the OT asset lifecycle covered.



Entry Point Validation:
TXOne Element

Industrial environments validate every physical input: raw materials, tools, personnel, even packaging. Digital inputs deserve the same discipline. Element validates USB devices, removable media, and contractor equipment before they touch production systems, without installing an agent, without modifying the target system, and without requiring a network connection.

The TXOne Element Family



Virtual Portable Inspector (new)

The software form factor of Element Security Inspection — bringing the same OT-grade inspection engine to connected assets without USB devices, persistent software, or on-site technicians.



Portable Inspector (Standard and Pro Editions)

USB-form-factor portable scanner for on-demand media and asset inspection. Multi-engine malware scanning, asset inventory collection, and no installation required on the scanned system. Pro Edition adds AES-256 hardware encryption for encrypted chain-of-custody scanning in regulated environments.



Safe Port

Desktop or wall-mount kiosk for high-throughput media scanning at facility entry checkpoints. Up to 7,200 files per minute (TXOne Networks Product Documentation, 2026). Glove-compatible touchscreen. LED pass/fail indicator for operators with zero security training.



ElementOne

Centralized policy management across every Element deployment. Scan-result aggregation, compliance reporting, fleet management, and REST API integration with SIEM and Sennin for enterprise visibility.

What Element Delivers

- Agentless inspection for systems that cannot accept software, including validated and air-gapped equipment.
- 100% air-gap compatible with full offline operation at remote sites and disconnected production zones.
- Lock feature that encrypts malicious files directly on the source device, preventing accidental reintroduction.
- LED-guided pass/fail workflows that let site operators validate every entry without specialist training.
- AES-256 hardware encryption in Pro Edition for regulated environments requiring tamper-evident audit trails.
- Centralized scan-result reporting across every site, every device, every contractor interaction.

Every USB. Every contractor device. Every piece of media. Validated before it touches your systems.

81.9%

of USB suspicious activity is file transfers (Nozomi Networks 2025 1H OT/IoT Security Report)

25%

of top OT incidents were triggered by USB plug-and-play events (Honeywell 2025 Cyber Threat Report)

1,826

unique threat types targeting OT have been detected through removable media (Honeywell 2025 Cyber Threat Report)

Endpoint Visibility & Protection: TXOne Stellar

Industrial endpoints run the oldest operating systems in the enterprise. IT endpoint tools assume cloud connectivity, modern operating systems, and IT-trained administrators. None of that describes an OT environment. Stellar delivers OT-native endpoint security across the full maturity journey, from visibility to full prevention, on Windows 2000 through Windows 11 plus Linux.

The Stellar Family

Stellar Discover (new)

Detection-only endpoint sensor. One-minute install, no drivers, no kernel access, user-space only. It is architecturally incapable of interfering with system stability. Fixed-price licensing for unlimited sensors, six-month term. Co-exists with IT EPP/EDR by design. Provides device inventory, software inventory, per-endpoint vulnerability detection, USB activity monitoring, login tracking, network flow records, and active malware reporting (log only).

Stellar Protect

All-in-one agent providing comprehensive protection with no internet connection required. Stellar Protect combines anti-malware, vulnerability scanning, application control, USB device control, application lockdown, CPSDR behavioral anomaly detection, per-device baseline generation, 70,000+ OT application recognition signatures, OT application safeguarding, and network access control.

StellarOne

Unified management for Stellar Discover and Stellar Protect agents across the entire endpoint estate. StellarOne supports both on-premises and cloud deployment, and forwards events to Splunk, Microsoft Sentinel, and QRadar through native connectors, so the SOC can continue operating with tooling it already knows.



Three Value Pillars

Focused on Operations

Stellar Discover runs in user space with no kernel access, so it cannot interfere with system stability by design. Stellar Protect establishes a behavioral baseline per device and blocks anything outside approved behavior, including fileless and living-off-the-land techniques.

Built for OT Constraints

Zero-reboot deployment and updates. Minimal resource footprint. Operationally safe response actions. Windows 2000 through Windows 11 with consistent protection and legacy OS coverage committed through at least 2031.

Security Without Compromise

Multi-engine defense combining signature, behavioral, and heuristic detection with per-device baseline enforcement and application lockdown. Air-gap ready. Market-proven across 3,600+ enterprise customers (TXOne Networks Internal Data, 2026).

51%

of organizations experienced legacy Windows security incidents in the past 12 months.

Source: TXOne Legacy OT Cybersecurity Report, 2026.

39%

have endpoint protection for legacy systems.

39%

report that IT endpoint tools conflict with OT operations.

Protect the endpoints you have. Extend their operational life. Modernize on your schedule.



Network Visibility & Protection: TXOne Edge

Ransomware executes in about four minutes. Best-case detection-to-enforcement coordination takes 35 to 45 minutes. A detection-only platform sees the threat, but someone else has to stop it. By the time that coordination finishes, the production line is already down. Edge closes that gap by design. It sits in the traffic path with deep packet inspection across 180+ industrial protocols, blocks threats in sub-seconds, and preserves operational continuity with hardware bypass fail-safe.

The Edge Family



EdgeIPS and vEdgeIPS Pro (new)

Inline IPS appliance family spanning nine physical models, from compact 2-port units for asset-level protection through 16-port fiber appliances for distribution and core network zones. Sub-500 microsecond latency. Hardware bypass fail-safe. Industrial grade design.

vEdgeIPS Pro brings the same OT-native security architecture to virtualized OT infrastructure, delivering consistent protection across physical and virtual environments from a single VM to full-scale production clusters.

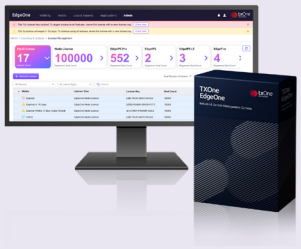
Sub-500
microsecond latency



EdgeFire

OT-native next-generation firewall purpose-built for remote sites. A single DIN-rail appliance replaces firewall, inline IPS, and site-to-site VPN concentrator. Deep packet inspection across 180+ industrial protocols with command-level enforcement. 700,000 hour MTBF. -40°C to 75°C operating range. Designed for the distributed production sites that IT firewalls cannot operate in and detection platforms cannot reach.

180+
industrial protocols



EdgeOne

Centralized information and control center for network security. Manages up to 1,000 nodes per instance. AI-powered auto-rule learning turns months of manual policy configuration into days of AI-guided deployment. REST API, syslog and CEF forwarding to SIEM, and integration with Sennin for portfolio-wide orchestration.

1,000
nodes per instance

What Edge Delivers

- Transparent inline deployment with no IP, no network redesign, and no production downtime.
- OT protocol deep packet inspection across 180+ industrial protocols with command-level filtering at Layers 2 and 3.
- System-independent virtual patching that protects unpatchable modern and legacy equipment.
- Multi-layer failsafe mechanism for maximum operational continuity during security events.
- Industrial form factors for every site size, budget, and mission profile.
- Complete visibility for connections, data flows, and protocol-level commands.
- Centralized management of security nodes and coordinated policy deployment.
- AI-driven traffic analysis that simplifies security configuration for lean OT teams.

Sub-second inline prevention closes the four-minute gap. Hardware bypass keeps production running while it does.



Enterprise Security Orchestration: TXOne Sennin

Every new OT security deployment creates a new console, a new policy set, a new ask for specialist staffing. Sennin aggregates security intelligence from across the TXOne portfolio into a single console with a centralized governance framework that unifies visibility and prioritizes vulnerabilities in operational context. One place to understand posture. One place to coordinate response. One place to prove the program is working.

Sennin, introduced at the Sennin 3.0 release in April 2026, delivers its value through two coordinated motions: Strategic Governance for organizations scaling a mature program, and Discover & Assess for organizations starting or restructuring one.

Strategic Governance with SenninOne

SenninOne is the investigation and orchestration platform for organizations with existing TXOne deployments who need centralized management across multiple sites, product families, and security operations teams. Enterprise success creates management complexity. SenninOne turns that complexity back into operational advantage.

- **Cross-Product Correlation.** MITRE ATT&CK for ICS mapping with cross-product event correlation across Edge, Stellar, and Element deployments. Investigate threats with operational context, not isolated alerts. Manages 500 to 100,000+ assets per deployment (TXOne Networks Product Documentation, 2026) with bi-directional SIEM integration for Splunk, Microsoft Sentinel, and QRadar, plus REST API.
- **Approval Workflows That Respect Operations.** Role-based access control and tailored recommendations for IT security and OT operations. No policy deploys enterprise-wide without operational sign-off. The IT/OT handoff is structured, documented, and auditable.
- **Asset Security Posture at Enterprise Scale.** Coverage of protected assets, asset health, degree of risk per asset, and asset lifecycle overview across every site and every product family.

Three Pillars of Unified Governance



Asset Security Posture

Coverage, health, risk, and lifecycle overview for every endpoint, appliance, and entry point across every site.



Vulnerability Management

Asset-linked vulnerability ticketing with VSAR-based prioritization by operational context, not just CVSS severity. Efficient risk mitigation that operations will approve.



Context-Driven OT Security

Multi-source data synthesis, Cyber-Physical Systems Detection and Response, and actionable insights that tie operational context to security control feedback across the portfolio.

67%
of organizations struggle with unified IT/OT visibility.

33%
of OT security incidents occur at IT/OT integration points.

Source: TXOne Networks / Omdia OT Security Survey, 2025.

71%
prefer single-vendor OT security platforms.

Source: TXOne Networks / Omdia OT Security Survey, 2025

For organizations beginning their first OT security program rather than scaling an existing one, the Discover and Assess entry point is as follows.

Discover + Assess: TXOne SenninRecon

You cannot protect what you cannot see. Before a protection program can be built, staged, or defended in front of a board, the organization needs an accurate inventory, a credible risk score, and a prioritized remediation plan that operations will actually approve. That is the Discover and Assess motion, and it is where SenninRecon leads. Paired with SenninOne for orchestration and, optionally, vPI and Stellar Discover for asset-level visibility, SenninRecon turns OT security from a deferred initiative into a funded program in a single engagement.

Where assets are connected but hard-to-reach, vPI requires no installation and is integrated into SenninOne, so endpoint and network findings share one VSAR score and one remediation plan. Where persistent monitoring is required, Stellar Discover can be deployed to managed endpoints.

SenninRecon: VSAR-Based Assessment Entry Point

Automated Discovery

Passive asset discovery across sites and network segments with no agent installation and no inline deployment. Discover assets without touching production.

Vulnerability Situational Awareness Rating (VSAR)

Vulnerabilities scored by operational context, not just CVSS severity. A critical CVE on a quiet jump host may be a lower priority than a moderate CVE on an engineering workstation running production-critical code. VSAR surfaces what matters most to operations.

Production-Safe Remediation Plans

Prioritized, actionable remediation recommendations that operations can approve. Not a thousand-line CVE list. A fundable, sequenced plan.

The Recon + Endpoint Discovery Bundle

For organizations with no existing asset inventory, SenninRecon is often paired with vPI and Stellar Discover in a combined Discover-phase engagement. The network-level view from SenninRecon and the endpoint-level view from vPI and Stellar Discover together produce the only end-to-end OT security posture workflow in the market that requires no site visit, no system modification, and no production interruption.

One engagement. Complete visibility. Evidence to fund the next phase of the program.

- SenninRecon surfaces network assets, traffic patterns, and network-visible vulnerabilities.
- vPI, integrated with SenninOne, extends the engagement to connected but hard-to-reach Windows assets — no agent, no hardware shipment, no on-site personnel.
- Stellar Discover surfaces continuous asset-level software inventory, per-endpoint vulnerabilities, USB activity, and active malware reporting on managed endpoints.
- SenninOne correlates all three streams, applies VSAR scoring, and produces the prioritized remediation plan.

One engagement. Complete visibility. Evidence to fund the next phase of the program.

Why Assessment Matters

47%
cite gaps in OT skills and resources.

Source: PWC 2025 Global Digital Trust Insights.

10%
allocate budget to OT security as a top-three priority.

Source: PWC 2026 Global Digital Trust Insights. Evidence-led assessments unlock budget because they turn hypothetical risk into quantified, prioritized findings.

29%
of national critical infrastructure organizations maintain centralized asset management.

Source: Bridewell CNI Cybersecurity Report, 2026.



TXOne SenninRecon

Keep the Operation Running. Start with a passive SenninRecon assessment (no agents, no network changes, no production interruption), schedule a 60-minute Edge proof of value, or begin a conversation with your TXOne team. Visit txone.com or contact your local TXOne representative.



Copyright © 2026 TXOne Networks. All rights reserved.