TXONE NETWORKS

Beyond Detection: A Proactive Framework for OT Threat Prevention

OT Security Intelligence Series



Executive Summary

Operational technology (OT) environments power the world's most critical infrastructure. Energy grids. Water treatment facilities. Manufacturing plants. Transportation networks. Yet despite record investment in security monitoring and detection tools, OT-targeted attacks continue to escalate in both frequency and impact.

The uncomfortable truth is this: **detection alone is not security. It is surveillance.** And in OT environments, where a single compromised controller can shut down a pipeline or endanger workers, the gap between seeing a threat and stopping it can be catastrophic.

22%

OT organizations with a cybersecurity incident in the past year; 40% caused operational disruption

SANS State of ICS/OT Security, 2025

119

ransomware groups targeting industrial organizations in 2025, up from 80 in 2024; 3,300+ victims

Dragos 9th Annual OT/ICS Cybersecurity Year in Review, 2026

$5.56M

average cost of a breach in the industrial sector

IBM Cost of a Data Breach Report, 2024

This e-book takes a close look at the detection myth and presents a comprehensive framework for moving from passive observation to active protection:

- **The Detection Trap**: Why visibility-centric approaches create false confidence and leave organizations vulnerable despite "seeing" threats.
- **The Proactive Prevention Framework**: Seven essential building blocks that shift security posture from reactive to preventive, addressing threats before they can cause damage.
- **Prevention in Action**: What a prevention-first architecture looks like across the full spectrum of OT security challenges.

The Detection Trap

ALERTS WITHOUT ACTION

Thousands of alerts per week, lean staff, and no automatic blocking. Each signal demands human triage — a bottleneck attackers routinely exploit.

MINUTES TO RESPOND, SECONDS TO EXECUTE

Ransomware encrypts in under four minutes; detection-to-enforcement coordination routinely takes 35 to 45. The math never works in the defender's favor.

BLIND SPOTS AT EVERY ENTRY

Compromised VPNs, USB media, and IT-to-OT lateral movement bypass passive monitoring entirely — as the three case studies that follow demonstrate.

Over the past decade, the OT security market has been dominated by a single proposition: visibility. Vendors promised that if organizations could only see everything on their networks, security would follow. The result has been a generation of passive monitoring tools that generate voluminous alerts but rarely stop attacks.

Why Visibility-Centric Approaches Fall Short

Detection-centric architectures carry four structural weaknesses that are especially pronounced in OT contexts:

- **Detection latency.** By the time an anomaly is detected, correlated, and escalated, adversaries have already achieved their objectives. In OT environments with lean security staff, alert fatigue compounds the problem.
- **Alert overload without action.** The average OT security team receives thousands of alerts per week. Without automated prevention, each one requires human triage, creating bottlenecks that attackers routinely exploit.
- **Passive posture in active threat environments.** Monitoring tools observe threats in transit but take no action. In critical infrastructure, where availability is paramount, operators are often reluctant to block anything, even known malicious traffic.
- **Coverage gaps at the perimeter boundary.** Passive network monitoring misses threats that arrive via compromised remote access credentials, supply chain tampering, or lateral movement from IT networks, some of the most common OT attack vectors.

Real-World Consequences: Three Case Studies

> **The Core Insight:** Detection tells you what happened. Prevention determines what does not happen. In OT environments where recovery is measured in days, not hours, the only acceptable security outcome is preventing the incident in the first place.

The consequences of these structural weaknesses are not theoretical. They are visible in the public record of OT incidents over the past five years.

CASE 1

Colonial Pipeline Ransomware Attack, May 2021. The DarkSide ransomware group gained access to Colonial Pipeline's network through a single compromised VPN account that lacked multi-factor authentication. Within hours, attackers exfiltrated approximately 100 gigabytes of data.

Colonial Pipeline, which carries 45% of the East Coast's fuel supply, proactively shut down its entire pipeline to prevent ransomware from spreading into OT systems. The shutdown triggered six days of disruption across 17 states and prompted a Presidential emergency declaration. The company paid approximately $4.4 million in ransom.

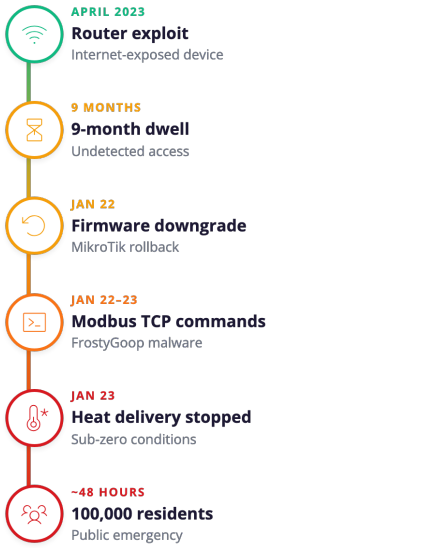
Post-incident review confirmed the entry point: a legacy VPN profile with no MFA. A known, preventable gap.



ATTACK CHAIN

Internet-exposed OT router cut heat to 100,000 residents

Two sub-zero days. Direct OT attack — no IT compromise needed.



ENTRY POINT

Internet-exposed OT device. No IT network compromise required — direct OT attack.

CASE 2

FrostyGoop ICS Malware, Lviv, Ukraine, January 2024. In one of the most consequential OT-specific malware attacks on record, threat actors deployed FrostyGoop (the ninth known ICS-targeting malware ever discovered) against Lvivteploenergo, a district heating company serving residents of Lviv, Ukraine.

Initial access was gained approximately nine months earlier by exploiting a vulnerability in an internet-exposed MikroTik router. The attackers used Modbus TCP commands to cause ENCO heating controllers to report falsely elevated water temperatures, stopping heat delivery entirely.

Over 600 apartment buildings, serving an estimated 100,000 residents, lost heat for nearly two days during sub-zero winter temperatures. The attackers downgraded controller firmware to a version that lacked monitoring capability, blinding operators to what was occurring. The entry point required no network compromise at all to exploit.

CASE 3

Norsk Hydro LockerGoga Attack, March 2019. Norsk Hydro, one of the world's largest aluminium producers, was struck by LockerGoga ransomware across its entire global network, affecting more than 35,000 employees in 40 countries and 22,000 computers across 170 locations.

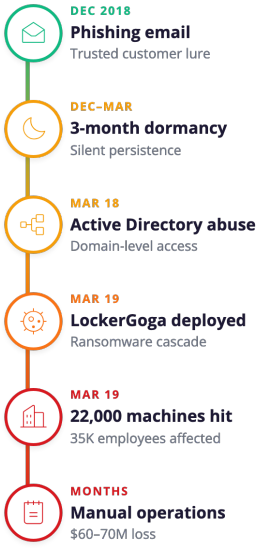
The infection originated three months before detonation, when a malicious payload was embedded in an email from a trusted customer. Once threat actors established domain-level access, they pushed the ransomware via Active Directory, locking files, disabling network adapters, and changing user passwords company-wide.

Multiple manufacturing facilities reverted to manual operations. Norsk Hydro refused to pay — rebuilding from backup cost an estimated $70 million over several months. IT-layer compromise, enabled by insufficient segmentation, cascaded directly into OT.

ATTACK CHAIN

Trusted-vendor email cascaded into a global OT shutdown

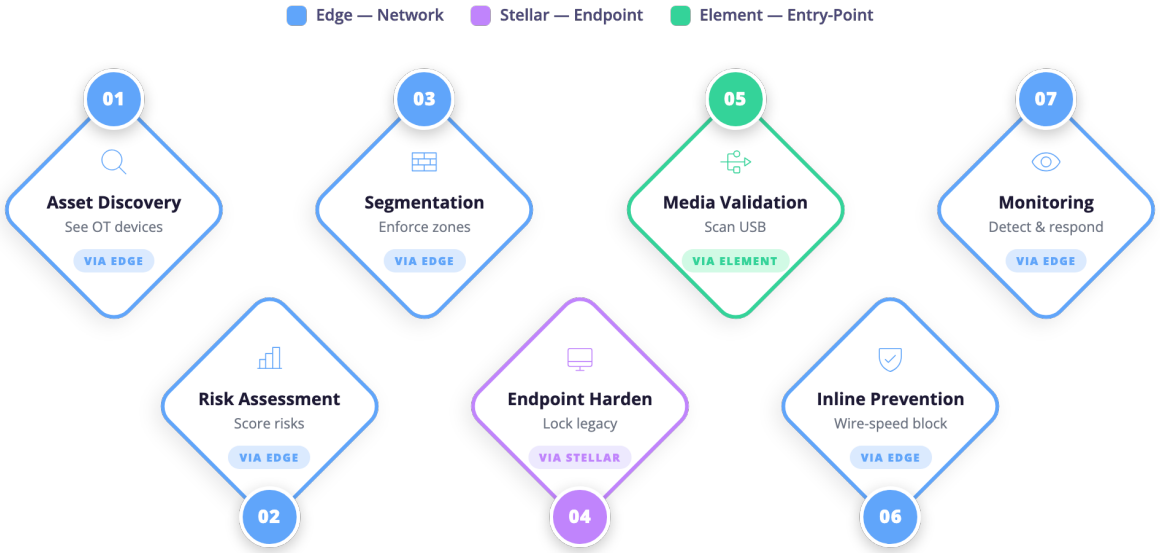
Manual operations lasted months. Loss: $60–70M.



ENTRY POINT

IT-layer compromise cascaded into OT — insufficient segmentation let ransomware cross zones freely.

The Proactive Prevention Framework



Moving from a detection-centric to a prevention-first posture requires systematic change across people, process, and technology. The following seven-pillar framework provides a structured path for OT security teams at any stage of maturity.

1. **Asset Inventory and Continuous Discovery.** Maintain a continuously updated, automatically enriched inventory of every OT asset, including firmware versions, communication patterns, and known vulnerabilities. Visibility is the foundation, not the destination.

2. **Risk-Based Vulnerability Prioritization.** Prioritize remediation based on exploitability, asset criticality, and compensating control availability. Use virtual patching to protect unpatched assets in the interim when the vendor patch is unavailable or cannot be applied.

3. **Network Segmentation and Trust Zone Enforcement.** Define and enforce trust boundaries between IT, DMZ, and OT zones. Implement unidirectional gateways or industrial firewalls and enforce allowlisting of permitted north-south and east-west communications.

4 **Endpoint Hardening and Application Control.** Apply application allowlisting, USB and removable media control, and memory protection to OT endpoints. Harden configurations against known attack techniques and lock down unnecessary services and ports.

5 **Removable Media and Physical Inspection Controls.** Require all removable media to be inspected and sanitized through a dedicated inspection kiosk before introduction to the OT environment. Enforce media policies at the technical level, not just through policy documents.

6 **Threat Intelligence Integration.** Connect OT security controls to curated OT/ICS threat intelligence feeds so that known malicious indicators of compromise are actively blocked, not just logged. Ensure feeds are OT-specific.

7 **Incident Response and Operational Continuity Planning.** Maintain tested OT-specific incident response playbooks, conduct regular tabletop exercises, and ensure backup and recovery procedures account for the unique recovery requirements of operational technology.

Prevention in Action

SPOTLIGHT: THE NETWORK APPROACH

The Network approach within TXOne Complete unifies inline network protection, an industrial firewall, and a centralized management console into a single, cohesive capability (Edge + Asset & Vulnerability Management, delivered as the Edge Complete capability for customers who need combined protection and visibility). Designed for prevention-first operation, it gives OT security teams the ability to discover, assess, and protect the network environment in one coordinated workflow, without disrupting production.

3,600+	60 min	40-60%
global deployments	proof of value	total cost reduction

This approach is backed by **3,600+ global deployments with zero unplanned downtime** (TXOne deployment data, 2026), a **60-minute proof of value** (versus 30 or more days for detection-only competitors), and a **40-60% total cost reduction** versus a multi-vendor detection-plus-enforcement stack (TXOne ROI Analysis, 2025).

How the Network Approach Maps to the Framework

The Network approach addresses four of the seven framework pillars at the network layer, providing the discovery, assessment, segmentation, and active protection capabilities that form the core of a prevention-first OT security posture.

Asset Visibility and Continuous Discovery (Pillar 1)

- Automatic discovery and fingerprinting of OT assets across L2 through L7 network traffic
- Network Graph visualization that maps every asset connection and communication path
- Continuous monitoring to surface shadow OT and unauthorized devices in real time

Risk-Based Vulnerability Assessment (Pillar 2)

- Built-in asset-vulnerability management with OT-specific CVE prioritization
- Risk scoring based on asset criticality, exploitability, and compensating controls
- Actionable remediation guidance delivered directly within the EdgeOne dashboard

Network Segmentation and Trust Zone Enforcement (Pillar 3)

- Industrial firewall (EdgeFire) with zone-based policy enforcement
- AI-powered auto-learning of OT protocol trust lists
- Adaptive segmentation that contains lateral movement and blocks worm propagation

Virtual Patching and Active Network Protection (Pillar 4, Network Layer)

- Inline virtual patching to protect unpatched assets without operational downtime
- Real-time allowlist and blocklist enforcement via command-level packet analysis
- Automated threat intelligence, signature, and firmware updates via EdgeOne

What This Looks Like in Practice

IN PRACTICE

A manufacturing customer deploys TXOne Edge in Monitoring mode across 14 production lines during a single maintenance window. Within 72 hours, EdgeOne's Network Graph surfaces 287 previously undocumented assets and 31 unauthorized device connections. The AI auto-learning engine observes normal OT protocol traffic for 14 days and generates allowlist trust rules without manual policy writing.

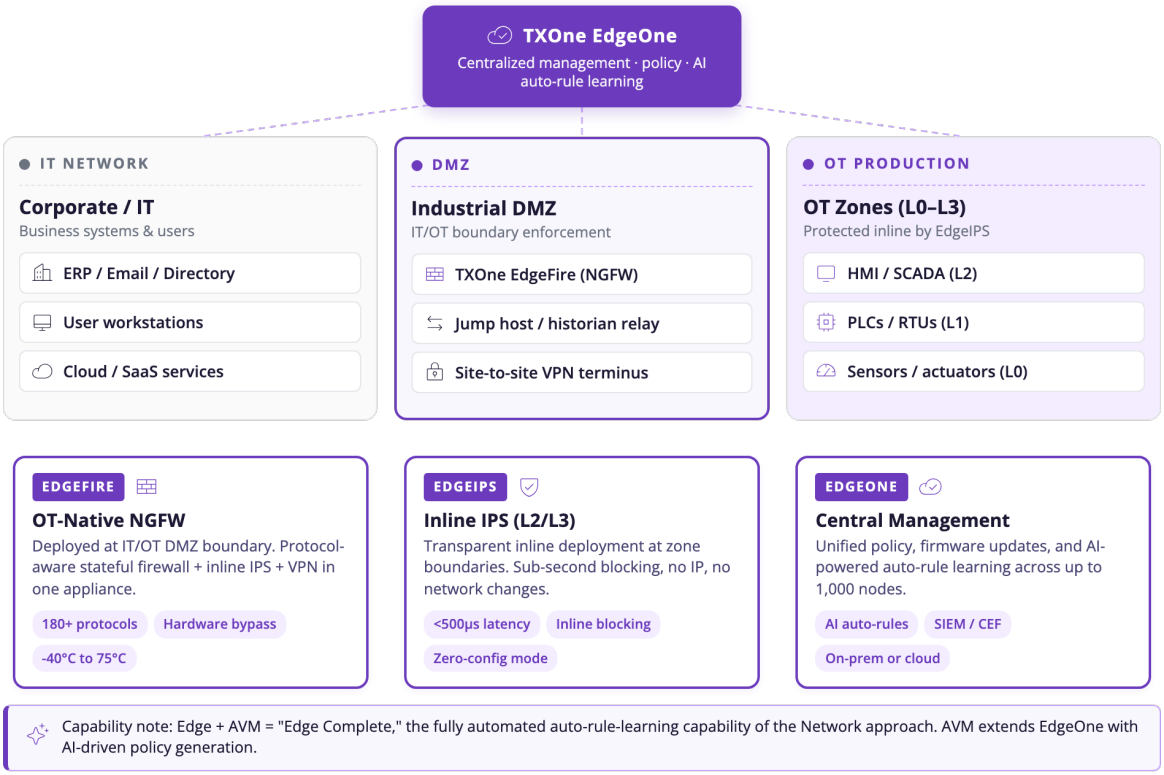
When enforcement activates, the EdgeIPS appliance intercepts a Modbus function-code injection attempt in under one second and blocks it before the instruction reaches the target PLC. **No alert triage. No vendor coordination. No production impact.**

The same attack, under a detection-only architecture, would have generated an alert, entered the queue, and required 35 to 45 minutes of human-coordinated response to be acted on. By then, the instruction would already have reached the PLC.

TXONE COMPLETE: THE NETWORK APPROACH

Edge products delivering the Network approach

EdgeFire at IT/OT boundary, EdgeIPS inline at zone perimeters, EdgeOne for centralized management.

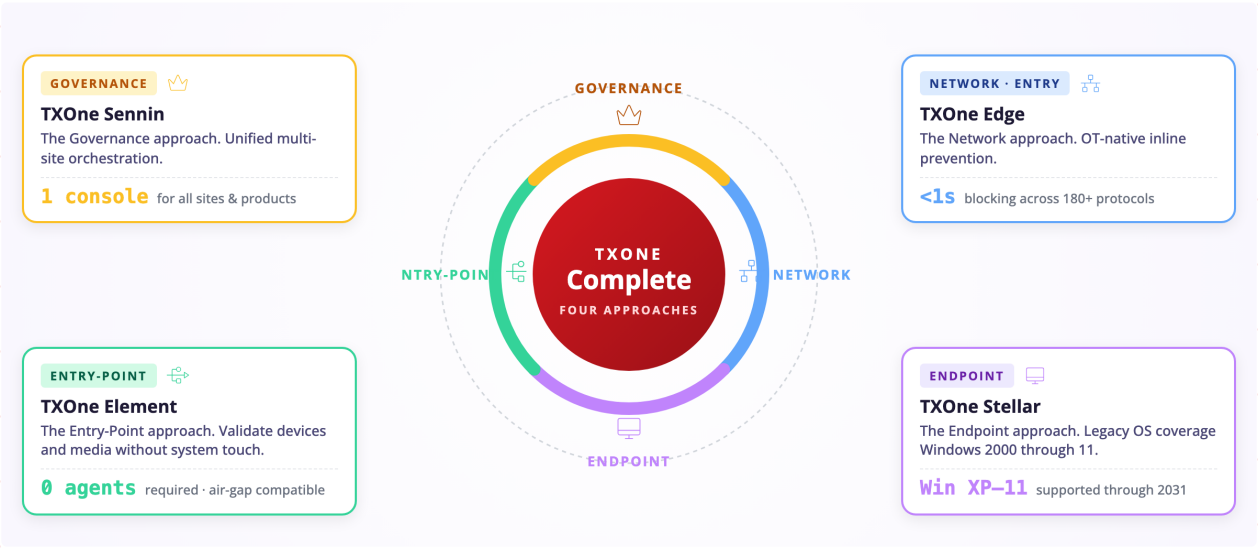


Reference deployment: mixed IT/OT manufacturing or energy site

Source: TXOne Edge deployment guide, 2026

The OT Prevention Roadmap

The Network approach is the critical first step. A complete prevention posture extends across the full TXOne Complete portfolio. Network covers pillars 1, 2, 3, 6, and 7 directly; Endpoint (Stellar), Entry-Point (Element), and Governance (Sennin) close the remaining gaps as the program matures.



Pillar	Network (Edge)	Expanded Coverage
1. Asset Inventory & Discovery	EdgeOne Network Graph + auto-discovery	Edge
2. Vulnerability Prioritization	AV management + risk scoring	Edge
3. Network Segmentation	EdgeFire zone enforcement + auto-trust	Edge
4. Endpoint Hardening	Network-layer virtual patching	Stellar
5. Removable Media Control	—	Element
6. Threat Intelligence	OT/ICS feed updates via EdgeOne	Sennin
7. Incident Response & Continuity	CPSDR logging + Sennin integration	Sennin

Conclusion and Next Steps

> **Prevention is a journey, not a switch.** The Network approach within TXOne Complete gives security teams a proven, network-first foundation to demonstrate measurable prevention outcomes quickly, building the organizational confidence and operational evidence needed to expand into the Endpoint, Entry-Point, and Governance approaches over time. Every step forward narrows the window of exposure.

The Proactive Prevention Framework presented in this e-book is not a distant aspiration. It is an achievable architecture for organizations willing to systematically address each of the seven pillars, beginning with asset discovery and risk prioritization, and progressively building toward a fully preventive security posture.

Take the Next Step

- Conduct an OT security posture assessment against the seven-pillar framework to identify your highest-priority gaps.
- Request a live demonstration of the TXOne Complete Network approach to see prevention-first architecture in action across your specific OT environment.
- Engage your channel partner for a co-sell consultation. TXOne's partner ecosystem is trained to deliver both technical proof of concept and business case development.
- Download TXOne's OT Security Maturity Assessment to benchmark your organization against industry peers.

Ready to Move Beyond Detection?

Contact your TXOne Networks partner or visit txone.com to schedule a prevention-first assessment for your OT environment.

Schedule a Prevention-First Assessment

About TXOne Networks

TXOne Networks specializes in OT-native cybersecurity for critical infrastructure and industrial control systems. Our solutions are deployed across energy, manufacturing, water, and transportation sectors globally.

As the operations-first OT security partner, TXOne helps industrial organizations protect critical operations, securely extend asset life, and build security programs without operational disruption. Purpose-built for industrial environments, TXOne enables organizations to discover their assets, assess risks in context, and protect operations without compromising productivity or safety.

Visit txone.com

TXOne Networks

© 2026 TXOne Networks, Inc. All rights reserved. TXOne and the TXOne logo are trademarks of TXOne Networks. Claroty, Dragos, and Nozomi Networks are trademarks of their respective owners. All external statistics remain the property of their respective publishers (Claroty, CrowdStrike, Dragos, Gartner, Honeywell, IBM, iVOX, Nozomi Networks, SANS); they are cited here for illustrative reference and are not reproduced in full. Gartner does not endorse any vendor referenced in this e-book. This document is for informational purposes only.