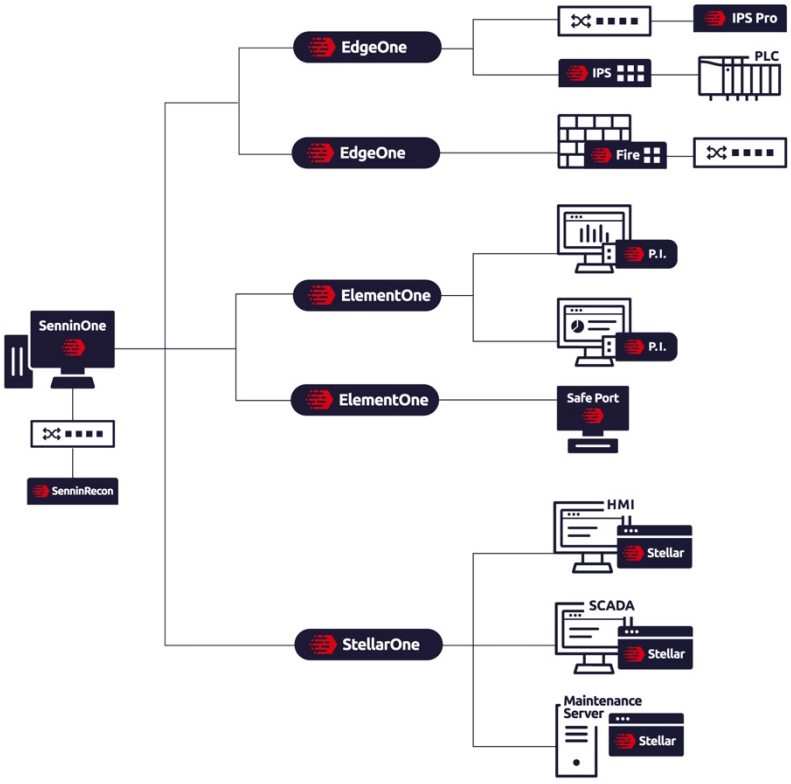
TXOne Sennin

Strategic Orchestration for OT Security Programs

From Findings to Fixes. Without Disrupting Production.

85% of organizations patch infrequently or not at all after identifying vulnerabilities (Frost & Sullivan OT Security Survey, 2024). The problem is not finding risk. It is acting on risk safely. Security teams should not have to choose between maintaining visibility into OT risk and being able to act on it safely. Every unacted finding is a documented exposure that compounds over time: regulatory findings, insurance reviews, and incident postmortems all trace back to the gap between what was identified and what was fixed.

TXOne Sennin is a centralized OT security governance platform that turns assessment findings into production-safe improvements. It combines passive network discovery with risk-prioritized orchestration, giving security and operations teams a shared system for identifying vulnerabilities, planning remediation, and coordinating deployment across distributed OT environments.



Sennin consists of two components:

SenninRecon is a network scanning appliance that discovers and assesses OT assets passively, requiring only a SPAN or mirror port.

SenninOne is a virtual appliance that consolidates findings from SenninRecon and other TXOne sensors into a single governance console, with risk scoring by operational context, IEC 62443 alignment, and approval workflows that keep operations in control of every change.

SenninRecon and SenninOne deploy together. For new customers, the minimum entry is both products. SenninOne also orchestrates existing TXOne Edge and Stellar deployments, adding unified governance across all deployed sensors.

Core Capabilities

Centralized Governance and Risk Oversight

SenninOne unifies visibility, policy enforcement, and compliance alignment across distributed sites. Site operations teams retain final approval on every policy change before it reaches their production environment. Enterprise governance recommendations are implemented only when sites confirm readiness.

Proactive Vulnerability Management

VSAR (Vulnerability Situational Awareness Rating) scoring combines CVSS, EPSS (a real-time public metric for the probability that a vulnerability will be exploited in the wild), real-world attack telemetry, and TXOne threat research intelligence. Vulnerability ticketing is prioritized by production impact, not just severity. Engineers receive actionable tickets tied to specific assets, not abstract advisories.

Proactive Vulnerability Management

VSAR (Vulnerability Situational Awareness Rating) scoring combines CVSS, EPSS (a real-time public metric for the probability that a vulnerability will be exploited in the wild), real-world attack telemetry, and TXOne threat research intelligence. Vulnerability ticketing is prioritized by production impact, not just severity. Engineers receive actionable tickets tied to specific assets, not abstract advisories.

Remote Investigation via Virtual Portable Inspector

When SenninRecon surfaces an unknown or elevated-risk asset, SenninOne can coordinate a remote, agentless inspection via Virtual Portable Inspector (vPI) without phys, USB media, or a technician present at the device. Security teams investigate elevated-risk assets across distributed sites from a single console, closing the gap between identification and investigation without dispatching personnel to the device location.

Operational Intelligence and Response Acceleration

Cross-product event correlation links network and endpoint activity into unified investigation timelines. MITRE ATT&CK for ICS mapping covers all 12 ICS tactics, translating OT threats into the framework IT security teams already use. Security findings are tied to specific systems, giving teams the context they need to act.

Zero-Disruption Architecture

SenninRecon discovers and assesses OT assets through passive monitoring. No agents, no reboots, no inline deployment. SenninOne deploys as a virtual appliance with no changes to OT devices or production traffic. Systems that cannot be patched or replaced remain visible and included in risk planning. Automated risk prioritization reduces daily management to scheduled review cycles, designed for small OT security teams without a dedicated security operations function.

Zero-Disruption Architecture

SenninRecon discovers and assesses OT assets through passive monitoring. No agents, no reboots, no inline deployment. SenninOne deploys as a virtual appliance with no changes to OT devices or production traffic. Systems that cannot be patched or replaced remain visible and included in risk planning. Automated risk prioritization reduces daily management to scheduled review cycles, designed for small OT security teams without a dedicated security operations function.

SenninOne Assistant (AI-Powered)

SenninOne includes an AI-powered assistant that answers questions about protection plan details, supports protection plan modification, and generates a RACI matrix based on organization size. The assistant is scoped to the Security Recommendation planning workflow.

Architecture Overview

SenninRecon sensors passively collect asset and vulnerability data from OT network segments via SPAN or mirror ports. Collected data is forwarded to SenninOne, which consolidates findings from all SenninRecon sensors alongside EdgeOne (network security management), StellarOne (endpoint security management), and ElementOne (inspection management) consoles into a single governance view. Risk-prioritized improvement plans are generated centrally and deployed through site-level approval workflows back to each product layer, ensuring no change reaches production without local operations sign-off.

Deployment Specifications

SenninOne with Pro or SenninRecon (Virtual Appliance)					
Number of Assets	**vCores**	**Memory**	**Required IOPS (read/write speed)**	**System Disk Space**	**Data Disk Space**
96,000	192	384 GB	28,000	20 GB	41.28 TB
32,000	64	192 GB	9,600		13.76 TB
16,000	32	64 GB	4,800		6.88 TB
8,000	16	32 GB	2,400		3.44 TB
4,000	8	16 GB	1,200		1.72 TB
2,000	8	16 GB	600		860 GB
Supported Hypervisors		Azure / VMware ESXi 6.5+ / VMware Workstation Pro 17+ / Hyper-V 10.0.18362.449+			
Supported Browsers		Google Chrome 90+ / Microsoft Edge 90+ / Mozilla Firefox 91+			

SenninRecon 716 (Hardware Appliance)	
Specification	**Detail**
Form Factor	1U rack-mount
Passive Scan Ports	16 ports
Active Scan Ports	1 scan port (active query for device identification and firmware collection)
Maximum Mirrored Traffic	7 Gbps total across all monitoring interfaces
OT/IT Protocol Detection	Passive detection across 80+ OT and IT protocols, including Modbus, PROFINET, EtherNet/IP, DNP3, BACnet, and OPC UA
Network Requirement	SPAN or mirror port
Hardware Isolation	Production traffic and management traffic on separate physical ports
Scanner Failure Impact	Passive monitoring only; scanner failure does not affect production traffic on monitored network segments
Power	Redundant (dual input, 100-240V AC)
Management	Browser-based (Edge 15+, Firefox 53+, Safari 10.1+, Chrome 63+)

SenninRecon License Tiers

Software licenses are sold per sensor and tiered by asset coverage capacity. Each physical or virtual SenninRecon sensor requires one software license.

License Tier	Assets Supported per Sensor
1K	Up to 1,000 assets
5K	Up to 5,000 assets
10K	Up to 10,000 assets
20K	Up to 20,000 assets
50K	Up to 50,000 assets

Integration and Interoperability

Sennin integrates with existing security infrastructure, adding OT governance context to IT security workflows.

Integration Type	Details
SIEM Forwarding	Syslog and CEF event forwarding to Splunk, Microsoft Sentinel, IBM QRadar, and other SIEM platforms; configurable event filters and severity mapping.
REST API	OpenAPI specification with HMAC-SHA256 authentication for custom integrations, CMDB export, asset inventory synchronization, and ticketing platform connectivity (ServiceNow, Jira).
Role-Based Access Control	Granular RBAC with customizable user roles and asset group assignments across multi-site deployments.
Identity Provider	SAML Single Sign-On for enterprise identity integration.
TXOne Portfolio	Bi-directional management of EdgeOne, StellarOne, and ElementOne consoles from a single SenninOne instance.
Investment Continuity	Sennin integrates with and adds governance context to existing third-party detection deployments. It does not replace visibility or detection platforms; it provides the assessment-to-action layer that they do not.
ServiceNow Service Graph Connector	The Service Graph Connector for TXOne is a certified application available on the ServiceNow Store. With it, integrate OT asset intelligence from SenninOne into the ServiceNow Configuration Management Database (CMDB).

Technical Evaluation Reference

Integration Type	Details
ATT&CK for ICS Coverage	Full MITRE ATT&CK for ICS framework mapping across all 12 ICS tactics; technique-level event correlation for investigation workflows.
OIT/IT Protocol Detection	Passive detection across 180+ OT and IT protocols, including Modbus, PROFINET, EtherNet/IP, DNP3, BACnet, OPC UA, and S7.
API Authentication	OpenAPI with HMAC-SHA256; supports CMDB sync, ticketing integration (ServiceNow, Jira), and custom automation workflows.
Event Correlation	Cross-product correlation linking EdgeOne network events, StellarOne endpoint events, and SenninRecon discovery data into unified investigation timelines.
SIEM Output Formats	Syslog (RFC 5424), CEF, and LEEF (IBM QRadar); tested integration paths with Splunk, Microsoft Sentinel, and IBM QRadar.
Data Retention	Configurable retention policies per deployment; sizing table reflects storage requirements for full retention at each asset tier.
Evaluation Path	Technical evaluation sessions available; request hands-on environment access at txo.network/contact.

What Changes After Deployment

47% of organizations cite gaps in OT skillsets and resources for cybersecurity initiatives (PwC Global Digital Trust Insights, 2025). Sennin is built for teams operating under those constraints.

1) Week 1

SenninRecon deploys passively on a SPAN or mirror port. No network changes, no agent installs. Asset discovery and vulnerability assessment begin immediately.

2) Week 2–3

SenninOne produces risk-prioritized improvement plans tied to specific assets, with VSAR vulnerability scoring as one input alongside operational context. Security and operations teams review findings through a shared console with approval workflows.

3) Ongoing

Risk-prioritized remediation plans replace static vulnerability lists. IEC 62443-3-3 gap analysis reporting is generated from live data when SenninRecon is deployed. Sennin adds the governance layer that detection platforms do not provide.

4) Analyst Recognition

Omdia Innovation Pioneer (OT Cybersecurity Platforms Market Radar, 2025). Frost & Sullivan Innovation Award for Industrial Cybersecurity (2025). Gartner Magic Quadrant for CPS Protection Platforms (2026).

Next Steps

Schedule Your Assessment: Passive deployment validates visibility, assessment, and improvement planning in your environment with zero operational risk.

Request Technical Documentation or Technical Evaluation Session: Detailed specifications, deployment guides, integration documentation, and a hands-on evaluation environment for technical validation.

Request Executive Briefing: Business case for leadership approval, including program overhead reduction analysis and full TXOne Complete portfolio positioning.

Explore: txo.network/sennin Contact: txo.network/contact