

TXOne OT Cybersecurity Portfolio



Erkennen. Bewerten. Absichern.

Copyright © 2026 TXOne Networks. Alle Rechte vorbehalten.





OT-Sicherheit mit Fokus auf den Betrieb

TXOne Networks unterstützt Industrieunternehmen dabei, den sicheren Betrieb kritischer OT-Umgebungen über den gesamten Lebenszyklus hinweg zu gewährleisten. Unsere Lösungen wurden speziell für betriebliche Anforderungen industrieller Umgebungen entwickelt und folgen konsequent dem Availability-First-Ansatz. Der Schutz von Cyber-Physical Systems (CPS) erfolgt dabei ohne Beeinträchtigung des laufenden Betriebs und umfasst Sicherheitsinspektion, Endpoint-Schutz, Netzwerksicherheit sowie eine zentrale Managementplattform.

Availability-First-Philosophie



OT-Sicherheit ohne Betriebsunterbrechungen



Verlängerung der Lebensdauer von Legacy-Systemen

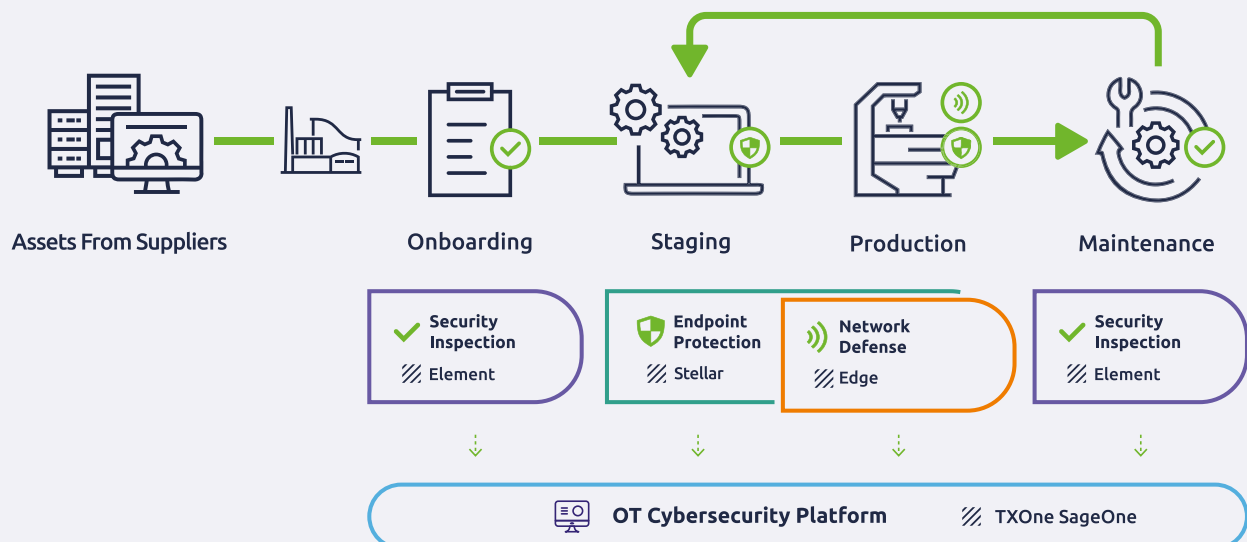


Ganzheitlicher Schutz industrieller OT-Umgebungen

Schutz von OT-Assets über ihren gesamten Lebenszyklus

TXOne Networks verfolgt einen ganzheitlichen Ansatz zum Schutz industrieller Assets, der jede Phase des OT-Lebenszyklus abdeckt und auf mehrschichtiger Sicherheitsarchitektur basiert. Vom Zeitpunkt der Anlieferung von Anlagen und Systemen bis hin zu ihrem produktiven Einsatz werden OT-Assets durch das Zusammenspiel aus Sicherheitsinspektion, Endpoint-Schutz und Netzwerksicherheit abgesichert.

Eine zentrale OT-Cybersicherheitsplattform verbindet diese Schutzebenen und ermöglicht eine konsistente Umsetzung des Discover-Assess-Protect-Ansatzes. Dieser Ansatz berücksichtigt sowohl moderne als auch Legacy-Systeme (ab Windows 2000 SP4 / Windows XP SP1/2/3) und stellt sicher, dass ein OT-Security-Konzept ohne Beeinträchtigung des laufenden Betriebs umgesetzt werden kann.





Security Inspection Element

Die Element-Produktlinie ermöglicht die Sicherheitsinspektion von Anlagen, Systemen und Wechselmedien in industriellen Umgebungen. Durch die Integration in bestehende Betriebsabläufe erhält das Betriebspersonal die Möglichkeit, regelmäßige Sicherheitsprüfungen und kontrollierte Medienfreigaben durchzuführen – ohne Änderungen an bestehenden Systemen.



Weitere Informationen ▲



Portable Inspector

Scannt kritische Assets und Datenträger, bevor sie in die OT-Umgebung eingebracht werden.



Safe Port

Prüft und bereinigt tragbare Speichermedien zur Einhaltung von Cyberhygiene.



ElementOne

Konsolidiert Scan-Ergebnisse und bietet eine zentrale Übersicht über Assets und Sicherheitsstatus.

- 3-in-1-Toolset für die Sicherheitsinspektion, einzeln oder kombiniert einsetzbar
- Echte agentenlose Nutzung ohne Softwareinstallation
- Vollständige Offline-Fähigkeit zum Schutz von Air-Gapped-Systemen
- Intuitive Bedienung, auch für Nicht-Spezialisten
- Hochgeschwindigkeits-Scanning mit AES-256-verschlüsselter, sicherer Speicherung
- Umfassende Erfassung von Systemschwachstellen auf Asset-Ebene

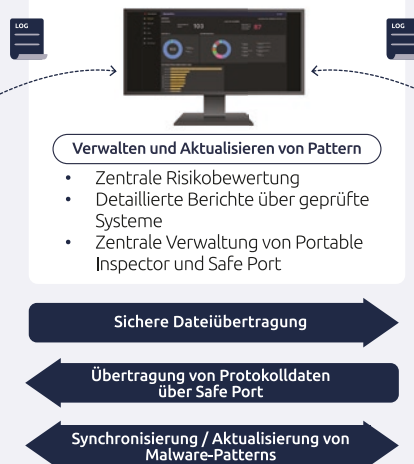
Element zur Sicherheitsinspektion von OT-Umgebungen

Schutz vor externen Bedrohungen

- Prüfung und Bereinigung von Wechselmedien
- Sichere Dateiübertragung



Ganzheitliche Sicht auf die OT-Umgebung



Interne Risiken identifizieren

- Agentenlose, malwarefreie Inspektionslösung
- Kein Neustart der Zielsysteme erforderlich
- Erweiterte IT-/OT-Transparenz





Endgeräte-Schutz Stellar

Stellar ist eine OT-native Endpoint-Sicherheitslösung, die speziell für industrielle Systeme und Legacy-Betriebssysteme entwickelt wurde. Sie schützt Endgeräte, indem unerwünschte oder unautorisierte Änderungen auf Anwendungs- und Prozessebene verhindert werden – ohne den laufenden Betrieb zu beeinträchtigen.

Damit stellt Stellar sicher, dass jedes industrielle Endgerät geschützt ist, auch dort, wo klassische IT-Sicherheitslösungen an ihre Grenzen stoßen.



Weitere
Informationen ▲



Betrieb im Fokus

Stellar etabliert für jedes Endgerät eine verhaltensbasierte Referenz, um unautorisierte Änderungen bereits vor der Ausführung zu blockieren.

- OT-kontextorientierte Datenbasis
- Cyber-Physical Systems Detection & Response
- Kontrolle zugelassener Peripheriegeräte



Speziell für OT entwickelt

Stellar schützt industrielle Assets ohne Beeinträchtigung des laufenden Betriebs – auch auf Legacy-Systemen.

- Umfassende Systemunterstützung inkl. Legacy-Support (ab Windows 2000)
- Betriebssichere Reaktionsmechanismen
- Installation ohne Neustart



Sicherheit ohne Kompromisse

Unterschiedliche Ziele und Prioritäten von IT-Sicherheit und OT-Betrieb führen häufig zu Spannungen. Stellar begegnet diesem Konflikt, indem es die Anforderungen beider Seiten gleichzeitig erfüllt.

- Marktbewährte Sicherheitsverfahren
- Mehrschichtige Bedrohungsabwehr



Netzwerkschutz

Edge

Edge schützt industrielle Netzwerke mit OT-spezifischen Sicherheitsfunktionen, die Stabilität und Resilienz gewährleisten.

Die Lösung sichert industrielle Kommunikation und Betriebsbefehle ohne Beeinträchtigung des laufenden Betriebs.



Weitere Informationen ▲



EdgeFire ist eine speziell für OT entwickelte Firewall mit integrierter VPN-Unterstützung.



EdgeIPS bietet eine Reihe von IPS-Appliances für OT-Umgebungen jeder Größe.



EdgeOne dient als zentrales Informations- und Kontrollzentrum für die OT-Netzwerksicherheit und Edge-Appliances.

- Transparente Inline-Integration ohne IP Address Änderung
- OT-spezifische Analyse industrieller Kommunikation und Protokolle (L2/L3)
- Systemunabhängiges Virtual Patching für Legacy- und moderne Systeme
- Mehrstufige Ausfallsicherheitsmechanismen für maximale Betriebskontinuität
- Breite Auswahl an Formfaktoren für unterschiedliche Budgets, Leistungsanforderungen und Einsatzszenarien
- Umfassende Transparenz über Verbindungen, Datenflüsse und Protokollbefehle
- Zentrale Verwaltung von Security-Appliances und Sicherheitsrichtlinien
- Automatisierte Analyse von Kommunikationsmustern zur Vereinfachung von Sicherheitskonfigurationen

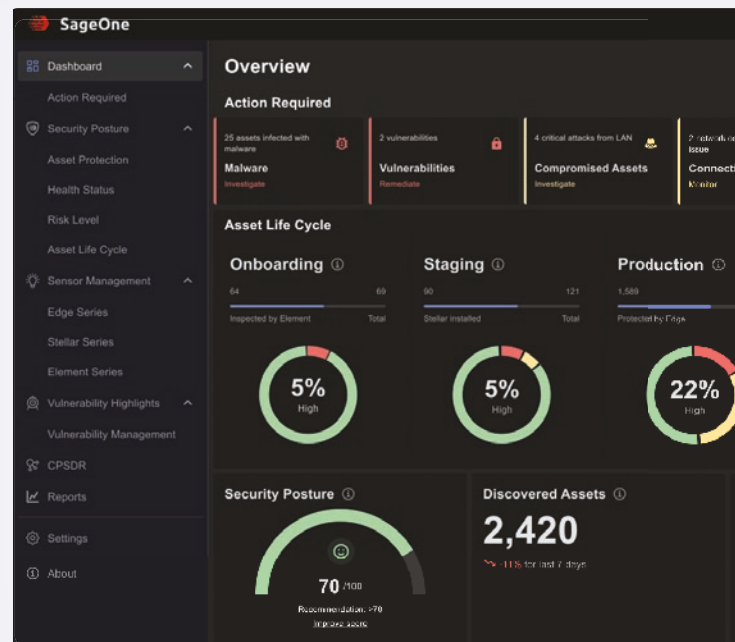


OT-Cybersicherheitsplattform TXOne SageOne

TXOne SageOne führt Sicherheitsinformationen aus dem gesamten TXOne-Portfolio in einer zentralen OT-Cybersicherheitsplattform zusammen. Die Lösung schafft durchgängige Transparenz, unterstützt bei der Bewertung und Priorisierung von Risiken und ermöglicht eine konsistente Sicherheitssteuerung über alle OT-Schutzebenen hinweg.



Weitere ▲
Informationen



Asset-Sicherheitsstatus

SageOne stellt den Sicherheitsstatus von Assets aus unterschiedlichen Perspektiven dar und bietet sowohl übersichtliche Zusammenfassungen als auch Detailinformationen.

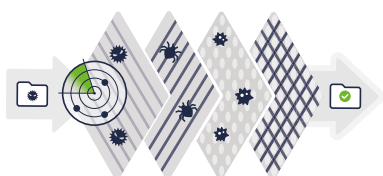
- Abdeckung und Status geschützter Assets
- Zustand von Assets und Erkennung von Anomalien
- Bewertung des Risikograds pro Asset
- Überblick über den Lebenszyklus von Assets



Schwachstellen-Management

Mit dem SageOne-Dashboard können Verantwortliche Schwachstellen bewerten, Prioritäten festlegen und geeignete Maßnahmen umsetzen.

- Präzise Identifikation von Risiken und betrieblichen Auswirkungen
- Priorisierung von Risiken aus einer übergeordneten Perspektive
- Effiziente Reduzierung von Risiken



Kontextorientierte OT-Sicherheit

SageOne verknüpft operativen Kontext mit Rückmeldungen aus den Sicherheitskontrollpunkten und liefert relevante, handlungsorientierte Sicherheitserkenntnisse.

- Zusammenführung von Daten aus mehreren Quellen
- Cyber-Physical Systems Detection & Response
- Konkrete, umsetzbare Sicherheitsempfehlungen