

TXOne 2024 OT Cybersecurity Portfolio



OT Cybersicherheit. **Einfach.**

Copyright © 2024 TXOne Networks. Alle Rechte vorbehalten.





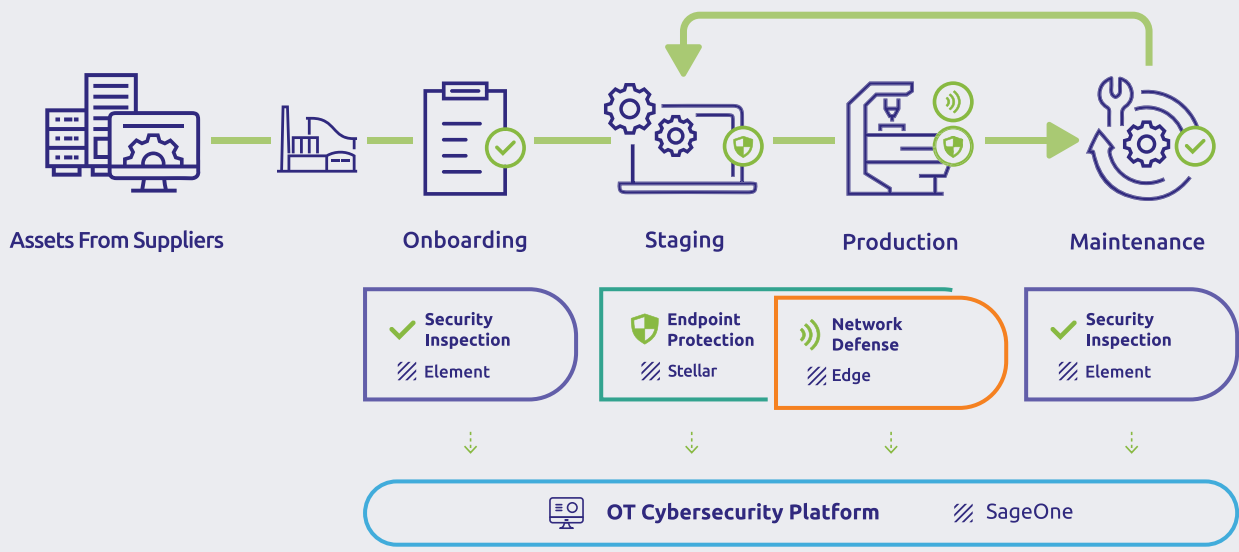
Assets From Suppliers

OT-Sicherheit mit Fokus auf das Unternehmen

Wir bei TXOne Networks haben uns zum Ziel gesetzt, eine Welt zu schaffen, in der Cybersicherheit den Fortschritt bei industriellen Innovationen unterstützt. Unser OT-Zero-Trust-Framework dient dem Schutz von Cyber Physical Systems (CPS) während des gesamten Lebenszyklus. Es besteht aus Sicherheitsinspektion, Endpoint- und Netzwerkschutz sowie einer zentralen Managementplattform.

Asset Lifecycle Protection

Das TXOne OT Zero Trust Framework schützt kritische Anlagen während ihres gesamten Lebenszyklus mit mehrschichtigen Sicherheitslösungen, einschließlich Sicherheitsinspektion, Endpoint- und Netzwerkschutz. Die darauf aufbauende Sicherheitsplattform bietet Visibilität und Kontrolle aus einer universellen Perspektive.





Security Inspection Element

Die Element-Produktlinie ermöglicht die Sicherheitsinspektion von Anlagen und Wechseldatenträgern. Die Integration in bestehende Protokolle gibt dem Betriebspersonal die Möglichkeit, regelmäßige digitale Säuberungen- und Bestandsverwaltungsaufgaben durchzuführen.



Weitere Informationen



Portable Inspector scannt kritische Assets und hält sie frei von Malware.



Safe Port bereinigt tragbare Speichermedien zur Aufrechterhaltung der Cyber-Hygiene.



ElementOne konsolidiert die Scanergebnisse, um einen Gesamtüberblick über das vorhandene Sicherheitsniveau zu erhalten.

- ✓ 3-in-1-Toolset für die Sicherheitsinspektion, das einzeln und gemeinsam eingesetzt werden kann
- ✓ Eigenständiges technisches Design, welches keine Installation erfordert
- ✓ Absicherung der Lieferkette durch Überprüfung der ein- und ausgehenden Geräte und Medien
- ✓ Sichere Datenübertragung zwischen den Geräten mit AES-256-Verschlüsselung
- ✓ Vereinfachung der Einhaltung von Vorschriften und Audits
- ✓ Erfassen und Zusammenfassen von Systemschwachstellen für jedes Asset

Element überprüft Ihre OT-Umgebung

Schutz vor externen Bedrohungen

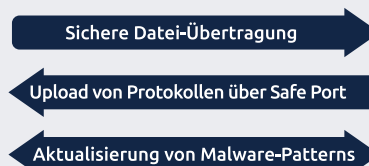
- Bereinigung von Wechseldatenträger
- Sichere Datei-Übertragung



Holistische Betrachtung über alles

Verwalten und Aktualisieren von Patterns

- Ganzheitliche Sicht zur Risikobewertung
- Detaillierter "Malware-Free"-Bericht
- Einfache Verwaltung von Portable Inspector und Safe Port



Identifizieren Sie interne Risiken

- Eine agentenlose Lösung zur Malware Bereinigung
- Kein Neustart des Zielsystems erforderlich
- Erweitern Sie die IT/OT-Sichtbarkeit





Endgeräte-Schutz Stellar

Stellar ist eine OT-native Software basierte Endgeräte-Sicherheitslösung. Sie schützt moderne und ältere Geräte, indem sie unbefugte Änderungen an dessen Basisanwendungen auf Anwendungs- und Prozessebene aktiv verhindert, ohne den normalen Betrieb zu unterbrechen.



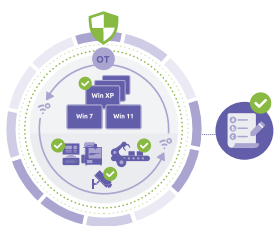
Weitere Informationen ▲



Betrieb im Fokus

Stellar vermeidet das Risiko unbefugter Modifikationen, indem es sich auf das Erkennen der Operationen und Geräte fokussiert und diese in Zusammenhang mit Sicherheitsergebnissen betrachtet.

- ✓ OT Kontextorientierte Datenbank
- ✓ Cyber-Physical System Detection & Response
- ✓ Kontrolle zugelassener Geräte



Speziell für OT entwickelt

Stellar schützt Anlagen, ohne den Betrieb zu beeinträchtigen. Es verringert Infrastruktur bedingte Schwierigkeiten zur Aufrechterhaltung der Cyber-Hygiene in der OT.

- ✓ Umfangreiche Systemunterstützung mit Legacy-Support (ab WIN 2000)
- ✓ Betriebssichere Response Maßnahmen
- ✓ Einfache Verwaltung



Sicherheit ohne Kompromisse

Die unterschiedlichen Ziele und Prioritäten zwischen Teams der IT-Sicherheit und des OT-Betriebs führen zu Spannungen und Unzufriedenheit. Stellar beseitigt die Notwendigkeit von Kompromissen, indem es die Anforderungen beider Teams gleichzeitig erfüllen kann.

- ✓ Marktbewährte Sicherheitsverfahren
- ✓ Bedrohungsabwehr mit multiplen Methoden



Netzwerkschutz Edge

Edge erhöht die Stabilität und Widerstandsfähigkeit von OT-Netzwerken. Identitätsbasierte Zero-Trust-Zugriffskontrollen regeln den Datenverkehr und die zwischen Geräten gesendeten Betriebsbefehle. Optimierte Analysetechniken für in der Industrie eingesetzte Protokolle bieten Präventions-, Erkennungs- und Remediation-Funktionen zur Sicherstellung der Betriebsstabilität.



Weitere 
Informationen



EdgeFire ist die ideale Firewall mit VPN-Unterstützung, die speziell für OT entwickelt wurde.



EdgeIPS bietet eine Reihe von IPS-Appliances, die für OT-Umgebungen jeder Größe geeignet sind.



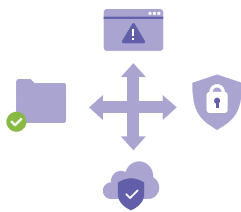
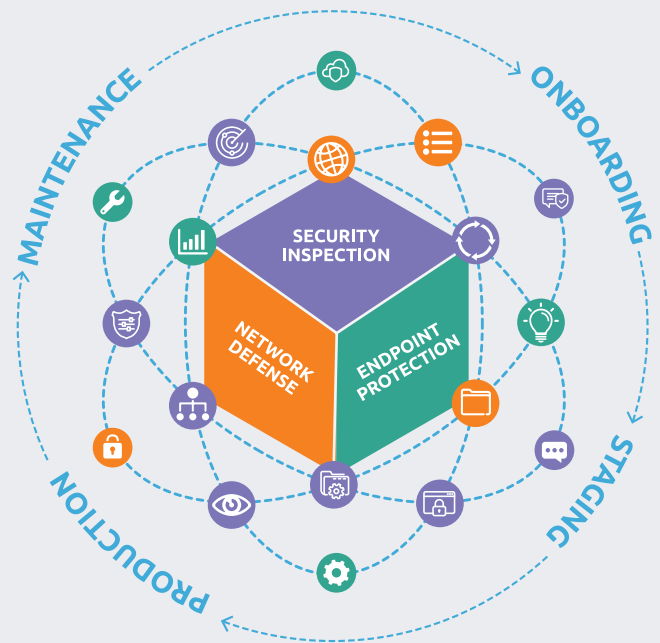
EdgeOne ist das Informations- und Kontrollzentrum für Ihre OT-Netzwerksicherheit und Edge-Appliances.

- ✓ Mikrosegmentierung des OT-Netzwerks zur Verringerung der Angriffsfläche
- ✓ Mehrschichtige Ausfallsicherheitsmechanismen zur Gewährleistung einer maximalen Betriebskontinuität
- ✓ Kontrolle von ICS-Protokollen mit Sicherheitsregeln, um echte OT-Sicherheit zu erreichen
- ✓ Eine breite Palette von Formfaktoren, die dem Budget, den Fähigkeiten und der Komplexität der Mission entsprechen
- ✓ Umfassende Sicherheitsreichweite durch Unterstützung von L2- und L3-Richtlinien
- ✓ Ganzheitliche Sichtbarkeit für Verbindungen, Datenfluss und Protokollbefehle
- ✓ Zentralisierte Verwaltung von Security Nodes und Richtlinienimplementierungen
- ✓ Adaptive, KI basierte Baseline-Erstellung zur Vereinfachung von Sicherheitskonfigurationen



OT-Cybersicherheitsplattform SageOne

SageOne fasst alle Sicherheitsinformationen aus dem gesamten TXOne-Portfolio zusammen und bildet eine ultimative Sicherheitsplattform. Es ist ein produktübergreifendes Kontrollzentrum, das in der Lage ist, potenzielle unbekannte Risiken zu entdecken, indem es KI-basierte Korrelationen aus mehreren Sicherheitskontrollpunkten und verschiedenen Blickwinkeln nutzt.



Asset Sicherheits-Status

SageOne stellt Ihren Sicherheitsstatus aus verschiedenen Blickwinkeln mit umfassenden Darstellungsmöglichkeiten dar. Es bietet ganzheitliche Sicherheitsinformationen auf granulare Weise.

- ✓ Erfassung geschützter Assets
- ✓ Asset-Status und Erkennung von Anomalien
- ✓ Grad des Cyber-Risikos für jede Anlage
- ✓ Überblick über den Lebenszyklus von Anlagen



Schwachstellen-Management

Mit dem SageOne-Dashboard können Anlagenverantwortliche auf einfache Weise Systemschwachstellen bewerten, priorisieren und Maßnahmenpläne ausführen.

- ✓ Risiken und betriebliche Auswirkungen genau identifizieren
- ✓ Priorisierung der zu behandelnden Risiken aus einer Makroperspektive
- ✓ Risiken effizient und effektiv reduzieren



Kontextorientierte OT-Suche

SageOne korreliert den operativen Bereich mit Feedback-Daten von Sicherheitskontrollpunkten und liefert wirklich aufschlussreiche Sicherheitsvorschläge.

- ✓ Zusammenführung von Daten aus mehreren Quellen
- ✓ Cyber-Physical System Detection & Response
- ✓ Handlungsfähige Sicherheitsinformationen