

# DAS TXONE 2023 CYBER DEFENSE PORTFOLIO

Cybersicherheit für Industrieunternehmen.  
**Ganz einfach.**

[txone.com](https://txone.com)

Copyright © 2023 TXOne Networks. Alle Rechte vorbehalten.

# Sicherheitsüberprüfung: Portable Inspector

Installationsfreies Scanning-Tool mit  
sicherer Dateiübertragung zur  
Überprüfung und Erkennung von  
Malware und Schwachstellen



Weitere Informationen ►

Der Portable Inspector bietet installationsfreie Sicherheitsfunktionen, die nicht nur von Sicherheitsteams, sondern auch von Technikern verwendet werden können. Das Tool in Form eines USB-Sticks kann zusätzlich zu bestehenden Prozeduren bei der Inbetriebnahme neuer Maschinen und dessen Wartung einen Scan durchführen, bevor diese in der Produktion eingesetzt werden.

Zudem können mit dem Portable Inspector regelmäßige Scans u.a. für das Auditing und die Bestandsverwaltung durchgeführt werden. Dieser liefert erweiterte Schutzvorrichtungen für OoB-Geräte (Out-of-Band) und Standalone-PCs.

- ✓ Regelmäßiges Scannen von unternehmenskritischen Systemen
- ✓ Lieferkettenschutz durch eine Sicherheitsüberprüfung von ein- und ausgehenden Geräten
- ✓ Erfassung und Zusammenführung der Logs- und Systemdaten mehrerer Scanning-Tools
- ✓ Übertragung von Daten oder Updates/Patches mit integrierten Speicherfunktion, die mittels AES-256 Verschlüsselung und automatischen Malwarescans vor Schadsoftware schützt und einen sicheren Datentransport ermöglicht
- ✓ Vereinfacht die Einhaltung von Compliance- und Auditing-Bestimmungen
- ✓ Erfassung und Zusammenführung von Systemschwachstellen gescannter Geräte

## Installationsfreie Überprüfung & Auditing

Leichte Erkennung und Entfernung von Malware, ohne dass Software auf den zu überprüfenden Systemen installiert werden muss. Die integrierten Status-LEDs ermöglichen eine einfache Handhabung.



Malware gefunden,  
weitere Maßnahmen  
erforderlich

Malware gefunden und  
beseitigt

Keine Malware gefunden,  
das System ist sicher

Anzeige des Scan-Status sowie des Ergebnisses mittels LED's

## Erweiterte Sichtbarkeit für OT-Systeme

Das Tool erfasst einen detaillierten Snapshot der Systemdaten, einschließlich Informationen über den Computer, den Status von Windows Updates, Systemschwachstellen sowie der installierten Software.

## Sichere Dateiübertragung

Dank AES-256-Hardware-Verschlüsselung und einer erweiterten Anti-Malware-Engine werden Dateien beim Übertragen auf dem sicheren Speicher gescannt, sodass nur malwarefreie Dateien gespeichert werden können und nur autorisierte Personen auf die Daten zugreifen dürfen.



Weitere Informationen ▲

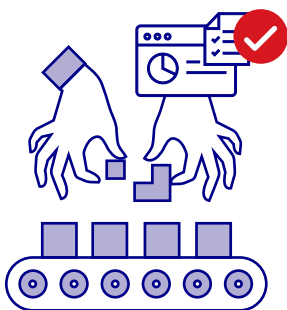
# Endgerätesicherheit: Stellar

Stellar ist ein agentenbasierter Schutz für in Produktionsumgebungen betriebener Windowssysteme, auf denen spezielle ICS-Applikationen laufen und unterstützt, insbesondere Altsysteme (Legacy) wie z.B. Windows 2000/XP.

Stellar stellt einen adaptiven, aktiven Malware- und Manipulationsschutz auf Anwendungs- und Prozessebene zur Verfügung, ohne den normalen Betrieb zu stören. Die neue Cyber Physical System Detection & Response (CPSDR) Funktion erkennt Verhaltensanomalien auf dem Endgerät zur Abwehr von Angriffen in der Produktionsumgebung.

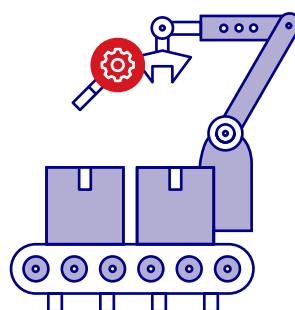
**Die weltweit erste OT-Lösung, die tausende von sicherheitskritischen OT-Anwendungen erkennen und schützen kann**

- ✓ All-in-One-Schutz
- ✓ Erkennung von OT-Anomalien
- ✓ Schutz von ICS-Anwendungen
- ✓ Schutz der betrieblichen Integrität
- ✓ Einschränkung bei der Verwendung von USB-Sticks



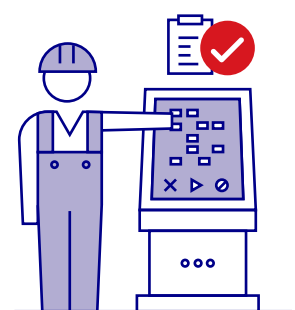
## All-in-1

Als „Ein-Agenten Lösung“ ist Stellar eine zentrale Sicherheitskomponente mit einem für OT optimiertem Virenschutz, Lock-down Funktionen und der Erkennung von OT-Anomalien



## Fokus auf den OT-Kontext

Das weltweit größte Repository für Industrieanwendungen (ICS) erstellt eine betriebliche Baseline, erkennt Systemanomalien und schützt die betriebliche Integrität



## Lebenslanger Schutz

Die bereichsübergreifende OT-Endgerätesicherheit schützt Systeme während ihres gesamten Lebenszyklus

# Netzwerkschutz: Die Edge-Serie

Effiziente Inline-Bedrohungserkennung zum  
Schutz der Betriebskontinuität



Die TXOne Edge-Serie mit OT-nativen IPS und Firewalls sind in verschiedenen Formfaktoren erhältlich, die eine Segmentierung und Mikrosegmentierung des OT-Netzwerks in produktionsbasierten Arbeitsgruppen ermöglichen.



Weitere  
Informationen ▲

- ✓ Transparente Implementierung (OSI-Layer 2) und Netzwerksegmentierung zur Beschränkung auf die für den Betrieb notwendige Kommunikation ("Need-to-know")
- ✓ Verhindert gefährliches Verhalten und Fehlbedienungen durch Kontrolle der in OT-Protokollen verwendeten Befehle (Zugriffslisten) in der Netzwerkkommunikation
- ✓ Schutz von angreifbaren, nicht gepatchten Geräten und veralteten Systemen durch Abschirmen von Schwachstellen („virtuelles Patchen“)
- ✓ Minimierung der Ausfallzeiten für Patching und Wartungsarbeiten
- ✓ Zentrale Verwaltung mit EdgeOne
- ✓ Gewährleistung der Betriebskontinuität durch ein erweitertes Fail-Safe-Design (Hardware Bypass)



txone.com

TXOne Networks | Keep the Operation Running



Kontaktieren  
Sie uns ▲