txOne networks

TXOne Stellar

DATA SHEET

ALL-TERRAIN SECURITY FOR OT ENDPOINTS AND CYBER-PHYSICAL SYSTEMS

Reduce security risks without compromising operations

Stellar is a comprehensive OT/CPS security solution providing continuous detection and response aligned to the specific requirements of the OT domain. With successful deployments in a wide range of industries, including electric power, oil and gas, manufacturing, pharmaceutical, semiconductor, and retail, *Stellar* is proven to boost operations' reliability, efficiency, and stability throughout the entire asset lifecycle.

Using a single-agent design, *Stellar* delivers seamless asset-centric protection with complete oversight for legacy OT devices and modern cyber-physical systems (CPS). Intuitive centralized management, consistent policy enforcement, and action-oriented alerts empower security teams of all sizes and skill levels to successfully mature their organization’s security posture.

Leveraging an expansive ICS application and certificate library, *Stellar* maintains CPS operational integrity through behavioral anomaly detection and eliminates configuration drift for legacy and fixed-use assets with device lockdown. Security teams can confidently deliver detection and response outcomes across the OT terrain, with *Stellar* meeting both security and operational needs alike.

KEY PRODUCT CAPABILITIES

OT INDUSTRY INFORMED PROTECTION

CPS Detection and Response (CPSDR) – Using an operation stability-focused approach, a unique device fingerprint of the baseline operating state is generated using telemetry from the app, network, system, user login, and device data categories. In a two-stage process, agents first inhibit unexpected changes by continually analyzing the device against its fingerprint to defend stability. Second, a broader analysis identifies what caused the change, threat, operator error, or otherwise.

Multi-Method Threat Prevention – A combination of patternless ML/AI and high-speed pattern detection methods provide real-time protection from known and unknown malware threats. Operations-focused tuning ensures accuracy without compromising availability.

Operational Configuration Lockdown – For fixed-function and devices with limited patching availability, run-time configuration lockdown enforcement prohibits unauthorized changes, including alterations to registry and function parameters, either inadvertently from operators or nefariously from threat actors.

Trusted Peripheral Control – Unauthorized access from external sources, such as USB devices, is configurable and controlled to reduce physical access threats.

OT DEVICE, APPLICATION, AND CERTIFICATE CONTEXT

OT/CPS Context-Focused Database – A comprehensive database maintained in partnership with device OEMs facilitates the accurate identification and evaluation of 8000+ apps, devices, and certificates.

Device Resource Management – Developed specifically for resource-constrained devices, the agent footprint and bandwidth demands are minimal. Intelligent agent-level event and telemetry filtering reduces network traffic burden by 90% without impacting accuracy or effectiveness.

Device-Centric Fingerprinting – Each agent generates a unique baseline fingerprint of its host device using OT/CPS database content, device configurations, and behavioral telemetry to drive CPSDR response actions.

COMPLETE ASSET LIFECYCLE COVERAGE

Long-Term OS Support – Updates and ongoing support for still-supported and end-of-life OS versions from Microsoft Windows 2000 to Windows 11 ensure coverage for modern CPS and legacy OT devices throughout their operable life.

Connected and Isolated Device Protection – With self-contained agent functionality, non-connected devices remain protected with updates made deliverable via USB download.

Operator Safety and Integrity Override – To ensure physical safety and process integrity contextual control, authorized operators can securely override agent policy in real time.

STELLAR BENEFITS

ALL-IN-1 AGENT

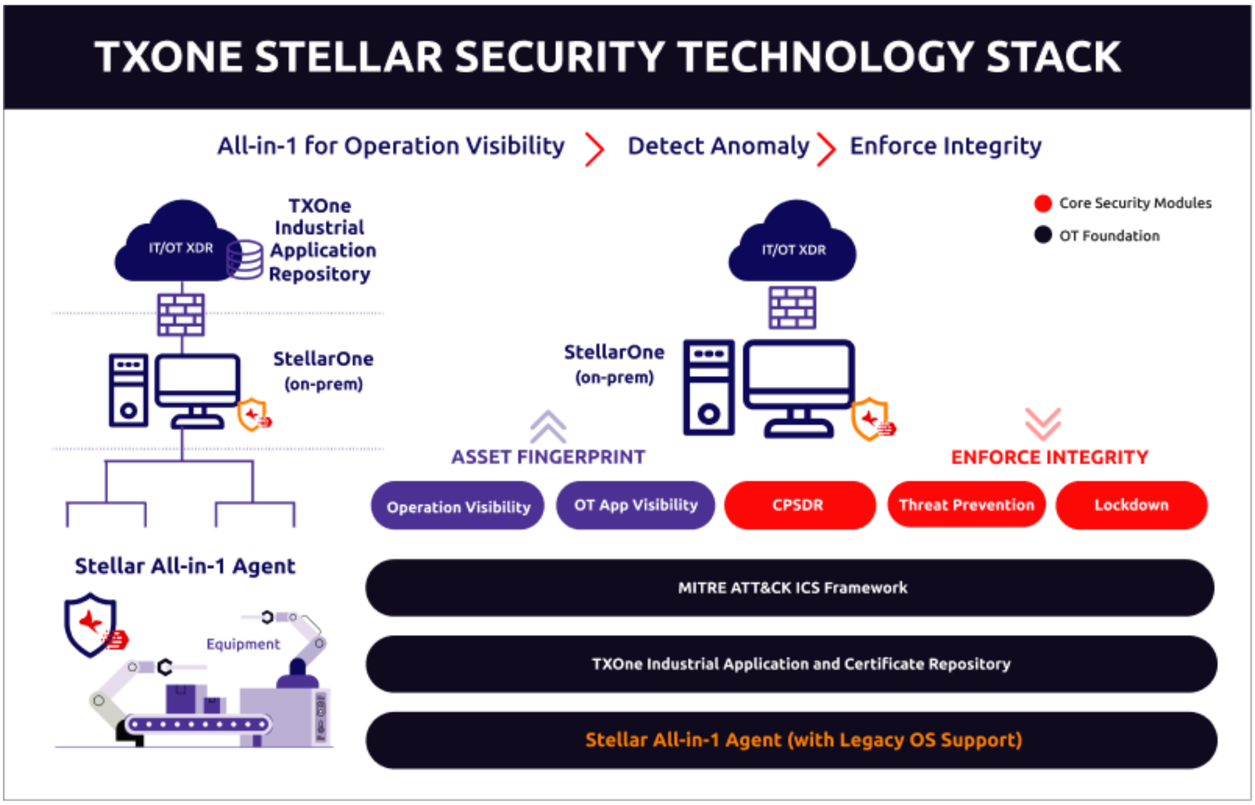
A lightweight unified agent simplifies security by combining CPS Detection and Response, threat prevention, and operations lockdown.

OT/CPS CONTEXT FOCUS

The industrial application repository builds the operational baseline, detects behavioral anomalies, and enforces operational integrity.

LONG-TERM OS SUPPORT AND PROTECTION

Broad OS version support, beyond OEM end-of-life, provides deploy-to-decommission compatibility and coverage.



LICENSE EDITIONS

Bundled features	Kiosk	ICS
Targeted users	**Lite** edition for Banking, Retail	**Complete** edition for Critical Infra, Manufacturing, Pharma
Industrial application repository		✓
OT application safeguard		✓
CPSDR (Operations behavior anomaly detection)	Limited*	✓
Operations lockdown	Limited**	✓
Multi-method threat prevention	✓	✓
Trusted USB device control	✓	✓
Support legacy systems	✓	✓

*For Kiosk license edition, StellarProtect or StellarProtect (Legacy Mode) CPSDR is limited to script-based or fileless attack prevention.

**For Kiosk license edition, operations lockdown is only available on StellarProtect (Legacy Mode) agent.

SUPPORTED OPERATING SYSTEM

TXOne StellarProtect Agent	
Windows Client	2000 SP4 (32-bit), XP SP1 or later (32-bit), Vista (32-bit), 7, 8.x, 10, 11
Windows Server	2000 SP4 (32-bit), 2003 SP1/SP2/R2 No-SP/SP2 (32-bit), 2008 SP1/SP2/R2 No-SP/SP1, 2012 No-SP/R2 No-SP, 2016, 2019, 2022

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2023

SC 2022 awards EUROPE WINNER

Best Endpoint Security

txOne networks

www.TXOne.com

@2023 by TXOne Networks, Inc. All rights reserved. TXOne Stellar series are trademarks or registered trademarks of TXOne Networks, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.