# First-of-a-Kind All-Terrain Endpoint Protection for ICS Devices

Securing ICS endpoints introduces difficulties for both operational engineers and security administrators. Though traditional antivirus has long been seen as a core part of cyber defense strategy, the test of time has shown it brings shortcomings to work sites. All antivirus software requires constant virus signature updates over the Internet to be able to scan for threats. These scans, in turn, place heavy demand on both CPU loading and memory consumption as intensive I/O hooking is conducted. This puts availability at risk even in work sites running modernized operational devices. Safeguarding ICS endpoints requires different priorities: chosen solutions must ensure daily working processes are never jeopardized, computation is never slowed, and production decisions are never delayed. TXOne StellarProtect is the first solution of its kind: all-terrain endpoint protection, a defensive solution custom-engineered for operational technology. Its advanced threat scanning brings known attacks to heel while its next-gen machine learning engine blocks unknown threats, requiring no internet access. StellarProtect's ICS filtering, based on an inventory of applications and certificates, eliminates unnecessary overhead to allow the most lightweight operation possible. Effective in a range of environmental conditions with high accuracy and very low impact on endpoint performance, StellarProtect provides full coverage in one deployment.
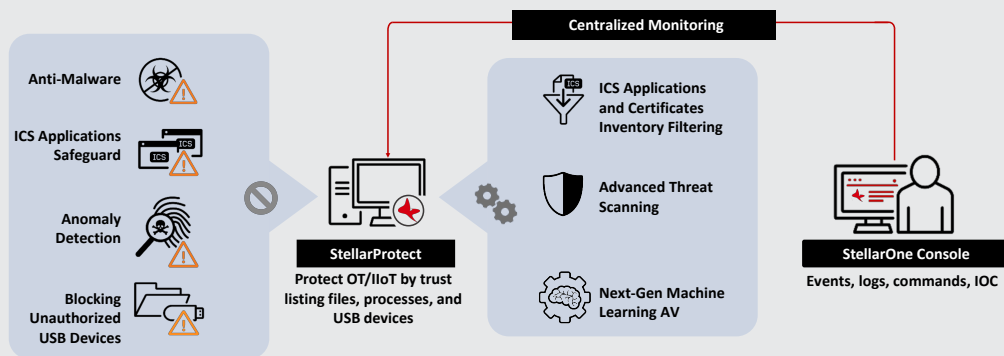
Benefits

Industrial-Grade Next-Generation Antivirus

- **ICS Focus**: Supports thousands of OT applications and OT vendors to increase compatibility, reduce false alarms, and protect critical OT tasks from harm
- **High Performance**: ICS application and certificate inventory filters out 90%+ files from the malware detection process
- **High Efficacy**: Advanced Threat Scanning blocks millions of types of known malware while machine learning automatically blocks unknown threats
- **Low Maintenance Cost**: Advanced Threat Scan patterns and machine learning modeling require updates only twice per year
- **IOC Integration**: Integrate with 3rd party threat intelligence to identify potential intrusions and malicious activity

Operations Behavior Anomaly Detection

- Detect abnormal operations with least privilege-based control to prevent malware-free attacks
- Learn and authorize operational behavior easily to minimize operational cost

ICS Application Safeguard

- Intelligently locate and secure the integrity of ICS processes from ICS targeted attacks

USB Vector Control

- Prevent insider threats

Secure Mission-Critical Devices

- Supervisory Control and Data Acquisition (SCADA)
- Human Machine Interfaces (HMIs)
- Engineering Workstations (EWSes)
- PC-based controllers
- Database servers
- Fixed-function devices
- Industrial IoT devices

Key Features

Agent

- Real-time malware protection
- Ransomware and fileless attack prevention
- Advanced threat protection
- Exploit prevention
- Behavior anomaly detection
- IOC integration
- USB device trust listing
- ICS application inventory informed by OT vendors
- Write-protection
- Support for both scheduled and on-demand AV scans
- Log aggregation

Management Console (StellarOne™)

- Centralized monitoring
- Notifications designed to minimize alert fatigue
- Account management
- Syslog forwarding
- Trusted certificate management
- Support for IOC integration
- Integrate MITRE ICS IDs in event logs
- Scan exclusion management

TXOne StellarProtect™ System Requirements

TXOne StellarProtect™ Agent

	Client OS	Server OS
OS	Windows 7 (No SP/SP1) [Professional / Enterprise / Ultimate] (32/64bit) Windows 8 (No SP) [Pro / Enterprise] (32/64bit) Windows 8.1 (No SP) [Pro / Enterprise / with Bing] (32/64bit) Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit) Windows Embedded Standard 7 (No SP/SP1) (32/64bit) Windows Embedded 8 Standard (No SP) (32/64bit) Windows Embedded 8.1 (No SP) [Pro / Industry Pro] (32/64bit) Windows 7 for Embedded Systems (No SP/SP1) (32/64bit) Windows Embedded POSReady 7 (32/64bit)	Windows Server 2008 (SP1/SP2) [Standard / Enterprise / Storage] (32/64bit) Windows Server 2008 R2 (No SP/SP1) [Standard / Enterprise / Storage] (64bit) Windows Server 2012 (No SP) [Essentials/Standard] (64bit) Windows Server 2012 R2 (No SP) [Essentials/Standard] (64bit) Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit) Windows Server 2008 R2 for Embedded Systems (No SP/SP1) (64bit) Windows Server 2012 for Embedded Systems (No SP) (64bit) Windows Server 2012 R2 for Embedded Systems (No SP) (64bit) Windows Server 2016 (No SP) [Standard] (No SP) (64bit) Windows Storage Server 2016 (64bit) Windows Server 2019 Standard (64bit)
CPU	Conforms to minimum OS system requirements	
Memory	Conforms to minimum OS system requirements	
Free Disk Space	300 MB or more	
Display Resolution	VGA (640x480) or more, 16 colors or more	

TXOne StellarOne™ Virtual Appliance

Target Max Managed Agent	20,000	15,000	10,000	5,000	1,000	500
vCore						
Memory						
Disk Storage (Recommend)						
Supported Hypervisors	VMWare ESX 6.X or above					
Browser	Microsoft Internet Explorer 11.0 Google Chrome 87 or latest Microsoft Edge 79 or latest Mozilla Firefox 78 or latest					