

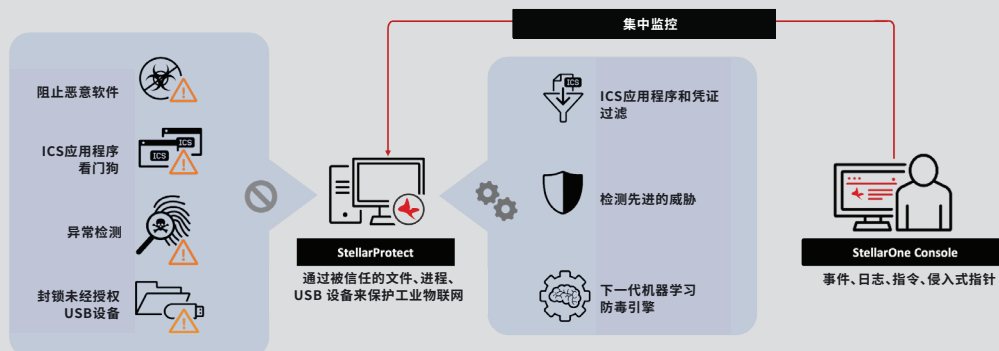
TXOne StellarProtect™

目录

行业领先的全方位 ICS 设备端点防护

工业控制系统 (ICS) 端点设备的防护, 对运营工程师及信息安全系统管理员来说都是一项艰难的工作。虽然工业环境的信息安全防御策略一直以来都是以传统防病毒软件为核心, 但随着时间的发展, 传统防病毒软件的缺点也逐一浮现。所有防病毒软件都需要不时通过因特网来更新病毒特征, 才能扫描威胁, 而扫描又会造成 CPU 严重负担, 同时会消耗内存, 因为必须密集拦截系统 I/O。这会影响设备的可用性, 进而冲击现代化工业环境的运营。ICS 端点设备的防护重点截然不同: 解决方案必须能确保日常运营流程的顺畅, 不能拖慢指令周期, 也不能造成生产决策的延宕。

TXOne StellarProtect 是行业领先的全方位端点防护, 也是专为运营技术 (OT) 环境设计的信息安全解决方案。其先进的威胁扫描技术可拦截已知攻击, 其下一代机器学习引擎则可拦截未知的威胁, 完全无须连上因特网。StellarProtect 的 ICS 过滤技术是以应用程序和凭证数据库为基础, 减轻不必要的系统负荷, 提供最轻量化的运作。StellarProtect 在各种环境都能提供极高的检测准确度, 对端点的性能的影响微乎其微, 单一解决方案就能提供完整的防护。



产品功能特点

工业级下一代防毒

- 专为 ICS 设计: 拥有更好的兼容性, 支持数千种 OT 应用程序与 OT 厂商, 减少误判, 防止关键 OT 作业受到冲击。
- 高性能: ICS 应用程序与凭证数据库可在恶意软件检测过程当中减少 90% 以上的文件。
- 高成效: 先进威胁扫描技术可拦截数百万种已知恶意软件, 而机器学习技术则可自动拦截未知威胁。
- 低维护成本: 先进威胁扫描的病毒特征与机器学习模型每年只须更新两次。
- IOC 集成: 集成第三方威胁情报来检测潜在的黑客入侵与恶意活动。

操作行为异常检测

- 采用最小权限原则管理机制来检测异常操作, 防范非采用恶意软件的攻击。
- 轻松学习操作行为并给予授权, 进而降低运营成本。

ICS 应用程序保护

- 精准发掘并保护 ICS 流程, 防范针对 ICS 的攻击。

USB 设备管理

- 防止内部威胁。

保护关键工业设备

- 监控与数据捕获系统 (SCADA)
- 人机界面 (HMI)
- 工程工作站 (EWS)
- 以 PC 为基础的控制装置
- 数据库服务器
- 固定功能设备
- 工业物联网 (IIoT) 设备



核心优势

代理程序	管理控制台 (StellarOne™)
● 实时恶意软件防护 ● 勒索病毒与无文件攻击防护 ● 先进威胁防护 ● 漏洞攻击防护 ● 异常行为检测 ● IOC 集成 ● USB 设备信任名单 ● ICS 应用程序数据库 (由 OT 厂商提供) ● 写入保护 ● 支持计划或按需防毒扫描 ● 日志汇总	● 中央监控 ● 通知功能设计可减少频繁警示 ● 账户管理 ● Syslog 系统日志转移存储 ● 信任凭证管理 ● 支持 IOC 集成 ● 将 MITRE ICS ID 集成到事件日志 ● 扫描例外清单管理

TXOne StellarProtect™ 系统要求

操作系统	服务器操作系统					
	Windows 7 (无 SP/SP1) [Professional / Enterprise / Ultimate] (32/64 位)			Windows Server 2008 (SP1/SP2) [Standard / Enterprise / Storage] (32/64 位)		
	Windows 8 (无 SP) [Pro / Enterprise] (32/64 位)			Windows Server 2008 R2 (无 SP/SP1) [Standard / Enterprise / Storage] (64 位)		
	Windows 8.1 (无 SP) [Pro / Enterprise / 含Bing] (32/64 位)			Windows Server 2012 (无 SP) [Essentials/Standard] (64 位)		
	Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64 位)			Windows Server 2012 R2 (无 SP) [Essentials/Standard] (64 位)		
	Windows Embedded Standard 7 (无 SP/SP1) (32/64 位)			Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64 位)		
	Windows Embedded 8 Standard (无 SP) (32/64 位)			Windows Server 2008 R2 for Embedded Systems (无SP/SP1) (64 位)		
	Windows Embedded 8.1 (无 SP) [Pro / Industry Pro] (32/64 位)			Windows Server 2012 for Embedded Systems (无 SP) (64 位)		
	Windows 7 for Embedded Systems (无SP/SP1) (32/64 位)			Windows Server 2012 R2 for Embedded Systems (无 SP) (64 位)		
	Windows Embedded POSReady 7 (32/64 位)			Windows Server 2016 (No SP) [Standard] (无 SP) (64 位)		
				Windows Storage Server 2016 (64 位)		
			Windows Server 2019 Standard (64 位)			
CPU	与操作系统的最低要求相同					
内存	与操作系统的最低要求相同					
可用硬盘空间	300 MB 或更多					
屏幕分辨率	VGA (640x480) 或更高，16 色或更多					
TXOne StellarOne™ 虚拟设备						
最多可管理的代理程序数量	20,000	15,000	10,000	5,000	1,000	500
支持的 Hypervisor 虚拟机 监控器	VMWare ESX 6.X 或更新					
浏览器	Microsoft Internet Explorer 11.0 Google Chrome 87 或最新版本 Microsoft Edge 79 或最新版本 Mozilla Firefox 78 或最新版本					

