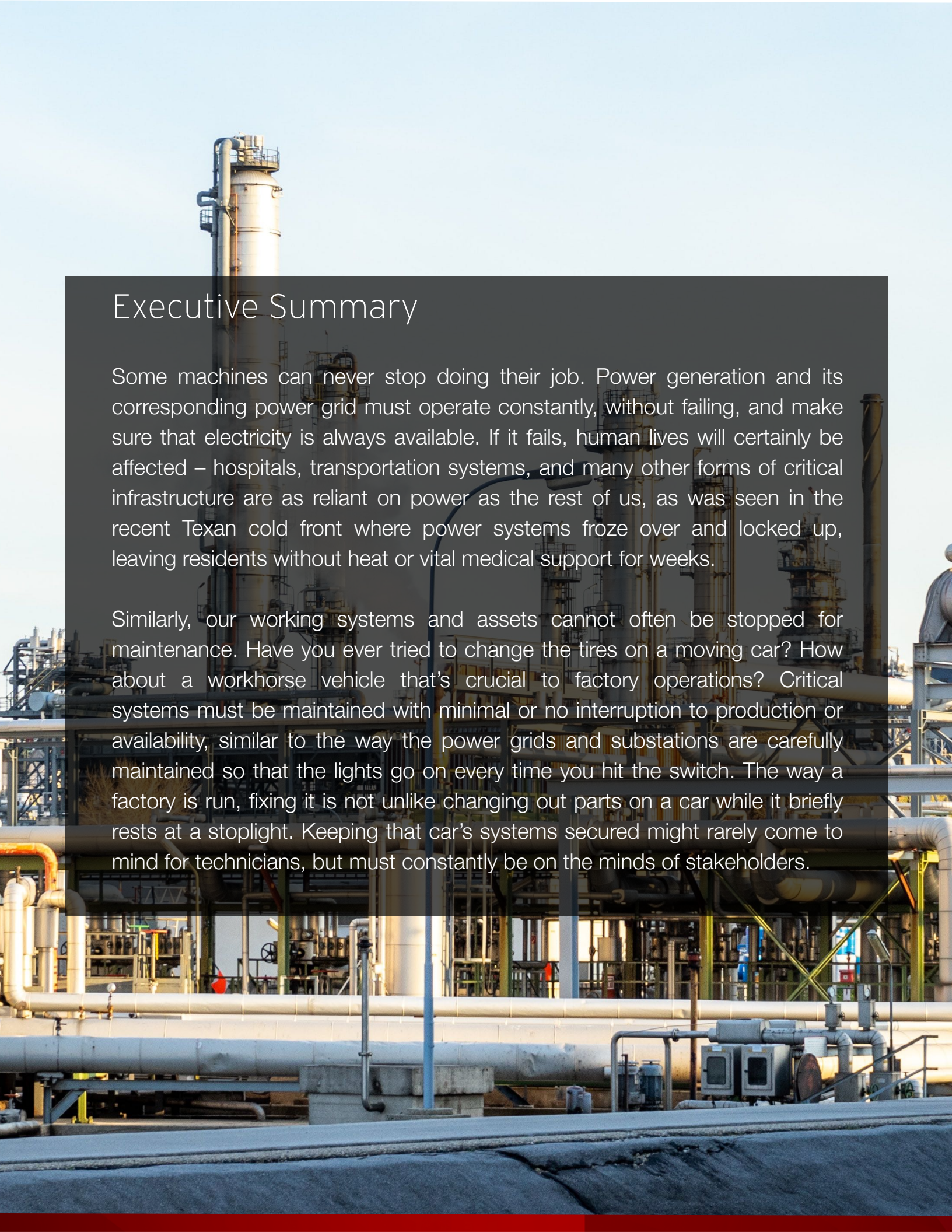
txOne networks

Safeguarding Endpoints with Maximized Operational Integrity

TXOne Networks Inc.

Chiyi Lin, Winfred Lin, Max Farrell

Table of Contents



Executive Summary

Some machines can never stop doing their job. Power generation and its corresponding power grid must operate constantly, without failing, and make sure that electricity is always available. If it fails, human lives will certainly be affected – hospitals, transportation systems, and many other forms of critical infrastructure are as reliant on power as the rest of us, as was seen in the recent Texan cold front where power systems froze over and locked up, leaving residents without heat or vital medical support for weeks.

Similarly, our working systems and assets cannot often be stopped for maintenance. Have you ever tried to change the tires on a moving car? How about a workhorse vehicle that's crucial to factory operations? Critical systems must be maintained with minimal or no interruption to production or availability, similar to the way the power grids and substations are carefully maintained so that the lights go on every time you hit the switch. The way a factory is run, fixing it is not unlike changing out parts on a car while it briefly rests at a stoplight. Keeping that car's systems secured might rarely come to mind for technicians, but must constantly be on the minds of stakeholders.

The Eye of Cyber Crime on Operational Environments

Advanced and coordinated large-scale attacks have never been more common than they are now, and the eyes of cyber crime are focused on government, banking, and manufacturing. For all of 2020, as revealed by the Trend Micro Smart Protection infrastructure, these were the top 3 most targeted industries. Trend Micro threat experts identified 127 new "families" of malware in 2020, a 34% increase over 2019[1]. These new threats are developed with the intention of forcing more pressure onto stakeholders to extract larger payments more quickly. Ransom demands continue to increase in amount, as shown by the 47% increase from Q1 to Q2 of 2020 alone[2].

DoppelPaymer, a kind of ransomware which typically arrives in systems via e-mails containing spear-phishing links or attachments, hit a Foxconn NA work site in November of 2020[3]. The attackers claimed that 1,200 servers had been encrypted, 100 GB of unencrypted files had been stolen, and 20-30 TB of backups had been deleted, while demanding a ransom of over $34 million to be paid in Bitcoin. While Foxconn did not make public how long it took them to return to routine operations, such recovery operations typically take weeks. It's likely that in this case Foxconn worked within the FBI's recommendation to not make payments to attackers, as they released a statement that they were working closely with both "technical experts and law enforcement agencies".

---

[1] Trend Micro, "A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report", Feb. 23 2021

[2] https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf

[3] Lawrence Abrams, "Foxconn electronics giant hit by ransomware, $34 million ransom", Bleeping Computer, Dec. 7 2020

In 2021, manufacturers have been under more pressure from cyber attacks than ever before. Just this April, the same group of hackers that targeted Acer in March of 2020 compromised servers belonging to Apple's manufacturer Quanta, demanding a payment of $50 million USD and threatening to leak confidential design documents if their demands went unmet[4]. We can only expect this trend to continue to worsen as organized groups of threat actors continue to improve their methods. Only cybersecurity solutions designed specifically with the needs of ICS and work sites in mind can safeguard systems from cyber threats while also safeguarding operational resources and productivity.

[4] J. Fingas, "Apple supplier is the latest target of a $50 million ransomware hack", Engadget, Apr. 2021

Securing and Maintaining Mission-Critical Assets in Perpetual Motion

The modern ransomware attack is similar to a thief who steals your truck's keys while it's loaded with valuable equipment and then tries to sell it all back to you at a premium. However, this thief often enters invisibly without ever leaving their computer chair, able to enter your work site through an unassuming e-mail or an infected thumb drive hanging off your trusted technician's keyring. In addition to malware-based attacks, modern cyber criminals go to great lengths to steal credentials, strongly preferring to take advantage of authentication systems and privileges that are already in place instead of breaking into a system. In other words, keep a close eye on your credentials or employ technologies that simplify the process and do it for you.

Deploying traditional antivirus is similar to hiring a few armed security guards to sit in your vehicle with you every time you operate it. The vehicle is secure, but its purpose now includes many extra security operations around and inside a mission critical resource where time and space are both at a premium. While cyber criminals represent a tremendous threat to operations, due to the resource-heavy nature of traditional cyber defenses the cure can be almost as disruptive as the disease.

This is a likely explanation as to why less than 50% of ICS endpoints are running traditional antivirus[5]. Work site operators know the pains of this problem – ditching traditional antivirus is immediately rewarding, offering the excitement and pleasure of lightweight operations without the frills of frequent slow, plodding pattern updates. However, this

[5] Trend Micro, "The State of Industrial Cybersecurity", Mar. 2021

efficiency comes at a high cost when vulnerabilities are left exposed to those who would wish to turn a profit from them. It does not need to be a choice between slow and plodding security or productive and lightweight cyber risk – security intelligence experts have already been building a superior set of software and hardware solutions exclusively developed for the availability and productivity of mission-critical ICS assets.

The Computer as the Mission-Critical Workhorse

A computer is a lot like a car. Office-side, factory-side, and in home life, computers are versatile assets that can take on many different purposes. In different industries, and different departments within those industries, computers will have very different roles even in how they apply the same technologies.

Two kinds of spaces exist within corporations: the office and the production line. Both are focused on productivity. However, both environments have the same end goal of maximized productivity.

Office computers are multi-purpose, usually run the latest OS, require internet connectivity for work due to a high reliance on cloud computing, and have high tolerance to interruption or latency. The biggest difference between an office computer and a production line computer is updates – office computers are quite convenient to regularly update and patch. Personnel might even complete updates over the lunch hour.

The bottom line for production line computers is the urgency of productivity and availability. These assets have low tolerance for interruption or latency, both of which come with a steep price tag. Commonly, production line environments will have computers running legacy and modern OSes operating side-by-side, usually with no internet connection, and stringent scheduling is necessary to make maintenance time for updates and patches.

While the office computer has time to conduct maintenance when the user takes lunch or goes home for the night, the mission-critical workhorse computer has no such luxury. For

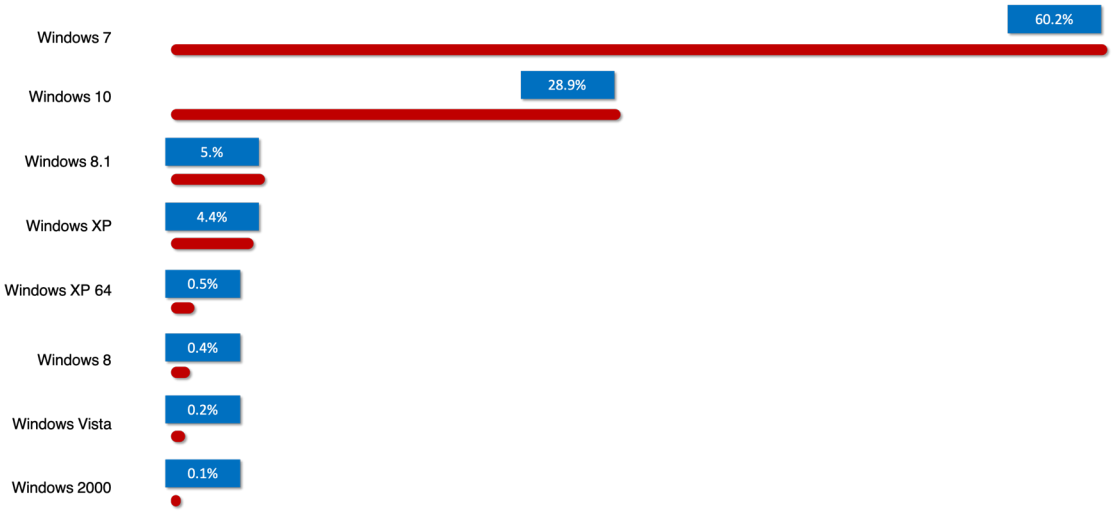
these computers, the lights must always stay on. Furthermore, some of these assets are under special regulations or accommodating applications that severely restrict the abilities of team members to modify them in any way – including patching or updating out high-risk vulnerabilities. They need an adaptive and precise approach that can provide security while still protecting vital operations and allowing for maximized productivity.

Patchable and Un-Patchable Endpoints

Within the ICS environment, computers are commonly categorized as either “patchable” or “un-patchable” endpoints. The patchable endpoint is like a modern electric car, which can receive updates on the fly that adjust specifications, fix bugs, or add features as often as every 16 days. For these vehicles, a full stop for hands-on maintenance only comes once every 3 years or so. An un-patchable endpoint is more similar to a much-beloved old muscle car, for which any kind of maintenance or alteration to the vehicle’s functionality requires hands-on intensive labor and manual adjustment by a mechanic who is very aware of the car’s unique needs. These two kinds of assets both require security measures that minimize risk while maintaining high productivity, but their needs and capabilities are very different – similar to caring for cars of different types and ages within the same garage, where some might have extremely delicate needs. The security officer responsible for safeguarding OT technology more often than not must accommodate the difficulty of protecting both kinds of assets side-by-side within the same production line, maintaining their integration and stability while keeping them optimized for productivity.

Patchable endpoints are generally much more flexible, and integrating new technology or updates into their processes is easier, as they are usually running an up-to-date operating system and modernized applications. These OT and ICS assets are likely to be handling a large amount of tasks in parallel or continuous sequence on any given working day. In contrast, an un-patchable endpoint often (but not always) will be running legacy operating systems, and is much less flexible – it may be against regulations to modify it in any way, and applications on it may be past their EOS (End of Service) date, leaving it with serious vulnerabilities that can’t be patched out. Un-patchable endpoints are likely to be “fixed-use” assets handling only a few tasks. Robotic manipulators in the factory, ATMs at the bank, and MRI scanners at the hospital are all likely to be based on fixed-use systems.

Even if the patches exist and it's not against regulations to modify the machine, stakeholders rarely want to risk even the smallest changes to settings, as such modifications to delicately fine-tuned and integrated equipment can easily lead to operational catastrophe.



Pic-1. Top operating systems in the manufacturing industry[6]

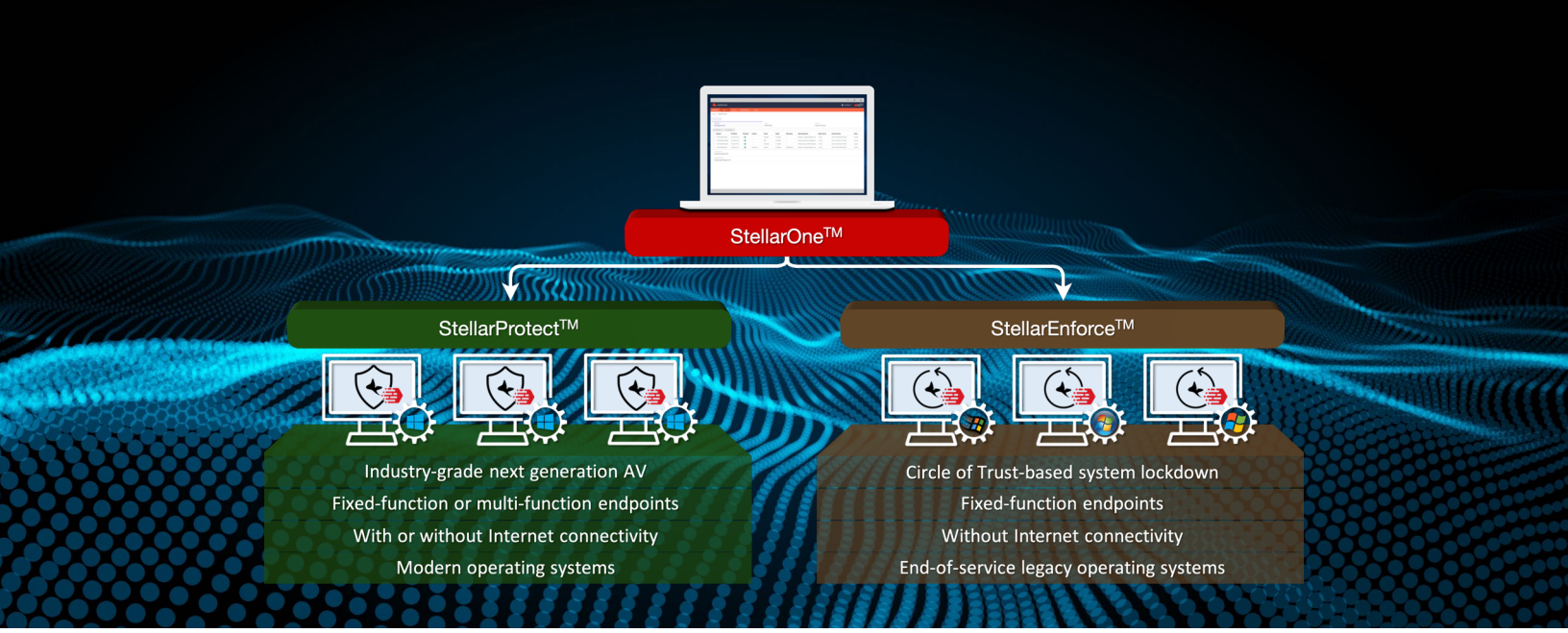
To take the perspective of a malicious actor, ransomware spreads through the ecosystem over networks with the end goal of compromising data, and endpoints are crucial to accomplishing this because of their integral relationship to that data. Data has three forms: data 'in transit' which is carried on networks, and data 'at rest' or 'in use' which is found on endpoints. Because of this, endpoints play a more important role to attackers, and compromising this data at rest or data in use allows attackers to demand a ransom by locking systems, endangering human lives, or damaging operations.

Attackers demonstrate a consistent pattern of seeking ways to up the ante on decision makers to acquire larger ransoms that are paid out faster. Chosen targets are often running an environment mixing patchable and un-patchable endpoints, which creates easy targets for cyber crime due to the challenge of managing these two different technologies. Such environments include almost any manufacturing center as well as critical infrastructure work sites like hospitals and water facilities. Patchable and un-patchable endpoints each require a different kind of protection tailored to their nature.

[6] https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

Patchable systems and a small percentage of un-patchable systems sometimes make use of traditional antivirus solutions. Unfortunately, traditional antivirus takes up a lot of processing power and can severely interfere with resource availability as well as being one more thing to patch and manage connectivity for – for example, exception lists require attentive manual effort to deploy properly. A unique pitfall to un-patchable endpoints is the temptation of using the air gap as the sole barrier to cyber attack.

Sadly, in the modern day, more and more devices are being built to automatically reach out for connectivity, and even if that function is successfully curbed, air gapped devices remain vulnerable to any device that a team member or on-site visitor might plug in. Any of these issues multiplies exponentially as the number of devices within the ICS network increases, and fully modernized manufacturing centers might have as many as 2,000 assets on one network. Solutions purpose-built to safeguard these two types of assets as they run side-by-side must also provide for remote administration and maintenance from a centralized location.



All-Terrain Solutions

Securing Patchable Endpoints: StellarProtect

Securing patchable endpoints begins with an inventory of ICS applications and licenses, which almost totally replaces the need to manually set up an exception list. With this inventory established, a pre-scan is conducted during installation and these important operations are freed from the constraints of routine threat scans, empowering the asset to focus on its work priorities. The ICS inventory can also protect files so that they can only be changed within a window scheduled by the administrator. With that aspect of the system's operations squared away, StellarProtect then secures the many paths malware can take into the system, scans the the system's non-inventory approved files for known threats that might be lying in wait, and identifies any unusual behavior or processes so that unknown cyber attacks can be identified and stopped in their tracks at the first sign of an anomaly.

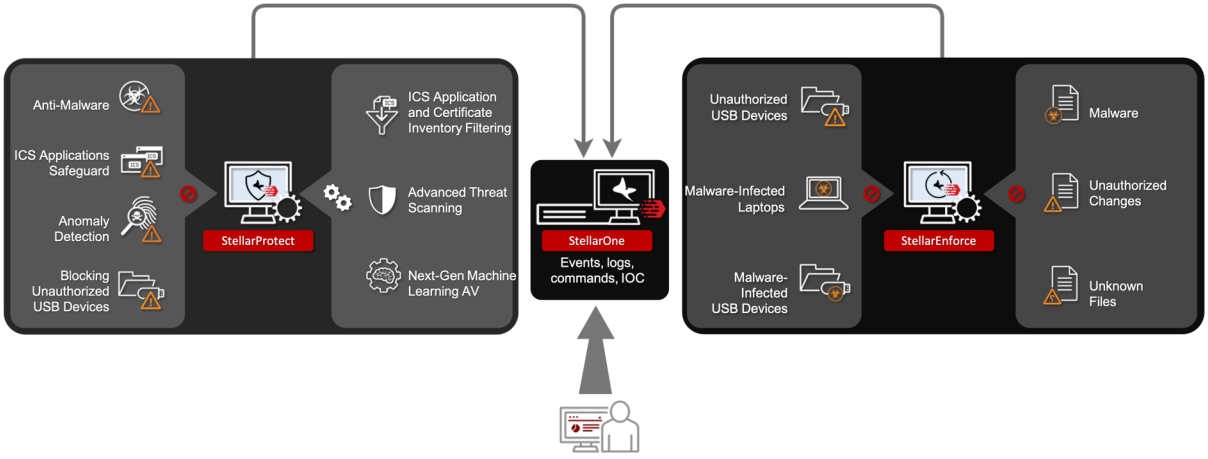
These scans catch known malware, but unknown malware requires special technology, StellarProtect's next-generation machine learning. This machine learning assesses the system's routine operations, enabling it to detect abnormal behavior and stop unknown attacks. Finally, insider threats must be controlled – malware attacks causing millions of dollars in damages often begin with an infected thumb drive entering the work site. It's speculated that the DoppelPaymer attack on Foxconn NA was one such attack. With StellarProtect's USB vector control, no device can connect to assets without case-by-case administrator approval. StellarProtect represents traditionally separate technologies that

are honed and interwoven to safeguard patchable systems while only requiring pattern updates every six months.

Securing Un-Patchable Endpoints: StellarEnforce

The ideal method for simplifying management and defense for fixed-use systems is a deceptively simple lockdown-based solution which secures the system with a trust list. The trust list can disallow un-approved applications, prevent changes from being made to configurations or secured data, and stop USB devices from connecting to the asset without administrator approval. This form of security is extremely lightweight, taking no more than 11% of system resources, and prevents cyber incidents without reliance on pattern files or other traditional antivirus-based measures. Even if somehow present on the asset, malware is unable to execute or function on the device, leaving un-patchable systems secured and operational at maximum integrity.

Coordinating Large-Scale Endpoint Security: StellarOne



Pic-2. Stellar Architecture

With StellarOne, managing even a vast number of StellarEnforce and StellarProtect deployments is a breeze. As the number of devices on the ICS network increases, credential and device organization and maintenance become so demanding as to be nearly impossible to finish within time constraints without assistive technologies. StellarOne provides account-based management for secured devices and the StellarOne dashboard

is made-to-measure for detailed awareness of security posture, giving a comprehensive, consolidated overview of assets, alerts, and events. Time spent on upkeep for secured assets is significantly reduced along with the potential for alert fatigue, and all upkeep tasks including viewing logs can be performed remotely via StellarOne. With StellarOne, one or both types of endpoint protection can be optimized and maintained from a single management console.

Created by the TXOne Networks Technical Marketing Team

TXOne Networks Inc.

TXOne Networks is a joint-venture company of Trend Micro and Moxa. TXOne Networks is mainly offering cybersecurity solutions to p[illegible]al control systems. Trend Micro has more than 30+ years of cybersecurity threat intelligent and MOXA has more than 30+ years of OT netw[illegible]e, which makes TXOne Networks have both IT and OT technology to provide the comprehensive adaptive ICS cybersecurity solution. TXOne Networks leverage those advantages to develop the ICS cybersecurity products including endpoint security and network security, both Trend Micro and Moxa are not just providing the technology and knowledge, they are also taking care the go-to market channel for both sales and support service in IT and OT

txOne networks | Keep Operations Running

www.txone-networks.com