Cybersecurity INSIDERS RECOMMENDED

PRODUCT REVIEW: TXONE NETWORKS FOR PROACTIVE OT DEFENSE

txOne networks

Securing Operational Technology (OT) in today's industrial environments has never been more challenging, with blind spots like unmanaged legacy assets, transient devices, and unauthorized USBs presenting significant vulnerabilities. To make things worse, OT systems often rely on older, specialized equipment that lacks built-in cybersecurity defenses and cannot afford downtime for updates and security audits.

However, these vulnerabilities extend far beyond individual devices and assets. The complexity of securing OT systems lies in the multiple, interconnected workflows that organizations must manage. From ensuring supply chain security to safeguarding air-gapped systems and performing regular machine inspections, every step introduces distinct challenges. Each process requires tailored security measures, making it difficult to maintain a unified and seamless defense strategy.

To overcome these challenges, organizations need a comprehensive cybersecurity strategy that integrates People, Process, and Technology into their operations. This strategy must not only establish secure supply chain practices but also ensure continuous protection for daily operations and isolated systems without disrupting business activities. By streamlining processes and adopting the right technology, organizations can prevent interruptions, minimize risks, and create a resilient OT environment capable of withstanding evolving cyber threats.

INTRODUCING TXONE'S ELEMENT PORTFOLIO: A Comprehensive Suite for OT Security

This is where TXOne Networks steps in, offering the Element portfolio, a suite of products designed specifically for OT security to support existing processes without introducing additional complexity or burden on already stretched-thin teams. The Element portfolio comprises several key solutions:

ElementOne: A centralized management platform at the heart of the Element portfolio that provides a holistic view of OT assets, risk assessments, and audit logs to mitigate risks while simplifying operations. It streamlines security management by integrating Portable Inspector and Safe Port, enabling centralized policy enforcement, configuration deployment, and scan log management, all from one interface.

Portable Inspector: An agentless, malware scanning USB-based tool designed for OT assets, including air-gapped and standalone systems. It inspects devices without the need for software installation or system reboots, making it ideal for environments requiring continuous uptime. Its Secure Storage feature ensures safe file transfer, allowing only clean data into the OT environment.

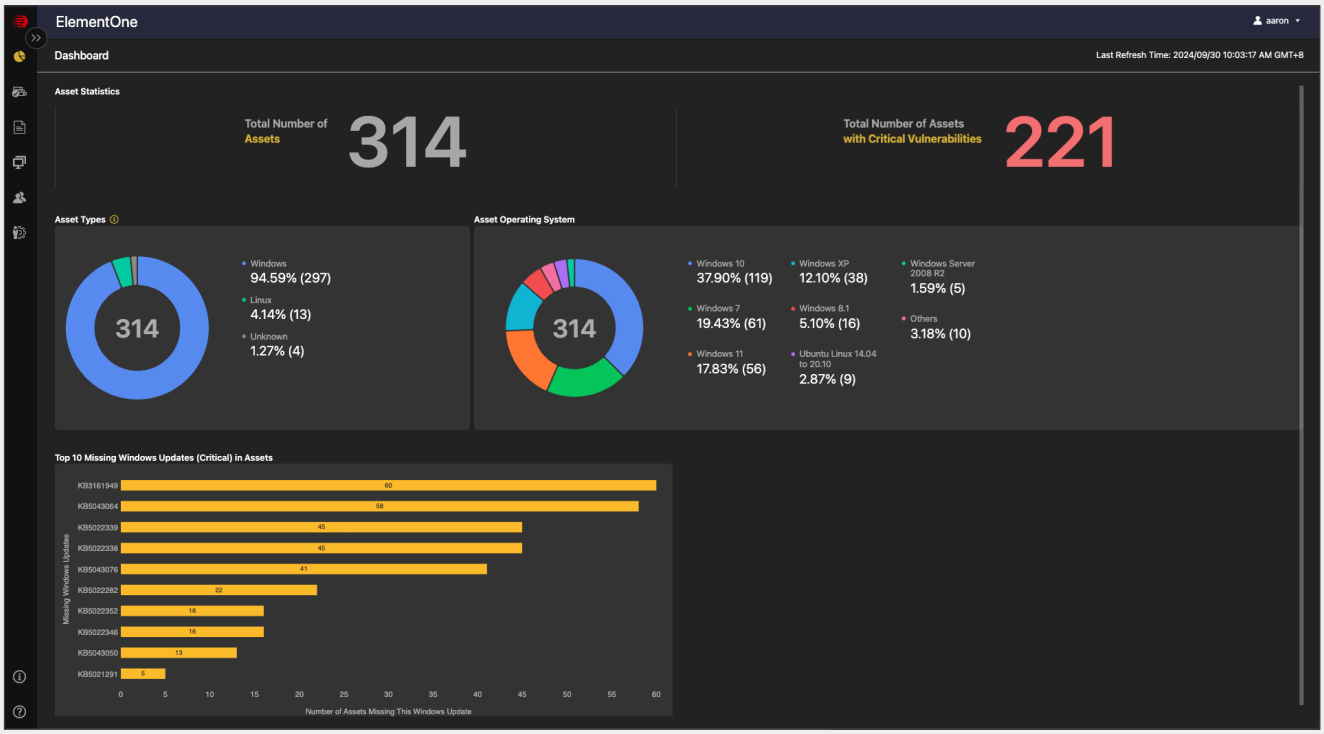
Safe Port: A media sanitization station that rapidly scans and cleans external media (like USB drives) before they are introduced into sensitive OT environments, preventing malware from entering critical infrastructure. It integrates with Portable Inspector to centralize audit log management, streamlining security processes and ensuring comprehensive protection across devices.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

ELEMENTONE: The Command Center for Comprehensive OT Security

A major challenge in OT environments is the lack of visibility into system vulnerabilities, assets, and security posture. Security teams often struggle to maintain a real-time understanding of which systems are running outdated software, which devices are compromised, and which patches are missing. This lack of insight forces organizations to adopt a reactive security approach, responding to threats only after they've caused damage.

ElementOne transforms this scenario by providing a comprehensive and unified platform that aggregates data from across the OT landscape. By integrating Portable Inspector and Safe Port, ElementOne enables centralized control over malware scanning, asset management, and log collection. This integration ensures efficient synchronization of scan logs and security data, creating a streamlined security workflow across all OT assets.



ElementOne Dashboard

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

KEY CAPABILITIES: ELEMENTONE

To better understand how ElementOne transforms OT security, let's look at its key capabilities:

- **Centralized Asset-Centric and Risk Management:** ElementOne provides a comprehensive overview of OT assets, displaying system specifications, OS versions, installed applications, and vulnerabilities, such as missing patches. This centralization ensures organizations have clear visibility into their OT environment and can assess risks more effectively.
- **Holistic View for Risk Assessment:** In addition to asset management, ElementOne offers a risk assessment dashboard that prioritizes vulnerabilities and highlights areas requiring attention, enabling security teams to proactively address critical risks.
- **Centralized Log Management:** ElementOne collects and consolidates logs from connected devices like Portable Inspector and Safe Port, simplifying audit trails and tracking malware scans and security events across the OT environment.
- **Detailed Asset Reporting:** The platform generates detailed, exportable reports on system configurations, installed applications, vulnerability scans, and active services. These reports are essential for meeting compliance requirements and ensuring operational transparency.
- **Audit and Compliance:** ElementOne streamlines compliance by providing automated malware-free reports and tracking all security-related activities, allowing organizations to meet regulatory requirements with minimal effort.
- **Pattern Distribution:** Portable Inspector and Safe Port obtain the latest malware patterns from ElementOne, ensuring all security products are up to date without manual intervention, significantly reducing the risk of outdated protection.
- **Role-Based Access Control with SAML SSO:** Security teams can assign access rights based on user roles, minimizing the risk of unauthorized access to critical systems and ensuring only the right personnel can interact with sensitive data. With support for SAML Single Sign-On (SSO), ElementOne integrates seamlessly with existing Identity Providers (IdPs), allowing users to authenticate using their corporate credentials and simplifying account management.
- **SIEM Integration:** ElementOne integrates with Security Information and Event Management (SIEM) platforms like Splunk, enabling enhanced threat detection, incident response, and centralized security management.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

These capabilities directly translate into several benefits for organizations:

KEY BENEFITS

1 | EFFICIENCY

By consolidating security processes such as asset and log management, vulnerability tracking, and reporting into a single platform, ElementOne eliminates the inefficiencies caused by fragmented tools and reduces the overhead required for manual operations such as vulnerability tracking and compliance reporting. This significantly reduces operational complexity and streamlines security processes across the OT environment.

2 | PROACTIVE RISK MANAGEMENT

ElementOne's risk assessment solutions allow organizations to prioritize remediation efforts based on real-time vulnerability insights. This proactive approach helps prevent breaches before they occur by addressing the most critical risks first.

3 | COMPLIANCE AND AUDIT SIMPLIFICATION

The platform automatically generates comprehensive asset reports and audit logs, ensuring that organizations meet regulatory requirements with minimal manual effort. The ease of generating these reports simplifies both internal and external audits.

4 | IMPROVED VISIBILITY

ElementOne provides a holistic view of OT systems, assets, and vulnerabilities, giving security teams better control over their environment and helping to identify hidden risks across isolated or air-gapped systems.

5 | SCALABILITY

ElementOne's flexible architecture supports both small businesses and large enterprises. As the needs of the organization grow, the platform scales to accommodate more assets, users, and security operations without compromising performance. With SIEM integration, it can seamlessly integrate with customers' existing SIEM systems, allowing organizations to scale their security operations without disrupting their current infrastructure

.

6 | REDUCED OPERATIONAL OVERHEAD

The platform's ability to synchronize malware pattern updates and centralize log management reduces the amount of manual work required from IT and security teams, freeing up resources for other critical tasks.

7 | ENHANCED SECURITY CONTROLS

With role-based access control and support for SAML Single Sign-On (SSO), ElementOne strengthens security by ensuring that only authorized personnel can access sensitive systems and by enhancing overall threat detection capabilities through advanced integrations.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

PORTABLE INSPECTOR: Agentless Malware Scanning for Isolated OT Systems

One of the greatest challenges in OT security lies in protecting OT assets, especially standalone or air-gapped systems—networks or devices isolated from the internet or broader IT infrastructure for safety and operational reasons. Additionally, ensuring supply chain security is crucial when shipping and receiving new machines. Both suppliers and customers must ensure that equipment is malware-free before it is deployed, maintaining its original state and security integrity. Conventional security tools are often inadequate for these systems because they rely on constant updates, internet access, or complex installations that disrupt operations.

Portable Inspector was designed specifically to overcome these limitations. As a portable, USB-based product, it delivers on-demand malware scanning for isolated OT devices, requiring no software installation or system reboots. This ensures that critical operations remain uninterrupted, while systems are thoroughly protected from external threats.

For instance, in a manufacturing plant with legacy equipment that cannot afford downtime, Portable Inspector allows security teams to scan systems on-demand without impacting production, ensuring continued uptime while maintaining robust protection. Additionally, Portable Inspector is ideal for both suppliers and customers in the supply chain. Suppliers can generate malware-free reports before shipping new machines, and customers can verify the machines are secure upon receipt, ensuring they are malware-free before deployment into production environments.



Portable Inspector

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

KEY CAPABILITIES: PORTABLE INSPECTOR

Let's explore the key capabilities that make Portable Inspector so effective:

- **Agentless Malware Scanning:** Portable Inspector provides on-demand malware scans without requiring software installation or a system reboot. This ensures that OT environments with critical uptime requirements are protected with minimal operational disruption, making it ideal for systems that cannot afford downtime.
- **Cross-Platform and Legacy System Support:** Portable Inspector is compatible with a wide range of operating systems, including both modern and legacy platforms such as Windows XP and Linux distributions. This extensive platform support ensures that even outdated or isolated OT assets are protected.
- **Detailed Asset Information Collection:** In addition to scanning for malware, Portable Inspector automatically collects detailed system snapshots, including information on the operating system, installed applications, and vulnerability status. This data is invaluable for improving visibility across OT environments.
- **AES-256 Encrypted Secure File Transfer (Pro Edition):** For environments requiring secure data transfer between air-gapped systems, Portable Inspector's Pro Edition offers AES-256 hardware encryption to ensure that sensitive files are safely transferred while remaining malware-free.
- **Centralized Log Management:** Portable Inspector integrates seamlessly with ElementOne, allowing scan logs and asset information to be uploaded either directly or via Safe Port. This centralization simplifies the auditing process and provides security teams with a unified view of all scanning activities across OT environments.
- **User-Friendly LED Indicators:** Portable Inspector features intuitive LED indicators that display scanning progress and results in real time. This feature allows even non-technical staff to quickly understand the scan status, ensuring easy deployment in industrial settings and reducing the need for dedicated security personnel on the ground.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

With these capabilities, Portable Inspector offers distinct benefits to OT environments:

KEY BENEFITS

1 | OPERATIONAL CONTINUITY

Portable Inspector's agentless design allows it to scan isolated or air-gapped systems without requiring installations or reboots. This ensures minimal disruption to operations, which is critical in OT environments where uptime is essential.

2 | ENHANCED SECURITY

The product provides robust protection for OT assets without the need to modify system configurations or add complex setups. By scanning without leaving a software footprint, Portable Inspector minimizes the attack surface while maintaining security on legacy systems.

3 | IMPROVED ASSET VISIBILITY

Beyond malware scanning, Portable Inspector collects detailed asset information, including OS, application versions, and patch statuses. This capability greatly enhances visibility into the OT environment, helping security teams identify hidden risks and shadow IT.

4 | SECURE DATA TRANSFERS

For organizations using the Pro Edition, Portable Inspector enables AES-256 encrypted file transfers between isolated systems, ensuring that sensitive data remains protected while being moved across air-gapped environments.

5 | SIMPLIFIED AUDITING AND COMPLIANCE

By integrating with ElementOne and Safe Port, Portable Inspector can automatically upload scan logs and asset data, either directly or via Safe Port, simplifying audit processes and providing a comprehensive view of security operations. This centralization reduces manual work, making it easier to meet compliance requirements.

6 | EASY DEPLOYMENT AND USE

The intuitive design of Portable Inspector, including its LED indicators, allows even non-technical personnel to operate the product effectively. This ensures that security processes can be integrated seamlessly into industrial workflows, reducing the need for extensive training.

7 | LEGACY AND CROSS-PLATFORM PROTECTION

With support for both modern and legacy systems, Portable Inspector ensures that even outdated OT systems are protected. This broad compatibility makes it easier for organizations to secure their entire infrastructure without needing multiple tools.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

SAFE PORT: Rapid Media Sanitization for OT Environments

Removable media continues to be one of the most significant attack vectors for malware in OT environments. USB drives and other external devices are essential for transferring data across OT systems, but they also introduce a potential entry point for cyberattacks, especially in environments where security controls are less stringent. This makes protecting against malware from external media a critical concern for industries with sensitive OT infrastructure.



Safe Port

Safe Port addresses this challenge by providing a ruggedized, industrial-grade media sanitization solution. It rapidly scans and cleans removable media, such as USB drives, before they can be introduced into OT systems, ensuring that malware is detected and neutralized at the perimeter. Built specifically for industrial environments, Safe Port is designed to handle the unique demands of OT plants, offering speed, simplicity, and enhanced protection.

Additionally, Safe Port integrates with ElementOne and Portable Inspector to further simplify security workflows. Portable Inspector logs and malware patterns can be automatically uploaded to ElementOne. This integration streamlines both the scanning and update processes, making Safe Port a central hub for both media sanitization and managing Portable Inspector's logs and pattern updates. This allows security teams to manage scan logs centrally and streamline compliance reporting. It combines ease of use with industrial-grade durability, making it a trusted solution for safeguarding OT environments against malware threats introduced via removable media.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

KEY CAPABILITIES: SAFE PORT

Let's explore the key capabilities of Safe Port:

- **Rapid Scanning and Media Sanitization:** Safe Port processes up to 7,200 files per minute, ensuring that removable media such as USB drives are scanned and sanitized quickly, minimizing operational delays in OT environments. It supports three flexible scan modes: "Log Only" for detailed reporting, "Clean" for malware removal, and "Lock" for isolating and encrypting unscannable or malicious files. This speed is critical in industries where continuous uptime is paramount, as it allows for fast media processing while preventing malware from entering sensitive systems.

- **Rugged Design for Industrial Environments:** Safe Port is built to withstand the demanding conditions of industrial OT plants, with a ruggedized design that ensures durability and reliability. Its construction allows it to operate effectively in harsh environments where typical IT equipment may fail, making it suitable for continuous operation in OT settings.

- **Centralized Audit Log Collection:** Safe Port integrates with ElementOne and Portable Inspector, allowing scan logs, sanitization data, and asset information to be automatically uploaded to a centralized management console. This simplifies audit trails, compliance processes, and overall security management by ensuring all activities are tracked and reported in real time.

- **Seamless Integration with ElementOne:** Safe Port works as part of the Element portfolio, allowing security teams to manage all scan logs and compliance data through the ElementOne platform. This centralization ensures that all removable media activities are part of a cohesive security strategy, reducing manual intervention and simplifying reporting.

- **Automated Malware Pattern Updates:** Safe Port can synchronize malware pattern updates with ElementOne, ensuring it has the latest threat definitions and protections in place. This capability eliminates the need for manual updates, reducing the risk of outdated security measures.

- **User-Friendly Touchscreen Interface:** Safe Port features an intuitive touchscreen interface that allows non-technical staff to easily scan and sanitize media. This simplicity ensures that Safe Port can be deployed quickly in industrial environments without requiring specialized training.

- **Hardened Security Features:** Safe Port enhances system security with several hardening measures, including TXOne's proprietary BIOS, restrictions on inbound transmissions, and the disabling of physical inputs (such as mouse and keyboard). These measures ensure that Safe Port itself is protected from external threats while handling sensitive media.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

By utilizing these capabilities, Safe Port delivers several key benefits for OT environments:

KEY BENEFITS

1 | IMPROVED SECURITY

By scanning all removable media before they are introduced into OT environments, Safe Port ensures that malware is detected and neutralized early, reducing the risk of infections in critical systems. This proactive approach strengthens the security perimeter and prevents the introduction of malicious software into industrial networks.

2 | OPERATIONAL CONTINUITY

With its rapid scanning capabilities of up to 7,200 files per minute, Safe Port ensures minimal downtime, allowing organizations to securely process media without disrupting operational workflows. This benefit is crucial for industries where continuous operations are essential.

3 | EASE OF USE

The intuitive touchscreen interface and simple operation make Safe Port accessible to non-experts, reducing the need for specialized security staff to manage media sanitization. This feature allows industrial staff to quickly sanitize media without the need for extensive training, making it suitable for a wide range of environments.

4 | CENTRALIZED MANAGEMENT WITH ELEMENTONE

When integrated with ElementOne, Safe Port enables security teams to manage media scans and sanitize logs from a centralized dashboard. Additionally, Safe Port can serve as a hub for Portable Inspector by uploading logs and malware patterns to ElementOne through Safe Port. This integration streamlines both media sanitization and asset management processes, optimizing workflows and simplifying audits.

5 | REGULATORY COMPLIANCE

Safe Port helps organizations maintain compliance with industry regulations by ensuring that all media sanitization activities are recorded and stored for audit purposes. This capability reduces the administrative burden of proving compliance and enables more streamlined reporting.

6 | REDUCED RISK OF HUMAN ERROR

Safe Port reduces the likelihood of human error by automating key processes such as scanning and logging through ElementOne. This automation ensures consistent scanning and logging of all removable media, minimizing the risk of malware bypassing protection due to human oversight.

7 | SEAMLESS INDUSTRIAL INTEGRATION

Safe Port is designed to integrate seamlessly into existing OT workflows without disrupting operations. Its durable, industrial-grade build ensures reliable performance in demanding environments, making it suitable for continuous use in OT settings.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

CONCLUSION: A Proactive, Game-Changing Solution for OT Security

The TXOne Element portfolio represents a transformative solution, uniquely addressing the complex security challenges faced by OT environments. With ElementOne at the core, security teams gain unparalleled visibility and control over OT assets, vulnerabilities, and audit logs through a single, unified platform. Complemented by Portable Inspector for seamless, agentless malware scanning in isolated systems and Safe Port for rapid, industrial-grade media sanitization, TXOne delivers a comprehensive and proactive approach to securing critical OT infrastructures.

By integrating these three products, the Element portfolio significantly improves people and process workflows. It reduces dependency on specialized security personnel by providing intuitive interfaces and automated processes that can be managed by non-expert users. With enhanced asset visibility, media sanitization, and secure file handling, the Element portfolio not only strengthens operational security but also ensures consistent protection across OT environments, all while maintaining operational uptime and reducing operational burdens.

Furthermore, streamlined workflows such as automated log collection, centralized management, and simplified compliance reporting enable organizations to optimize resources. These capabilities allow security teams to focus on addressing critical threats rather than being bogged down by manual tasks, ultimately improving both security outcomes and operational efficiency.

In a world where cyber threats evolve rapidly, the TXOne Element portfolio stands out as a robust, scalable, and future-proof solution. With its ongoing updates and flexibility to scale alongside organizational growth, TXOne ensures that businesses are always equipped to tackle emerging risks. This suite of products positions itself as an essential investment for any OT environment seeking to strengthen its security posture while confidently protecting its most critical systems against today's and tomorrow's cyber threats.

ABOUT TXONE

At TXOne Networks, we work together with both leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense. The OT zero trust-based technologies we've developed go beyond the limitations of traditional cyber defense to streamline management, reduce security overhead, and resolve challenges faster. We offer both network- and endpoint-based solutions that integrate with the layered arrangements and varied assets common to work sites, providing real-time, defense-in-depth cybersecurity to both mission critical devices and the OT network.

www.txone.com

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved