Keep the Operation Running

Understanding Cybersecurity in FDA Medical Devices Guidance:

Considerations and Solutions

March 2024 **TXOne Networks**

Contents

Introduction

According to data from the World Health Organization (WHO), there are more than 2 million different types of medical devices globally. Medical devices are intended to a) maintain or improve health; b) treat diseases or medical conditions; or c) facilitate the diagnosis or monitoring of disease conditions. These devices encompass a broad range of constantly evolving technologies that incorporate software components at an increasing rate. For instance, Magnetic Resonance Imaging (MRI) machines use software for signal processing and data visualization. Infusion pumps possess firmware for control and management. Insulin pumps use wireless connections to display medical parameters and allow for the adjustment of medication dosages. Consequently, cybersecurity threats to the healthcare sector have become more frequent and severe, which could lead to greater potential clinical impacts. Cybersecurity incidents have rendered medical devices and hospital networks inoperable in the past, disrupting patient care services at healthcare facilities worldwide. Such cyberattacks and vulnerabilities can result in delayed diagnoses or treatment, exposing patients to considerable health risks, given their time-sensitive nature[1].

To address this, regulation is the logical recourse; governments in the United States and Europe are beginning to compel medical device manufacturers to attend more seriously to their cybersecurity posture. This includes improvements in risk assessments during the premarket phase and cybersecurity monitoring in the post-market phase. On September 27, 2023, the US FDA issued the “Cybersecurity in Medical Devices: Quality System Considerations and Content for Premarket Submissions” guideline, emphasizing that cybersecurity is not an element independent of the overall security and effectiveness of medical devices, but part and parcel of them. In the European Union, the Cyber Resilience Act (CRA) is also developing rapidly, potentially having a significant impact on the IoT security landscape, including medical IoT devices. The CRA is expected to require organizations to implement a range of security measures for their IoT devices, such as secure software updates and vulnerability management processes. This has prompted Original Equipment Manufacturers (OEMs) to start preparing for the CRA by reviewing their IoT security practices and making changes as necessary.

This article analyzes the FDA’s recommendations to include cybersecurity information in premarket submissions, helping organizations understand the cybersecurity design and content submissions that are most crucial, and providing solutions from the TXOne Networks perspective. This will aid medical device manufacturers in adopting a proactive approach to addressing potential vulnerabilities before device market entry. This is vital for ensuring that device design takes security into serious consideration, reducing the risk of exploitation after its market release.

Scope of Application

"The FDA's 'Guidance for Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions' document recommends including cybersecurity information in the documents submitted before marketing. This guidance applies to all devices requiring cybersecurity consideration, not only those with software functions, but also devices containing software (including firmware), or programmable logic. Moreover, this guidance is relevant for any devices that can connect to the network or have other connectivity functions, commonly referred to as medical Internet of Things (IoT) devices."

In summary, when organizations need to submit premarket applications to the FDA's Center for Devices and Radiological Health (CDRH) or the Center for Biologics Evaluation and Research (CBER), they are advised to provide information about device cybersecurity. According to section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), the range of devices covered is very broad, including instruments, apparatus, implements, machines, implants, in vitro reagents, or other similar or related articles, ranging from the simplest medical supplies (e.g., bandages, thermometers) to the most complex machines (e.g., stents and advanced imaging equipment), as well as implants and wearable devices that are used for [2]:

1. Diagnosis, cure, mitigation, treatment, or prevention of disease: This includes devices used for medical or surgical purposes, such as X-ray machines, MRI scanners, pacemakers, blood glucose monitors, etc.

2. Affecting the structure or function of the body: This includes devices intended to alter the body's structure or function, rather than through chemical action or being metabolized, such as stents, artificial joints, dental implants, etc.

3. In vitro diagnostic use: This refers to devices used for the diagnosis or monitoring of diseases or other conditions from samples obtained from the human body (e.g., blood, saliva), such as various test kits and analytical instruments.

According to section 524B of the FD&C Act, 'cyber devices' specifically refer to those medical devices that have networking capabilities and can communicate over the network. This definition encompasses the following aspects:

1. Network connectivity: The ability of the device to connect to the Internet or any internal network, including wired or wireless connections. This means the device can send or receive data, enable remote access, or be accessed remotely.

2. Data exchange: These devices can not only communicate over the network but also exchange data. This might involve patient health information, device performance data, remote monitoring, and control signals, etc.

3. Remote functionalities: Network devices may have remote monitoring, diagnostic, or therapeutic functionalities, allowing medical professionals to operate them remotely or patients to use the device at home for treatment.

In essence, if the organization produces devices that can process and transmit sensitive information, the devices must have appropriate security measures built in to prevent data breaches or unauthorized access. If the organization's produced devices are hybrids (part of which involves electronic technology) and this part could be subject to cybersecurity risks, then this guidance applies to them as well.

Navigating Through the Guidance: Insights and Strategies

Medical device manufacturers are required to adhere to a set of quality system standards known as QS regulation to ensure their products consistently meet necessary safety and performance standards. These standards, detailed in Part 820 of Title 21 of the Code of Federal Regulations (CFR), span from product development to post-market stages. Specifically, for devices that entail cybersecurity risks, such as those incorporating software or programmable logic, manufacturers must demonstrate how their adherence to the QS regulation addresses these risks. This may include conducting software verification and risk analysis during the product design process to ensure product safety and efficacy.

Using an SPDF to Manage Cybersecurity Risks

The FDA's guidance suggests that the Secure Product Development Framework (SPDF) is an effective approach within the premarket stage, focusing on three pivotal areas: Designing for Security, Cybersecurity Transparency, and Submission Documentation. These methods help identify and mitigate vulnerabilities in products, thereby reducing cybersecurity risks. This framework, which covers the entire product lifecycle from design to discontinuation, aims to prevent the untimely discovery of security vulnerabilities post market launch. By integrating the SPDF into existing product development, risk management, and quality system processes, manufacturers can more efficiently comply with QS regulation while ensuring product cybersecurity.

In evaluating the cybersecurity of medical devices, the FDA considers various factors, focusing on the device's capability to consistently meet security goals throughout its architecture. These goals apply to all devices within scope, including those utilizing artificial intelligence (AI), machine learning (ML), or cloud services.

Designing for Security

The premarket submission documents should detail how the design addresses and integrates these security objectives. The specifics of these should include security risk management, supply chain management, architecture, cybersecurity testing, and the risk of patient harm.

Device design should consider the exploitation of known vulnerabilities and weaknesses in cybersecurity controls as foreseeable failure modes, thereby incorporating security from the design phase. Utilizing the SPDF ensures that medical devices are secure by design throughout their system/network use across the device lifecycle.

Table 1. Designing for Security and Corresponding Solutions

Category	Subcategory	Description	TXOne Networks Support
Security Risk Management	**Threat Modeling**	The FDA suggests submitting threat modeling documentation with new medical devices to identify potential safety risks. Manufacturers can use various methods for this analysis. The documentation should detail the threat modeling conducted, ensuring the device's security features are thoroughly evaluated for security and effectiveness.	**TXOne Threat Research** continuously monitors and detects IoT/ICS threat terrain via our large-scale fully automated threat hunting system. Threat data is continuously gathered through a worldwide network of hunting engines, submissions, feedback loops, customers & partners, and our own Threat Research Labs researchers. These threat intelligence systems quickly protect our customers' critical assets and operations.
	Cybersecurity Risk Assessment	Before launching a medical device, the FDA advises providing a cybersecurity risk assessment. This should cover control measures for risks identified in threat models, including strategies for mitigating risks before and after they occur, acceptance criteria, and methods for transferring security risks.	**EdgeIPS** offers cutting-edge protection against unidentified threats by leveraging its comprehensive and up-to-date threat intelligence. Utilizing the Zero Day Initiative (ZDI) vulnerability reward program, EdgeIPS provides exclusive protection for your systems against undisclosed and zero-day threats. By implementing virtual patching, your network gains a robust and up-to-date initial defense against known threats (including CISA Known Exploited Vulnerabilities Catalog).

		This assessment should be part of the premarket submission. It's wise to prepare for the worst-case scenarios by implementing suitable controls or explaining how risks across the device's total product lifecycle (TPLC) are managed and controlled.	This gives users greater control over the patching process, creating a proactive defense strategy during incidents and offering additional protection for legacy systems. **Stellar** can monitor legitimate vulnerable processes by learning and authorizing operational behaviors at a minimum under the control of permissions, establishing a baseline which Stellar can use to detect abnormal operational behavior. Additionally, Stellar is equipped with unique application trust lists and locking technology to ensure system integrity, including Operational Lock, USB Device Lock, Data Lock, and Configuration Lock. It can comprehensively protect endpoints that cannot execute short-term Windows Patches and legacy endpoints. Our Stellar endpoint protection solution can be used as an alternative to help asset owners buy more time until their assets can be upgraded to the final patch provided by the OEM.
	Interoperability Considerations	When assessing the cybersecurity of end-to-end medical device systems, interoperability is a key factor to consider. This includes how the medical device interacts with related accessories and their communication interfaces, network protocols, Electronic Medical Records, medical imaging systems, and general computing platforms.	**EdgeIPS & EdgeFire** support OT network visibility and look into assets from specific vendors and all network elements, assets, software, and devices as well as application traffic, including DICOM and Modbus or Ethernet/IP (for hospital facility management systems). **EdgeIPS & EdgeFire** are capable of safeguarding session integrity. They have the power to reject any usage of invalid session IDs, reinforcing the security of your digital interactions.

	Third-Party Software Components	Medical devices frequently use third-party software, requiring their security risks to be part of the device's risk management. The FDA recommends manufacturers inform users about these risks, including vulnerabilities and configurations. An SBOM is essential for managing these risks and tracking the device's software components.	**Portable Inspector** can be used in the risk assessment process. It performs vulnerability assessments on various operating systems, identifying and reporting the criticality of each vulnerability found. Along with providing effective malware scanning and removal for standalone computers and air-gapped systems, PI also automatically collects detailed snapshots of asset data which includes computer information, Windows Update status and application lists.
	Security Assessment of Unresolved Anomalies	The FDA advises including a list of software anomalies with their potential security implications and their resolution criteria in the premarket submission documentation.	**Portable Inspector** collects details of asset data, including device information, Windows Update status, and application lists. Asset scanning results and logs are centralized in the console to create a comprehensive security overview and generate malware-free reports with the ElementOne console for auditing purposes. Such visibility is key for vulnerability management.
	TPLC Security Risk Management	The FDA recommends including differences in risk management, marketed or not, for all devices in documentation. Assessing vulnerabilities across all versions is crucial, particularly for devices that can't be updated. Manufacturers should track risk management metrics like vulnerability update percentages and the time from identification to patch application. These details should be part of premarket submissions and PMA annual reports (21 CFR 814.84) to confirm the effectiveness of safety measures and to maintain device integrity.	**EdgeIPS & EdgeFire** series are able to restrict access achieved through dial-up connections or connections from other sites' networks and prevent unauthorized connections (such as VPNs). **Stellar** allows management from a single pane of glass with support for Syslog forwarding, indicators of compromise (IoC) integration, and centralized monitoring. **ElementOne** creates an inventory of OT asset information during routine scans, allowing verification of vulnerability status, OS (Operating System) updates, installed applications, and asset specifications.

Security Architecture	**Authentication**	In premarket submissions, manufacturers must outline tested authentication measures, confirming that: 1. The information is from a trusted source and was not changed in transit, affirming data integrity and authenticity. 2. The identity of system-interacting endpoints or operators is verified.	The **EdgeIPS & EdgeFire** series can restrict access obtained through connections from other site networks and prevent unauthorized connections (such as VPNs). Network access can only be established when necessary and after authentication, thereby enabling businesses to reduce attacks on their OT networks. **Stellar** has the ability to detect behavioral anomalies and swiftly determine the trustworthiness of operations using an expanded ICS application and certificate library, achieving an optimal balance between performance and detection rates. Furthermore, Stellar employs trust list technology for the validation of software applications, preventing malicious programs from sending and receiving commands.
	Authorization	Authorization grants system entities—such as devices or servers—access rights to system resources. It enforces privileges based on identities or roles, allowing or denying actions in order to secure resource access by only authorized users.	**EdgeIPS** series supports the principle of least privilege, allowing businesses to minimize their OT attack surface, restrict OT network attacks, enhance operational performance, and mitigate the impact of human error. By implementing fine-grained access control at different levels, businesses can strike a balance between availability and security while safeguarding critical data and systems. **Stellar** supports OT/ICS endpoints by enforcing custom-defined cybersecurity policies and procedures to ascertain whether the operations requested by users are actually permissible. It also supports segregation of duties and the principle of least privilege, all while minimizing the negative impact on operational processes.

	Cryptography	To achieve secure design goals, the FDA recommends using industry-standard encryption algorithms and protocols. It advises selecting proper methods for key generation, distribution, management, and protection, along with robust "nonce" (number used once) mechanisms.	When encryption is required, the Edge network defense solutions can employ encryption algorithms, key sizes, key creation and management mechanisms as needed, in line with widely accepted security industry practices and recommendations. **Portable Inspector** is a multipurpose secure transporter malware monitoring/ inspection scanning and clean-up tool, for air-gapped systems and standalone PC's with 64GB of AES-256 encrypted storage for secure file transfer. It also provides greater OT visibility and insights into asset information.
	Code, Data, and Execution Integrity	Maintaining integrity involves ensuring that the code stored on a device, incoming data, and code in operation are kept unaltered, free from malicious software infections, and are not modified in any unauthorized manner during execution. Achieving this requires continuous monitoring and verification of the code's integrity and behavior throughout the entire process from storage and loading to execution.	**EdgeIPS & EdgeFire** support multiple OT protocols such as DICOM to protect OT network communications. It also facilitates in-depth analysis of L2-L7 network packets by node group to prevent invalid inputs from causing system security issues, or unauthorized instructions, ensuring that network transmissions adhere to network security policy guidelines. Meanwhile, administrators can use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. **Stellar** can lock down sensitive assets, limit access, and preserve system resources with its simple and reliable trust list technology. Once deployed, this solution allows only the execution of approved applications necessary to daily operations, preventing the spread and execution of malware without reliance on pattern files or other resources.

	Confidentiality	Manufacturers should protect the confidentiality of any data that, if leaked, could harm patients, such as through unauthorized access or lack of encryption. Losing confidentiality of credentials could enable attackers to harm multiple patients.	**EdgeIPS & EdgeFire** support various technical means, such as network segmentation and encryption, to ensure information confidentiality while making certain that it does not impact the performance of the OT/ICS systems.
	Event Detection and Logging	Event detection and log recording are essential functions within devices and their broader systems, ensuring that suspicious and successful attempts to compromise medical devices can be identified and tracked. These capabilities should ideally include storage for future forensic analysis.	**EdgeOne** manages the policies of networking and endpoint security assets, ensuring operational integrity across distant sites. It allows administrators to modify OT protocol allowlists for asset interoperability and to conduct deep network analysis. It organizes alerts, assets, and incident events, permitting direct monitoring of the enterprise's industrial control system security, in addition to providing insight into the shadow OT environment. **StellarOne** allows management from a single pane of glass with support for Syslog forwarding, indicators of compromise (IoC) integration, and centralized monitoring. **ElementOne** collects asset information that can be converted to the CSV format through the centralized management program as an asset inventory, and/or sent to a SIEM or log server for further asset management (such as maintaining OT asset inventory or identifying impact levels, known vulnerabilities, and cyber risks).

	Resiliency and Recovery	Devices need to be resilient against potential cyber incidents to maintain availability. This cyber resilience is vital for medical devices, as it offers a margin of security against unforeseen vulnerabilities.	**EdgeIPS & EdgeFire** support the principle of least privilege, allowing businesses to minimize the OT attack surface, constrain OT network attacks, enhance operational performance, and mitigate the impact of human error. By implementing fine-grained access control at different levels, businesses can strike a balance between availability and security to safeguard critical data and systems. **EdgeIPS & EdgeFire** are built with durable, industrial-grade components for harsh environments and temperatures. Meanwhile, their redundant power design is suitable for OT environments. **Stellar** uses a system lockdown feature to block unauthorized access and malware. Stellar can operate without an internet connection, using policies designed around “least privilege” to thwart both known and unknown malware as well as fileless attacks. It also monitors easily exploitable legitimate processes by learning and authorizing actions under permission control, which gives Stellar the ability to detect unusual activity and respond appropriately, such as by blocking script execution and malware execution, to ensure system integrity without affecting the system’s regular operation.
	Updatability and Patchability	Devices should be capable of secure and timely updates to remain safe and effective throughout their lifecycle.	By implementing virtual patching, your network gains a robust and up-to-date initial defense against known threats. This gives users greater control over the patching process, creating a proactive defense strategy during incidents and offering additional protection for legacy systems.

		The FDA recommends that manufacturers not only enable device updates but also plan for rapid testing, evaluation, and patching of devices in use.	**Stellar** can monitor legitimate vulnerable processes by learning and authorizing operational behaviors at a minimum under the control of permissions, thus enabling Stellar to detect abnormal operational behavior. Additionally, Stellar is equipped with unique application trust lists and locking technology to ensure system integrity, including Operational Lock, USB Device Lock, Data Lock, and Configuration Lock. It can comprehensively protect legacy endpoints and endpoints that cannot execute short-term Windows Patches. Our Stellar endpoint protection solution can be used as an alternative to help asset owners buy more time until their assets can be upgraded to the final patch provided by the OEM.
Security Architecture View	**Diagrams**	The FDA suggests manufacturers use diagrams to illustrate the architecture of medical device systems, including interfaces, communication protocols, threats, and cybersecurity controls used throughout the system.	**EdgeOne** supports OT network visibility and looks into assets from specific vendors and all network elements, assets, software, and devices as well as application traffic.
	Information Details for an Architecture View	Manufacturers are advised to provide a system-level description and analysis, covering end-to-end security analysis of all communications within the medical device system, regardless of its intended use.	**EdgeIPS & EdgeFire** support multiple ICS protocols to protect OT network communications. They also facilitate in-depth analysis of L2-L7 network packets by node group to prevent invalid inputs from causing system security issues or unauthorized instructions, ensuring that network transmissions adhere to network security policy guidelines.

Cybersecurity Testing	**Security Requirements**	Manufacturers should present evidence that each design input requirement has been successfully implemented, including rationale for their boundary analysis and assumptions.	**EdgeIPS & EdgeFire** can handily manage the group policies of networking and endpoint security assets, ensuring operational integrity across distant sites. It allows administrators to modify OT protocol allow-lists for asset interoperability and to conduct deep L2-L7 network analysis. **Stellar** ensures operational integrity through application lockdown to minimize downtime. It can check whether the input syntax of the control system complies with rules to verify that the information has not been tampered with and is in accordance with baseline specifications. Furthermore, Stellar also supports real-time malware scanning in maintenance mode to quickly identify threats.
	Threat Mitigation	Manufacturers must provide detailed information and evidence of tests that verify effective risk control measures based on threat models outlined in global system perspectives, multi-patient harm, updatability, patchability, and security use case views.	**EdgeOne** can centrally manage the network defense provided by the Edge series nodes, and gives you comprehensive logs of activities including cybersecurity, policy enforcement, protocol filtering, system logs, audits, and asset detection at each EdgeIPS Family and EdgeFire Family node. **Stellar** can run on modern and legacy assets and allows for centralized management from a single platform through StellarOne, enhancing both management of modern assets and defense of legacy equipment. **ElementOne** creates an inventory of OT asset information during routine scans, allowing verification of vulnerability status, OS (Operating System) updates, installed applications, and asset specifications.

	Vulnerability Testing	Manufacturers should also detail vulnerability testing and analysis, including, but not limited to, abuse or misuse cases, handling of malformed and unexpected inputs, analysis of the attack surface, chaining vulnerabilities, closed-box testing using known vulnerability scans, and software composition analysis of binary executable files, among others.	All products of TXOne Networks undergo rigorous security feature verification, such as software security testing, input/output validation, stability and reliability tests. Additionally, we support our customers in deploying security features, including anti-virus alerts, effectiveness of intrusion detection system rules, proper security monitoring and incident handling, as well as logging in accordance with security policies.
	Penetration Testing	These tests aim to identify and describe security-related issues within the product. During penetration testing, testers attempt to uncover vulnerabilities by actively trying to exploit them, simulating the actions of real attackers.	

Cybersecurity Transparency

A lack of information on how to integrate device security into the use environment and how users can maintain cybersecurity throughout the device lifecycle could jeopardize the safety and effectiveness of the device.

To address this issue, it is crucial for device users to have access to information regarding the device's cybersecurity controls, potential risks to the medical device system, and other relevant details. For instance, not disclosing all communication interfaces or third-party software could conceal potential risks; insufficient information about known but undisclosed cybersecurity vulnerabilities in a device could impact the assessment of the device's safety or effectiveness; and labels lacking information on how to securely configure or update devices may limit users' ability to properly manage and protect their devices. This information helps users understand the defenses their devices have against cyber threats, the threats they might face, and how to prevent or mitigate these threats. The absence of such information could lead to undisclosed, incorrectly identified, or improperly responded to security risks, thereby threatening the device's safety and effectiveness.

The FDA emphasizes that the cybersecurity information discussed in the guidance is crucial for the safe and effective use of devices and should be included in device labeling.

Table 2: Cybersecurity Transparency and Corresponding Solutions

Category	Description	TXOne Networks Support
Labeling Recommendations for Devices with Cybersecurity Risks	Manufacturers must include security information in labels to help users manage cybersecurity risks and use devices safely. Risks passed to users should be clear and tested (e.g., in human factors testing) to ensure users can effectively handle these risks.	The **Edge series** and **Stellar** are recommended for inclusion in network security control descriptions and product specifications suitable for intended use environments, such as using firewalls or anti-malware software. The **Edge series** can detail the list of network ports and other interfaces for receiving and/or sending data. This list should describe the function of each port, indicating whether it is for incoming, outgoing, or both types of traffic, along with the approved destination endpoints. Based on the expected use environment, **Edge series** or **Stellar** provides descriptions for capturing forensic evidence, including maintaining security event log files. The **Edge series** supports defenses for systems all throughout their lifecycle and at the end of service. When support ends, manufacturers may not reasonably offer security patches or software updates but can continue vulnerability management through Virtual Patching capabilities.
Cybersecurity Management Plans	Manufacturers submit their cybersecurity management plans in premarket submissions, allowing the FDA to assess if they have adequately addressed maintaining device safety and effectiveness post market authorization. For networked devices, timely and proper monitoring, identification, and resolution of post-market cybersecurity vulnerabilities, including coordinating vulnerability disclosures and related programs, are essential.	**SageOne** aggregates cybersecurity intelligence from all TXOne products to construct the most comprehensive security platform available. It not only centralizes management with strategic oversight but also leverages AI to intelligently compare and identify potential security risks from various angles at every cybersecurity control point. **SageOne** offers a multi-dimensional view of an organization's cybersecurity posture through visual representations. It provides a holistic security perspective with granularity, including the proportion of protected/unprotected assets, asset health status and anomaly detection, asset exposure level assessment, and an overview of the asset lifecycle. Asset managers can efficiently evaluate system vulnerabilities through the SageOne dashboard, setting

		priorities and response plans. This enables a macroscopic ordering of risk management priorities to effectively and accurately reduce the level of risk. **SageOne** integrates an overview of daily manufacturing operations and massive data from all cybersecurity control points to generate insightful and actionable cybersecurity recommendations.

Submission Documentation

The design and documentation of a device's cybersecurity should align with the risk-based approach associated with the device. Manufacturers should consider how the device is used within a broader system. For instance, for a simple, non-networked thermometer, the cybersecurity risk is lower, thus only a limited security architecture and a few security controls based on the device's features and design are needed. However, if the thermometer is used in a critical control environment or is networked, its cybersecurity risk increases, necessitating more substantive design control measures. When submitting premarket applications to the FDA, manufacturers should include documentation of the design controls used in developing devices with cybersecurity risks as a reasonable assurance of safety and effectiveness. The cybersecurity information presented in this guide is intended to support premarket submissions for devices within the scope of this guide.

Table 3: Submission Documentation and Corresponding Support

Category	Description	TXOne Networks Support
Cybersecurity Risk Management Report [+]	**Threat Model [+]**	**TXOne Threat Research** continuously monitors and detects IoT/ICS threat terrain via our large-scale, fully automated, threat hunting system. Threat data is continuously gathered through a worldwide network of hunting engines, submissions, feedback loops, customers & partners, and our own Threat Research Labs researchers. The threat intelligence systems quickly protect our customers' critical assets and operations.

	Cybersecurity Risk Assessment [+]	Before hitting the market, **Edge series** can act as one of the risk mitigation strategies, capturing identified risks in the threat model and offering corresponding compensatory controls. This includes methods for both preemptive and subsequent risk mitigation, as well as techniques for transferring security risks (e.g., virtual patching) as part of the premarket submission's risk control measures.
	SBOM [*]	**Portable Inspector** automatically collects detailed snapshots of asset data which includes computer information, Windows Update status and application lists.
	Vulnerability Assessment and Software Support [+]	All products of TXOne Networks undergo rigorous security feature verification, such as software security testing, input/output validation, stability and reliability tests. Additionally, we support our customers in deploying security features, including antivirus alerts, effectiveness of intrusion detection system rules, proper security monitoring and incident handling, as well as logging in accordance with security policies.
	Unresolved Anomalies Assessment [+]	**Portable Inspector** collects details of asset data, including device information, Windows Update status, and application lists. Asset scanning results and logs are centralized in the console to create a comprehensive security overview and generate malware-free reports with the **ElementOne** console for auditing purposes. Such visibility is key for vulnerability management.
	Traceability [+]	Using products like **Edge**, **Stellar**, and **Portable Inspector**, as detailed in Table 2, offers comprehensive cybersecurity controls and security posture information. This allows users to maintain ongoing security and ensures devices remain secure and effective throughout their lifecycle.
Measures and Metrics [+]		TXOne's solutions offer valuable assistance to customers in addressing a wide range of controls and subcontrols outlined in the FDA guidelines. This includes several security controls in Table 1 including Authentication; Authorization; Cryptography; Code, Data, and Execution Integrity; Confidentiality; Event Detection and Logging; Resiliency and Recovery; and Updatability and Patchability.
Architecture Views [*]	**Global System View**	**EdgeIPS** & **EdgeFire** provide a comprehensive system view, encapsulating the entirety of networked medical device systems. This includes assets from specific vendors, all network elements, software, devices, and application traffic. For interconnected and networked devices, this view identifies all interconnected components, covering software update infrastructures, impacts on medical facility networks, intermediary connections or devices, and so on.

	Multi-Patient Harm View	**Edge series** can protect an organization's network from the latest variants of malicious software, spyware, and other content-level threats, thereby reducing the risk of data leaks or damage resulting from malware infections. Meanwhile, use **Edge series** appliances to create special rules for traffic that allow assets to communicate on a strictly need-to-know basis in order to do their work, while highlighting all suspicious or potentially harmful activity. **Stellar** offers OT native protection with its next generation antivirus, application lockdown, and anomaly detection via a lightweight agent. It also includes an industrial application repository for operational baselines, anomaly detection, and real-time malware scanning to ensure operational integrity.
	Updatability and Patchability View	**SageOne** offers a multi-dimensional view of an organization's cybersecurity posture through visual representations. It provides a holistic security perspective with granularity, including the proportion of protected/unprotected assets, asset health status and anomaly detection, asset exposure level assessment, and an overview of the asset lifecycle.
	Security Use Case View	**SageOne** has become a medical OT security management tool, offering a comprehensive view of the system and acting as an information and control center. It directs all installed product lines through policy supervision. It also continually monitors the cybersecurity posture, covering various operational states of elements within the medical device system and assesses the clinical functionality status of the medical device system (e.g., asset health status and anomaly detection, alarms, providing massive data from all cybersecurity control points, and diagnostic results of risk reports).
Testing [+]		All products of TXOne Networks support customers in conducting security functionality verification, such as antivirus software alerts, effectiveness of intrusion detection system rules, appropriate security monitoring and event handling, and log recording in accordance with security policies among other security tests.
Labeling [*]		Using **Edge series** or **Stellar** products enables manufacturers to offer comprehensive descriptions of security controls and product specifications, fully tailored for medical environments. Additionally, TXOne Networks supports complete visualization capabilities, providing detailed diagrams that allow users to clearly implement security controls.
Cybersecurity Management Plans [+]		**SageOne** synthesizes a panoramic view of day-to-day manufacturing operations with abundant data harvested from all cybersecurity control points, culminating in the generation of perceptive and pragmatically actionable cybersecurity advisories.

	This integration not only supports but elevates the documentation process within a cybersecurity management program, rendering it an indispensable ally in the unending quest for cybersecurity excellence in the realm of medical OT/ICS.

Note: “[*]” signifies that submission may be recommended.
“[+]” signifies that submission may be advantageous, although not strictly recommended.

Conclusion

The FDA’s new Medical Devices Guidance mandates that all applicants for new medical devices submit a comprehensive plan detailing their strategies for “monitoring, identifying, and addressing” cybersecurity vulnerabilities. This includes establishing a secure development lifecycle for devices, providing security updates and patches both regularly and in emergency situations, and submitting a “Software Bill of Materials” to the FDA to safeguard patient safety and data integrity. This means that devices found to have cybersecurity flaws that could impact patient or hospital safety, or present other significant security concerns, will not be permitted to enter the market until these issues are resolved. For device manufacturers, this could lead to delays in product launches and potential loss of significant market share.

In collaboration with TXOne Networks, medical device manufacturers can confidently monitor, identify, and resolve potential cybersecurity challenges within medical OT systems, such as TPLC Security Risk Management, Code, Data, Execution Integrity, and Event Detection and Logging. TXOne primarily offers Security Inspection, Endpoint Protection, and Network Defense solutions to help clients strengthen their cybersecurity risk management processes. Additionally, TXOne enhances traceability and transparency through an advanced, visual management interface, enabling manufacturers to quickly assess the security posture of their products without the burden of extensive documentation.

Reference

[1] *Lorenzo Bracciale, Pierpaolo Loreti, Giuseppe Bianchi, "Cybersecurity vulnerability analysis of medical devices purchased by national health services", Nature Portfolio, November 09, 2023.*

[2] *U.S. Department of Health and Human Services Food and Drug Administration, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions", U.S. Department of Health and Human Services Food and Drug Administration, September 27, 2023.*

txOne networks