nuvolo

OT SECURITY FOR HEALTHCARE

Safeguarding Medical Devices, Patients and Your Reputation

Contents

Managing OT Security Risk for your Healthcare System

Operational technology, or OT, is defined as any non-IT device that can connect to your network. According to the American Hospital Association (AHA), there are a total of 931,203 hospital beds in the United States[1]. If an average hospital room has between 15-20 medical devices[2] that would mean that there are approximately 18.6 million medical devices operating in US hospitals with an estimated 74% connected to the network[3]. The proliferation of OT, which in this case refers to network connected medical devices along with healthcare facilities systems such as heating, ventilation, and air conditioning (HVAC) controls, represents a clear and present danger to your healthcare system. Network connectivity increases the risk to device safety, accessibility, and availability. OT security events are caused by unpatched software, misconfigurations, or non-authorized access. Your unmanaged or improperly managed OT can result in:

- **Adverse patient outcomes**
- **Reduced medical device availability**
- **Decreased safety**
- **Financial exposure**
- **Brand and public relations risk**
- **Loss of revenue**

Managing OT Security Risk for your Healthcare System

Slow or extended security event remediation efforts can have a direct impact on patient care. One study reports several minutes of delays in patient time for providing critical electrocardiogram (ECG) testing after a security event[4].

The availability, safety and quality of your medical device fleet is core to the mission of patient care. Network connected medical equipment also serves an important secondary purpose - data analytics. Medical devices that generate data provide insights into the quality of patient care. With longer life expectancy, there is an increased demand for medical devices that generate data. This data is used to derive better patient outcomes. Your connected medical devices allow healthcare teams to share generalized data for clinical engineers and for remote teams, medical device data allows them to perform better device monitoring, and more effective and safer maintenance.

This ebook provides an understanding of how modern, OT security works and why it is important to select, deploy and operationalize these capabilities to protect patients, medical devices, and your healthcare system reputation on a sustainable and cost-effective basis.

Closing the Gap in OT and IT Security

Securing traditional IT devices such as laptops, servers and printers is generally a high priority for IT security teams. In contrast, teams such as clinical engineering that oversee OT that includes medical devices has had no historical security mandate, their focus has been on clinical safety and device availability. Times have changed and medical and facilities systems devices represent a material business risk and patient safety threat to your healthcare system.

There is a growing realization that closing the OT security gap by addressing medical device security threat requires both organizational and financial commitment. Commitments that require collaboration between your clinical engineering and IT teams, along with process improvements and modern, SaaS- based service management technology. Your IT security teams have the benefit of mature active monitoring capabilities, vulnerability management tools and nearly universal remote remediation capabilities for IT devices.

Closing the Gap in OT and IT Security

But for OT security, most of these tools and resources are not available, or cannot be used for medical devices:

- Active monitoring cannot be performed on most medical devices because the installed operating system and network protocol configuration are often not configured to withstand your active monitoring tools. These tools may cause these medical devices to "crash" or become unresponsive.
- Passive monitoring is the standard. Like the choice to avoid active monitoring, passive monitoring will provide needed data about medical devices without interacting directly with the device itself. Specialized tools passively "sniff" the network, identifying and classifying network traffic and medical device signatures. The industry term is fingerprinting.
- Standard operating procedures for security remediation for your medical devices can only be executed by an authorized, trained, and certified clinical technician or engineer, not IT traditional IT security personnel.
- Specialized skills, training, tools, and experience are required for medical device risk mitigation and remediation
- In some cases, OEM or third-party service providers must be utilized to perform OT security corrective maintenance activities versus internal IT security teams.

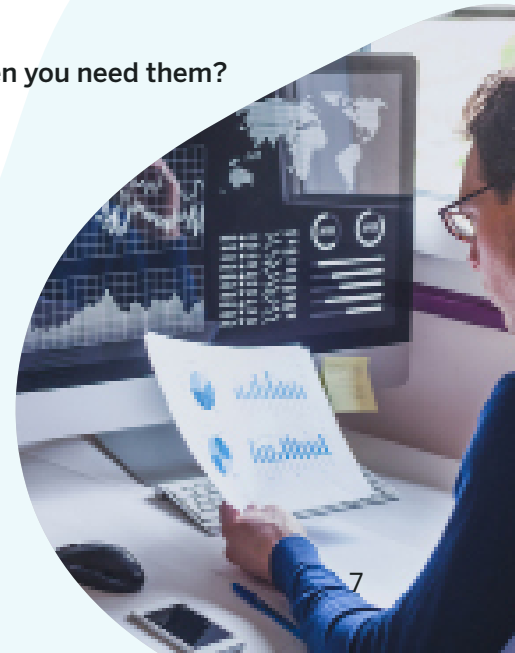
These issues can be complicated by the historical gaps, culturally and organizationally, between your IT and clinical engineering teams. Closing the gap is critical as more sophisticated and determined attackers are actively exploiting network connected medical devices as a new and highly vulnerable entry point into the health system. The threat is real and growing, and a new era of cooperation is essential.

OT Security and Your Responsibility

There are several myths surrounding the security of your medical devices. One myth is that in the United States, the Food and Drug Administration (FDA) tests all medical devices for vulnerabilities. In fact, testing is the responsibility of the medical product manufacturer and once in use, security must be addressed by a medical device security expert, team, or manufacturer resource in collaboration with clinical engineering teams. Healthcare providers are also leveraging third-party service providers for these activities as well. While the manufacturer must comply with federal regulation regarding risk, including security, the ultimate responsibility and risk lives with you[5].

Medical device security requires more than just ensuring compliance with security best practices. Because it directly impacts the safety and availability of your critical life sustaining technologies, some fundamental questions must be answered as part of maintaining your medical device security posture.

- **When do you know critical medical devices are safe to use?**
- **How can you confirm the availability of your medical devices?**
- **How do you make sure your medical devices are accessible when you need them?**



People, Process & Technology

Important gaps in your medical device security occur when people, processes, and technologies, are not working together to identify and respond to security events. These gaps can be narrowed by with approaches to make sure your teams, processes and tools are aligned as follows:

People

Your clinical engineering team needs a single, accurate, trusted inventory of all medical devices, available wherever they are working, accessible via a mobile device or laptop. Your clinical team management need accurate reporting on inventory with information reflecting condition, disposition, and location of all medical devices. Your security operations center (SOC) needs access to an “intelligence hub” of device inventory, combined with device monitoring information that empowers them to monitor medical device security and activity on your network.

People, Process & Technology

Process

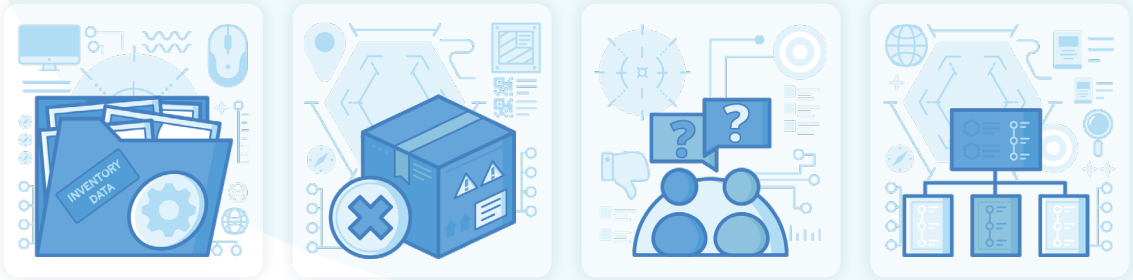
You need a way to accurately capture the medical device lifecycle, as part of a standard onboarding process. Without this, it's difficult to determine device disposition, maintenance, and security. When a medical device security threat, vulnerability or exploit occurs, timely remediation can be difficult or impossible to achieve with the absence of a common data model for matching, contextualization, and security event correlation. The process of creating a standard data model enables the technology to perform to expectations. Without this process commitment, the technology will not meet expectations and risk will remain persistent.

Technology

Multiple computerized maintenance management system (CMMS) or other service management technologies will prevent your healthcare technology team from achieving a successful medical device security posture. Consolidating legacy technologies onto a single, modern, SaaS-based service management and medical inventory platform is a key first step for your enterprise. Without this commitment, your healthcare system will struggle and accrue risk over time.

Figure 1 provides some examples of critical sources of risk and exposure in your healthcare system.

Figure 1:



Disparate & Unmanaged Inventory Data

Ineffective Medical Device On-boarding Process

Non-standard Naming Conventions & Location Data

Multiple Disparate Legacy CMMS Platforms

Disparate technologies used for managing your medical devices with device profile data and network information in different forms, adds enormous complexity, cost, and risk when a security event takes place. How can your devices be matched to security threats if there is no standard data model? How can your healthcare technology team understand what other devices of similar risk are potentially at risk without a common data model? It is essentially impossible at scale to manage medical device security across multiple inventory and service management technologies with disparate data. Consolidation and a common, standard data model are the only options.

Connected Medical Device Discovery - Intersecting OT & IT

How do you discover and monitor medical devices and healthcare facilities systems that live on your network? Step one is to leverage a healthcare technology service provider or acquire OT discovery technology. Once in place, you can utilize those capabilities together with the deployment of a single,

This service management platform is where the device discovery data is ingested, contextualized, and acted upon in a way that mitigates threats to your healthcare system and drives remediation work activity. The service management platform should be authoritative in nature and represent a single, trusted inventory for your healthcare system.

Connected Medical Device Discovery - Intersecting OT & IT

A single, trusted inventory system helps your healthcare technology team manage your entire network connected device lifecycle. Regular, ongoing updates take place when your clinical engineering team performs tasks such as routine planned or corrective maintenance, provisioning new devices, or medical device firmware or software updates.

The inventory system includes, but is not limited to data such as:

- → Owner
- → Device make
- → Device model
- → Location
- → Department
- → Usage
- → Serial number
- → Latest software version
- → Maintenance history

When your medical device discovery payload, derived from a security event, is enriched by the service management and inventory data, your data security, IT, and clinical engineering teams can now all intersect with the same information. Having everyone on the same page is essential for visibility and rapid remediation of medical device security events. This "intelligence hub" allows HTM teams and IT to work together effectively for the very first time.

Trusted Device Data with Monitoring & Remediation

An essential part of safeguarding the medical device fleet is ensuring 24x7 visibility using medical device discovery capabilities to help prevent security blind spots. medical device monitoring and discovery should be part of any proactive monitoring of both internal and external activity by security professionals with an understanding of healthcare clinical operations.

These professionals help analyze vulnerabilities and provide security event assessment and remediation. These teams of qualified SOC or field-based resources also ensure that only trained, certified and authorized resources are utilized or dispatched to remediate the affected device(s). A key driver here is regulatory mandates. For example, a device manufacturer may require only certified, authorized personnel to work on a device for warranty or compliance reasons. Most importantly, these requirements help ensure that a patient's health, medical information, or a medical procedure are not put at risk.

Trusted Device Data with Monitoring & Remediation

When a security event takes place, the security team can see the full context of the medical device. They'll know who the device owner is and what remediation process must be followed so a work order can be dispatched to the qualified technician. Using a single, modern, SaaS-based platform, all activities are tracked, time stamped, date stamped and available as data for reporting and compliance purposes. In this model, information security, IT, and the medical device service management teams have fully visibility and reporting on all activities for remediation.

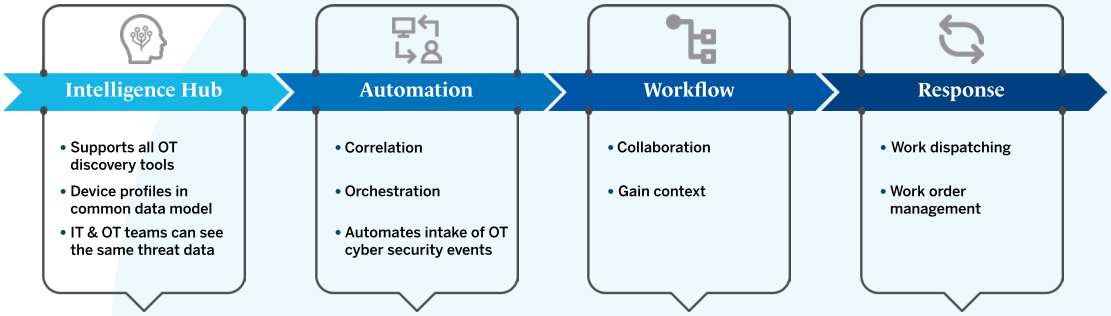
This combination of medical device expertise, modern, SaaS-based technology and well documented and operationalized processes help keep the connected medical device fleet safe and resilient in the face of an increasingly omnipresent OT security threat.

HTM & IT Teams - Using the Same Data Means Faster Remediation

When there are thousands of connected OT devices in use in your organization, it's critical to have a scalable, orchestrated, and automated response process to security events.

A best practices automated response process is outlined below in Figure 2.

Figure 2:



This approach to medical device security is where Nuvolo OT Security for healthcare provides:

- The ability to receive data when authorized medical devices are added to the network Single system of inventory
- Common device data model
- Workflow and orchestration
- Dispatch
- Tracking and reporting
- Matching capability for "like" affected devices

Conclusion

Nuvolo provides a single, trusted inventory system for medical device and facilities systems security that helps the healthcare system manage the entire connected device lifecycle. Regular, ongoing updates take place when the clinical engineering team performs tasks such as routine planned or corrective maintenance, provisioning new devices, or installing medical device firmware or software updates.

When a medical device is connected to the network or a security event takes place, Nuvolo receives that information from device discovery and monitoring tools, creating an intelligence hub of device and event information. This allows Nuvolo to leverage an existing discovery tool, natively embedded as part of the solution to be utilized by the healthcare provider if they have
not already selected one. Alternatively, if the healthcare system has already purchased and operationalized a device discovery tool, the intelligence hub allows for easy integration. For most of the established device discovery tools, the integrations are already completed and available to healthcare providers out-of- the-box.

When a security event takes place, the key is that both the information security and clinical engineering teams can see the full context of the device. The intelligence hub also helps facilitates full knowledge and visibility of the affected device(s) including theater of operation, device owner, life-saving designation, and many other attributes as well as the remediation process to be followed.

Nuvolo enables this seamless approach, accelerates remediation, and improves quality and safety when a medical device security events occur.

[1] AHA, Fast Facts on US Hospitals, 2019, www.aha.org/statistics/fast-facts-us-hospitals

[2] https://hitinfrastructure.com/news/iot-sensors-critical-to-successful-health-it-infrastructure

[3] https://hitinfrastructure.com/news/healthcare-wireless-network-coverage-capacity-top-challenge

[4] Data breach remediation efforts and their implications for hospital quality, Sung J. Choi PhD M. Eric Johnson PhD Christoph U. Lehmann MD https://doi.org/10.1111/1475-6773.13203

[5] https://www.fda.gov/media/103696/download