Nuvolo OT Security

with Industry Leading Standards

Available as an additional option, Nuvolo OT Security with industry leading standards leverages a process developed by Mayo Clinic for the implementation of device security procedures across your organization.

Security-Focused Lifecycle Management

The healthcare industry constantly focuses on patient safety and positive outcomes. To support this, your healthcare technology management (HTM) team must ensure the safe and smooth operation of network connected, non-IT medical devices along with healthcare facilities systems such as heating, ventilation, and air conditioning (HVAC) controls. The responsibility for this operational technology (OT), applies from the moment a device is provisioned, through to ongoing maintenance, repairs, and retirement.

However, when it comes to security, your devices have complex systems that require specialized work during the entire lifecycle from onboarding, to performing ongoing patch and vulnerability management.

Part of the process of setting a framework for securing your devices involves determining who will be implementing security standards and applications. In addition, devices need specially trained technicians to perform planned and corrective maintenance. Specific device discovery and security monitoring solutions are also needed to support these types of non-IT devices. If a security event or vulnerability is found there must be a clear process for remediation.

In the event of device disruption, patient safety, reputation, and liabilities are put at risk. The challenge is that your HTM team needs to ensure that medical devices and healthcare facilities systems have an appropriate security posture before the devices are put it into operation. You don't want devices deployed without being properly configured, and you need to have an audit trail of those configuration activities.

However, many mitigating controls for device intake don't follow a standard operating procedure because the controls are vendor specific or they're not achievable, such as fixed firmware that can't be updated. In addition, if there are controls, questions arise around what team or individual is responsible for performing the work.

Your healthcare organization may desire a specific medical device, but you have no standard procedures to evaluate the security posture of that device. Importantly, specialized skills and personnel are required in maintaining device security, tracking vulnerabilities, and prioritizing remediation.

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 equate to approximately 18.6 million medical devices in US hospitals.

These medical devices and the facilities in which they operate, together with the healthcare personnel diagnose and treat people to help them overcome injury or illness. The devices' availability, safety and reliability are core to a healthcare team's mission.

Healthcare organizations continue to be a target for malicious actors. In a recent identity breach report[3], the healthcare industry was shown to be the most targeted, accounting for 43% of all breaches of major industries in 2020.

The average time to identify and contain a breach is 329 days in the healthcare sector[4]. If that breach results in disruptions to infusions pumps, MRI machines or hospital HVAC systems, then clearly patient safety and the mission is put at risk.

From the moment a medical device or a healthcare facilities system is provisioned, implementing an appropriate level of device security requires compliance with best practices. Because it directly impacts the safety and availability of critical life sustaining technologies, fundamental secure operating procedures must be followed as part of maintaining a strong medical device and healthcare facilities system security posture.

Lifecycle Gaps - Medical Devices and Healthcare Facilities Systems Security

Your HTM team may not have an effective device lifecycle process in place that incorporates procedures to manage product security risk. Thus, your devices may not be secured properly, and your business may be unable to determine whether you're willing to take documented risks to use some devices. Or your IT security team can't determine the level of security for devices that were allowed in the environment. In addition to onboarding devices securely, your HTM team also needs to ensure device safety following routine planned maintenance or a return from off-site warranty work by a third-party vendor.

Without documented security standards, inconsistencies can occur when re-assessing a device post-warranty work. Establishing the most effective security standards for medical devices and healthcare facilities systems requires specialized knowledge, thorough development, testing, and overhead to keep the standards up to date.

> Without documented security standards, inconsistencies can occur when re-assessing a device post-warranty work.

People, Process & Technology

The challenge to secure device lifecycle management is further complicated when people, process and technology are not working together as detailed below:

People. Your HTM team needs a trusted device inventory resident in a single database, available wherever they work, on a mobile device, tablet, or laptop. HTM needs accurate reporting on device inventory with information reflecting security standards applied along with condition, disposition, and location of all devices.

Process. Without a way to accurately capture the full device lifecycle as part of a secure onboarding process, it's difficult to determine disposition, maintenance, and security. When a 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 device data model enables the technology to perform to expectations.

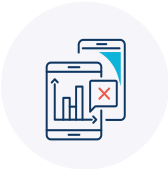
Technology. Complexity and ambiguity arising from using multiple computerized maintenance management system (CMMS) or other service management technologies will prevent your devices from achieving a successful security posture. Consolidating legacy CMMS onto a single, modern, device inventory and service management platform is a key first step for your enterprise. Without this commitment, your HTM team will struggle, and devices will accrue security risk over time.

These gaps in people, process and technology are summarized in Figure 1 below.

Multiple Device Inventories

Ineffective Secure Device Lifecycle Management from Intake to Retirement

No Common Data Model For Security Event Correlation



No Single Source of Truth

No Authoritative Source To Guide Evaluation And Secure Deployment

Timely Remediation Difficult Or Impossible To Achieve

Secure Lifecycle Management, Device Data & Remediation

Your HTM team needs security standards for medical devices and healthcare facilities systems. Then, when a device is onboarded or returned from offsite maintenance or warranty work, the standards act as the authoritative source to guide your HTM team to evaluate and securely deploy the device. These standards are validated by the device OEMs and tested by industry experts in your HTM department.

Once security standards are incorporated into the device lifecycle, your HTM team can then proactively improve device security posture. In addition, by leveraging people, process and technology device lifecycle security gaps can be narrowed. They can ensure that equipment is functional and optimized to meet patient safety, business continuity, regulatory, and security requirements with accountability through the entire technology lifecycle.

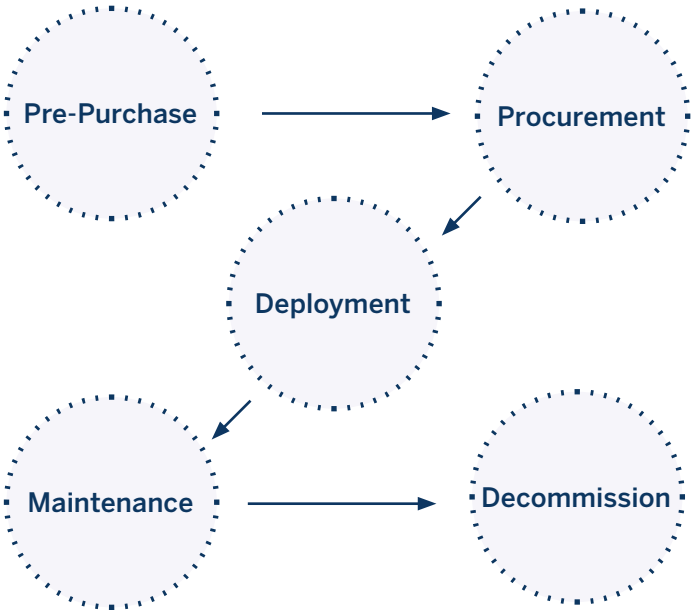
Along with secure onboarding of devices using security standards, ensuring persistent visibility, and monitoring and discovery of medical devices should be a standard everyday activity for medical device security professionals, with an appreciation and understanding of the growing importance of healthcare operations.

These resources help analyze vulnerabilities and provide a security event assessment and remediation recommendations. It is critical that only trained, certified, and authorized resources are utilized or dispatched to remediate the affected medical devices or healthcare OT. 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.

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

This combination of device expertise, modern technology and well documented and operationalized processes help keep your connected device fleet safe and resilient in the face of a rapidly growing medical device and healthcare facilities systems security threat for the entire equipment lifecycle as shown in **Figure 2.**

Security Operations within the Network-connected Medical Device and Healthcare OT Lifecycle



> No level of investment offers us 100% protection for our medical devices.
>
> With Nuvolo OT Security with industry leading standards solution we can close the gap as much as possible by ensuring that we can understand and mitigate risks to device safety, accessibility and availability.

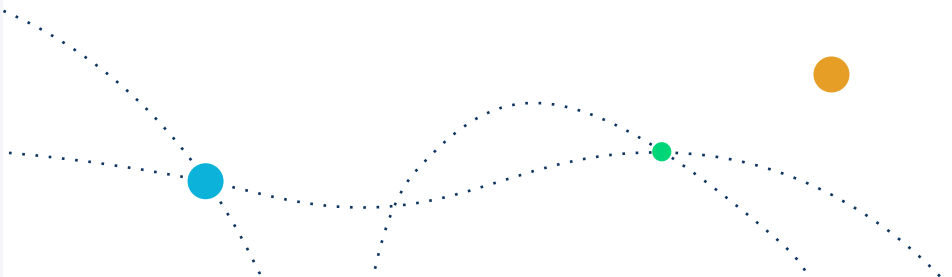
Full Visibility into Medical Device & Healthcare Lifecycle

The Mayo Clinic Healthcare Technology Management Cybersecurity team has created a standardized process for the implementation of device security procedures across the organization. This structured system and standardized approach to securing medical devices and healthcare facilities systems ensures they meet organizational and security requirements throughout their lifecycle.

This security framework is based on National Institute of Standards and Technology (NIST) and Association for the Advancement of Medical Instrumentation (AAMI) standards. These security standards are comprised of a template of activities that are applied as part of a secure device lifecycle management. This management includes initial device evaluation and onboarding through retirement.

Managing Medical Device and Healthcare Facilities System Lifecycles

Nuvolo OT Security leverages these leading healthcare standards developed by the Mayo Clinic, providing an operational workflow to enable robust asset security through the entire device lifecycle. This Nuvolo OT Security solution with industry-leading standards provides device context and correlation and an orchestrated and automated response, which ensures the rapid remediation of medical devices and healthcare facilities systems affected by security events.



Operational Flow using Nuvolo OT Security with Industry Leading Standards

Nuvolo OT Security with industry leading standards solution includes a comprehensive security package for the secure onboarding and lifecycle management of your medical devices and healthcare facilities systems. Nuvolo also provides a trusted medical device inventory, resident in a single database and available from any mobile or desktop platform. The healthcare standards integrate seamlessly with the Nuvolo asset management system to provide asset level security visibility and operational workflows for your fleet of connected medical devices and healthcare facilities systems.

By capturing the full lifecycle, as part of a standard medical device onboarding process, the disposition, maintenance, and security can be well established. When a security threat, vulnerability or exploit occurs, rapid remediation is achieved leveraging a common data model for matching, contextualization, and security event correlation. The process of creating a standard medical device data model enables your technology to perform to expectations.

This library of manufacturer and model specific risk remediation procedures, developed by Mayo Clinic, is made up of a template of activities that are applied to your device evaluation and onboarding as part of your device lifecycle management. These activities include settings such as strong default passwords, confirming installation of the latest software patches, and vendor recommended network and security settings.

This device lifecycle management using leading healthcare standards that are made up of operationalized processes is shown in Figure 3.

Figure 3 – Industry Leading Healthcare Standards for Connected Devices

This proactive approach adds significant value to the Nuvolo medical device security solution and an orchestrated and automated response for the rapid remediation of devices affected by security events. Nuvolo OT Security with industry leading standards solution together provide a simple, achievable, and operational security solution for your healthcare organization.

Nuvolo Provides the Operational Tools to Execute and Automate Security Operations

- Robust CMMS solution (lifecycle maintenance)
- Enterprise asset management solution
- Flexible and robust work orders
- Support risk scoring and modeling
- Support vulnerability management module
- Create device lifecycle profiles, and remediation plans for mitigation efforts
- Integrate with configuration management database (CMDB) and other enterprise security tools

An example of how to manage the medical and facilities device lifecycle is shown in Figure 4 below:

Figure 4 – Nuvolo OT Security with Industry Leading Standards Device Lifecycle Management & Visibility

Features: Nuvolo OT Security with Industry Leading Standards Solution

Nuvolo OT Security with industry leading standards includes the following capabilities that are required for the end-to-end secure lifecycle management of your medical devices and healthcare facilities systems:

→ Equipment security management

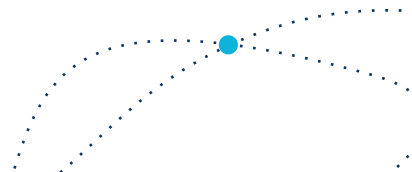
From security assessment to disposition within your organization Nuvolo medical device security with leading healthcare standards provide the ability to record and track comprehensive asset detail, including model specific security risks and remediation procedures.

- Record and track risks and remediation
- Perform security risk assessment on devices using baseline security criteria prior to making purchase decisions
- Know what information is stored in the device if it's connected to the network
- Data sanitization after use to prevent unintentional disclosure of information

→ Vulnerability management

The healthcare standards include end-to-end vulnerability management components; including ability to track vendor follow-up relating to specific disclosure notifications or alerts. In addition, it includes an engine to drive remediation efforts related to your connected medical device fleet.

- Document vendor inquiry, vendor response, and accepted/unaccepted remediation steps
- Vendor provides information on mitigation to address device weakness prior to use
- Includes pre-determined security controls as part of the deployment
- Enhance computerized maintenance management system (CMMS) asset inventory with attributes for vulnerability management activities such as operating system and third-party software, firmware updates and, information on communication protocol
- Track software vulnerabilities from various sources such as internal threat intelligence and external such as the NIST (National Institute of Standards and Technology) National Vulnerability Database
- Prioritize remediation in the context of impacted asset and patient impact, exploitability, and exposure
- Standardize patching procedure; by model, by type; creating work order for tracking completion and status
- Monitor and track status of all remediation
- FDA Post Market Guidance for patching, that provides recommendations for managing post market cybersecurity vulnerabilities for marketed and distributed medical devices



Risk remediation plans

The healthcare standards also include model specific security profiles, providing a summary of risks and roadmap of suggested controls to secure complex and variable devices. The profiles have been developed while considering sensitivities related to the proprietary nature of vended devices and industry regulatory requirements. In addition, the suite also leverages a library of standard security remediation procedures for the lifecycle of medical devices.

- Assign ownership to the authorized device engineer
- Provide instructions to remediate risks
- Deploy, track, and apply security mitigations using device security lifecycle profile
- Address ongoing security issues through a vulnerability management process that includes patching and mitigating controls

Reporting

Customizable dashboard security metrics encompassing the entire lifecycle of your connected medical device fleet. These reports can be crafted to be shared from the C-Suite to operational service teams.

Medical Device Security Workflow Management

The healthcare standards include asset specific risk remediation assignment and tracking features and provides the same look and feel as the standard enterprise asset management workflows via the Nuvolo CMMS

- Orchestrated and automated work orders that are tied to remediation tasks
- Remediation task and work order ticket ties back to the findings
- Security Risk Scoring- Based on customizable security attributes and remediation status the solution provides comprehensive risk scoring at the device, model, and fleet level.
- The risk scoring that combines the extent of the weakness and the value of the asset. This drives the remediation steps to address the vulnerabilities and weaknesses

Third Party Integration

Integrating and capitalizing on best-in-class risk management and automated asset identification tools. For a list of Nuvolo technology collaboration businesses visit www.nuvolo.com/solution/cyber-security/

Benefits: Nuvolo OT Security with Industry Leading Standards Solution

- Achieve secure onboarding and ongoing lifecycle management of your medical devices and healthcare facilities systems to reduce risk to patient safety and ensure accessibility and availability
- Facilitates the secure network onboarding of connected medical devices by operational support teams to meet organizational security requirements
- Meet executive requirements with detailed reporting on device risk assessment and mitigation status
- Help ensure the accessibility and availability of medical devices and healthcare facilities systems by leveraging tried and tested security standards
- Reduce the risk to reputation and exposure to legal liabilities from compromised and uncorrected devices

> Nuvolo OT Security solution with industry leading standards leverages a process developed by Mayo Clinic sets a world class standard for how to secure medical devices and facilities devices within an organization. Our structured process helps us assess what things are coming in, using instructions for applying security controls or applying security measures to equipment that are very digestible understandable and achievable."

nuvolo

You can learn more about Nuvolo OT Security for healthcare and the standardized process developed by Mayo Clinic for the implementation of device security procedures across the organization at **nuvolo.com/leadingstandards**

[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] ForgeRock Consumer Identity Breach Report 2020 https://www.forgerock.com/resources/2020-consumer-identity-breach-report

[4] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/