Ensure Non-IT Device **Safety**, **Accessibility** and **Availability**

Benefits

Real-Time security alerts
Proactively identify vulnerable connected devices before they can be exploited. Cynerio provides continuous device discovery and security assessments that notify Nuvolo OT Cyber Security when issues arise.

Streamlined remediation workflow
Generate maintenance work orders automatically based on real-time alerts from Cynerio's security monitoring system. Close the loop on determining the risk of a cyber attack and take quick measures to remediate the threat on any vulnerable connected devices.

Rogue device discovery

Cynerio continuously monitors every device on the network, whether it's a new device or an existing device that constantly changes locations. Real-time alerts sent to Nuvolo OT Security generate inspection requests so devices can be validated and logged in the inventory.

Pre-emptive maintenance

Cynerio tracks device utilization data healthcare organizations can leverage to ensure required maintenance doesn't interfere with critical medical services.

Respond Faster to Vulnerabilities in Medical Devices

Healthcare organizations must ensure the safety, accessibility and availability of their connected devices to guarantee continuous services, patient safety and confidentiality. With the proliferation of *network-connected* devices, your health technology management (HTM) and IT security teams are entering uncharted territory. That's because tracking, monitoring and patching devices for security risks can be complex and time consuming.

That's where Cynerio and Nuvolo have you covered.

Nuvolo provides the integral identification, service management of the OT device events and life-cycle processes with full visibility across IT, security, and OT teams.

Cynerio discovers and profiles every connected device, from Enterprise IoT to OT and IoMT, and contextualizes behavior based on clinical impact. Nuvolo receives OT device information into a single trusted device data source. This data is enriched by clinical engineers and IT security professionals during the entire device lifecycle, using a cloud-based mobile app. Cynerio provides network-wide security event information to Nuvolo and together, Cynerio and Nuvolo correlate all OT devices to security events, along with clinical context.

Nuvolo enables expedited work-order dispatching and full visibility into lifecycle processes across clinical engineering and IT security teams.

Customers choose Cynerio and Nuvolo for two main reasons:

#1: Network-connected device discovery and maintaining an accurate, cloud-based, single trusted inventory.

#2: Faster response to OT cyber security threats by utilizing advanced monitoring technology and streamlined processes driven by health technology management (HTM) device and IT security experts.

- **Device Inventory**
- **Customizable Reporting**
- **Remediation Workflow**
- **Real-Time Monitoring & Alerts**
- **Recognize Rogue OT Devices**
- **Secure Mobile Application**

Solution Value

Accurate asset inventory

Empower supervisors with accurate inventory data, detailed metrics on device performance, and current patch levels to make maintenance decisions for outdated and vulnerable equipment.

Auto-generated segmentation policies

Identify vulnerable devices connected to the network and automatically define segmentation policies that can be pushed to the firewall and NAC.

Lifecycle management

Automate the onboarding process for new devices and perform the documented checklist steps when retiring devices.

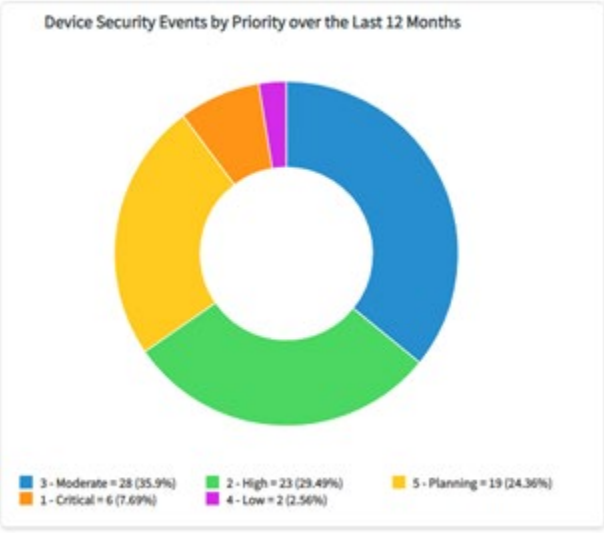
Discover the **Cynerio** and **Nuvolo OT Cyber Security** Solution Advantage

Nuvolo OT Cyber Security acts as the intelligence hub as a system of enrichment and engagement and action for security events.

For devices that need urgent action, the Nuvolo OT Cyber Security solution speeds up your cycle time by automatically assigning the correct clinical engineer or IT security professional immediately.

Nuvolo OT Cyber Security enables intelligent work order routing to identify the specific engineers and IT security professionals with the skills and certifications to perform the corrective maintenance to address the security issue.

Cynerio knows the vulnerabilities and risk impact of specific device models and can automatically define segmentation policies to limit vendor access to appropriate devices and safeguard the security of ePHI. Segmentation policies can then be tested for violations, fine-tuned, and approved before being enforced on the live network to ensure continuous medical services and patient safety. This real-time functionality proactively protects critical devices that cannot be patched and only allows authorized connections.



sales@nuvolo.com | +844-468-8656

For more information about how Nuvolo ensures the safety, accessibility, and availability of medical devices, contact a Nuvolo sales representative or visit the website. www.nuvolo.com

info@cynerio.com

For more information about the Cynerio device security and management solution, contact a Cynerio sales representative or visit the Cynerio website.

www.cynerio.com