

Secure IoMT and Improve Operational Efficiency by Maximizing Medical Device Utilization in Real-Time

Strengthen medical device security, reduce cyber risk, and improve operational efficiency with a unified approach to securing IoMT, IoT, and OT assets through risk prioritization, configuration control, and device hardening.



305-828-1003



info@infosightinc.com

Secure Medical Devices Beyond Basic Visibility

Most solutions stop at device inventory and vulnerability lists. Real improvement comes from understanding exposure, controlling configuration drift, and reducing risk in ways that also improve operational efficiency. This approach helps healthcare organizations strengthen medical device security, reduce cyber risk, and improve operational performance across IoMT, IoT, and OT environments.

1) Gain visibility that drives action

Go beyond basic inventory with deeper insight into device exposure, connections, and risk. See where vulnerabilities matter most, understand attack paths, and use risk simulation to prioritize the actions that strengthen security with less operational disruption.

2) Detect issues earlier and investigate faster

Identify abnormal behavior sooner and investigate with greater speed and context. Anomaly detection, policy monitoring, rule creation, and packet capture help teams understand what changed, what is at risk, and what needs immediate attention.

3) Reduce risk and strengthen control

Lower cyber risk and improve device security through patching, password management, segmentation, hardening, and configuration control. Built-in change tracking and recovery support also help maintain operational stability and audit readiness.

BUILT FOR HEALTHCARE ENVIRONMENTS

- Healthcare-specific device coverage
- IoMT imaging scan details
- Recall visibility
- Machine learning-based device classification
- MITRE-based exploitability analysis in your environment
- Validated recommendations to reduce attack vectors
- Pre-purchase risk analysis for safer device decisions
- Automated firmware deployment for supported IoT devices
- Safer known device configuration guidance

Secure medical devices more effectively, reduce cyber risk with greater precision, and improve operational efficiency with stronger visibility, faster investigation, and better control over device change and exposure.

**Exposure clarity through inventory, traffic mapping, vulnerability prioritization, and risk simulation.
Faster investigation through anomaly detection, packet capture, and policy monitoring.
Stronger control through patching, segmentation, hardening, configuration management, and audit-ready change history.**

Visibility & Inventory (built for IoMT reality)

AI + deep packet inspection builds a comprehensive inventory with normalized device intelligence for faster results.

IoT Patching (remediation at scale)

Firmware updates for common IoT devices in a few clicks—solving scattered patch repositories, inconsistent manufacturer processes, and the manual overhead of tracking/deploying patches.

Threat Detection (policies without complexity + evidence on demand)

Built-in anomaly detection, centralized packet capture, and policy-based detection from network traffic without complex coding; packet capture on any device accelerates response and investigations.

Vulnerability Prioritization (exploitability, not noise)

Exploitable vulnerability pinpointing with device and manufacturer context (MDS2s, SBOMs), auto-prioritized by real-time risk. Security gets precise remediation steps; clinical engineering gets safe, actionable guidance with zero risk to device functionality.

ProSecure (stop risk before it enters)

Automated risk assessments before purchase/upgrade, side-by-side comparisons, and upstream prevention before devices connect to the network.

Configuration Control (the blind spot most programs ignore)

Complete configuration snapshots for IoMT/IoT/OT devices, monitoring, reversion to known-good states, audit readiness, and stronger detection—built to combat configuration drift caused by software, people, and manufacturer access.

THE INFOSIGHT DIFFERENCE

- ✓ Assessment(s) OT/SCADA Cybersecurity Risk Assessment + IT Security Assessment if needed or desired.
 - a. Platform Solution + Project Mgt + Implementation
 - b. Platform Training & Support
- ✓ 24x7 IoMT MDR Threat Defense & Incident Response + SOCaaS for IT Assets if required/requested.
- ✓ Complementary GRC Services – HIPAA Security & Risk Assessment, vCISO, Cyber Controls Reviews, BCP/DR, Governance and Risk Management Services

TAKE THE NEXT STEP

Get an IoMT exposure readout with prioritized mitigation actions

