# Cynerio and Keysight: Reduces Cyber Risk for IoMT Devices

Overview

Security in a healthcare environment is crucial because lives and sensitive data are on the line. Many hospitals and other medical facilities are taking advantage of ubiquitous wireless networking to roll out connected medical devices to help diagnose and monitor patient health. These devices are knowns as *internet of medical things* (IoMT). Connected medical devices, however, are frequently opaque to conventional IT management tools, making them nearly impossible to protect and secure.

What's needed is a security tool that not only understands medical devices and the IoMT ecosystem but can also determine the function of IoMT devices and the context of their behavior without disrupting patient care or network operations. That way you can prioritize risks based on their potential impact on patient safety and patient care. Cynerio's security solution, working together with the Keysight Network Visibility solution, provides the healthcare-driven behavior analysis necessary to give IT teams insight into IoMT networks.

Sample Keysight and Cynerio Joint Deployment
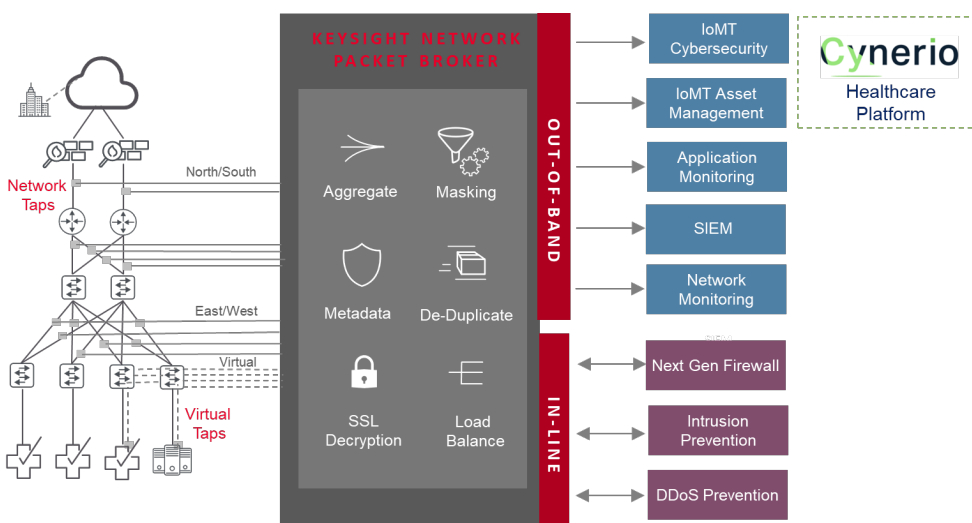
How it works: Keysight's Network Visibility solution includes Taps, and Network Packet Brokers which provide aggregation, de-duplication, and passing exactly the right data to Cynerio and other tools.

Key Benefits

- **Detect Cyber risks:** Identify vulnerabilities that can lead to conditions for ransomware and malware on Medical Devices
- **Pervasive visibility:** Traffic from throughout a healthcare facility's network can be collected and analyze by the Cynerio IoMT security solution
- **Deduplicated packets:** Removes duplicate packets from traffic harvested across network cutting down on unnecessary tool overhead
- **Inspect encrypted traffic:** Decrypts SSL traffic for out of band inspection and analysis
- **Data masking:** Obfuscates personal patient information to avoid compliance violations
- **Metatdata generation:** Unsampled Netflow/IPFIX metadata is provided to Cynerio for additional analysis

KEYSIGHT TECHNOLOGIES

Cynerio: Healthcare IoT Cybersecurity Platform

Cynerio's focus is to identify risks on Medical Devices and provide actionable mitigations strategies to reduce or eliminate those risks. Cynerio detects and classifies new IoMT devices as they come online and is able to provide a healthcare centric analysis of the potential threats and vulnerabilities these devices present. Cynerio can analyze network data, provide mitigations strategies, test those strategies, and route it to third-party integrated tools when ready to enable the migration.

Cynerio's security solution is based on the industry's first technology that thoroughly analyzes the medical workflows in the IoMT ecosystem. Cynerio provides an ongoing healthcare specific risk analysis that accurately detects anomalies and stops threats, preventing service disruption, data theft and compliance violations. Cynerio's cybersecurity solution provides continuous discovery and classification of connected medical and IoT devices, visibility into the associated risk for each connected device with clinical context, and protection against cyber-attacks.

Keysight: Deliver the Right Data from Everywhere in your Healthcare Network

Cynerio, through the Keysight Network Visibility solution, connects to IoMT networks out-of-band, which means it doesn't interfere with network traffic or clinical workflows. Keysight enables traffic from across the network to be managed and delivered efficiently and in the correct format. Traffic is collected, aggregated, and optimized to ensure Cynerio has access to all the network traffic as efficiently as possible. For example, Keysight removes duplicate packets when traffic is collected from different parts of the network, and Cynerio removes personal patient information (ePHi) so that security analysts need not see it, an important consideration for compliance.

To ensure that Cynerio doesn't miss any potential threats lurking in an IoMT network, Keysight decrypts SSL-encrypted traffic for inspection and provides extended metadata such as Netflow/IPFIX that can drive detailed, contextual analysis of network and security events. Keysight then processes the monitoring data and filters out unnecessary data packets so that Cynerio and other monitoring tools get the right set of data that it needs to perform its job function. Keysight load balancing ensures that tools can have enough inspection capacity, even as network traffic surges.

About Cynerio

The Cynerio Healthcare IoT platform provides healthcare facilities with a comprehensive suite of solutions that caters to every IT need, from healthcare-safe Zero Trust cybersecurity to asset and risk management. Our platform covers every medical/IoMT, Enterprise IoT and OT system in the healthcare environment plus every threat vector, equipping hospitals with the tools, insight, and control they need to get cyber-secure fast and stay secure. www.cynerio.com

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications, or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus