Cynerio
Secure. Faster.

Solution Brief

&

KEYSIGHT TECHNOLOGIES

Cynerio and Keysight: Reduce Cyber Risk for Medical & IoT Devices

Overview

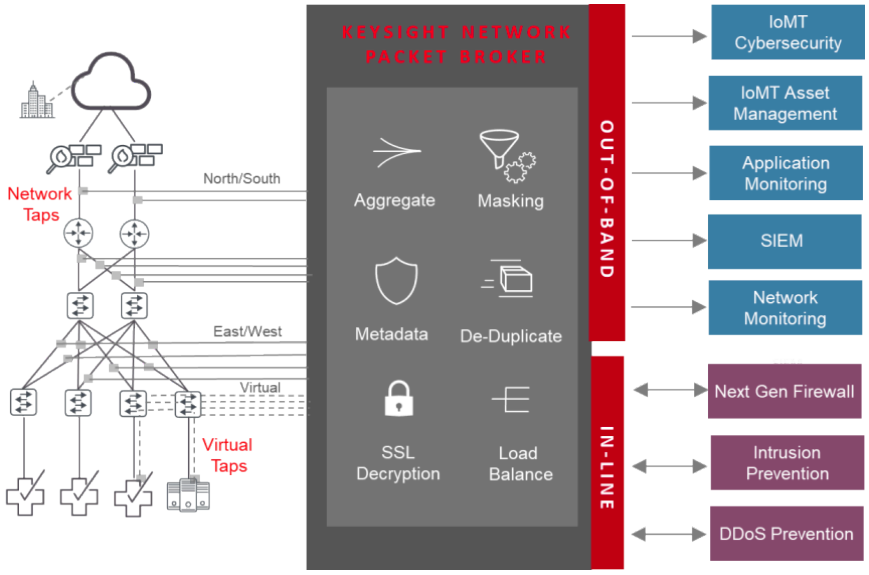
Security in a healthcare environment is crucial because lives and sensitive data are on the line. Many hospitals and other medical facilities are taking advantage of ubiquitous wireless networking to roll out connected devices to help diagnose and monitor patient health. Connected medical devices, however, 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 IoT ecosystem but can also determine the function of connected devices and the context of their behavior — without disrupting network operations. That way, hospitals can prioritize risks based on their potential impact on patient safety and patient care. Cynerio security, working together with the Keysight Network Visibility solution, provides the healthcare-driven behavior analysis necessary to give IT teams insight into IoT and medical device networks.

Key Benefits

- **Detect Cyber Risks:** Identify vulnerabilities that can lead to ransomware and malware attacks on medical devices
- **Pervasive Visibility:** Traffic from throughout a healthcare facility's network can be collected and analyzed by the Cynerio IoT security solution
- **De-Duplicated Packets:** Removes duplicate packets from traffic harvested across the 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

Sample Keysight and Cynerio Joint Deployment

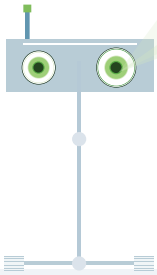


Cynerio Healthcare Platform

How it works: Keysight's Network Visibility solution includes taps and network packet brokers which provide aggregation, de-duplication, & directing exactly the right data to Cynerio & other tools.

Cynerio
Secure. Faster.

Healthcare IoT Cybersecurity Platform



Cynerio's focus is to identify risks on medical and other connected devices and provide actionable mitigation and remediation strategies to reduce or eliminate those risks. Cynerio detects and classifies new IoT devices as they come online and can provide a healthcare-centric analysis of the potential threats and vulnerabilities these devices present. Cynerio can analyze network data, provide mitigation strategies, test those strategies, and route them to third-party integrated tools when ready to enable the comprehensive mitigation and remediation of the threats it identifies.

Cynerio's security solution is based on the industry's first technology that thoroughly analyzes and secures the medical workflows in an IoT 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 device with clinical context, and protection and response against cyber-attacks.

KEYSIGHT TECHNOLOGIES

Deliver the Right Data from Everywhere in Your Healthcare Network

Cynerio, through the Keysight Network Visibility solution, connects to IoT 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. Keysight can also mask personal health information so that security analysts don't need to see it, an important consideration for compliance.

To ensure that Cynerio doesn't miss any potential threats lurking in an IoT 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 enables sharing traffic with other tools — such as network and performance monitoring products — replicating and filtering to ensure each tool precisely gets the traffic it needs. Keysight load balancing ensure tools can have enough inspection capacity, even as network traffic surges.

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. We provide hospitals the control, foresight, and adaptability to keep their rapidly growing IoT footprint cyber-secure in a constantly evolving threatscape. Our solutions empower hospitals to stay compliant and proactively manage every device connection with powerful IoT threat detection, mitigation, and response tools, so that they can focus on healthcare's top priority: delivering quality patient care. Follow us on Twitter @Cynerio. visit us at cynerio.com or write us at info@cynerio.com.

C· Forrester Wave Leader 2020

C· Gartner Cool Vendor 2020