Cynerio
Secure. Faster.

Solution Brief

& IBM QRadar

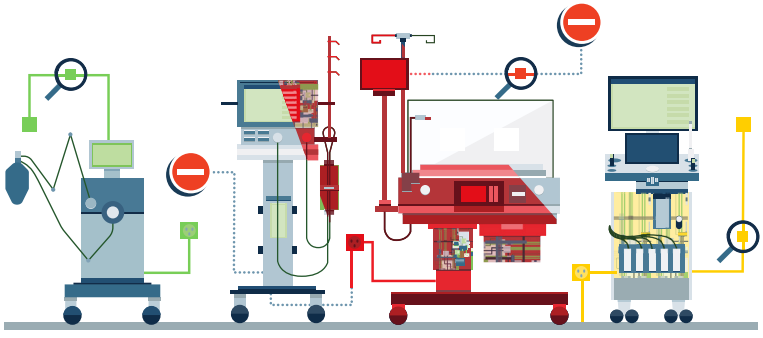
# QRadar SIEM and Cynerio: Optimizing Healthcare IoT Cybersecurity

## Unleashing Powerful Integration

The Cynerio--QRadar frictionless integration infuses risk identification and security event monitoring in healthcare environments with clinical context, enabling expedited threat remediation and incident response while ensuring patient safety, data confidentiality, and clinical operational continuity. Cynerio's integration with QRadar's products streamlines medical-specific data consumption and processes. Together, they empower healthcare IT security departments and SOC teams with a centralized, single-pane-of-glass view into clinically contextualized medical/IoMT device behavior and analysis.

## The Growing Threat to Healthcare IoT

As healthcare suffers relentless barrages of cyber attacks, identifying at-risk devices and vulnerabilities, managing risk, and remediating threats have become progressively more difficult. Weak security and widespread use of devices running legacy firmware/OS combined with medical and IoT devices' inherent vulnerabilities (e.g. open services and ports, TCP/IP stack vulnerabilities), unique communications patterns, and traditional IT tools' inability to recognize medical/IoMT devices have made healthcare facilities easy and lucrative targets for threat actors. Executing clinically-blind risk management and incident response risks compromising device functionality, disrupting medical workflows and services, and even network slowdown or total shutdown. Patient safety and data confidentiality are paramount, meaning none of these scenarios is ever an option.



**Cynerio–QRadar integration expedites healthcare-safe Zero Trust risk management and security incident response**

## Solution Components

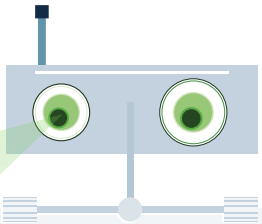
- Cynerio Healthcare IoT Cybersecurity Platform
- QRadar SIEM
- QRadar on Cloud

## Integration Benefits

- Real-time risk detection with alerts sent to relevant team members
- Ongoing monitoring of device behavior enriched with clinical context
- Easy incident detection, investigation, and diagnosis with end-to-end observability with QRadar
- Frictionless multi-site deployment, and agentless, network-based monitoring
- Automated and continuous, real-time Healthcare IoT asset (medical/IoMT, Enterprise IoT, and OT) discovery and fingerprinting data is passed to QRadar
- Stay compliant with HIPAA, GDPR and other global regulations and simplify audits

## How It Works

The integration between IBM Security QRadar SIEM and Cynerio's Healthcare IoT Cybersecurity Platform provides a suite of scalable healthcare-specific solutions developed to address the increasing cyber threats to healthcare. A centralized view into clinically-contextualized security events, vulnerabilities, and policy violations streamlines risk management and incident response and offers SOC and IT security teams the ability to easily monitor and enforce healthcare-safe policies on medical and IoT devices with the ease of enforcing them on standard IT assets.



**Cynerio's device discovery** inventories every connected device, whether it's a medical/IoMT device, Enterprise IoT device, or OT system, and automates ongoing inventory. Every asset is fingerprinted using deep packet inspection (DPI), and Cynerio provides granular, clinically-contextualized information on device communications, vendor, model, OS/firmware, version, MAC address, serial number, utilization patterns, VLANs, and more.

The **combined power of Cynerio's AI and in-house threat intelligence research team and IBM's QRadar SIEM,** pinpoints every at-risk Healthcare IoT device, identifies vulnerabilities (i.e. legacy firmware/OS, CVEs, open services, etc.), monitors for threats, and calculates device risk impact according to clinical context and mission criticality.

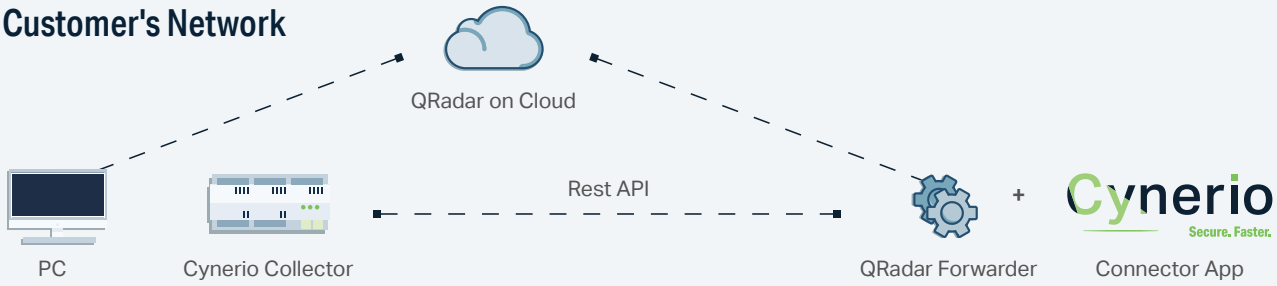
**IBM's QRadar SIEM ingests Cynerio's clinically-enriched data** and integrates it with its proprietary risk management solutions, alerts teams in real time to any suspicious/ anomalous activity, unmanaged devices, and newly discovered vulnerabilities.

Cynerio provides **step-by-step remediation paths** built on Zero Trust policies optimized for hospital-specific workflows and network topologies for every device, vulnerability, and risk.

Cynerio's **Virtual Segmentation capability** auto-configures robust, **healthcare-safe Zero Trust security policies** in seconds and allows them to be tested for violations and edited before they're enforced.

**The combination of Virtual Segmentation with QRadar's powerful violation monitoring facilitates streamlined risk management and automated incident response while ensuring the preservation of clinical workflows and patient safety.**

## Customer's Network




## Integration Components

Cynerio
Secure. Faster.

Cynerio's clinical security intelligence on every Healthcare IoT device can be easily consumed by QRadar products to streamline clinical risk management and automate incident response. The platform's healthcare-focused solutions adapt to rapidly evolving threats, technological advancements, and healthcare industry standards. Its AI-powered, full-suite Healthcare IoT cybersecurity platform empowers hospitals with the ability to act fast, ensure compliance, and achieve sustainable and robust security posture with foresight and easily deployable, scalable, and adaptable IT solutions tailored to healthcare.

IBM QRadar

### QRadar SIEM

IBM Security™ QRadar® Security Information and Event Management (SIEM) helps security teams detect, prioritize and respond to threats across the enterprise. It automatically analyzes and aggregates log and flow data from thousands of devices, endpoints and apps across your network, providing single alerts to speed incident analysis and remediation. QRadar SIEM is available for on-prem and cloud environments.

## Integration Benefits

- Clinically enriched risk scores calculated according to device risk impact
- Automated mitigation executes actions across security infrastructure in seconds
- Automation enables offloading of repetitive security tasks and enables staff to focus on mission-critical projects
- Frictionless and automated sync of complex workflows across every team and security tool facilitates a unified defense strategy with the QRadar product suite
- Healthcare-safe Zero Trust mitigation and incident response strategies infused with clinical context
- Ability to configure and test mitigating segmentation policies for violations before enforcing them with Cynerio's **Virtual Segmentation** capability

## 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.

Forrester Wave Leader 2020

Gartner Cool Vendor 2020