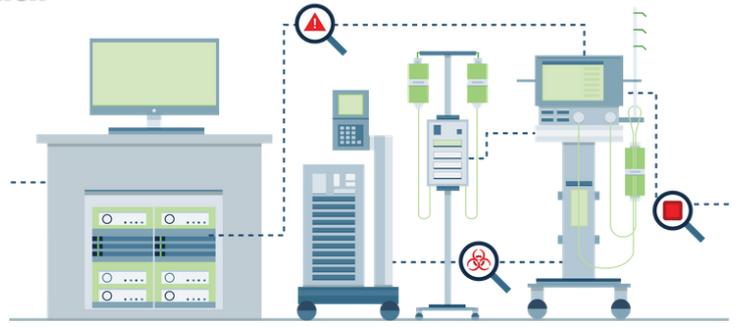


QRadar and Cynerio: Optimizing Healthcare IoT Cybersecurity with a Clinical SIEM



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.

How It Works

The integration between QRadar's SIEM solutions 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-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
- QRadar Advisor with Watson

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 Advisor
- 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



1. **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.

2. The **combined power of Cynerio's AI and in-house threat intelligence research team and QRadar's SIEM solutions**, 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.

3. **QRadar 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.

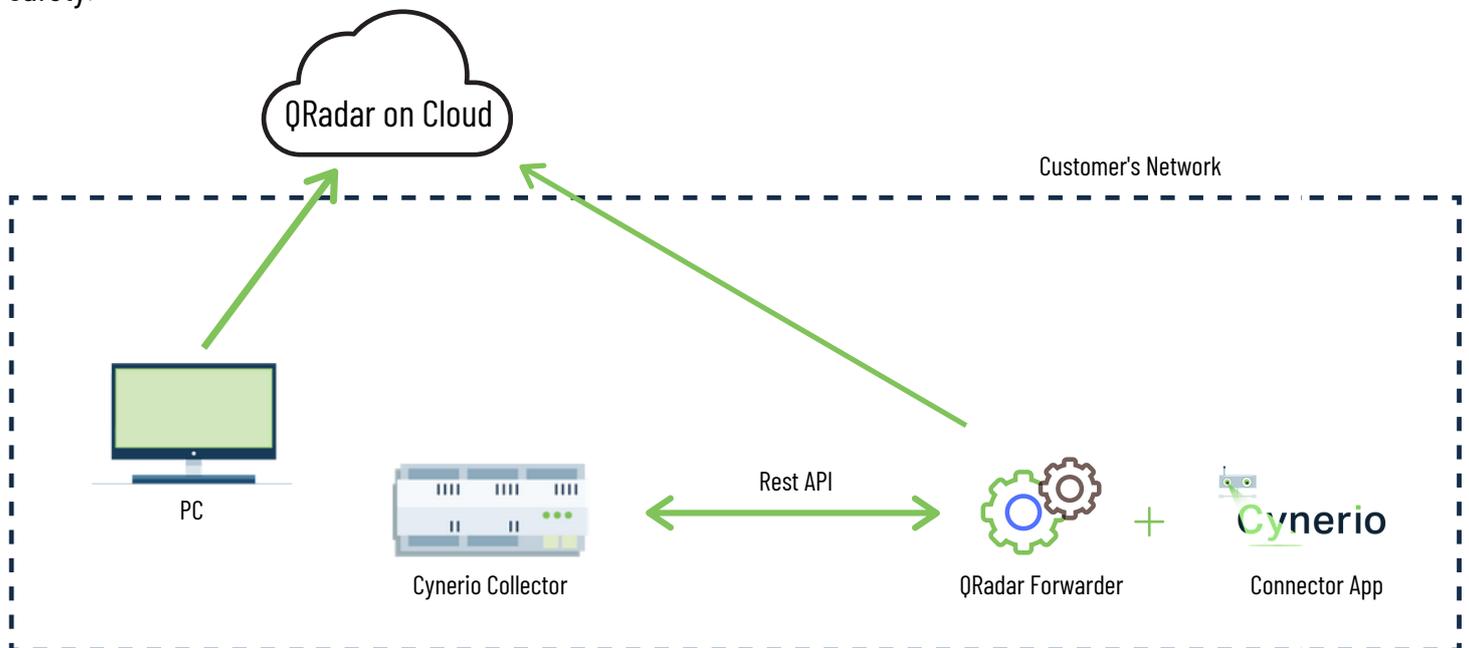
4. Cynerio provides **step-by-step remediation paths** built on Zero Trust policies optimized for hospital-specific workflows and network topologies for every device, vulnerability, and risk.

5. 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.

Integration Benefits (cont'd.)

- 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



Integration Components

Cynerio

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.

QRadar

QRadar SIEM

The QRadar SIEM is the analytics-driven SIEM solution that gives you the ability to quickly detect and respond to internal and external attacks. It makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results. Identify, prioritize and manage security events with event sequencing, alert management, risk scores, and customizable dashboards and visualizations. Gather all the context you need in one view to perform rapid investigations and response. Take care of existing and newly discovered threats fast with contextual threat detection and incident response.

QRadar on Cloud

QRadar on Cloud is a hosted SIEM designed to help you take action on attacks and network breaches before considerable damage is done. From infrastructure management to data compliance, QRadar on Cloud delivers elastic scalability and rapid time to value. Designed to ingest vast amounts of data and prioritize incidents, QRadar on Cloud enables real-time analytics to accurately identify threats and correlates activities to prioritize incidents.

QRadar Advisor

QRadar Advisor leverages advanced AI to automate routine SOC tasks and provide complete threat coverage, prioritize alerts, and expedite security investigations. With QRadar Advisor, security teams can automate tasks, orchestrate workflows and support a broad range of security operations center (SOC) functions and reduce dwell times by aligning attacks to the MITRE ATT&CK chain.

