



## Securonix & Cynerio Focus on Reducing the Risk of Connected Medical Devices

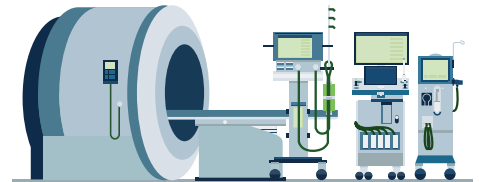
### Unleashing Powerful Healthcare IoT Security Integration

The Cynerio-Securonix 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 Securonix streamlines medical-specific data consumption and processes. Together, they empower healthcare IT security departments and SOC teams with a centralized view into clinically contextualized medical/IoT device behavior and analysis.



### Optimize Your SOC With 100% IoT Device Visibility and Control

The Cynerio and Securonix integration creates additional functionality by providing a bi-directional integration with the Securonix SIEM. The combined Securonix-Cynerio integration solution delivers unparalleled insight and incident response capabilities across all Medical Devices and associated OT (Operational Technologies), such as Facility Security Systems, HVAC and Internet of Things IoT. This includes, for example, printers, camera and card readers regardless of device or network tier.



### The Cynerio | Securonix Integration provides:

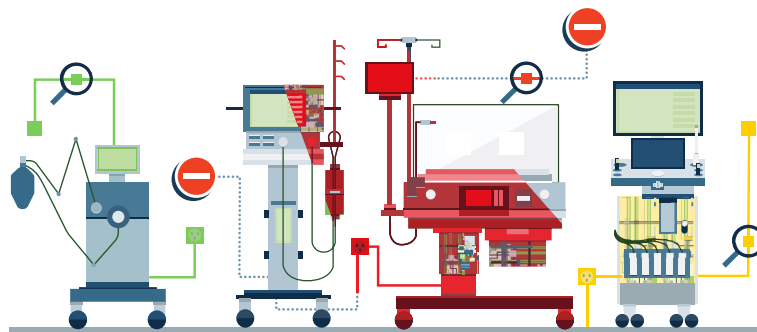
**1** Deep insights to 100+ medical device properties that are pre-correlated and continually fed by Cynerio to Securonix for real-time insight, long-term storage, trend analysis, visualization and incident investigation and response (SOAR)

**2** Correlation of high-value device context from Cynerio with other data sources in Securonix to better manage assets and rapidly identify and prioritize anomalous behaviors and events

**3** Accelerated incident response and results reporting with closed-loop policy-driven actions and workflows for full incident life-cycle managements

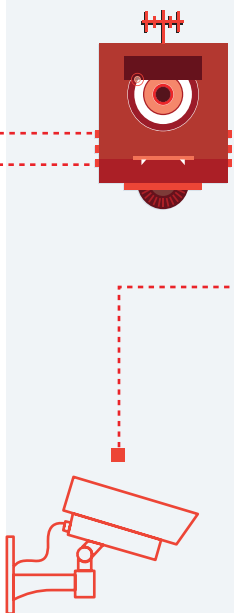
## How It Works

The integration between the Securonix Security Operations & Analytics Platform and Cynerio's Healthcare IoT Cybersecurity Platform provides a suite of scalable healthcare-specific solutions developed to address the increasing cyber threats to healthcare.



### Cynerio–Securonix integration expedites healthcare-safe Zero Trust risk management and security incident response

#### The Growing Threat to Healthcare IoT



As healthcare suffers relentless barrages of ransomware and other 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/IoT devices have made healthcare facilities easy and lucrative targets for threat actors.

Cynerio and Securonix have joined together to offer an industry-leading solution that captures the network and security information of medical devices. This comprehensive and real-time cyber status provides for risk analysis and an actionable mitigation strategy for every device. The metadata is shared with the Securonix Security Operations & Analytics Platform to display an expanded and actionable view of the larger cyber and network infrastructure including behavior (UEBA) of medical devices as well as many IT devices through integrations with the non-medical (IT) device environment.

The Securonix platform delivers healthcare-specific content that includes connectors to leading electronic medical record (EMR) applications, as well as healthcare-specific threat use cases that leverage Securonix security analytics capabilities. Securonix analytics go beyond the signature-based detection of legacy SIEM solutions to find unknown threats quickly. To do this, Securonix leverages the latest advances in machine learning and artificial intelligence to baseline normal behavior patterns, detect suspicious data access patterns, and identify threats to patient data, quickly and accurately.

#### Solution Components

**Cynerio**

Healthcare IoT Cybersecurity Platform

**+ securonix**

Operations & Analytics Platform



## Integration Benefits

- ✓ Real-time risk detection with alerts sent to relevant team members, ongoing monitoring of device behavior enriched with clinical contextual data
- ✓ Clinically enriched risk scores calculated according to device risk impact
- ✓ Frictionless and automated sync of complex workflows across every team and security tool facilitates a unified defense strategy with Securonix
- ✓ Easy incident detection, investigation, and diagnosis with end-to-end observability with Securonix
- ✓ Automated mitigation executes actions across security infrastructure in seconds
- ✓ Healthcare-safe Zero Trust mitigation and incident response strategies infused with clinical context
- ✓ Automated and continuous, real-time Healthcare IoT asset (medical/IoMT, Enterprise IoT, and OT) discovery and fingerprinting data is passed to Securonix
- ✓ Automation enables offloading of repetitive security tasks and enables staff to focus on mission-critical projects
- ✓ Ability to configure and test mitigating segmentation policies for violations before enforcing them with Cynerio's **Virtual Segmentation** capability

## Integration Features



**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 Securonix** 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.



**Securonix ingests Cynerio's clinically-enriched data** and integrates it with risk management solutions to discover new vulnerabilities, alert teams in real-time to suspicious/anomalous activity, and report unmanaged devices.



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.



A centralized view into clinically contextualized security events, vulnerabilities, and policy violations streamlines risk management and incident response that 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 policies on IT assets.

## Securonix and Cynerio: Better Together



The combination of virtual segmentation with powerful Securonix violation monitoring facilitates streamlined risk management and automated incident response while ensuring the preservation of clinical workflows and patient safety.

Cynerio's clinical security intelligence on every Healthcare IoT device can be easily consumed by Securonix 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 a sustainable and robust security posture with foresight and easily deployable, scalable, and adaptable IT solutions tailored to healthcare.

## securonix About Securonix

Securonix delivers positive security outcomes with zero infrastructure to manage. The Securonix platform automates security operations while our analytics capabilities reduce noise, fine tunes alerts, and identifies threats both inside and out of the enterprise. Securonix delivers analytics driven SIEM, SOAR, and NTA, with UEBA at its core, as a pure cloud solution without compromise. For more information visit [www.securonix.com](http://www.securonix.com).

## About Cynerio

**Cynerio** is the one-stop shop Healthcare IoT security platform. With solutions that cater to healthcare's every IoT need—from Enterprise IoT to OT and IoMT—we promote cross-organizational alignment and provide hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection and response and rapid risk reduction tools, so that they can focus on healthcare's top priority: delivering quality patient care. For more information, visit us at [www.cynerio.com](http://www.cynerio.com) or email us at [Securonix@cynerio.com](mailto:Securonix@cynerio.com).

