securonix

SOLUTION BRIEF

Securonix and Cynerio

Gain visibility to detect and respond to threats across your medical and IoT devices

The Growing Threat to Healthcare IoT

As cyberattacks targeting healthcare organizations continue, identifying at-risk devices and vulnerabilities is essential for threat detection and response. Healthcare facilities are lucrative targets because patient records are valuable. Additionally, these organizations have widespread use of devices running legacy firmware, and medical and IoT devices may also have inherent vulnerabilities such as open services and ports.

securonix | Cynerio

Why Securonix + Cynerio?

The combined solution allows you to optimize your SOC with deep insights from IoT and medical devices. A bi-directional integration delivers unparalleled detection and response across all medical devices and associated operational technologies (OT), such as facility security systems, HVAC, and IoT devices.

The Benefits

Our combined solution reduces the risk associated with connected medical devices and electronic medical records (EMR).

Understand When Anomalies Are a Threat

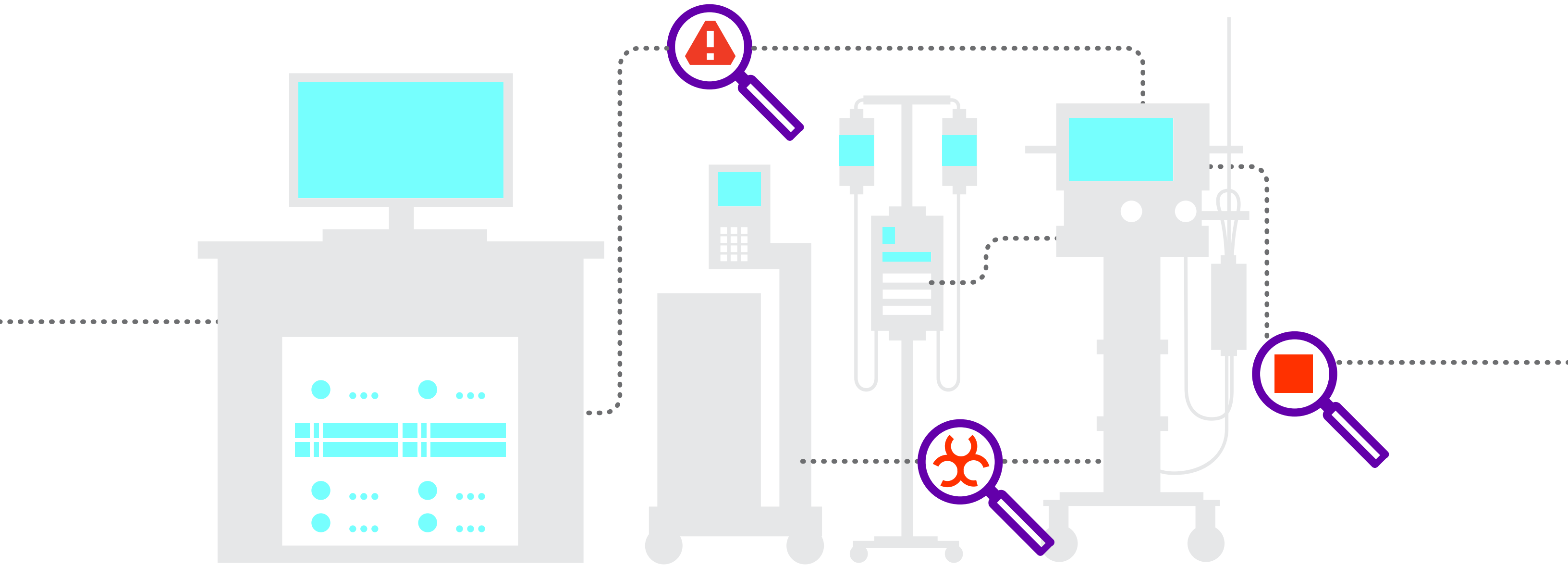
Get real-time alerts when anomalies are detected. Our joint solution continuously monitors medical device behaviors and enriches the data with clinical context to assign risk scores.

Adhere to a Zero Trust Framework

Cynerio provides step-by-step remediation paths built on zero trust policies optimized for hospital-specific workflows for every device, vulnerability, and risk.

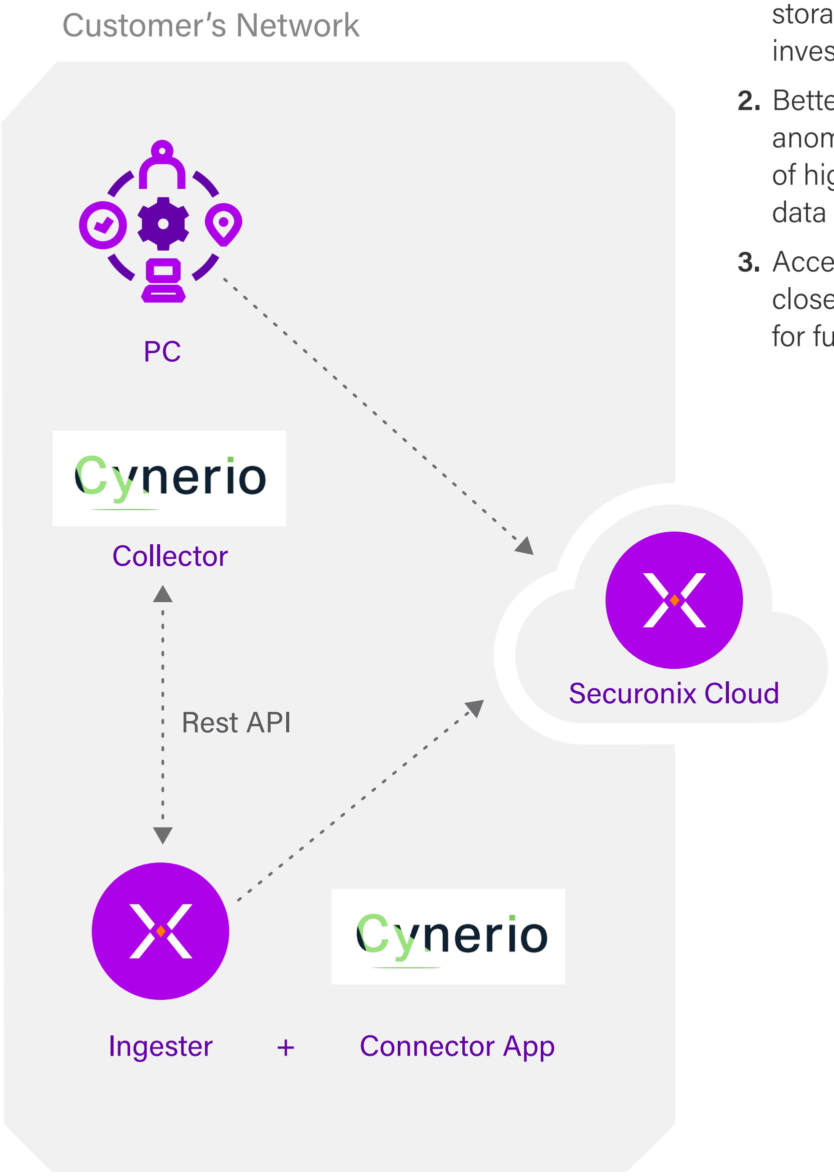
Reduce Resource Constraints

Execute actions across your security infrastructure in seconds with automated mitigation. This helps offload repetitive security tasks and enables your staff to focus on mission-critical projects.



How It Works

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



The Securonix and Cynerio Integration allows organizations to:

1. Gain deep insights into over 100 medical device properties that are pre-correlated and continually fed by Cynerio to Securonix in real time. Our joint solution provides actionable insights, long-term storage, trend analysis, visualization, and incident investigation and response.
2. Better manage your assets and rapidly identify anomalous behaviors and events with the correlation of high-value device context from Cynerio with other data sources from Securonix.
3. Accelerate incident response and reporting with closed-loop, zero trust driven policies, and workflows for full incident lifecycle management.

Top Features

The integration's robust feature set includes:

Centralized View: A centralized view into security events, vulnerabilities, and policy violations allows you to streamline risk management and incident response. SOC and IT security teams now have the ability to easily monitor and enforce healthcare safe policies on medical and IoT devices with the ease.

Industry-leading Analytics: Securonix analytics goes beyond the signature-based detection of legacy SIEM solutions to find unknown threats quickly. Leveraging the latest advances in machine learning and artificial intelligence, Securonix baselines normal behavior patterns and identifies threats to patient data, quickly and accurately.

Threat Content as a Service: The Securonix platform delivers healthcare-specifc content that includes connectors to leading electronic medical record (EMR) applications, as well as healthcare threat use cases that leverage Securonix's security analytics capabilities. Securonix will continue to release this content as requirements grow.

Device Discovery: Cynerio's device discovery inventories every connected device, whether it's a medical/IoT device, enterprise IoT device, or OT system, and automates ongoing inventory. Every asset is fingerprinted using deep packet inspection (DPI), so you have granular, clinically contextualized information on device communications, vendor, model, OS/firmware, serial number, utilization patterns, and more.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo.