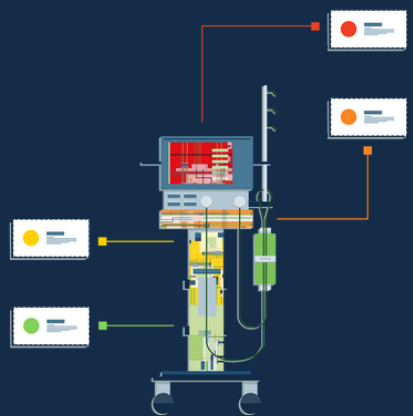
Cynerio | cisco

Cisco ISE and Cynerio Healthcare IoT Solutions:

Enhanced Security with a NAC for Healthcare Environments



Executive Summary

Cynerio and Cisco SecureX have joined forces to give healthcare facilities unparalleled actionable insights into clinically contextualized risk. The frictionless Cynerio–Cisco ISE integration provides healthcare organizations with optimal, real-time risk mitigation plans built on the NIST Zero Trust framework to guarantee network security, operational continuity, data integrity, and patient safety.

Healthcare IoT's Unique Challenges

Inadequate security combined with Healthcare IoT devices' (medical/IoMT, Enterprise IoT, and OT systems) inherent vulnerabilities have made the healthcare industry threat actors' easiest, most lucrative, and most propitious target.

50%

More than half of hospitals don't conform to NIST guidelines

90%

of all healthcare organizations have reported a breach

40%

of all connected medical devices run an unsupported OS

300%

rise in cyber attacks since January 2020

The Healthcare IoT Surge & the Expanding Threat Landscape

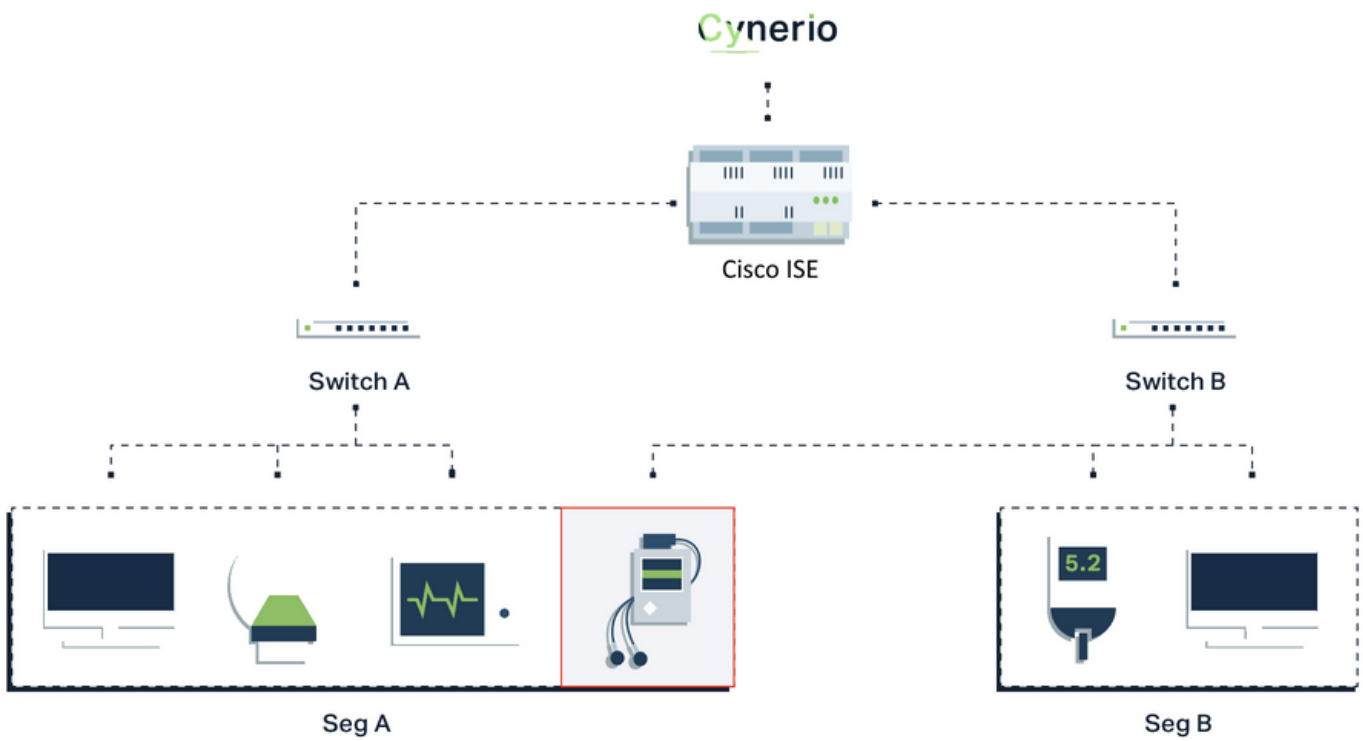
The growing footprint of connected medical and IoT devices has transformed the healthcare industry by accelerating medical procedures and providing patients with more control over their data, care regimens, and greater accessibility to treatment. Despite the conveniences, these advancements expand healthcare organizations' attack surfaces, exposing them to bad actors and cyber exploitation.

Widespread use of devices running vulnerable firmware or unsupported operating systems that cannot be updated leaves segmentation as the only option for mitigating risk in clinical environments. However, traditional IT tools lack clinical context and fail to successfully secure vulnerable healthcare networks. Segmenting clinical networks without a deep understanding of Healthcare IoT's unique communications patterns and network topology, device criticality, and medical impact risks disrupting device functionality and jeopardizing critical medical services.

The Power of Cynerio–Cisco ISE Integration

How It Works

1. **Cynerio enriches device and network data with medical context and complete visibility into Healthcare IoT assets (medical/IoMT, Enterprise IoT, OT systems)** to provide unparalleled insights into asset locations, communications, criticality and impact profiles, and risk assessments.
2. **Operational insights** provide healthcare security teams with comprehensive and actionable data on Healthcare IoT device usage (including granular breakdowns of weekly, daily, and hourly utilization patterns), criticality, and impact on patient outcomes.
3. **Cynerio's Virtual Segmentation** ensures confidence in clinical service continuity and patient safety. This capability automatically generates robust, hospital-specific segmentation policies that can be tested, validated, and edited before enforced on the live network.
4. The **Cisco SecureX Identity Services Engine's (ISE) best-in-class NAC** enables automatic policy enforcement, microsegmentation, and threat response to secure complex clinical networks against cyber threats of any sophistication level.



Use Cases

Build Security Policies Enriched with Medical Context

Hospitals using the SecureX platform and Cisco Identity Services Engine (ISE) benefit from centralized management, access control, streamlined device onboarding, and endpoint posture services. Integration with Cynerio provides medical context and ensures continuous medical services. Every device (e.g. X-Ray machines, IV pumps, security cameras) is detected, and identified (e.g. model, vendor, serial number, OS). Risk scores derived from medical and IoT devices' criticality, medical impact, and inherent vulnerabilities enrich Cisco ISE's robust solution.

Enable Safe Healthcare IoT Segmentation

The Cynerio–Cisco ISE integration enables hospitals to enforce a security policy they can be confident will protect their clinical network while ensuring uninterrupted clinical services. Cynerio's Healthcare IoT security solution detects devices and identifies them, profiles their network behavior, and generates segmentation policies according to device criticality and medical impact. Cynerio's Virtual Segmentation capability enables hospital security teams to define and validate security policies to ensure their safety and be confident medical services continue uninterrupted once they are pushed to Cisco ISE and enforced through the NAC.

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. With solutions that cater to healthcare's every IT need—from Enterprise IoT to OT and IoMT—we promote cross-organizational alignment and give hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We give you the power to stay compliant and proactively manage every connection on your own terms with powerful asset management, threat detection, and mitigation tools so you can focus on healthcare's top priority: delivering quality patient care. For more information, visit us at www.cynerio.com

About Cisco ISE

The Cisco ® Identity Services Engine (ISE) is your one-stop solution to streamline security policy management and reduce operating costs. With ISE, you can see users and devices controlling access across wired, wireless, and VPN connections to the corporate network. Cisco ISE allows you to provide highly secure network access to users and devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.