Cynerio | aruba CLEARPASS

# Aruba and Cynerio Integration: Transforming Healthcare IoT Security with a Clinical NAC

## The Healthcare IoT Footprint

Patients have more control over their data and treatment plans than ever, thanks to connected medical and IoT devices. These devices have transformed the healthcare industry and provided greater accessibility to treatment for patients and streamlined workflows for healthcare professionals, but they have also broadened the attack surface and exposed healthcare facilities to myriad threat actors and cyber exploitation.

### Healthcare IoT's Unique Challenges

Inadequate security combined with Healthcare IoT devices' (medical/IoMT, Enterprise IoT, and OT systems) inherent vulnerabilities have made healthcare facilities the number-one target for cyber attacks.

## An Expanding Threat Landscape

Broad use of devices running vulnerable legacy operating systems and firmware that cannot be updated further exposes networks to exploitation and leaves segmentation as the only option hospitals have for mitigating risk. However, because traditional IT tools lack clinical context, segmentation is extremely time-consuming and often just as dangerous as the risk itself. To avoid disrupting device functionality and operational continuity, safe and successful segmentation requires an in-depth understanding of Healthcare IoT's unique network topologies, communications patterns, medical impact, and criticality.

**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

## Cynerio & Aruba: The Power of Integration

The Cynerio Healthcare IoT Cybersecurity platform's integration with the Aruba ClearPass Policy Manager (CPPM) gives healthcare facilities actionable insights into clinically contextualized risk and the ability to enforce policy quickly, safely, and with confidence.

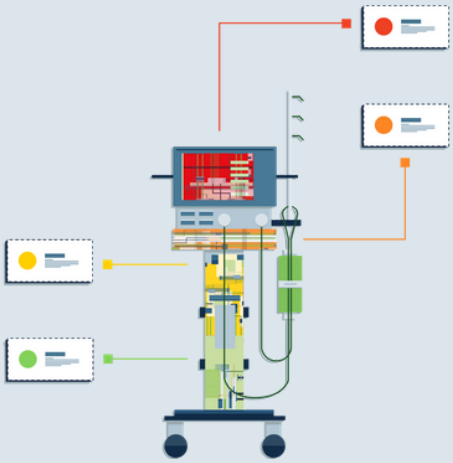
Frictionless integration provides healthcare organizations with complete visibility into every connected medical and IoT asset. Deep Packet Inspection (DPI) of every device combined with granular classification taxonomy tracks device types, functions, models, vendors, serial numbers, firmware/OS, MAC and IP+methods. The joint solution further provides insight into VLANs, ports, kernels, and hundreds of proprietary healthcare protocols.

After conducting clinically-contextualized risk analysis, Cynerio's automatically configured healthcare-safe Zero Trust security policies and risk mitigation plans are pushed into the Aruba CPPM and enforced, guaranteeing security, operational continuity, data integrity, and most importantly, patient safety.

# How It Works

## Complete Visibility

**Cynerio and Aruba ClearPass provide complete visibility into every Healthcare IoT asset (medical/IoMT, Enterprise IoT, OT systems).** Cynerio fingerprints and profiles every device and enriches the data with medical context and clinically-assessed risk. Unparalleled insights into asset locations, communications, criticality and impact profiles are then fed to the Aruba CPPM.

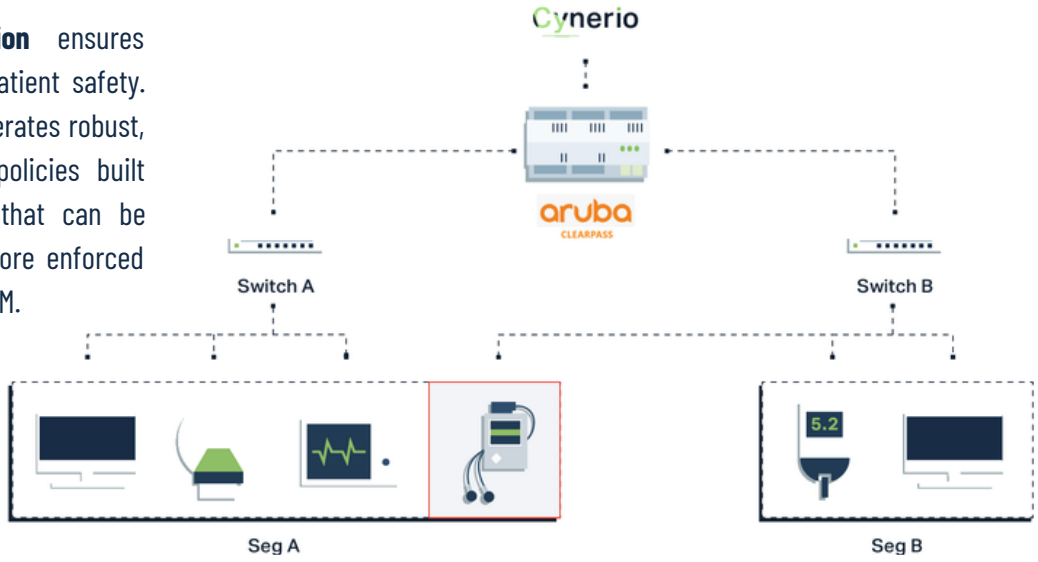


## Actionable Operational Insights

**Operational insights** provide healthcare security teams with comprehensive threat detection, automatically configured healthcare-safe Zero Trust security policies, and risk impact scores. Teams also receive actionable data on Healthcare IoT device usage (including granular breakdowns of weekly, daily, and hourly utilization patterns), risks, device- and organizational-level vulnerabilities, criticality, and impact on patient outcomes.

## Secure with Confidence

**Cynerio's Virtual Segmentation** ensures clinical service continuity and patient safety. This capability automatically generates robust, hospital-specific segmentation policies built on the Zero Trust framework that can be tested, validated, and edited before enforced on live networks by the Aruba CPPM.




## Stop Threats in Their Tracks

The **Aruba ClearPass Policy Manager** employs the clinically-enriched policy provided by Cynerio and automatically enforces it, enabling microsegmentation and predetermined threat response that limits lateral movement across the network. This allows healthcare facilities to safely secure complex clinical networks against cyber threats of any sophistication level and prevents threats from causing damage.

## Cynerio & Aruba ClearPass: Putting Patients First with Healthcare-Safe IoT Cybersecurity

**In healthcare, patients come first** and in Healthcare IoT, cybersecurity is patient security. By joining forces, **Cynerio** and **Aruba ClearPass empower healthcare facilities** with the ability to manage every connected medical and IoT device. The combined power of this integration pinpoints threats, isolates risks, and safeguards patients with healthcare-safe Zero Trust security policies that secure complex clinical ecosystems and ensure high-quality, uninterrupted patient care.