aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba & Cynerio

Transforming Healthcare IoT Security with a Clinical NAC

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. However, they have also broadened the attack surface and exposed healthcare facilities to a myriad of threat actors and cyber exploitation.

Due to long useful life cycles, it's common in healthcare to have a large number of devices still running vulnerable legacy operating systems and firmware that can't be further updated. This exposes networks to exploitation and leaves segmentation as the only option hospitals have for mitigating risk. However, because traditional IT tools can sometimes lack clinical context, segmentation is time consuming and can still leave residual risks. 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.

As a key component of Aruba's Edge Services Platform (ESP), Aruba ClearPass Policy Manager provides role-based network access control for devices registered on the network. Granular policy enforcement is based on a user's role, device type, authentication method, MDM attributes, traffic patterns, location, and time-of-day.

New York-based Aruba 360 Exchange security partner Cynerio makes a full suite of zero trust solutions built to secure healthcare facilities. Key features include auto-configured zero trust policies, device inventory, IoT communications mapping, at-risk asset identification, and service hardening.

BETTER TOGETHER

Cynerio and Aruba have partnered to help ensure that only compliant medical devices can access and remain on the network. 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.

WHY ARUBA AND CYNERIO

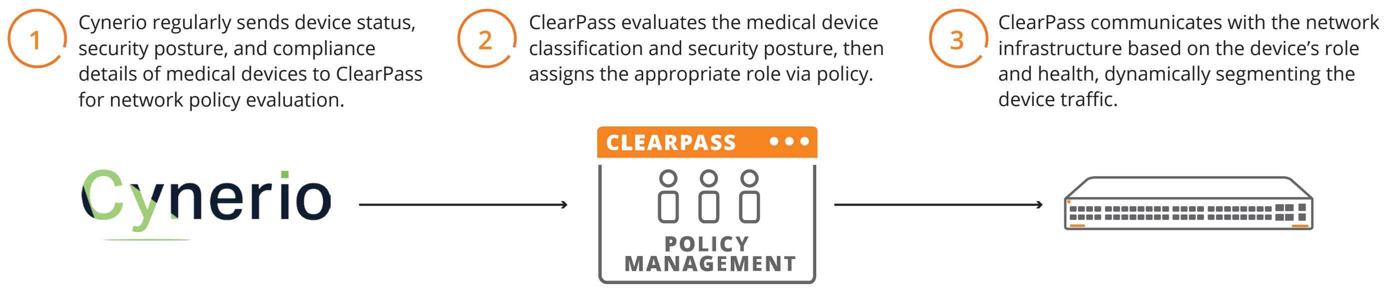
- Detect breaches on medical devices earlier, which can help prevent lateral movement
- Policy-based network access using device compliance details and device health
- Quick network isolation for compromised medical devices
- Fast, automated service restoration once remediation has been completed
- Aruba validated interoperability

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

After conducting clinically contextualized risk analysis, Cynerio automatically configures healthcare-safe zero trust security policies and risk mitigation plans which are then pushed into Aruba ClearPass Policy Manager. ClearPass then enforces these policies throughout the infrastructure, improving security, operational continuity, data integrity, and most importantly, patient safety.

The joint solution provides an end-to-end solution that assists in detecting early indicators of potential compromise or infection. Then, along with quick network isolation and segmentation it can greatly limit any lateral movement. This rapid detection and isolation can help prevent one infected medical device from becoming a thousand – and stop a malicious campaign in its tracks.

Cynerio



1 Cynerio regularly sends device status, security posture, and compliance details of medical devices to ClearPass for network policy evaluation.

2 ClearPass evaluates the medical device classification and security posture, then assigns the appropriate role via policy.

3 ClearPass communicates with the network infrastructure based on the device's role and health, dynamically segmenting the device traffic.

Figure 1: Aruba ClearPass and Cynerio architecture

HOW IT WORKS

Cynerio and ClearPass provide visibility into healthcare IoT assets across medical/IoMT, enterprise IoT, and OT systems. Cynerio fingerprints and profiles medical devices and enriches the data with medical context and clinically assessed risk. Insights into asset locations, communications, criticality and impact profiles are then fed to ClearPass Policy Manager.

CERTIFIED INTEROPERABILITY

We've certified the interoperability of ClearPass Policy Manager and the Cynerio IoMT/IoT Cybersecurity Platform to deliver an enhanced level of security for medical devices. Configuration of both solutions is quick and easy; simply define an API client in ClearPass, and then the Cynerio platform will use the ClearPass REST API to push data into ClearPass. Cynerio will use this API to regularly and automatically send key medical device attributes such as the device category, operating system, serial number, and device name into ClearPass Policy Manager for zero trust policy enforcement.

SUMMARY

By joining forces, Cynerio and Aruba have empowered healthcare facilities to manage connected medical and IoT devices. The combined power of this integration can assist with pinpointing threats, isolating risks, and safeguarding patients with healthcare-safe zero trust security policies that secure complex clinical ecosystems and ensure high-quality patient care.

Aruba's secure platform and trusted security partners are the ideal way to help protect your network from infected or compromised devices, starting from the point of infection to the prevention of lateral movement. Contact your local sales representative to see how Aruba and Cynerio deliver a comprehensive medical device security and secure network access solution.

DEPEND ON CYNERIO

Cynerio

Cynerio provides a healthcare IoT platform to address zero trust cybersecurity and risk management. With control, foresight, and adaptability, healthcare facilities can stay compliant and proactively manage their network.

aruba
a Hewlett Packard Enterprise company

PSO_Aruba&Cynerio_SK_042121 a00112935enw

Contact us at www.arubanetworks.com/contact