aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba & CyberMDX

Comprehensive visibility and threat prevention for medical devices and IoMT

Internet of Medical Things (IoMT) devices like remote patient monitoring systems, smart continuous glucose monitoring (CGM), connected inhalers, and ingestible sensors typically lack the security features required by enterprise zero trust framworks. As such they are often weak links in what is otherwise a secure healthcare network. Risks include communication protocols with little to no security, fixed passwords, unpatched software, and misconfigured settings. These risks are compounded by devices running old or outdated operating systems that lack root of trust and related security features needed to fend off cyber attacks, malware, and ransomware.

The best way to protect medical devices is by strictly controlling network access and micro-segmenting devices to allow communications only with approved applications and network resources. This approach is foundational to a zero trust framework because it can minimize the attack surface and, by extension, the chances of a successful attack by infections in otherwise trusted devices.

The Aruba ClearPass policy management platform centrally enforces security policies with any device operating on any vendor's network. Granular policy enforcement is based on a user or device's role and type, authentication method, Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) attributes, device health, traffic patterns, location, and time-of-day.

CyberMDX, an Aruba 360 Security Exchange technology partner, provides medical cybersecurity software for healthcare organizations by adding layers of cyber protection and improving cyber insights.

Aruba and CyberMDX have partnered to integrate Aruba ClearPass Policy Manager with the CyberMDX platform to enforce security policies across IT and IoMT networks. REST APIs provide ClearPass with the real-time status of medical devices on a network, which then assigns the appropriate level of network access.

WHY ARUBA AND CYBERMDX

- Identification and classification of connected medical devices
- Per-device level risk assessment and automated network policy assignment
- Tag-based, context-aware policies to reduce the attack surface
- Aruba validated Interoperability

HOW IT WORKS

At the time a device authenticates on the network, a risk analysis is conducted based on known vulnerabilities, detected threats, original research, and deviations observed from baseline performance measures collected by CyberMDX. CyberMDX automatically pushes these updates to ClearPass Policy Manager (CPPM) via device custom attributes for policy enforcement, VLAN assignment, and dACL policy management.

These attributes are further used to define and enforce context and risk aware policies within CPPM, including VLAN assignment and downloadable ACLs, to reduce the attack surface. Together, the itemized inventory and individualized risk assessment provide comprehensive visibility into devices and their cybersecurity posture.

CYBER MDX

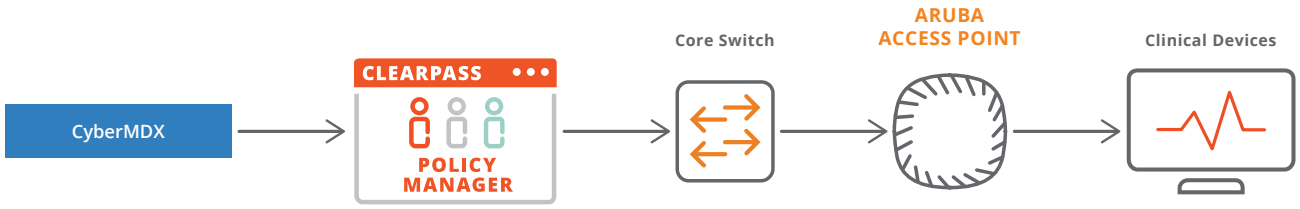

Figure 1: Aruba ClearPass Policy Manager and CyberMDX Joint Solution Diagram

CERTIFIED INTEROPERABLE

We've taken the guesswork out of IoMT threat prevention and clinical assets network micro-segmentation by certifying the interoperability of CyberMDX with Aruba infrastructure. The integration set-up, including creating an API Client and an API administrator user, resides within ClearPass, while setting the client ID and user credentials happens inside CyberMDX. Deployment is quick and hassle-free.

SUMMARY

Together, the Aruba and CyberMDX ensures the resiliency and safety of clinical networks with identity-based policy enforcement. Contact your local sales representative to see how together we deliver the most comprehensive threat prevention solution for clinical networks in the industry.

For more information on Aruba ClearPass, please visit: https://www.arubanetworks.com/products/security/network-access-control/

For more information on CyberMDX, please visit: https://www.cybermdx.com/

DEPEND ON CYBERMDX

We are a team of top cybersecurity specialists and technology entrepreneurs with decades of collective experience in cyber warfare and cyber intelligence, addressing the growing security challenges hospitals and clinical networks are facing. We understand what potential attackers want and know how to prevent them from getting it.

www.cybermdx.com Phone: 646-794-4160 1216 Broadway, New York, NY 10001

PSO_CyberMDX_050120 a00090832enw