aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba and Medigate

Protecting Hospital Operations from Compromised Medical Devices

The exploding number of medical and IoT devices within clinical networks is putting the data privacy and ongoing operations of healthcare delivery organizations at risk. According to a recent study[1], 82% of healthcare organizations experienced a cyberattack on their IoT devices in the past 12 months and 39% of medical respondents study indicated IoT security incidents ended in a loss of intellectual property.

To protect their information and resources, healthcare organizations need to accurately identify and then effectively mitigate the risks all connected medical and IoT devices pose. However, medical devices are not like general IoT devices, so additional low-level details about the devices can be helpful during discovery and mitigation. It takes deep clinical expertise to be able to identify different devices and understand the role they play in clinical workflows and patient care to establish safe, secure access policies and remediation actions.

Protecting clinical networks requires a deep understanding of clinical workflows and medical devices – including manufacturer operating systems (OS), proprietary protocols and expected device functionality. This is one of the best ways to accurately inventory all assets, assess risks, and enforce effective access control policies.

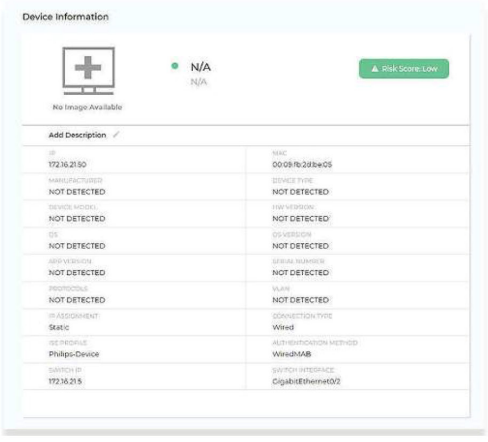
Medigate provides medical device and IoT security software for healthcare providers. By offering granular clinical intelligence, healthcare IT teams are able to bolster their risk management, network protection, clinical detection and response time, and clinical asset optimization.

Aruba and Medigate have partnered to integrate Aruba ClearPass Policy Manager with Medigate's platform to deliver the medical and cybersecurity expertise needed to effectively protect the data and operations of healthcare delivery organizations. The solution makes it possible to maintain total visibility of the network while gathering valuable insights, accurately detect risks and threats, and assure streamlined enforcement.

WHY ARUBA AND MEDIGATE

- Centralized and clinically-driven policy management for Medical IoT devices
- Policy based enforcement enables zero trust access to the network
- API integration enables swift action against compromised medical devices
- Aruba validated interoperability, and quick deployment

Device information received from Aruba ClearPass



Updated device information after Medigate's analysis

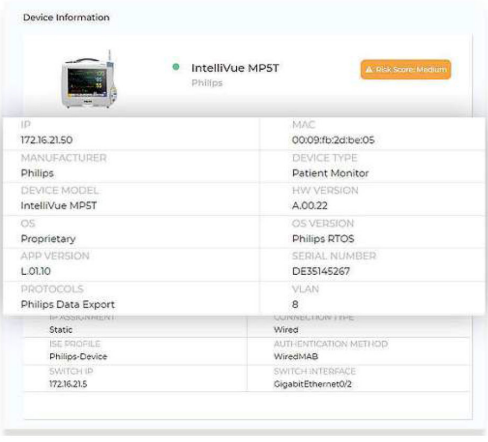


Figure 1: Medigate Dashboard

[1]"82% of Healthcare Organizations Have Experienced a Cyberattack on Their IoT Devices," HIPAA Journal, Sept. 2019

Configuration » Enforcement » Policies » Edit - medigate-enforcement-and-segmentation

Enforcement Policies - medigate-enforcement-and-segmentation

Summary | Enforcement | Rules

Enforcement:

Name:	medigate-enforcement-and-segmentation
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Endpoint:Source *EQUALS* Medigate) *AND* (Endpoint:medigate_device_type *CONTAINS* Anesthesia Cart)	medigate-cart
2.	(Endpoint:Source *EQUALS* Medigate) *AND* (Endpoint:medigate_location *CONTAINS* Surg)	medigate-nurse-vlan
3.	(Endpoint:Source *EQUALS* Medigate) *AND* (Endpoint:medigate_os_version *NOT_EQUALS* 11.5.5) *AND* (Endpoint:medigate_device_type *EQUALS* Glucose Meter)	[Deny Access Profile]

Figure 2: ClearPass Enforcement Policy on Medical Device

BETTER TOGETHER

Healthcare delivery organizations can leverage their existing ClearPass infrastructure and configure Medigate's automated identification and profiling capabilities to gain greater visibility into their connected medical devices and ensure appropriate authorizations, based on device function and risk level, to best mitigate risk.

The Aruba and Medigate solution maps all internal and external communications of connected devices to detect suspicious activity that deviates from expected clinical workflows and intended manufacturer behaviors.

Once detected, Medigate generates clinically-driven policies, based on the device type and risk level, which are fed to ClearPass Policy Manager to trigger appropriate enforcement. With policies that have been tailored to effectively address the specific risks to the hospital's network, ClearPass Policy Manager can implement precise enforcement and network segmentation that effectively protects clinical networks from potentially damaging activity.

Figure 3: ClearPass and Medigate Integration Architecture

HOW IT WORKS

The joint solution provides hospitals complete visibility into all connected devices on their network, including core characteristics, such as the manufacturer, make, model, operating system (OS), embedded software and protocols it uses. These detailed characteristics are the foundation for creating granular device profiles and clinical-contextual risk assessments, which can be used to establish effective network access and micro-segmentation policies.

First, Medigate continuously monitors the network, using deep packet inspection (DPI) to provide a real-time inventory of all the medical and IoT devices attempting to connect to the network, and alerts on risky or anomalous activity. Medigate creates a dedicated enforcement profile for each device, which it feeds to Aruba ClearPass Policy Manager. ClearPass then takes the profile and attaches the appropriate enforcement policy to ensure safe network access and prevent risky communications and attack propagation. Finally, Aruba can take immediate action - quarantining the device, restricting Internet access, or placing devices in a separate VLAN - to mitigate any risks.

CERTIFIED INTEROPERABILITY

This joint solution has been certified under the Aruba 360 Security Exchange technology partner program and is easy and quick to deploy. Medigate utilizes the ClearPass API to populate key endpoint attributes into the ClearPass Endpoint Database. These attributes are then used by ClearPass policies to enable/restrict network access, and also to establish the proper permissions on the network using a zero trust methodology. Once this integration is configured, Medigate will automatically synchronize these attributes at a user-defined interval, ensuring that the ClearPass Endpoint Database is always kept up to date. All of this configuration is done via a browser based GUI, and is easy to set up.

SUMMARY

Aruba and Medigate have taken the guess work out of protecting clinical operations. Contact your local sales representative to see how Aruba and Medigate deliver a comprehensive clinical network protection solution.

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

DEPEND ON MEDIGATE

MEDIGATE Medigate provides medical device & IoT security for healthcare providers and is based out of Brooklyn, NY.

www.medigate.io Phone Number: (855) 908-0775 134 N 4th St., Brooklyn, NY 11249

aruba
a Hewlett Packard Enterprise company

© Copyright 2020 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

PSO_ArubaandMedigate_RVK_111920 a00106963enw