aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba and Asimily

What's on your network?

Healthcare and life sciences facilities have seen a surge in the number of connected IoT devices, and as connectivity has increased so, too, have cyberattacks. Approximately 25% of cyberattacks involved IoT devices in 2020, and by 2025 attacks are expected to grow by 500%.

Many IoT devices subject to attack are vital to patient care, including blood glucose monitors, infusion pumps, imaging devices, patient monitors, and laboratory processing equipment. Managing and protecting connected medical devices is a challenge. Organizations need to identify and classify all devices on their network, understand normal communication patterns, and then apply security policies to manage legitimate communications, block unauthorized ones, and quarantine or segment devices if a threat is detected.

Asimily is a California-based company whose solutions monitor and manage healthcare devices throughout their life-cycle in the environment. The solution aggregates medical device data from different sources, many of which are unique to healthcare, and appends it to device data derived from Asimily's machine learning tools. Asimily tools then monitor which devices are on the network and how they are used, determine how data should flow between devices, assess risk and the priority of patches, conduct anomaly assessments, manage policies, and track device location.

Aruba and Asimily have partnered to detect and protect against cyberattacks on medical facilities. The joint solution addresses these challenges by integrating the Asimily platform with Aruba ClearPass Policy Manager. After Asimily identifies and classifies medical devices on a network, these data are passed to Aruba's ClearPass Policy Manager to centrally enforce network access policies for these devices.

WHY ARUBA AND ASIMILY?

- Precise medical device classification and profiling that are essential for driving network policies
- Centralized zero trust enforcement of policies based on device behavior and context
- Rapid network isolation for compromised medical devices
- Automated service restoration upon remediation
- Aruba validated interoperability

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

HOW IT WORKS

Asimily and Aruba have made it easier for organizations to better understand and secure networked medical devices:

- Use machine-learning to understand devices and their risks, sending medical device details and threat information to ClearPass via API;
- ClearPass uses the medical device metadata for policy evaluation at the time the device connects to the network, or when a notification is received that a device has been compromised; and
- ClearPass instructs the network infrastructure to enforce zero trust network access policies on the network.

ASIMILY

Figure 1:

HOW IT TIES TOGETHER

API configuration is done both on the ClearPass and the Asimily platforms to ensure seamless and automatic data transfer to ClearPass. Once the system has been configured, medical device metadata is automatically pushed to ClearPass, ensuring that its policies are always up to date without manual intervention. The rich medical device metadata is then immediately available to drive zero trust network policies.

Figure 2: Asimily metadata utilized by ClearPass

CERTIFIED INTEROPERABILITY

Interoperability between ClearPass Policy Manager and the Asimily Medical Device Management Platform has been validated 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 the Asimily platform uses the ClearPass REST API to regularly push data into ClearPass. Asimily also uses the REST API to automatically update ClearPass with key medical device attributes such as the device type, operating system, FDA recall count, and threat status for zero trust policy enforcement.

SUMMARY

Cybersecurity is key to protecting patient health and privacy. By joining forces, Asimily and Aruba help healthcare organizations monitor medical devices on the network, and enforce zero trust security policies. The joint solution ensures that medical devices are only allowed on the network when compliant and healthy, and are continuously monitored for threats that may compromise patient safety or privacy.

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 Asimily deliver the most comprehensive medical device security and secure network access solution in the industry.

DEPEND ON ASIMILY

ASIMILY Asimily is a Healthcare and Life Sciences focused firm solving for use cases around inventory, cyber-security and operational management for medical, laboratory, and connected devices.

aruba
a Hewlett Packard Enterprise company

PSO_Asimily_SK_041321 a00112525enw

Contact Us **Share**