aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

VISIBILITY AND INSIGHT FOR TODAY'S IOT-DRIVEN NETWORKS

A roadmap to improved device security and compliance

As the breadth and complexity of devices in the network continues to grow at a staggering rate, many organizations are struggling to address an expanding attack surface. With the growing ubiquity of Internet of Things (IoT) and new use cases, the adoption of IoT has outpaced critical security and compliance best practices in favor of improved operational efficiencies and business outcomes.

With this shift, IT and security teams are often unaware when, where and what types of new devices are being connected to the network. This lack of visibility prevents them from implementing key security and compliance safeguards. Best practices would require that each new device be onboarded and assigned a policy, but IT is often caught off guard.

"BLIND SPOTS" IN CURRENT APPROACHES

The existing network visibility toolset has focused on a fairly narrow set of devices that have been easily identified using basic discovery and profiling techniques. This included finding things like popular endpoints running common desktop or mobile operating systems. Identifying a smartphone running Android, from a laptop running Windows has been a common use case using these techniques.

The challenge of identifying IoT devices, however, has become particularly difficult for a number of reasons, some of which include:

- Many IoT devices are produced by emerging vendors and cannot be communicated with using standard discovery and profiling techniques, making them difficult to accurately profile.
- It is also common to see IoT devices that are built with generic hardware and software, such as a raspberry pie that serves different roles, making it difficult to decipher as well.
- Due to inaccurate or partial profiling, devices are often identified as generic "Windows" or "Linux" devices, which makes it difficult to apply accurate policies

THE IMPORTANCE OF CONTEXT

With this shift, a full-spectrum approach to visibility across the entire wired and wireless infrastructure is needed that doesn't require using agents or logging onto devices to see what they are. This means understanding the actual behavior of a device –what protocols are being used, what applications and URLs are being accessed – and in the end, what function a device is serving on the network. For many purpose-built, IoT devices, such as those found in a hospital or manufacturing plant, this context is the only way to accurately fingerprint a device.

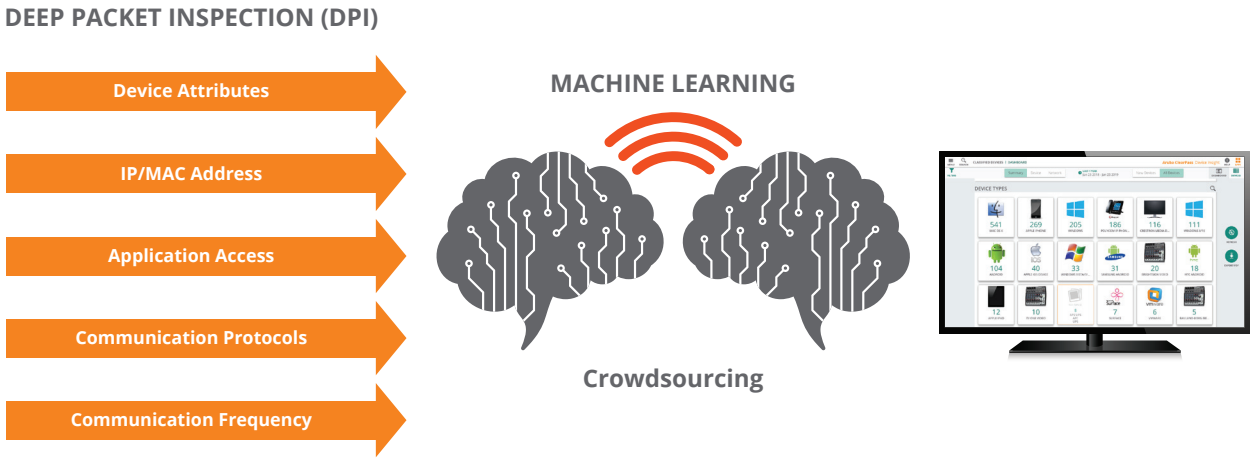

Figure 1: ClearPass Device Insight utilizes advanced machine learning and crowdsourcing to accurately identify devices.

THE ARUBA SOLUTION: AI-POWERED VISIBILITY

ClearPass Device Insight builds on Aruba's leadership in network visibility and access control through a new approach – using machine learning and a unique set of both active (NMAP, WMI, SNMP, SSH) and passive discovery methods (SPAN, DHCP, NetFlow/S-flow/IPFIX) – in order to identify and profile a wider range of device types.

These capabilities are further enhanced through the use of Deep Packet Inspection (DPI), which provides additional context and behavioral information to accurately identify those hard-to-detect devices. By introducing DPI in addition to active and passive techniques, ClearPass Device Insight is able to utilize a broader set of device attributes for more accurate device identification

As device signatures evolve over time, the ability to leverage a controlled crowdsourcing model speeds the time it takes to accurately identify new devices to help eliminate blind spots. As devices are labeled and signatures are submitted by ClearPass Device Insight users, those signatures are validated by Aruba researchers to ensure accuracy, before making them available to other Aruba customers.

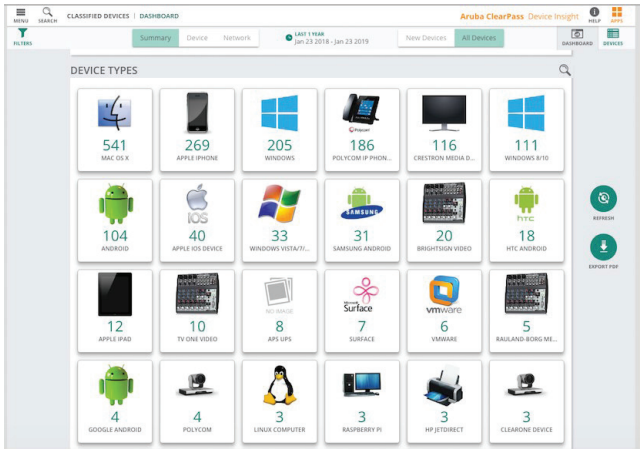

Figure 2: The ClearPass Device Insight dashboard shows all connected devices by category.

For devices previously seen as generic devices, sophisticated machine learning models are used to analyze device attributes and group similar devices together. As devices are grouped, they can be easily labeled based on key attributes. Once labeled, new devices connecting to the network are automatically added to their specific cluster and labeled accordingly.

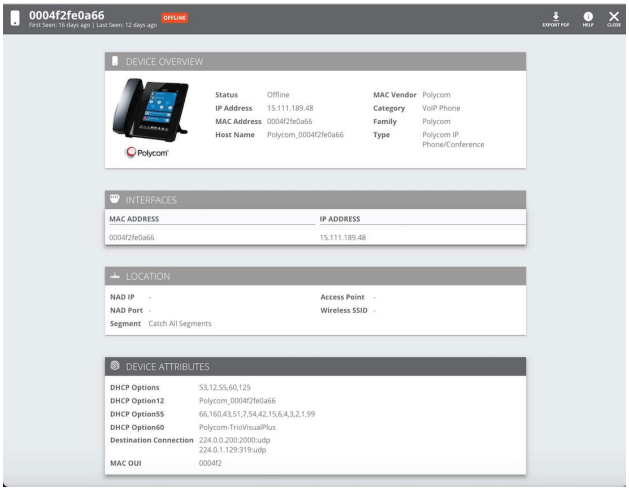

Figure 3: Drill-down capabilities within the dashboard provide detailed device profiles

THE VALUE OF AUTOMATED POLICY ENFORCEMENT

Visibility without proper control can leave organizations open to security and compliance risks. ClearPass Device Insight, combined with Aruba ClearPass Policy Manager, provides closed loop, end-to-end access control. This delivers visibility and automated policy enforcement, and greatly reduces the need for manual intervention for any multi-vendor wired and wireless network.

Automated policy enforcement addresses a number of different use cases, starting from the point in time when devices initially join the network, to where an unwanted event triggers the need to remove a device due to security or compliance concerns. For instance, when a new device first connects to the network, it can be can automatically be segmented as an unknown device type to ensure that it does not affect critical infrastructure or servers. If a device has been compromised or acts in a suspicious fashion, that device can be quarantined completely in order to be tested, repaired or replaced.

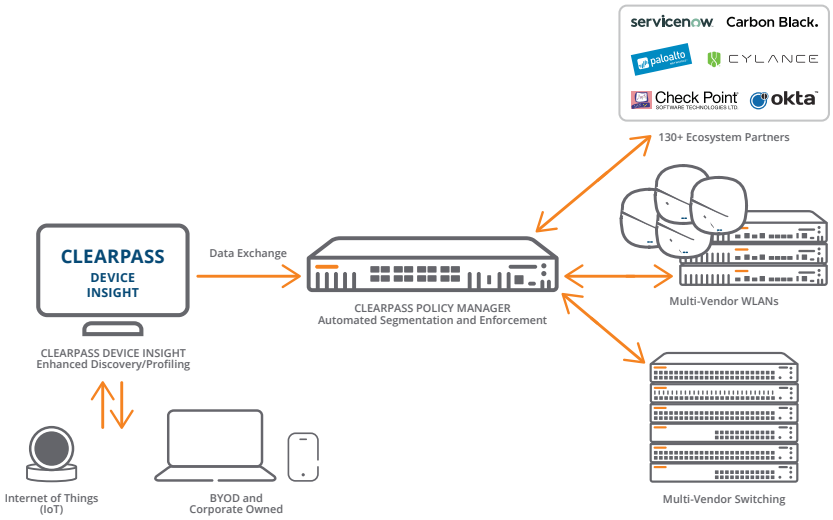

Figure 4: ClearPass Device Insight seamlessly integrates with ClearPass Policy Manager for automated segmentation and enforcement

THE ARUBA EDGE: ACCELERATING TIME-TO-VALUE

Managing business critical applications across an expanding mobile environment drives the expectation for heightened availability, performance and security. Aruba's software-defined platform is open, cloud-native and built using modern web scale technologies and methods to deliver traditional NMS, advanced AI/ML and security features – enabling IT organizations of all sizes to deliver amazing experiences with amazing simplicity.

ClearPass Device Insight leverages these unique features to reduce deployment time and accelerate time-to-value. On-premises data collectors are used to continuously gather device attributes, which are sent to the ClearPass Device Insight Analyzer hosted in the cloud. This approach provides centralized, uninterrupted discovery and monitoring of all network connected devices.

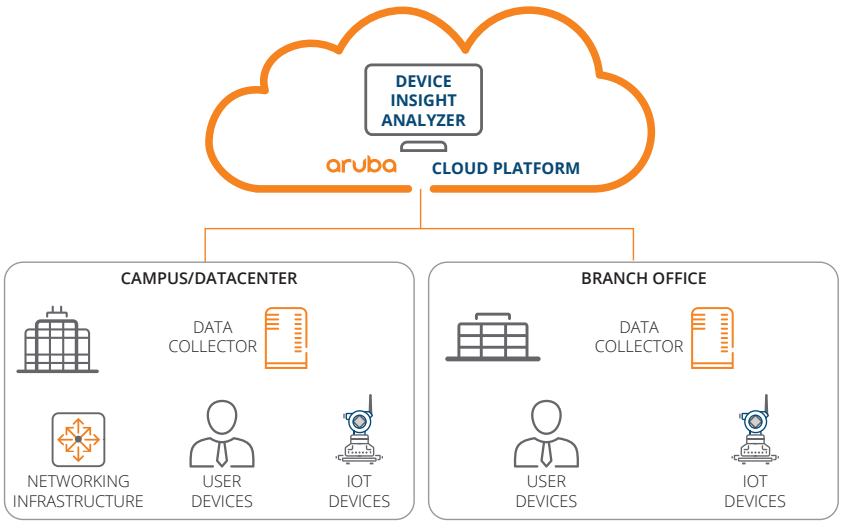

Figure 5: Attributes collected on the network are sent to ClearPass Device Insight Analyzer to accurately identify connected devices.

SUMMARY

With the accelerated adoption of IoT, comprehensive visibility is necessary to ensure security and compliance best practices keep pace. When devices are discovered on the network, granular policies ensure each device has the right level of access control in order to reduce overall levels of risk related to a security or compliance incident.

As IoT devices continue to grow in number and evolve, creating new use cases, security and compliance will become increasingly important for organizations looking to gain the operational efficiencies that come with the adoption of an IoT infrastructure.

SO_Visibility and insight_SK_032819 a00069032enw