SOLUTION OVERVIEW

Visibility and insight for today’s IoT driven networks

An AI-powered approach to securing network endpoints with Client Insights

As the breadth and complexity of endpoint clients 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 generated by digital transformation initiatives, 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 of when, where, and what types of new clients are being connected to the network. This lack of visibility prevents them from implementing timely security and compliance safeguards. Best practices would require that each new client be accurately identified, 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 clients that are easily identified using basic discovery and profiling techniques. This includes finding things like popular smartphones and laptops running common desktop or mobile operating systems. Identifying a smartphone running Android, from a laptop running Windows has been common using these techniques.

Identifying clients such as IoT devices is particularly difficult for several 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 pi that serves different roles, making it difficult to decipher as well.
- Due to inaccurate or partial profiling, clients are often identified as generic “Windows” or “Linux” clients, which makes it difficult to apply accurate policies.
- Most network visibility solutions require collectors or agents, and it is not always feasible to deploy collectors across locations at scale.

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 clients 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 client is serving on the network. For many purpose-built IoT devices, such as those found in a hospital or manufacturing plant, this rich context is the only way to accurately fingerprint them.

THE ARUBA SOLUTION: AI-POWERED CLIENT INSIGHTS

Aruba’s network management solution Aruba Central cloud now includes AI-powered Client Insights which offers the most granular profiling and visibility in the industry. Client Insights leverages native infrastructure telemetry from access points, switches, and gateways, as well as clients without requiring installation of physical collectors or agents. ML-based classification models are used to fingerprint , identify, and accurately profile a wide variety of clients across the entire wired and wireless infrastructure.

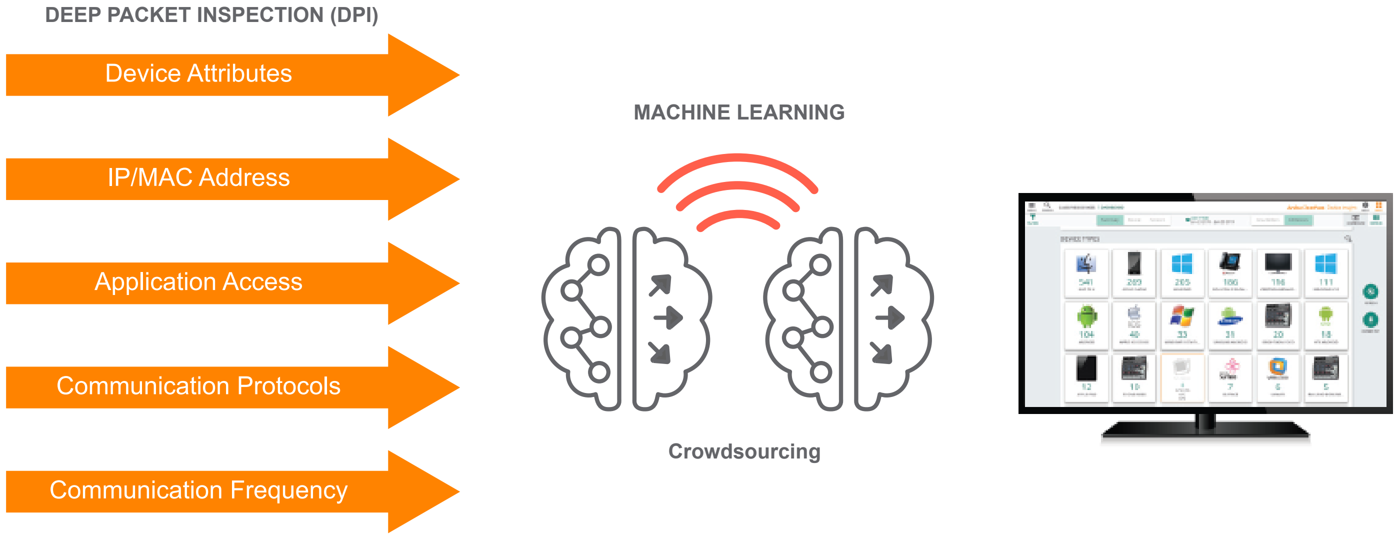

Figure 1. Client Insights utilizes advanced machine learning and crowdsourcing to accurately identify any client type.

These capabilities are further enhanced with Deep Packet Inspection (DPI), which provides additional context and behavioral information that helps to accurately identify those hard-to-detect IoT devices. By leveraging DPI, Client Insights can utilize a broader set of device attributes for more accurate identification. Client attributes that include communication and behavioral patterns are analyzed to dynamically build clusters of similar devices.

Machine learning models are used to constantly learn and update these attributes to dynamically update fingerprints and provide classification recommendations. Controlled crowd-sourcing technology is used to validate fingerprints at multiple customer sites before adding them to the Aruba classification database. This increases the precision and comprehensiveness of the classification engine.

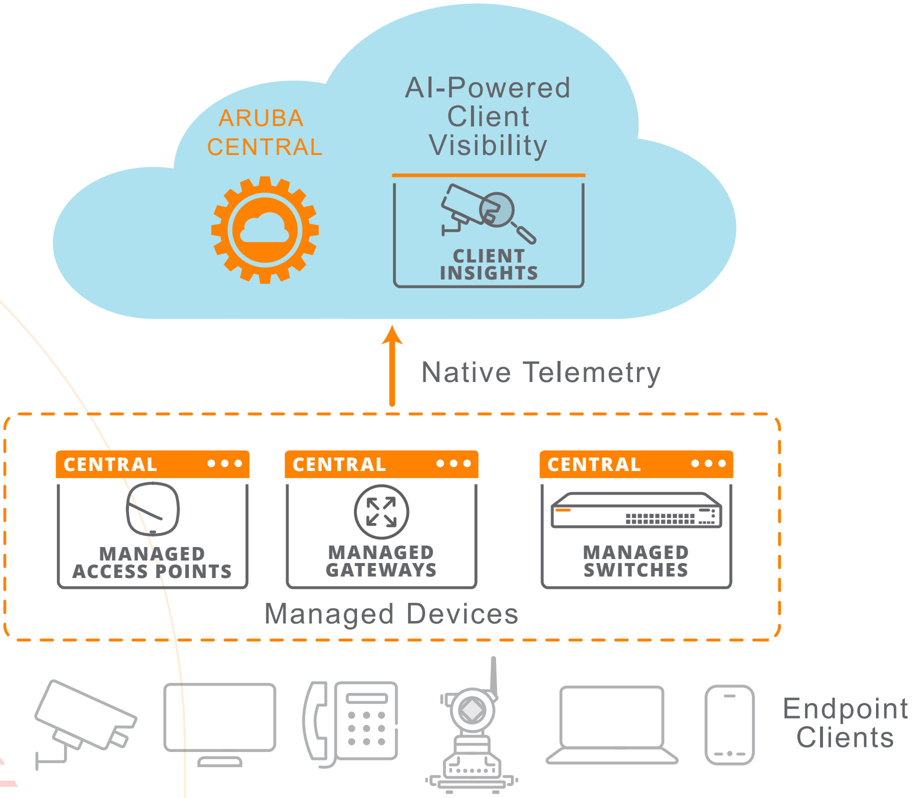

Figure 2. Native telemetry from Aruba networking infrastructure is used to accurately identify connected clients using ML-based classification

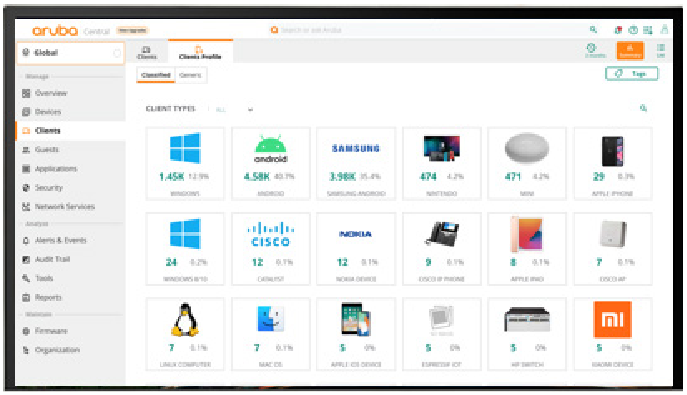

Figure 3. Aruba Central cloud Client Insights dashboard shows all connected devices by category.

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

For environments that are not currently managed by Aruba Central cloud or for environments with third-party network devices, ClearPass Device Insight (CPDI) can be leveraged for ML-based identification and profiling of clients. CPDI requires the installation of either a physical or a virtual collector and is separately licensed.

THE VALUE OF AUTOMATED POLICY ENFORCEMENT

Visibility without proper control can leave organizations susceptible to security and compliance risks. Client Insights allows for continuous monitoring of clients, which when paired 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 in any multi-vendor wired and wireless network. CPDI also integrates seamlessly with ClearPass Policy Manager.

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

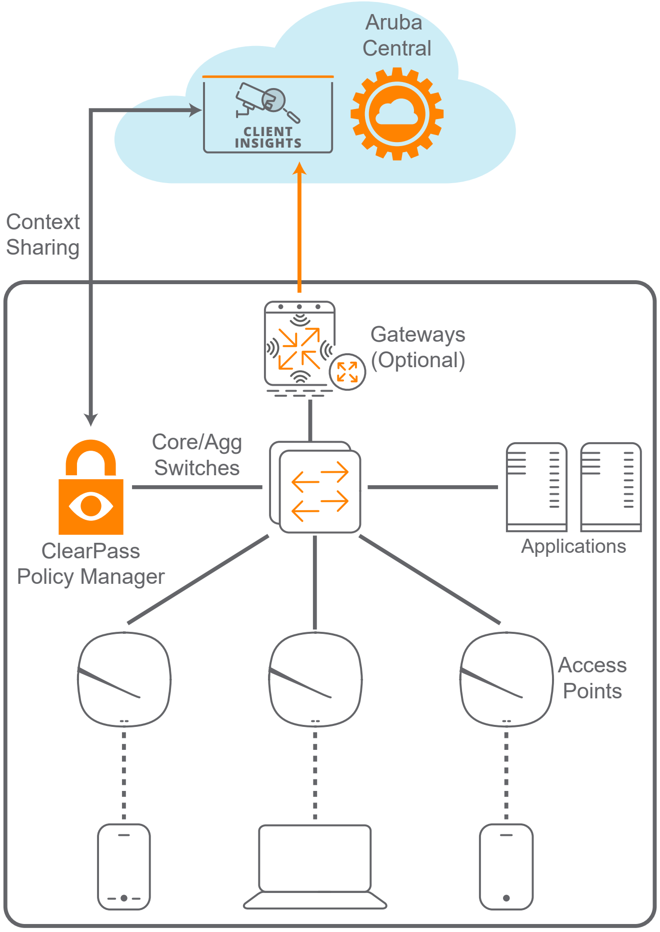

Figure 4. Client Insights integrates with Aruba ClearPass Policy Manager for automated segmentation and enforcement

ARUBA CENTRAL CLOUD WITH CLIENT INSIGHTS: ACCELERATING TIME-TO-VALUE

Managing business critical applications across increasingly distributed environments drives the expectation for improved availability, performance, and security. Aruba Central cloud offers modern features, scale, management and orchestration, that include advanced AI/ML and security features - enabling IT organizations of all sizes to deliver superior user experiences with amazing simplicity.

Client Insights leverages these unique features and native telemetry from network infrastructure to reduce deployment time and cost, accelerating time-to-value. This approach provides centralized, uninterrupted discovery and monitoring of network endpoints across distributed deployments while increasing your visibility and security posture.

SUMMARY

With the accelerated adoption of IoT devices, the number of clients on customers networks continues to grow, creating new use cases while also expanding attack surface. Comprehensive visibility is essential to ensure security and compliance best practices keep pace with the operational efficiencies that come with the adoption of IoT.

Accurately identifying and profiling clients for fine-grained role-based policies and ensuring that each have the right level of access control to reduce overall risk levels is no longer a nice to have – it's a requirement.

aruba
a Hewlett Packard
Enterprise company

SO_ClientInsights_RVK_010522 a00069032enw

Contact us at www.arubanetworks.com/contact