aruba
a Hewlett Packard Enterprise company

ARUBA AT A GLANCE

ENDPOINT VISIBILITY FOR WIRED AND WIRELESS

Today's prerequisite for enhanced security and compliance

It used to be easy to walk by someone's desk and see what they had connected to the network, but those days are long gone. Bring Your Own Device (BYOD) and unmanaged devices, like surveillance cameras and other emerging endpoints in the Internet of Things (IoT) category, are making it impossible for IT to maintain complete visibility.

THE CHALLENGE

To help identify connecting endpoints, legacy practices often meant deploying comprehensive endpoint management solutions, agents, and manually updating multiple endpoint databases. None of these delivered the desired results because IT was overwhelmed by BYOD, guest access deployments, and rogue wired and wireless endpoints; many of which come and go with users.

With the billions of IoT devices expected to connect to networks in the next three years, and the well-publicized security breaches of late, there is a warranted demand among IT professionals for real-time visibility and reporting. They need a solution that offers continuous monitoring and profiling rather than periodic updates, regardless of location, time-of-day, or endpoint type.

TODAY'S INTELLIGENT VISIBILITY SOLUTION

Aruba's ClearPass family offers network and security organizations a unique advantage versus the competition as real-time, agentless profiling can be acquired as a standalone appliance or within a comprehensive policy enforcement solution.

Both allow you to continuously identify endpoints, and network devices on non-AAA or AAA enabled wired and wireless networks — whether via dynamic or static IP addresses. Comprehensive dashboard visuals make it easy to see the total number of endpoints, and the number by category, family and device type.

ARUBA CLEARPASS BENEFITS

- Automatic detection and categorization of endpoints for security and audit demands
- Continuous monitoring of all devices, and those that come and go
- Agentless visibility that lets you find devices like BYOD smart phones, and IoT
- Contextual attribute sharing that extends visibility to a wide range of security and IT-services solutions
- Elimination of labor required with manually maintaining database updates
- Improved network performance and security by understanding how many endpoints, what types, and their attributes

Aruba ClearPass Universal Profiler: A standalone virtual appliance that can be deployed and running in minutes, is designed for those organizations that are not ready for a complete NAC solution, or for remote or restricted areas where NAC has not been deployed. It is available to fit any organization's scalability needs.

Aruba ClearPass Policy Manager: Virtual or physical appliances that include comprehensive profiling, non-AAA and AAA wired and wireless policy enforcement, guest access, BYOD onboarding, endpoint assessment capabilities, reporting, and built-in third party security and user experience oriented solution integration.

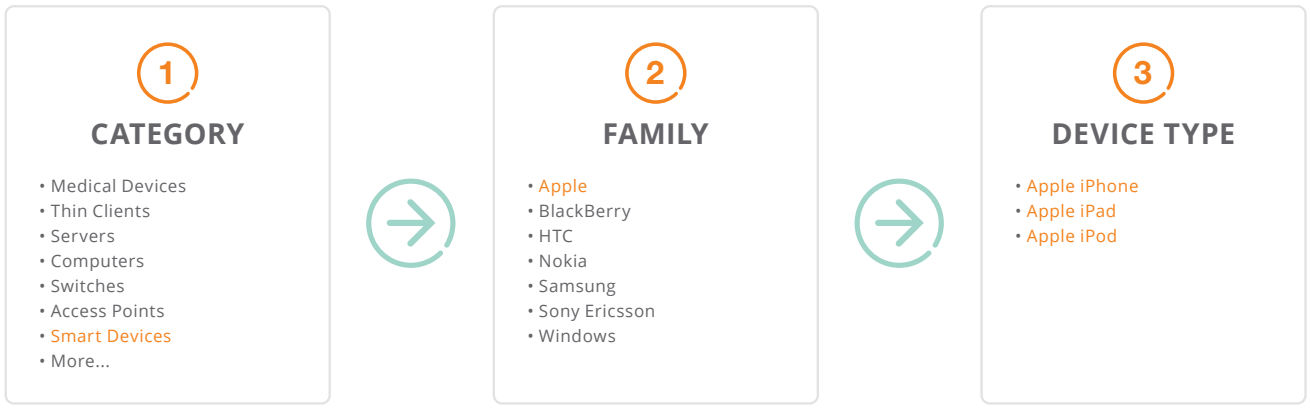

Figure 1: Granular visibility by device category, family and type

The ClearPass family discovers endpoints with unsurpassed ease, identifying and profiling attributes that determine device category, vendor, operating system, IP address, hostname, owner, and more. Automatic and IT-customizable endpoint classification ensures that new and unknown IoT devices are quickly placed into the proper device families for visibility and/or security enforcement.

For added flexibility, ClearPass provides options for dynamic network discovery using standard network or SPAN port monitoring. This is contrary to legacy IT network access control solutions that may require you to dedicate multiple and expensive 10G ports to mirroring in large endpoint deployments.

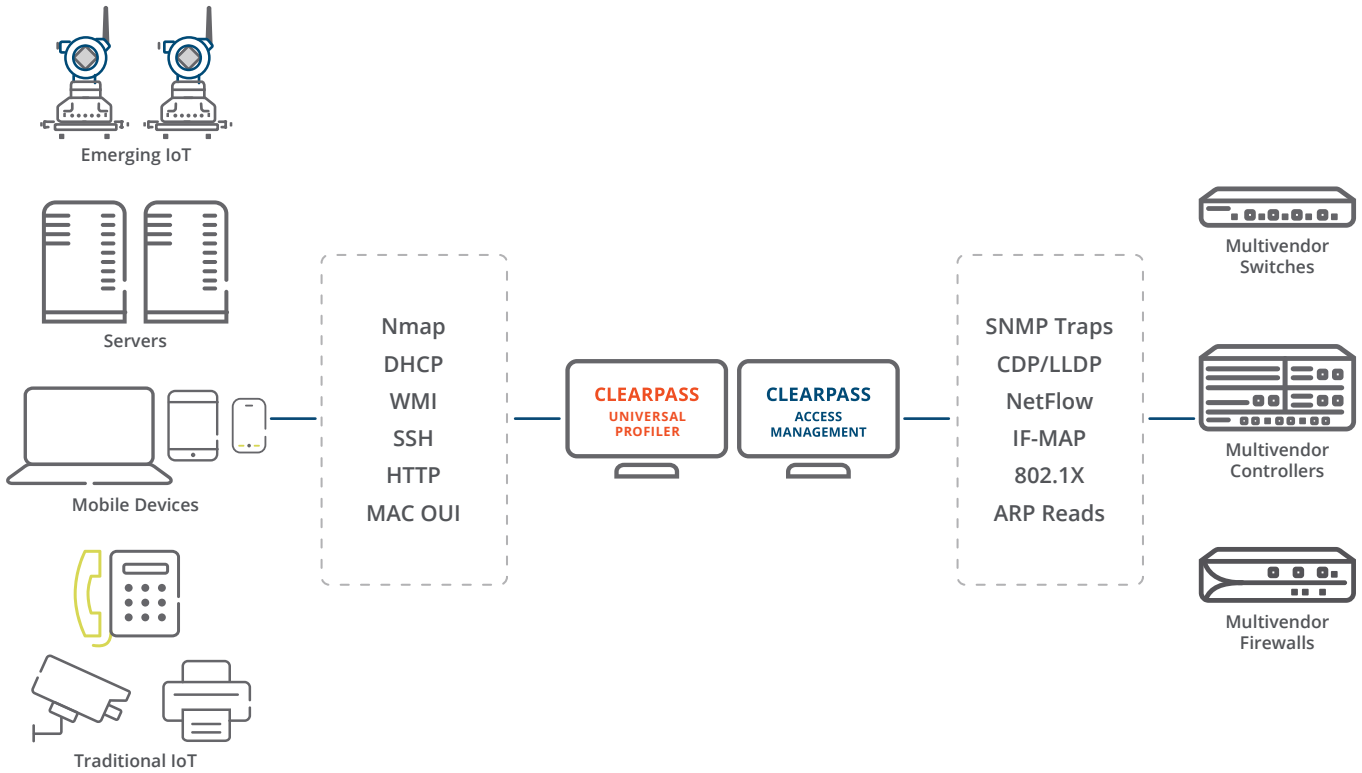

Figure 2: Granular Identity and Profiling Methods

GRANULAR DISCOVERY METHODS

Multiple profiling methods helps collect granular endpoint attributes per device that can help identify possible performance issues and threat risks. This increased visibility and contextual insight can be shared by both ClearPass solutions or used directly by the ClearPass Policy Manager to help optimize policies for what can connect and how quickly IT can respond to potential threats.

LEVERAGING ENDPOINT VISIBILITY WITH THIRD-PARTY SOLUTIONS

ClearPass API's, syslog messaging and Extensions capability makes it easy to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management. These solutions can ingest endpoint attributes to match traffic patterns, per their specific rules for each device category, to optimize connections or remediate suspect traffic.

LEARN MORE

To learn more about the ClearPass Universal Profiler and ClearPass Policy Manager and how they offer the unique ability to identify all endpoints, help enforce policies, and better protect your wired and wireless networks, visit www.arubanetworks.com/clearpass.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com

IB_Visibility_111616