airheads TECH TALK LIVE

aruba
a Hewlett Packard Enterprise company

Eliminating the blind spots with ClearPass.

How visibility is the key to securing the experience

September 2019

#ArubaAirheads

EXPERIENCE EDGE

SECURING new experiences that are personalized, relevant, and timely.


WORKPLACES


STORES


HOSPITALS


INDUSTRIAL


HOTELS

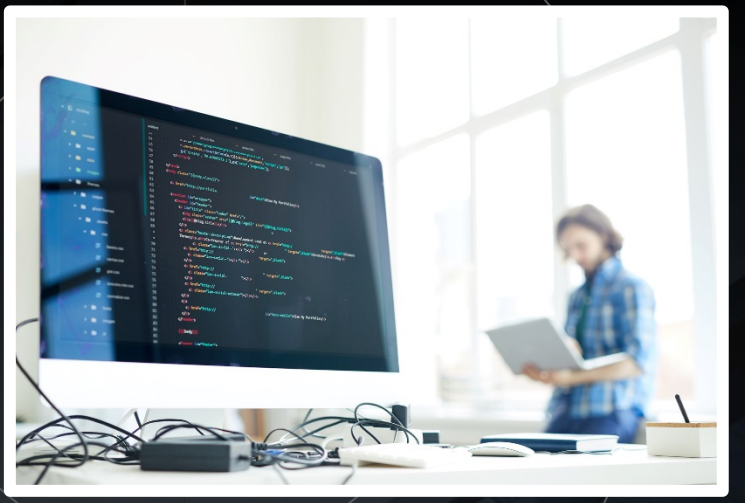

SCHOOLS

Stepping towards the edge

Securing a great experience for everyone and everything

Enhancing User experience

Securely enabling IoT



Easing policy administration

The aim?

Zero-Trust Framework

The untrusted LAN

What you can access doesn't depend on from where you have connected

AuthN, AuthZ, Encrypt

The reality

A shot too far

- Lack of segmentation
- Outdated policies
- Policy gaps between departments
- Too many unknowns
- Insider threats
- Shadow IT

Zero-Trust Framework

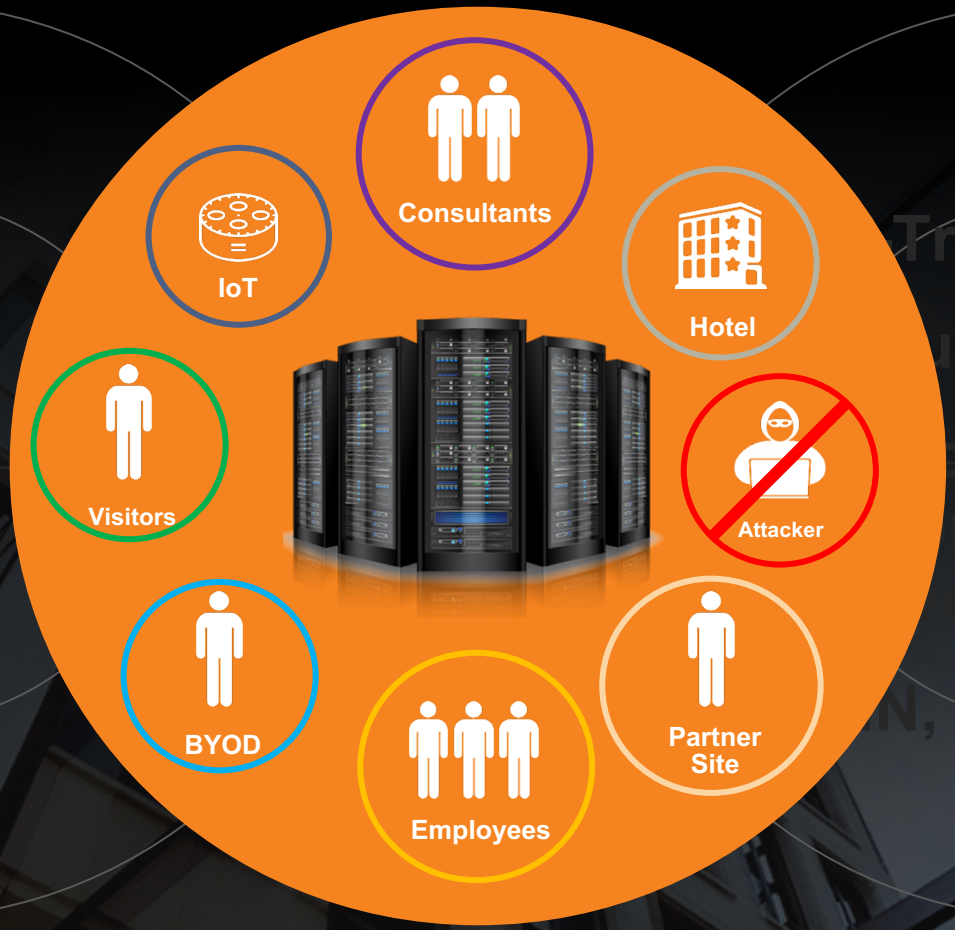
The untrusted LAN

What you can access doesn't depend on from where you

AuthN, AuthZ, Encrypt

The measured response

Adaptive Trust and Continuous Visibility



Creating Access Policy Control

Putting it all into context…

- **People – Roles**
  - More than Staff Vs. Non-Staff
  - e.g. AuthZ on location/department

Creating Access Policy Control

Information we should consider

- **People - Roles**
- **Devices – Types/Uses**
  - More than managed vs. unmanaged!

Device Visibility: ClearPass Policy Manager

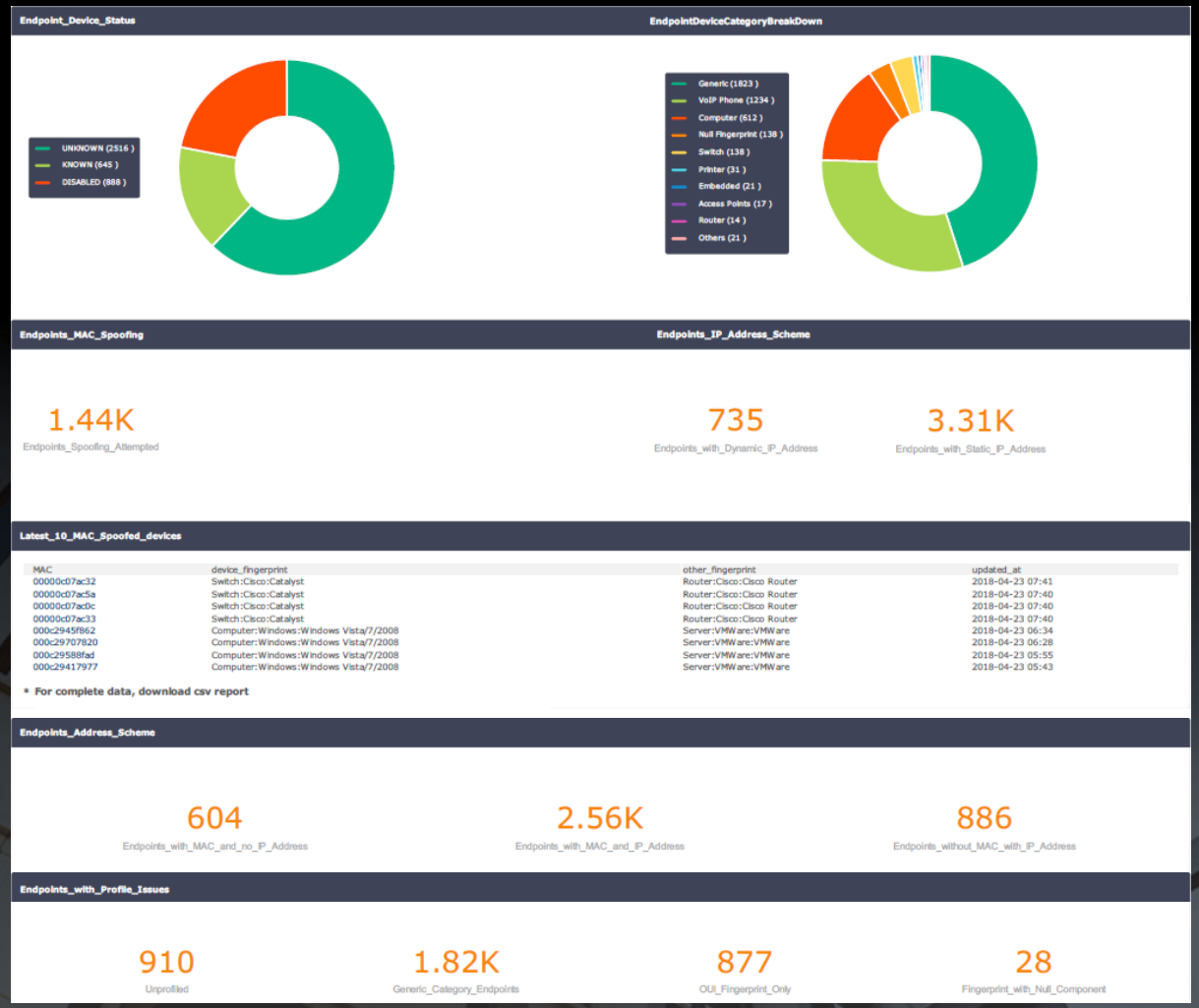
An easy start to regaining control

- **Single C1000 ClearPass server – minimal Access licensing**

- Visibility of what's on the network – up to approx. 5K devices
  - Includes install guide and specific report generation
- Visibility of what's changing on the network
  - TACACS to secure and monitor network config changes + reporting
- RADIUS and/or Guest services for up to 100 concurrent users

Device Visibility: ClearPass Policy Manager

An easy start to regaining control



Creating Access Policy Control

Information we should consider

- **People - Roles**
- **Devices – Types/Uses**
  - More than managed vs. unmanaged!
  - When’s a phone not a phone?

TRADITIONAL PROFILING TECHNIQUES
LACK DEVICE CONTEXT

STATIC ATTRIBUTES

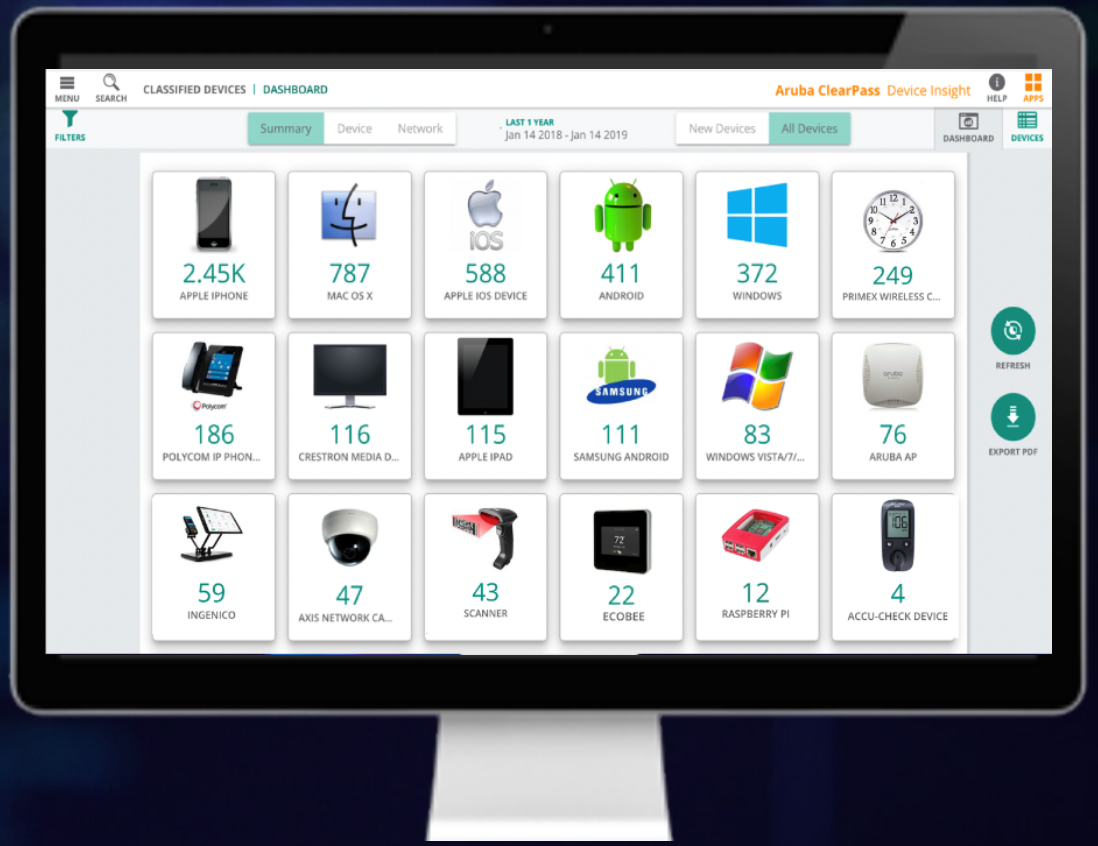
NMAP | SNMP | WMI

GENERIC "WINDOWS" OR "LINUX" DEVICE

CLEARPASS DEVICE INSIGHT

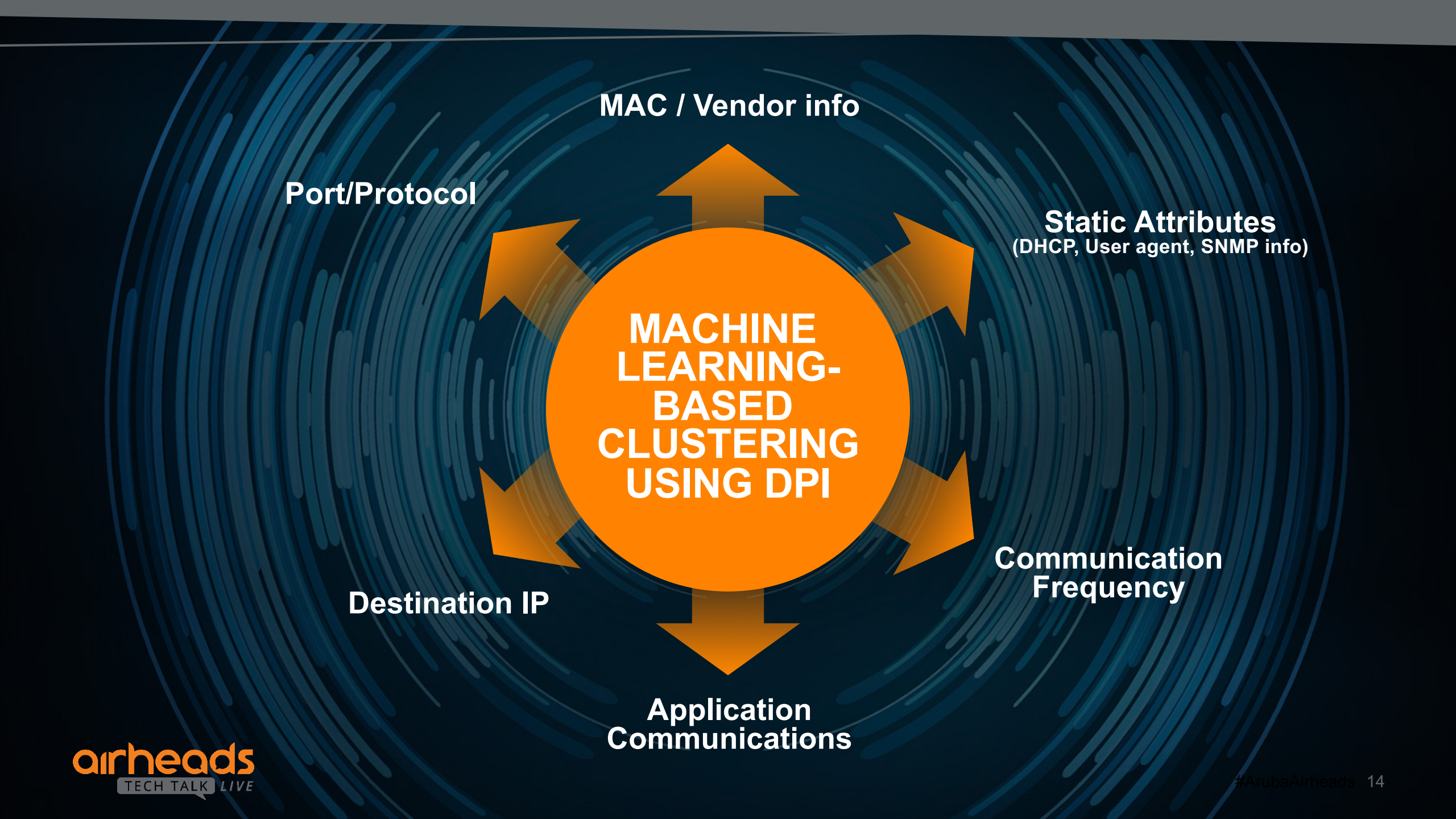
ELIMINATES BLIND SPOTS

Delivers automated, ML powered device classification to enhance policy-based access control



airheads TECH TALK LIVE

***New and Existing ClearPass OnGuard Subscription customers get free access!**


MAC / Vendor info
Port/Protocol
Static Attributes
(DHCP, User agent, SNMP info)
MACHINE LEARNING-BASED CLUSTERING USING DPI
Communication Frequency
Destination IP
Application Communications

ARCHITECTURE OVERVIEW

Combination of on-premises data collector (appliance or virtual) and cloud-based analyzer

Through Deep Packet Inspection (DPI), device attributes are are extracted and metadata is sent to the cloud for analysis

DEVICE CLASSIFICATION

Discovered Devices

Static Rules

Classify known devices with established patterns - Crowd-Sourced Signatures

Rule Matches

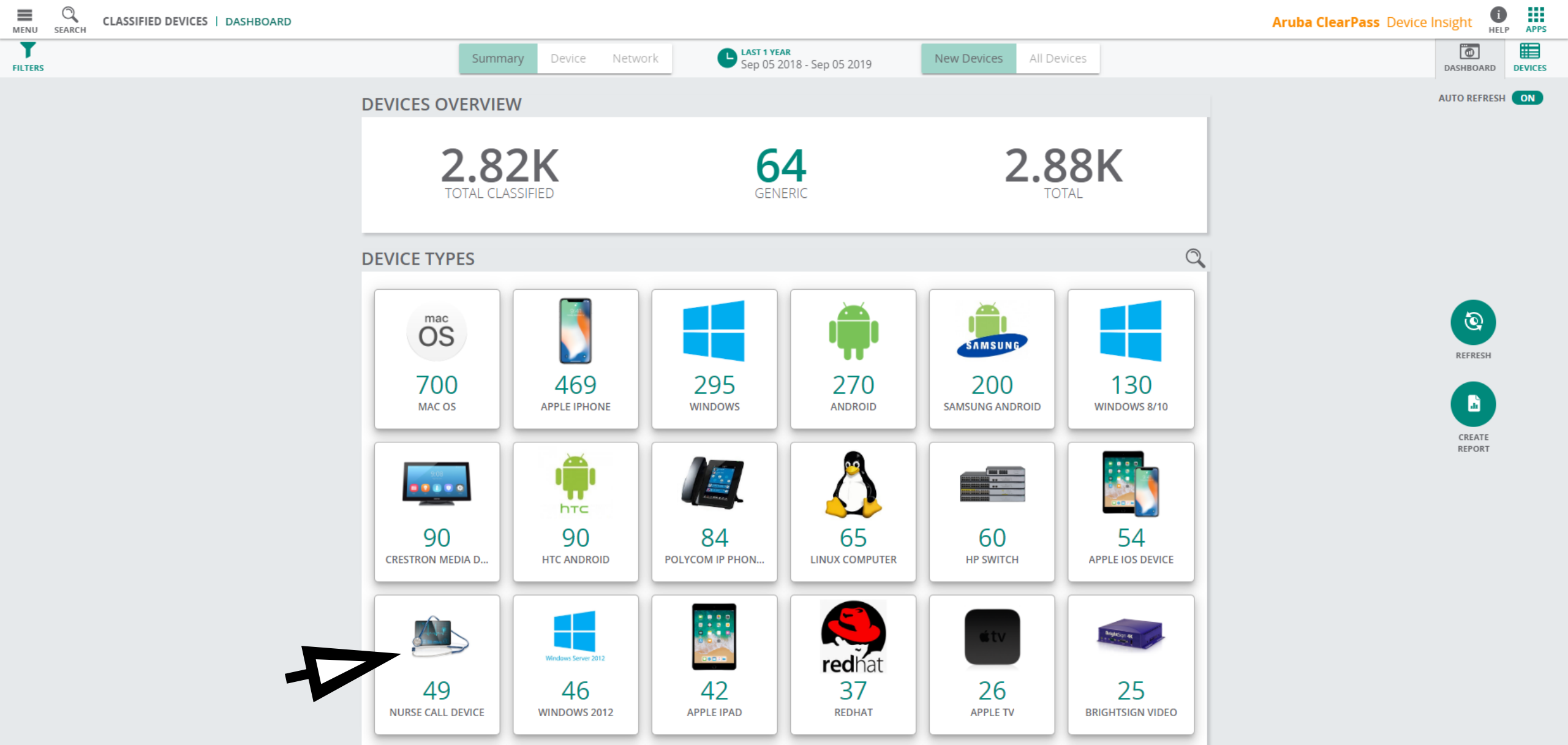
Device Identified and Labeled

No Rule Match

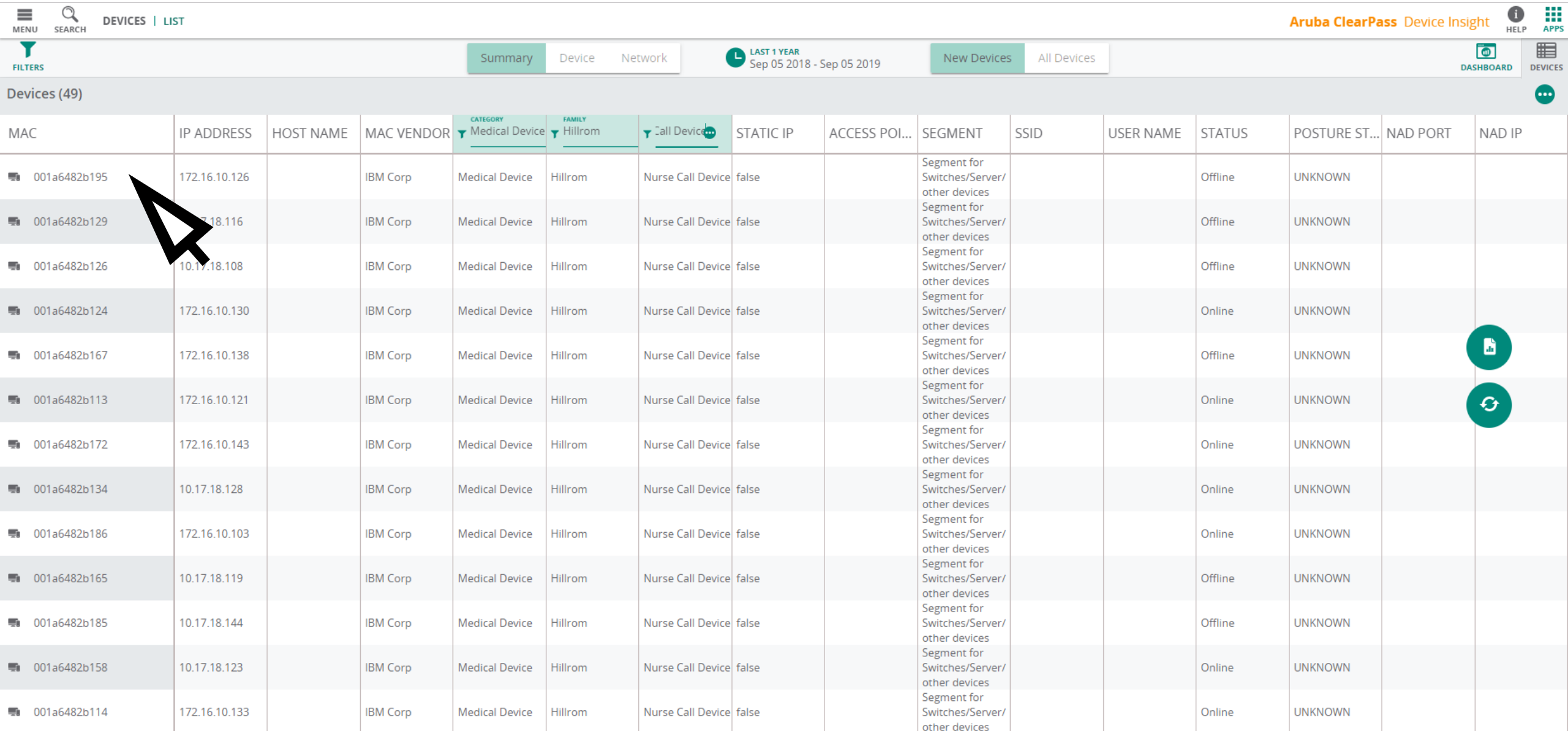
ML-based Classification

Classification based on static, flow and behavior based attributes

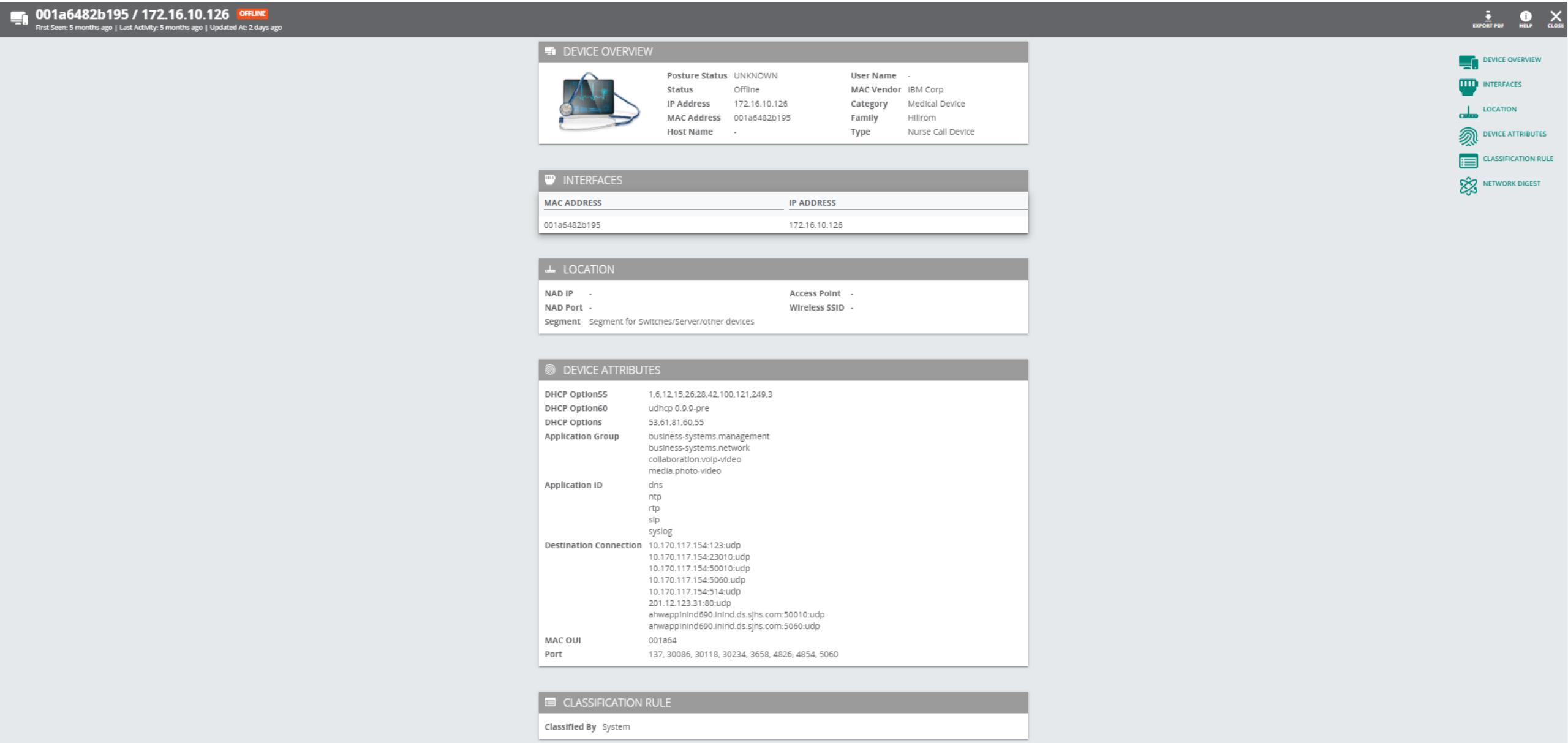
ClearPass Device Insight – Accurate Classification



ClearPass Device Insight – Accurate Classification



ClearPass Device Insight – Accurate Classification



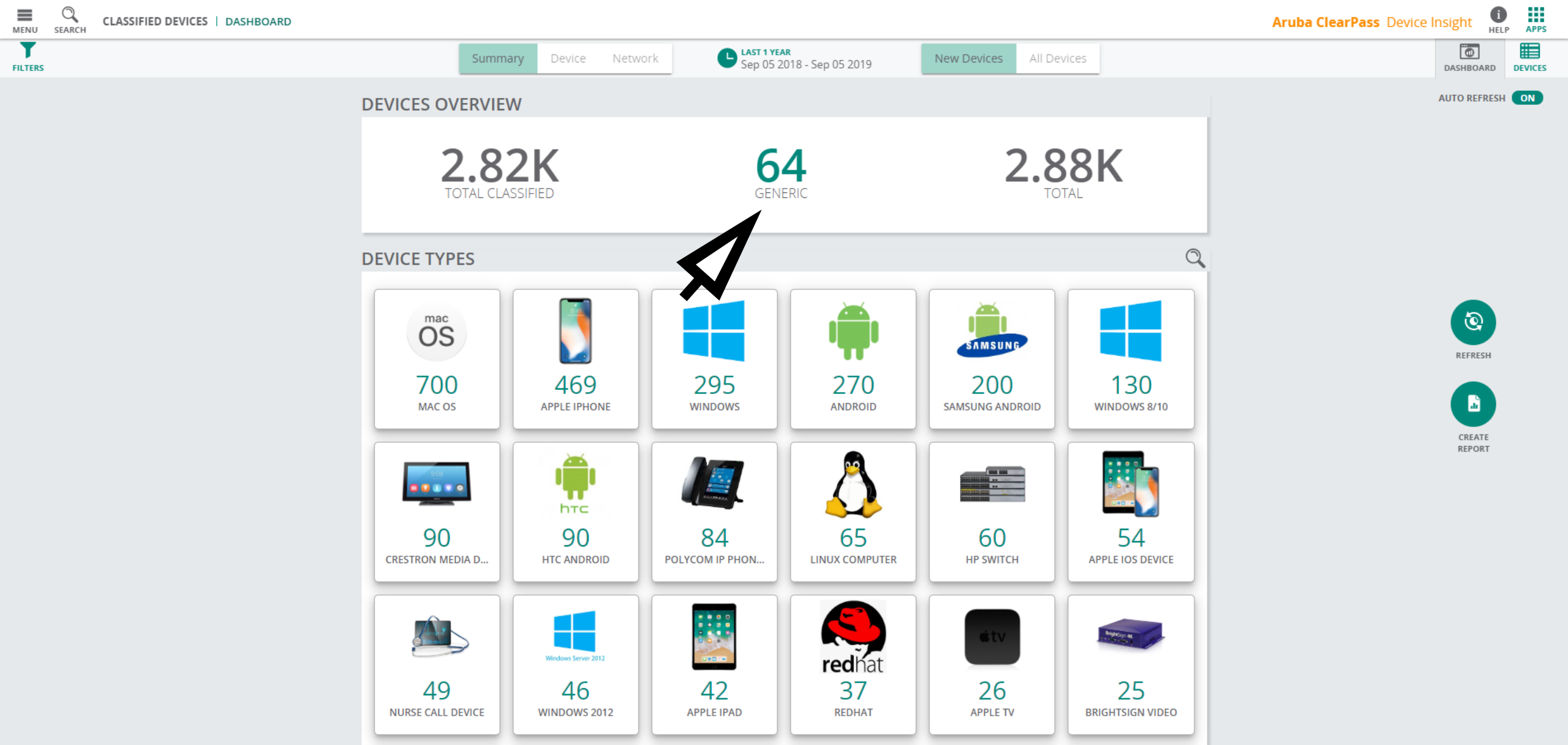
ML-ENABLED
DETERMINE THE UNKNOWN DEVICES

Static Attributes:
Operating System, Hardware Vendor
Active and Passive techniques
such as MAC OUI, NMAP, etc.

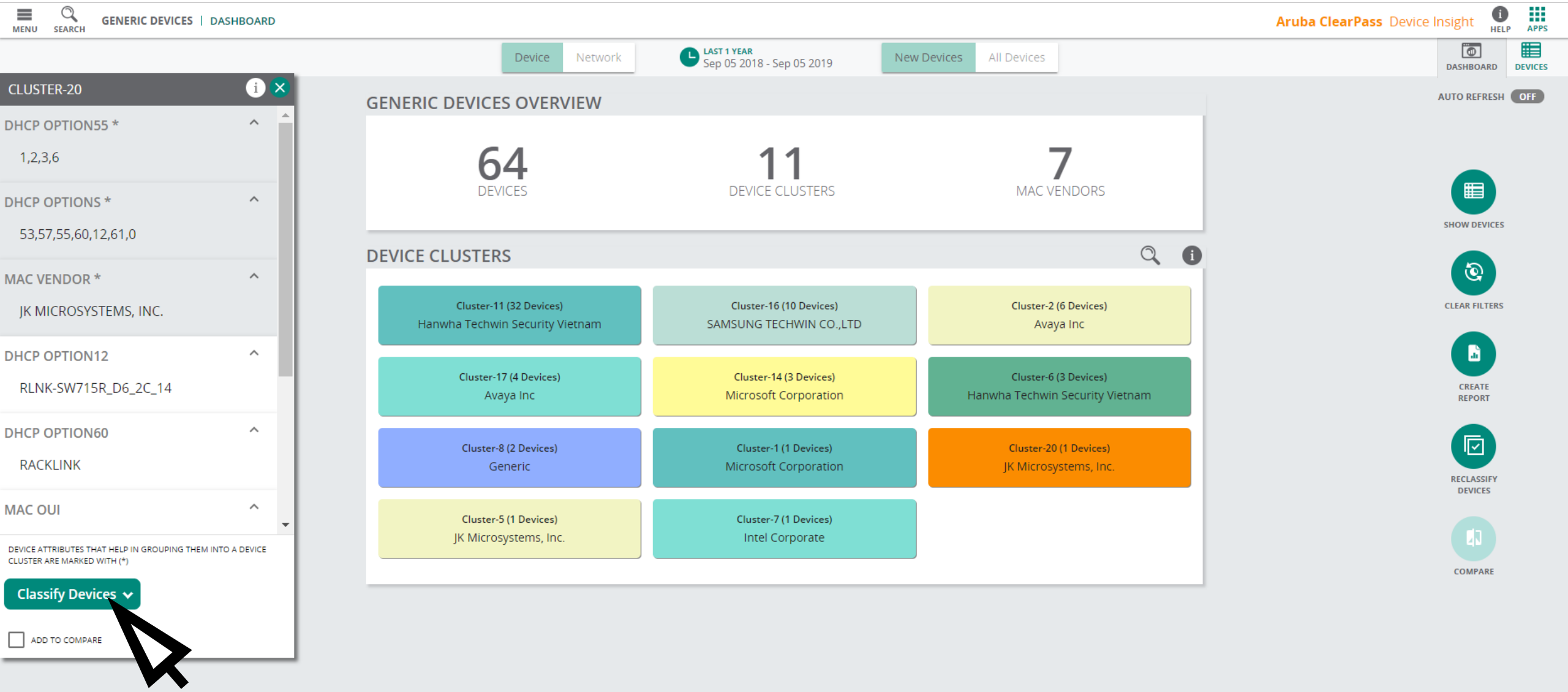
Dynamic Attributes:
Understanding Behavioral Attributes
Deep Packet Inspection (DPI) and Machine
Learning to leverage communication patterns,
applications, etc.

Comparative Attributes:
Finding Commonality
Continuous monitoring of device traffic
and crowdsourced intelligence to refine
and update device fingerprints

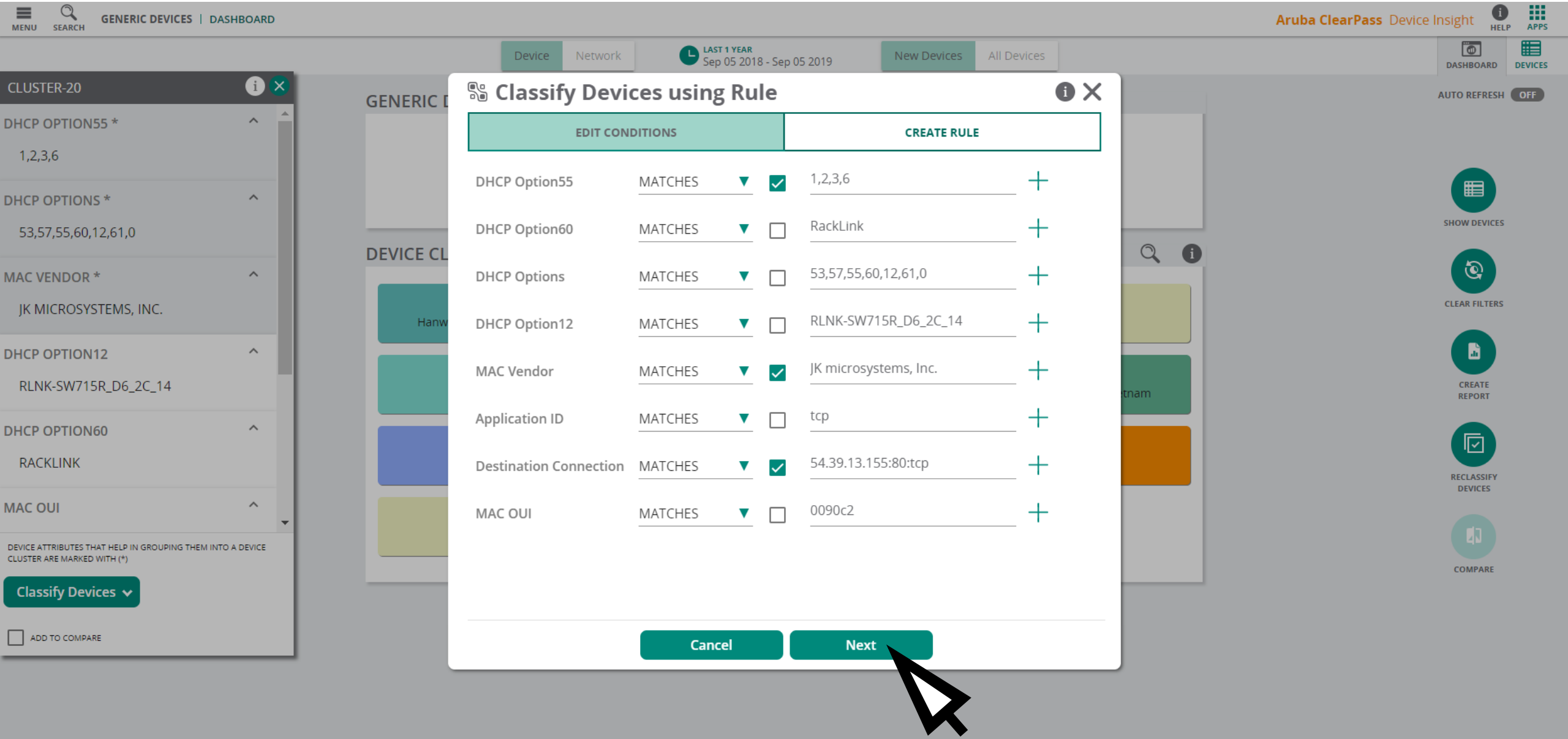
ClearPass Device Insight – Generic to Granular



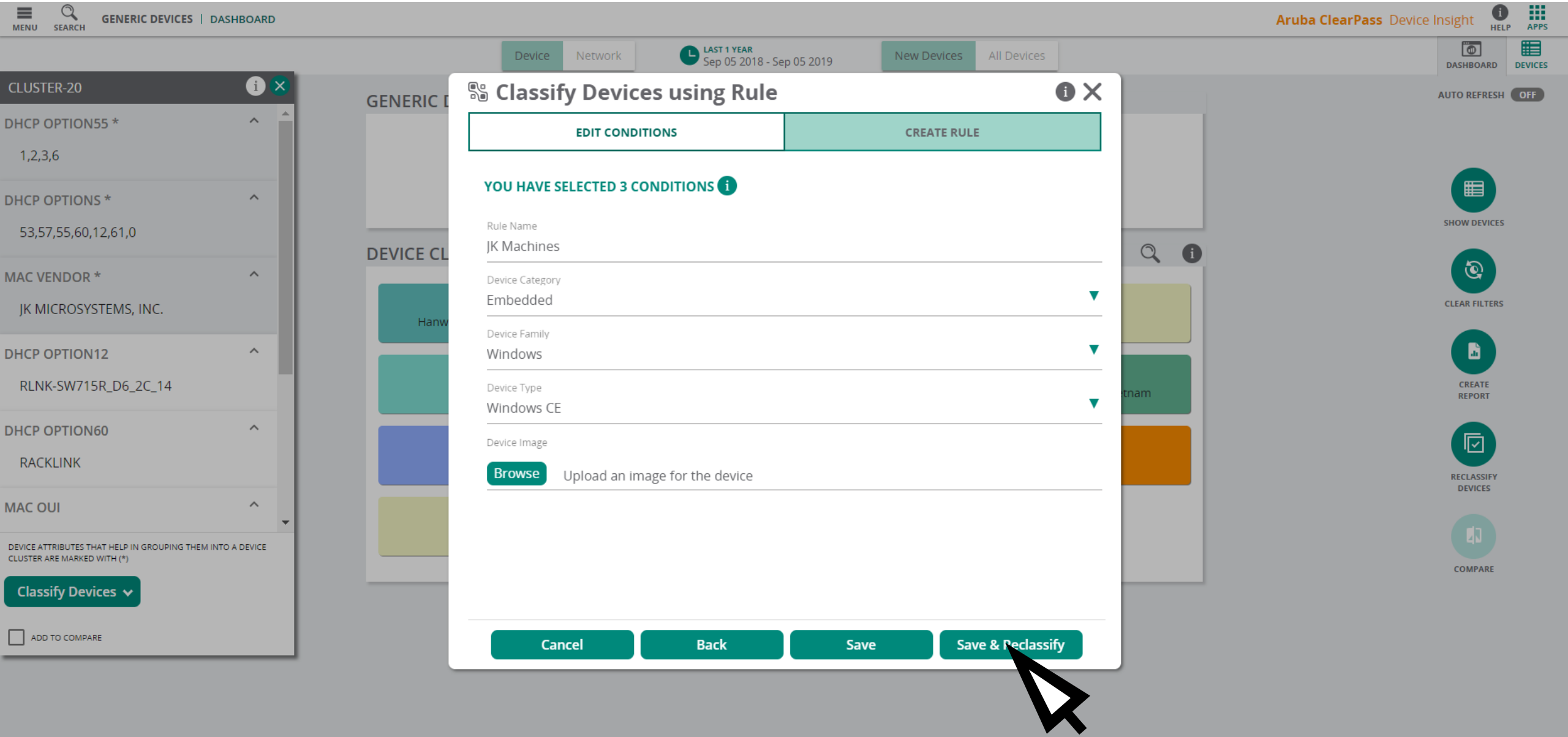
ClearPass Device Insight – Generic to Granular



ClearPass Device Insight – Generic to Granular

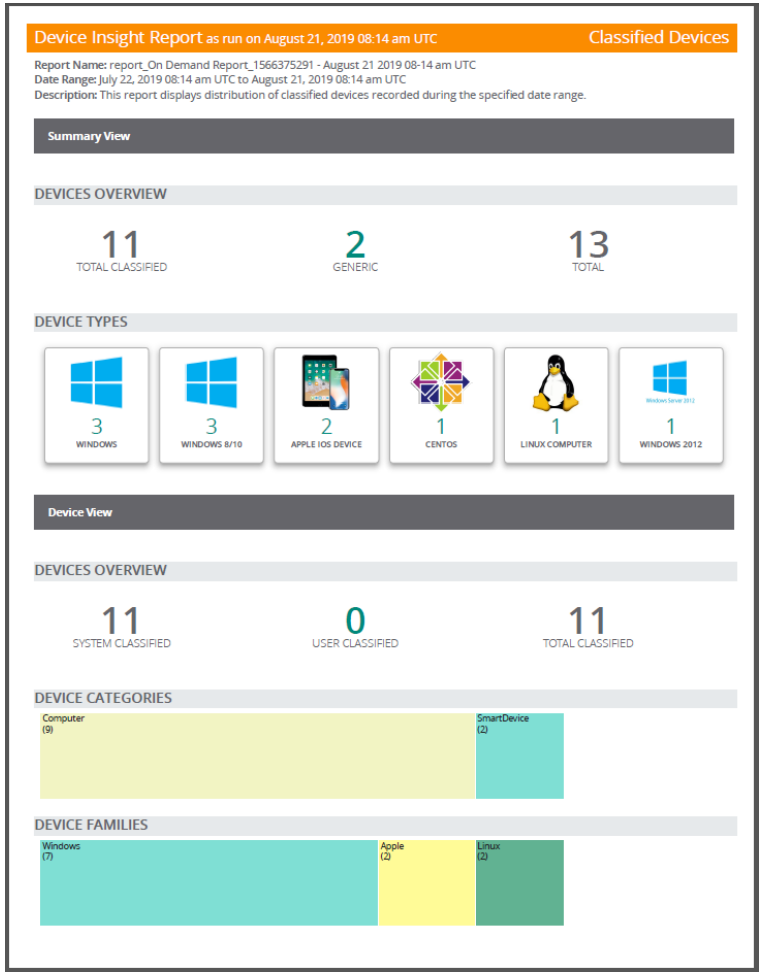


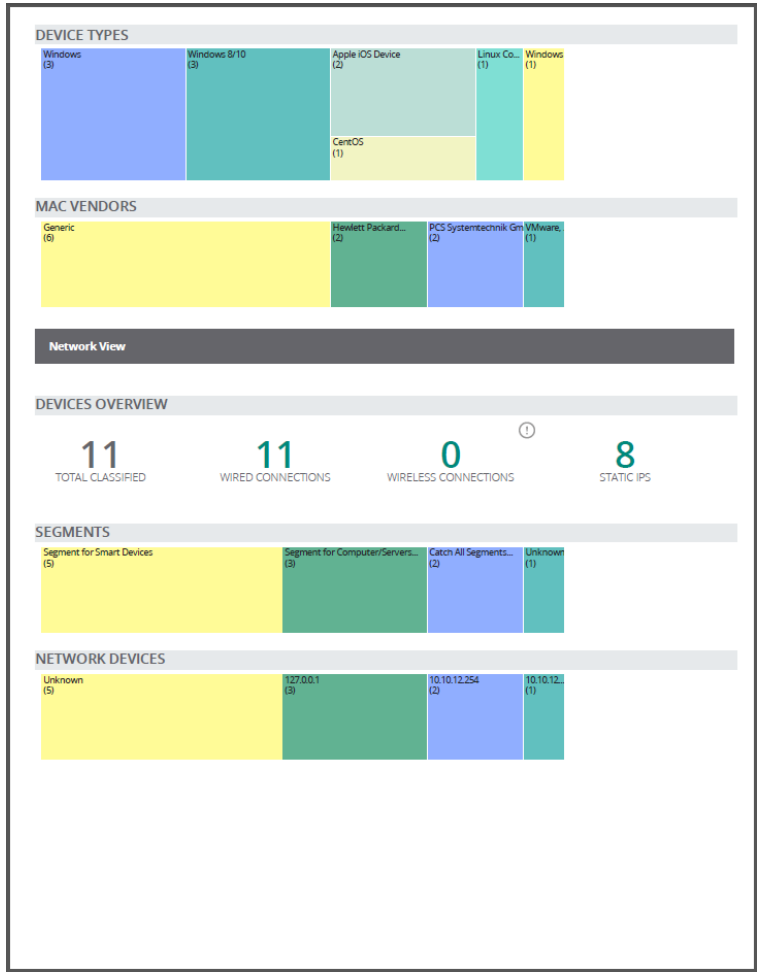
ClearPass Device Insight – Generic to Granular

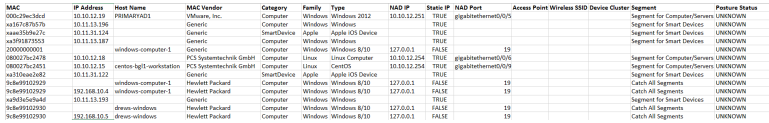


Report on anything you can filter!

– Example: New “Unknowns”







MAC	IP Address	Host Name	MAC Vendor	Category	Family	Type	NAD IP	Static IP	NAD Port	Access Point	Wireless SSID	Device Cluster	Segment	Posture Status
000c29ec3dcd	10.10.12.19	PRIMARYAD1	VMware, Inc.	Computer	Windows	Windows 2012	10.10.12.251	TRUE	gigabitethernet0/0/5				Segment for Computer/Servers	UNKNOWN
xa167cf67b7b	10.11.13.196		Generic	Computer	Windows	Windows		TRUE					Segment for Smart Devices	UNKNOWN
xaae35b9e27c	10.11.31.124		Generic	SmartDevice	Apple	Apple iOS Device		TRUE					Segment for Smart Devices	UNKNOWN
xa3f91873553	10.11.13.187		Generic	Computer	Windows	Windows		TRUE					Segment for Smart Devices	UNKNOWN
200000000001		windows-computer-1	Generic	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19					UNKNOWN
080027bc2478	10.10.12.18		PCS Systemtechnik GmbH	Computer	Linux	Linux Computer	10.10.12.254	TRUE	gigabitethernet0/0/6				Segment for Computer/Servers	UNKNOWN
080027bc2d51	10.10.12.15	centos-lg01-workstation	PCS Systemtechnik GmbH	Computer	Linux	CentOS	10.10.12.254	TRUE	gigabitethernet0/0/9				Segment for Computer/Servers	UNKNOWN
xa310eae2e82	10.11.31.122		Generic	SmartDevice	Apple	Apple iOS Device		TRUE					Segment for Smart Devices	UNKNOWN
9c8e99102929		windows-computer-1	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19				Catch All Segments	UNKNOWN
9c8e99102929	192.168.10.4	windows-computer-1	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19				Catch All Segments	UNKNOWN
xa9d3e5e9a4d	10.11.13.193		Generic	Computer	Windows	Windows		TRUE					Segment for Smart Devices	UNKNOWN
9c8e99102930		drews-windows	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19				Catch All Segments	UNKNOWN
9c8e99102930	192.168.10.5	drews-windows	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19				Catch All Segments	UNKNOWN

CLEARPASS POLICY MANAGER
AUTOMATES SECURE ACCESS

ClearPass Device Insight
ENHANCED DISCOVERY / PROFILING

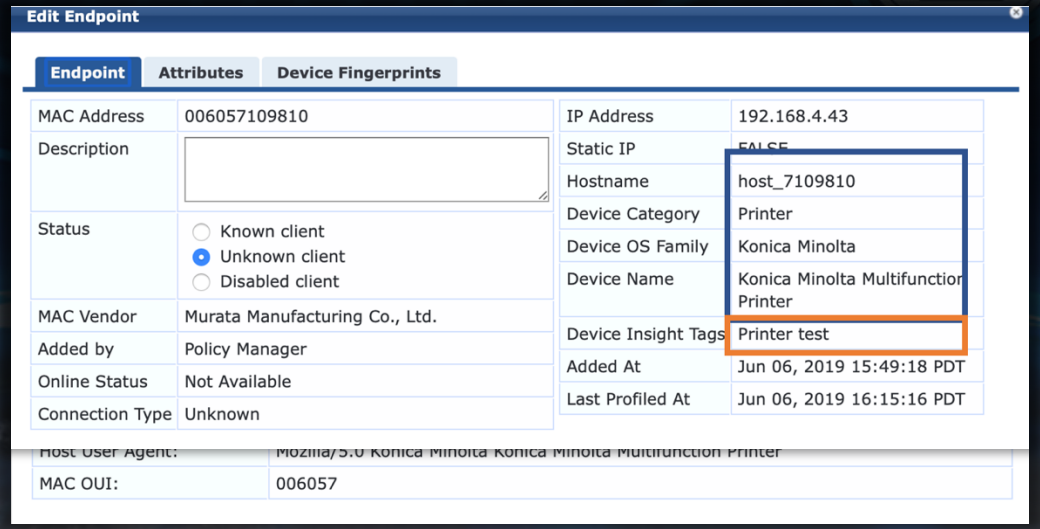
Bi-Directional
Data Exchange

ClearPass Policy Manager
AUTOMATED SEGMENTATION AND ENFORCEMENT

Bi-Directional
Data Exchange

Aruba Security Exchange
INTELLIGENCE SHARING AND AUTOMATION WITH OVER 140 PARTNERS

paloalto NETWORKS · servicenow · Carbon Black. · Check Point SOFTWARE TECHNOLOGIES LTD. · CYLANCE · okta

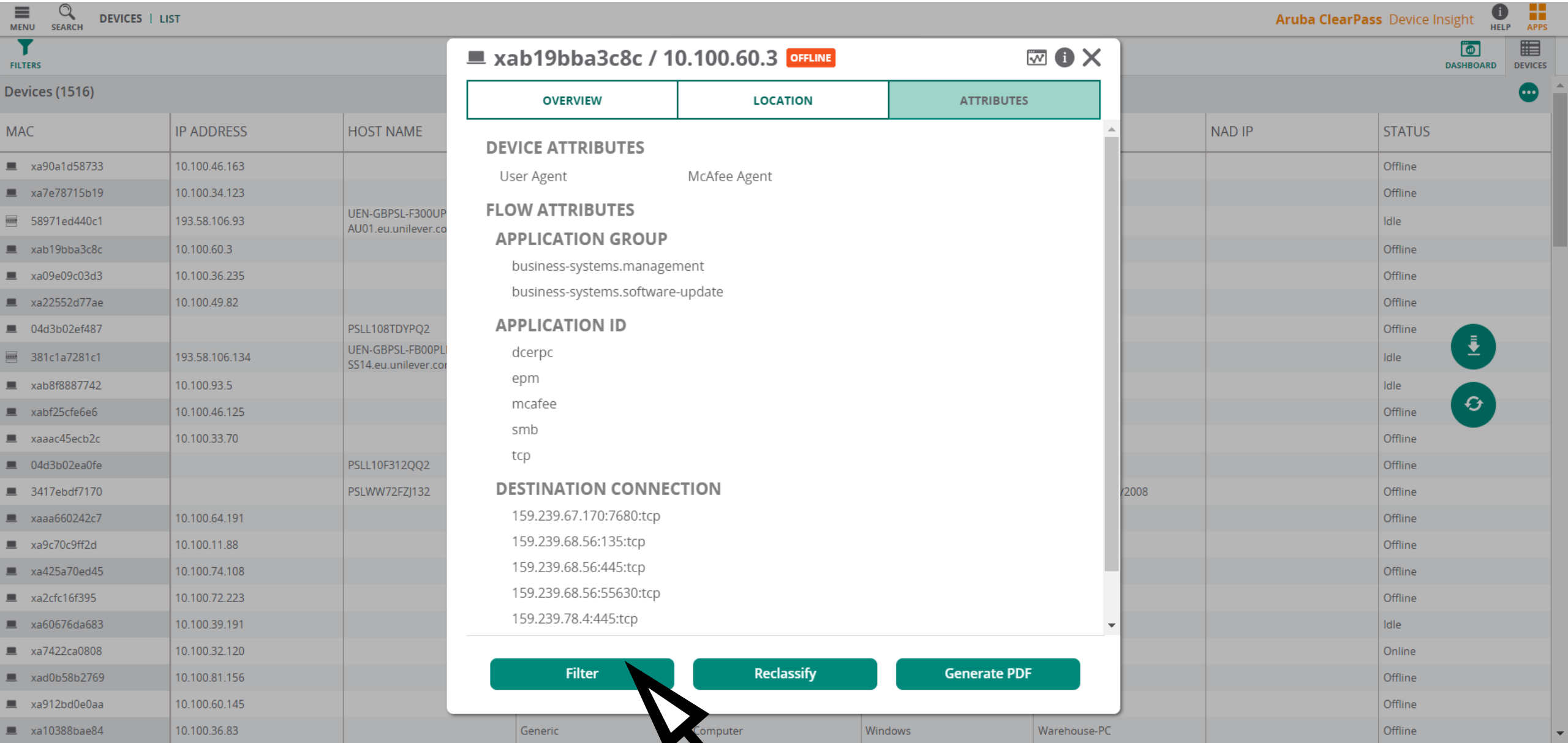


Edit Endpoint

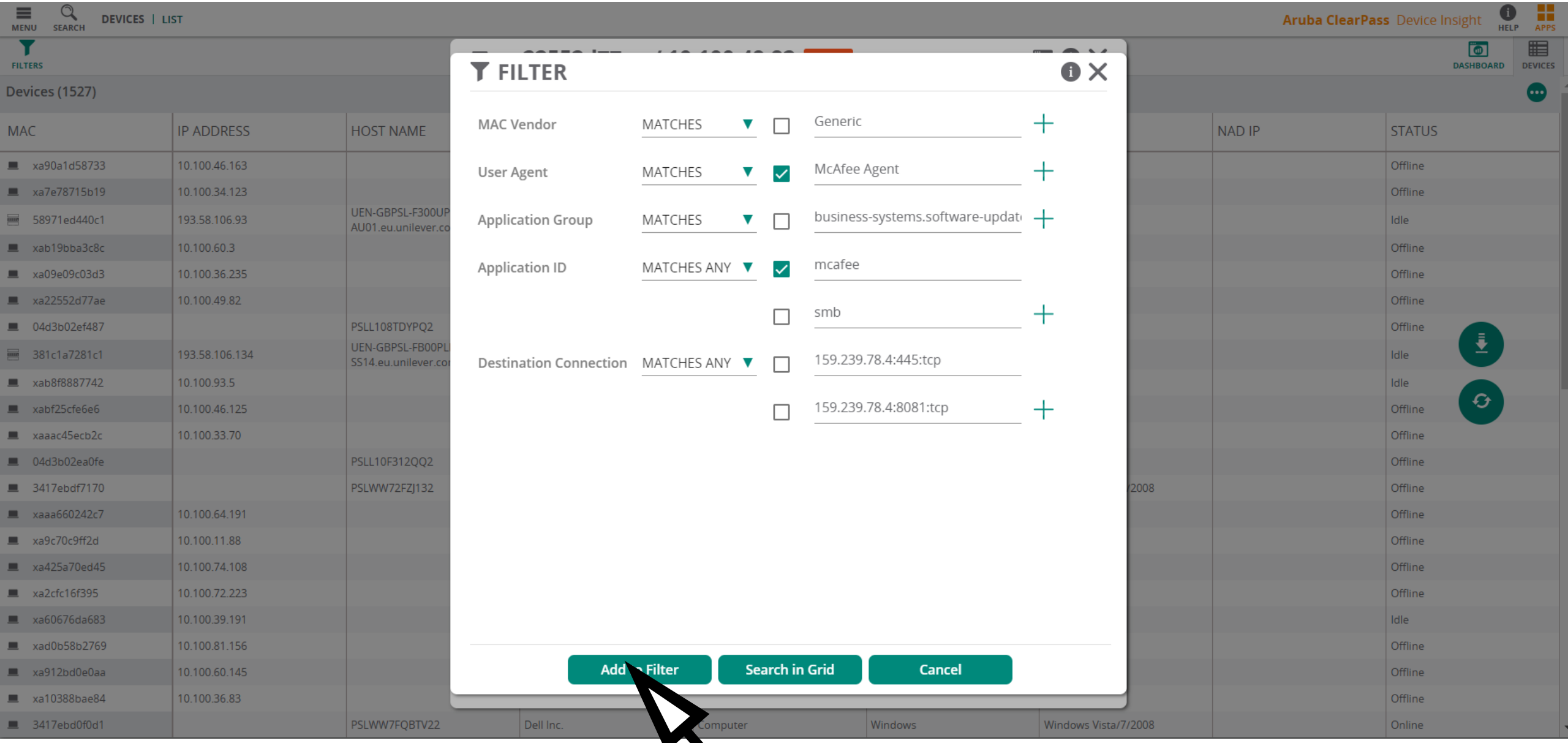
Endpoint | Attributes | Device Fingerprints

MAC Address	006057109810	IP Address	192.168.4.43
Description		Static IP	FALSE
Status	Known client / Unknown client / Disabled client	Hostname	host_7109810
		Device Category	Printer
		Device OS Family	Konica Minolta
		Device Name	Konica Minolta Multifunction Printer
MAC Vendor	Murata Manufacturing Co., Ltd.	Device Insight Tags	Printer test
Added by	Policy Manager	Added At	Jun 06, 2019 15:49:18 PDT
Online Status	Not Available	Last Profiled At	Jun 06, 2019 16:15:16 PDT
Connection Type	Unknown		
Host User Agent:	Mozilla/5.0 Konica Minolta Konica Minolta Multifunction Printer		
MAC OUI:	006057		

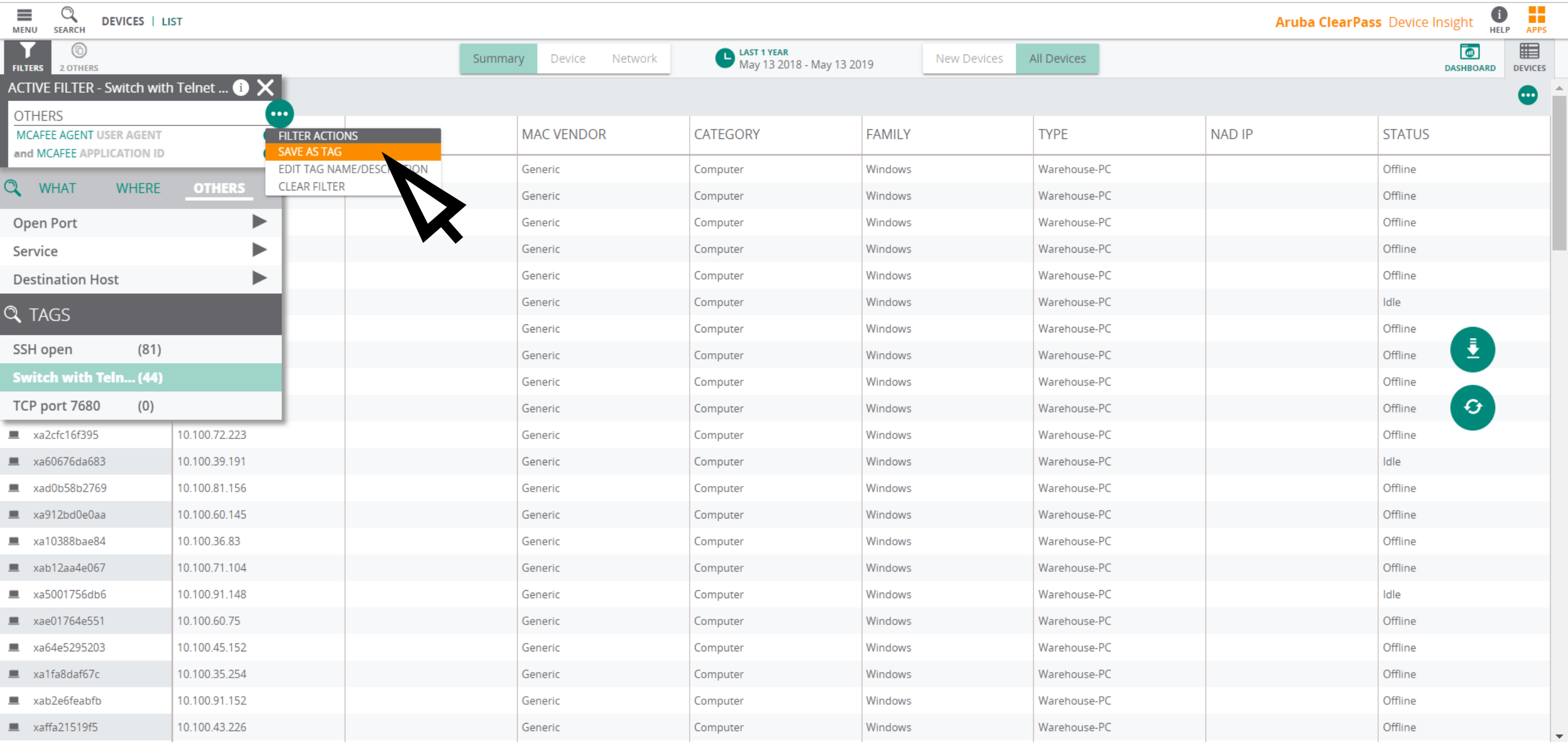
ClearPass Device Insight – Enhancing Policy



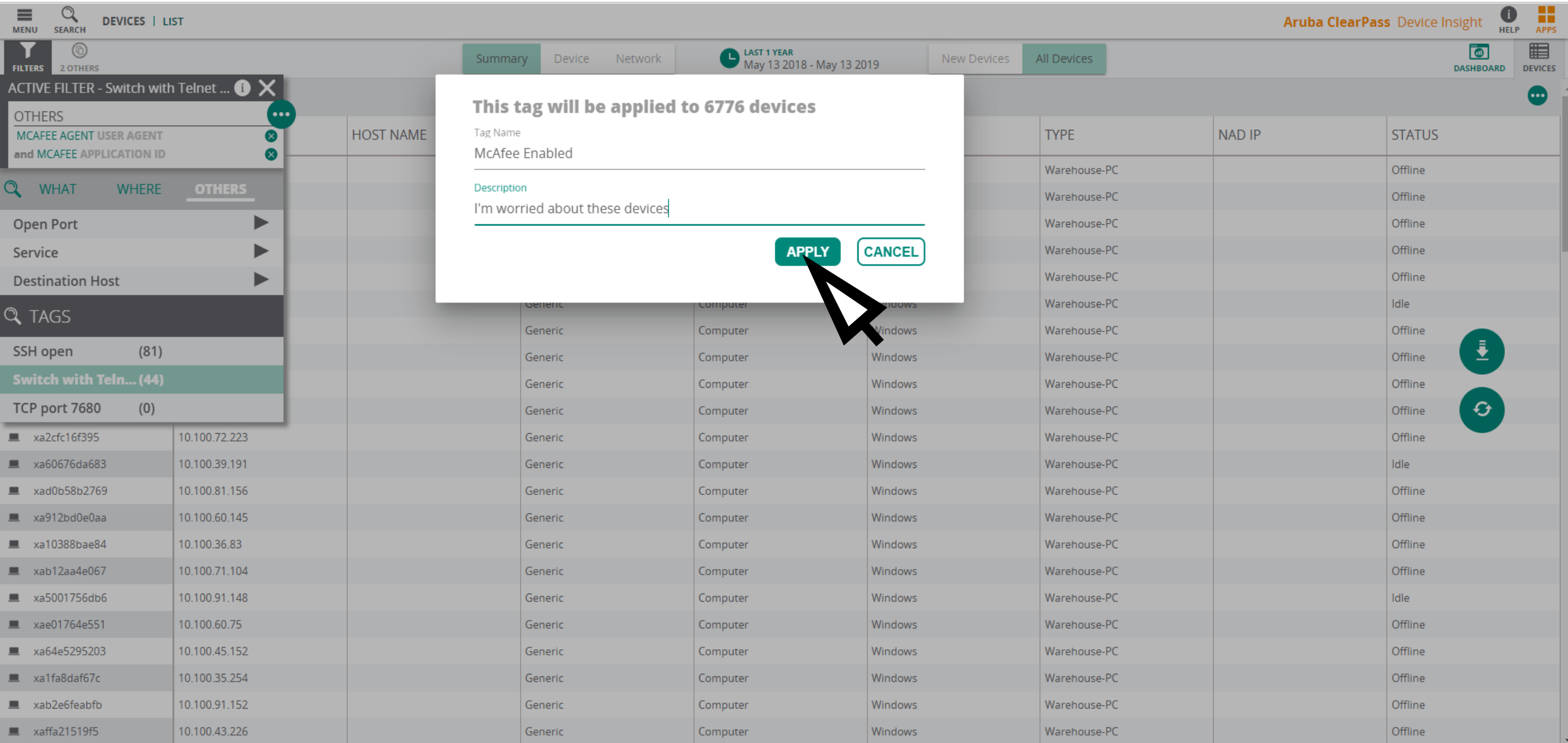
ClearPass Device Insight – Enhancing Policy



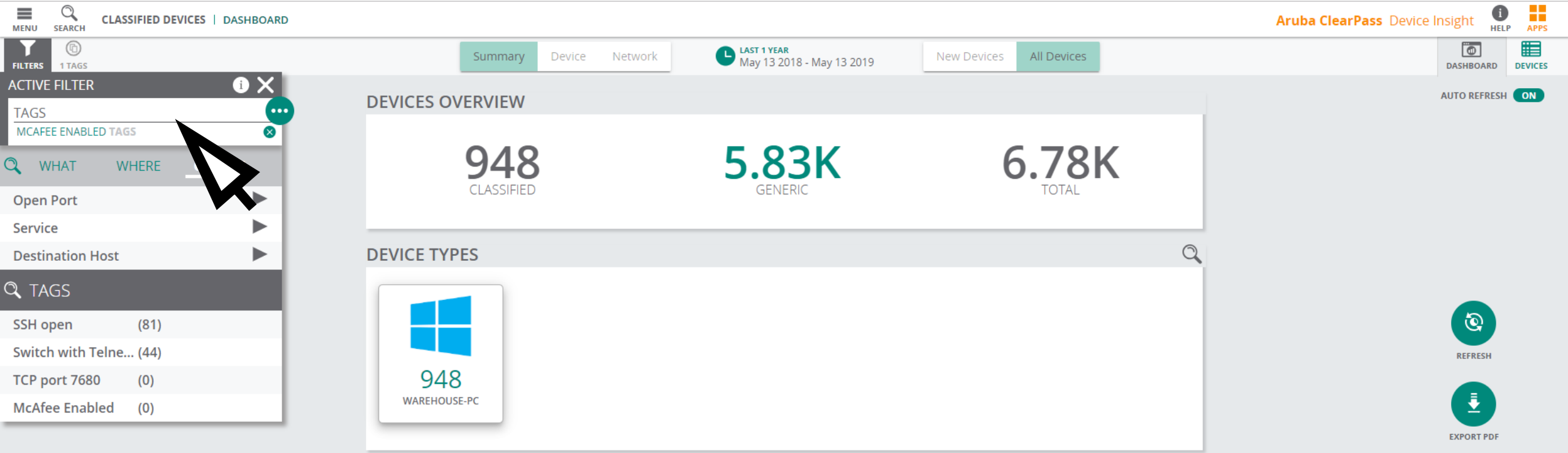
ClearPass Device Insight – Enhancing Policy



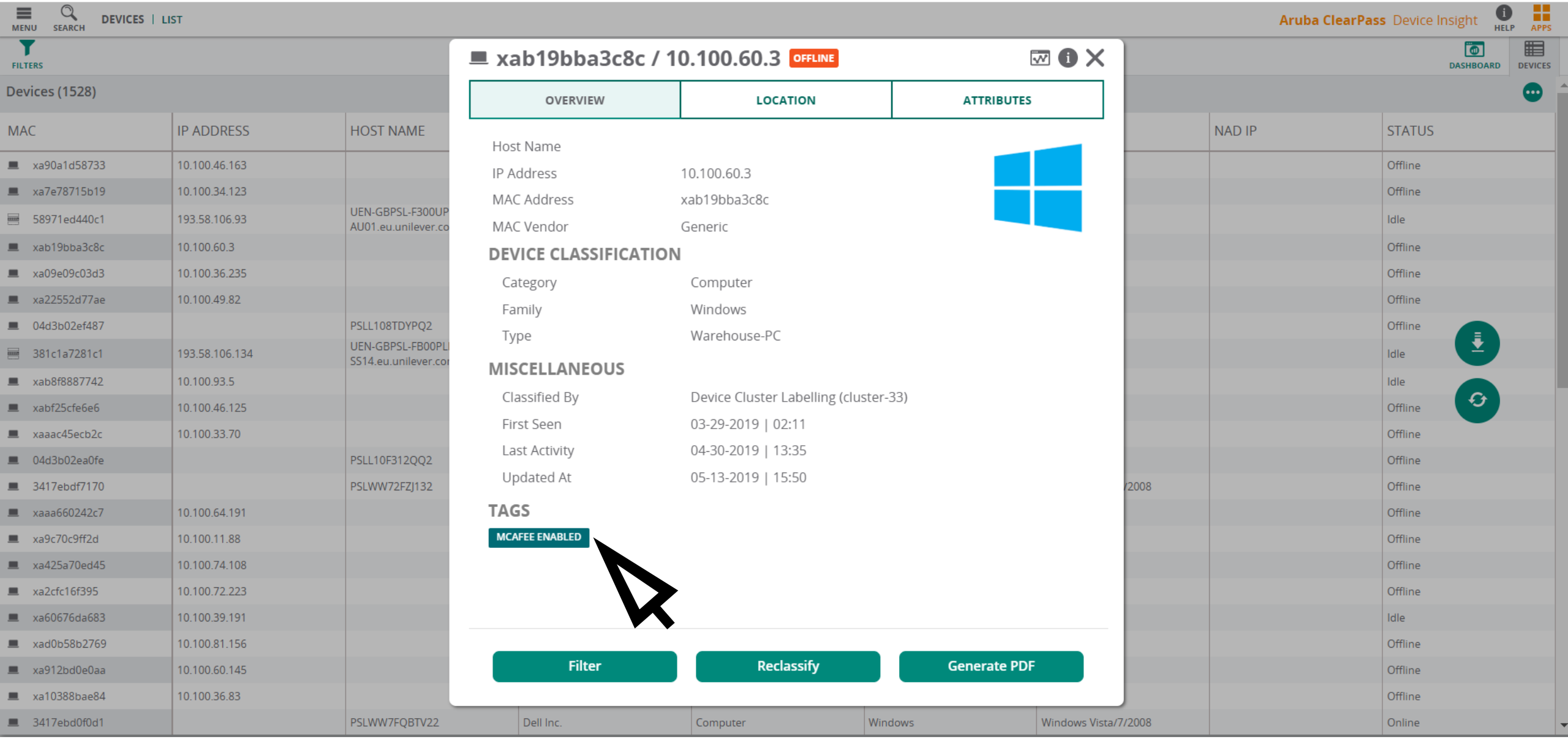
ClearPass Device Insight – Enhancing Policy



ClearPass Device Insight – Enhancing Policy



ClearPass Device Insight – Enhancing Policy



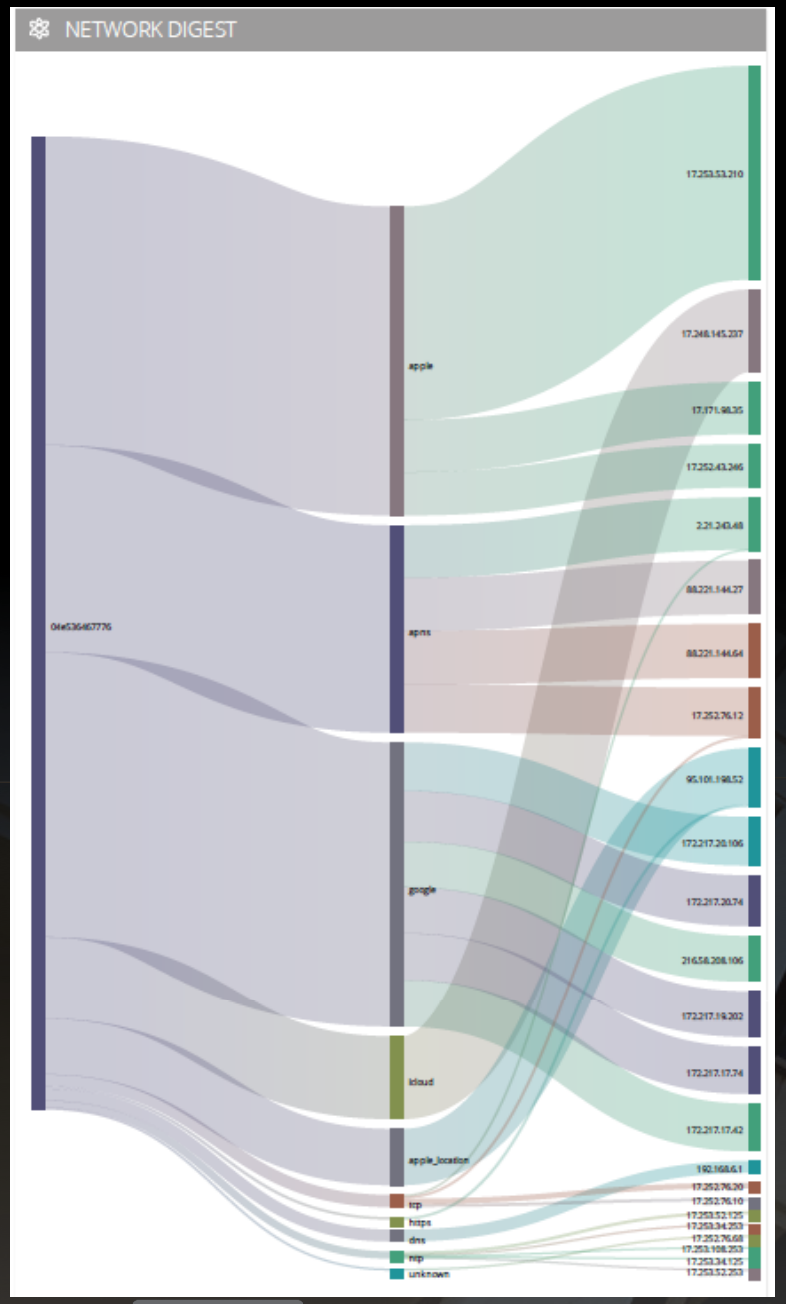
Creating Access Policy Control

Information we should consider

- **People - Roles**
- **Devices – Types/Uses**
- **Traffic Permissions**
  - What do these devices need?

Creating Access Policy Control

Device Insight – Traffic Permissions



DEVICE ATTRIBUTES

User Agent — McAfee Agent

FLOW ATTRIBUTES

APPLICATION GROUP

- business-systems.management
- business-systems.software-update

APPLICATION ID

- dcerpc
- epm
- mcafee
- smb
- tcp

DESTINATION CONNECTION

- 159.239.67.170:7680:tcp
- 159.239.68.56:135:tcp
- 159.239.68.56:445:tcp
- 159.239.68.56:55630:tcp
- 159.239.78.4:445:tcp

```
ip access-list session logon-control
    user any udp 68 deny
    any any svc-icmp permit
    any any svc-dns permit
    any any svc-dhcp permit
    any any any permit log
```

Creating Access Policy Control

Information we should consider

- People - Roles
- Devices – Types/Uses
- Traffic Permissions
- Location Context
  - Based on AP / Switch – GPS or beacon?

Creating Access Policy Control

Information we should consider

- People - Roles
- Devices – Types/Uses
- Traffic Permissions
- Location Context
- Time Context
  - Working hours are still valid somewhere!

Creating Access Policy Control

Information we should consider

- People - Roles
- Devices – Types/Uses
- Traffic Permissions
- Location Context
- Time Context
- 3rd Party Queries / Integrations Context
  - A wealth of information…

Creating Access Policy Control

ClearPass Policy Manager Integrations

Creating Access Policy Control

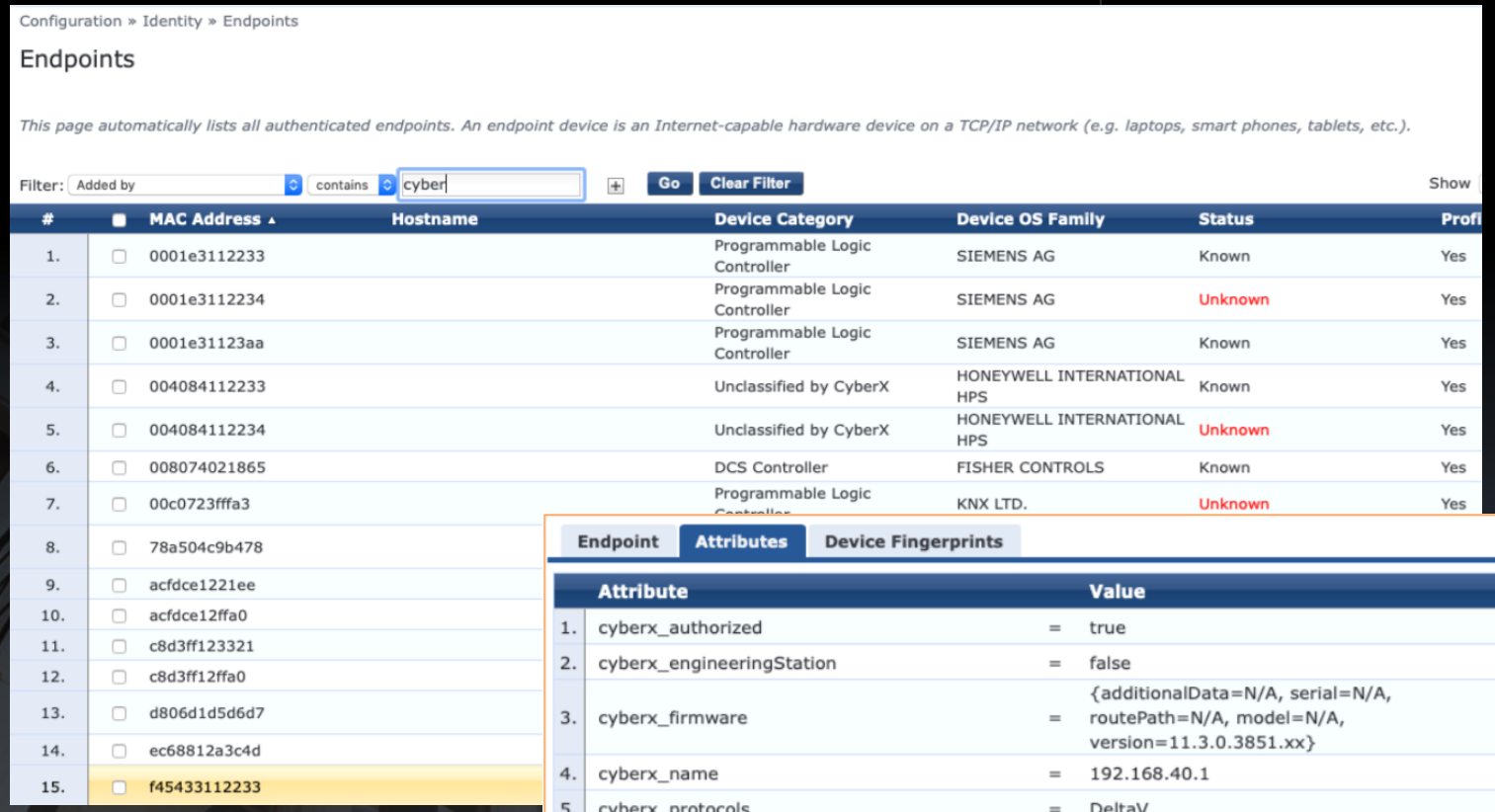
ClearPass Policy Manager Integrations

Indegy

NOZOMI NETWORKS

CLAROTY
Clarity for OT Networks

CYBERX
BATTLE-TESTED INDUSTRIAL CYBERSECURITY



Adaptive Trust – Visibility into Action

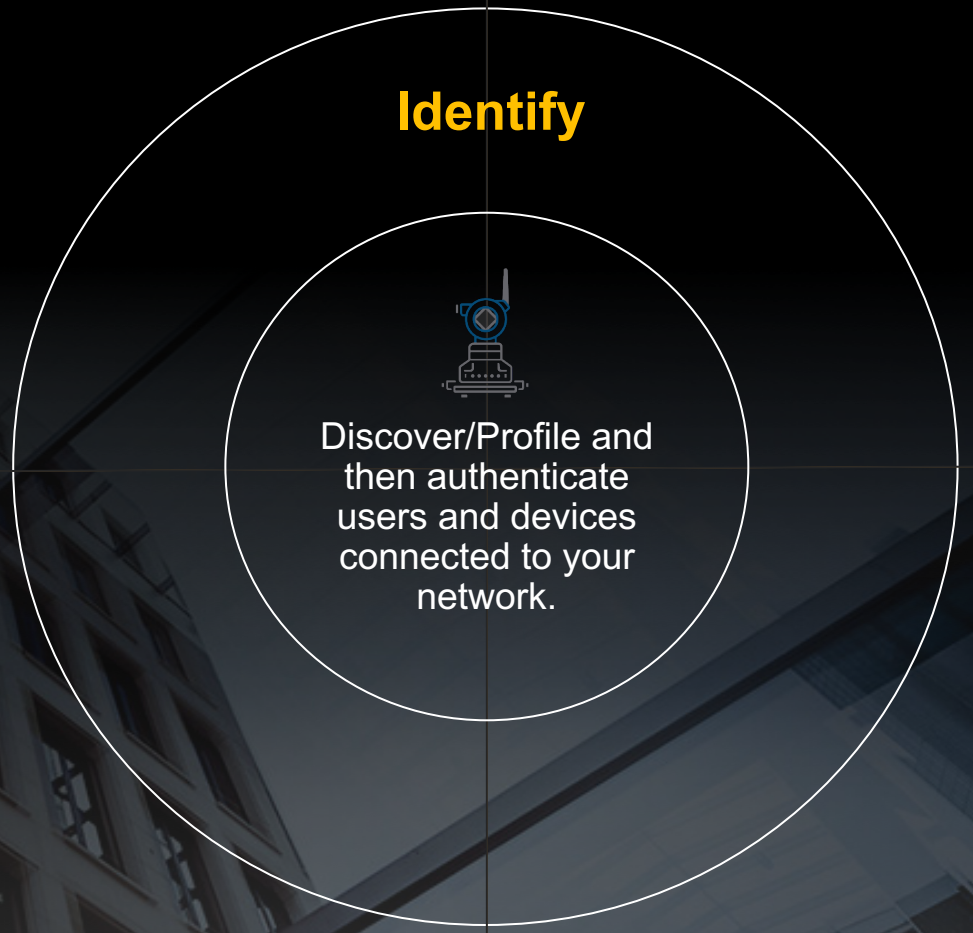
The Closed Loop approach to Security

Request Details

Summary | Input | Output | Accounting

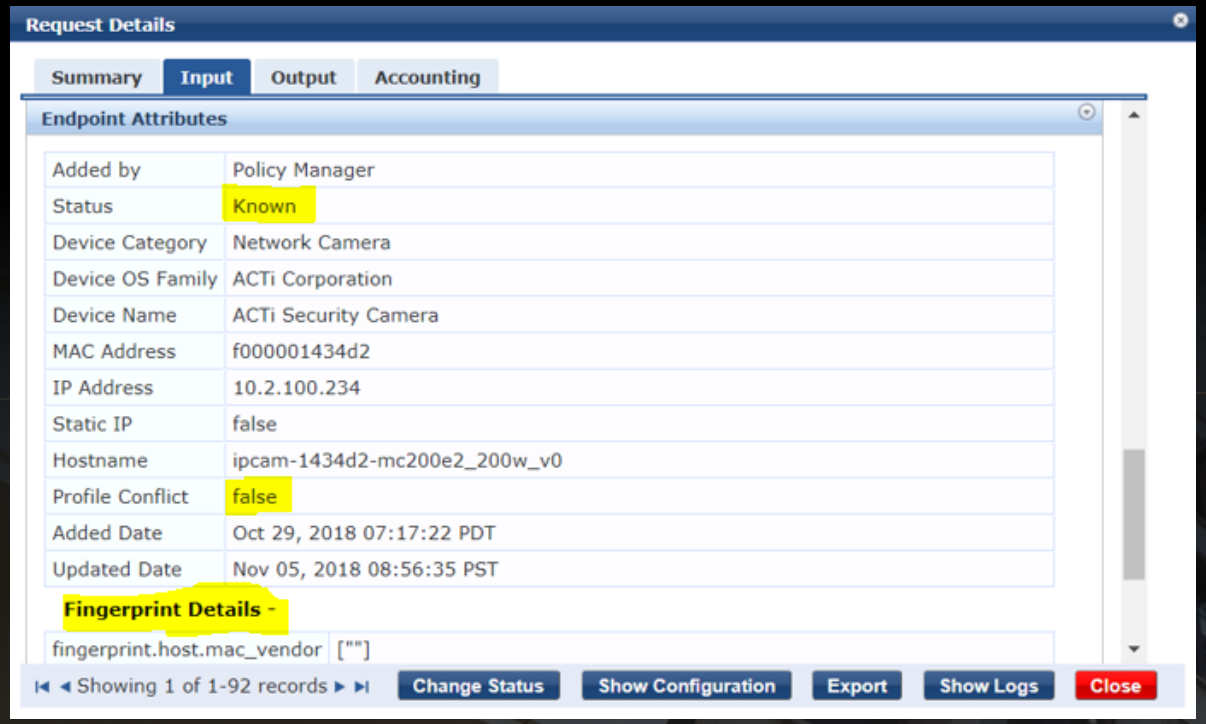
Login Status:	ACCEPT
Session Identifier:	R00000119-01-5be07642
Date and Time:	Nov 05, 2018 08:56:34 PST
End-Host Identifier:	F000001434D2 (Network Camera / ACTi Corporation / ACTi Security Camera) Open in AirWave
Username:	f000001434d2
Access Device IP/Port:	10.2.100.20:54 (10.2.100.20 / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	MAC-based Authentication Service
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Endpoints Repository], [Time Source]
Roles:	[User Authenticated]
Enforcement Profiles:	IoT-mac-auth-allow-access
Service Monitor Mode:	Disabled

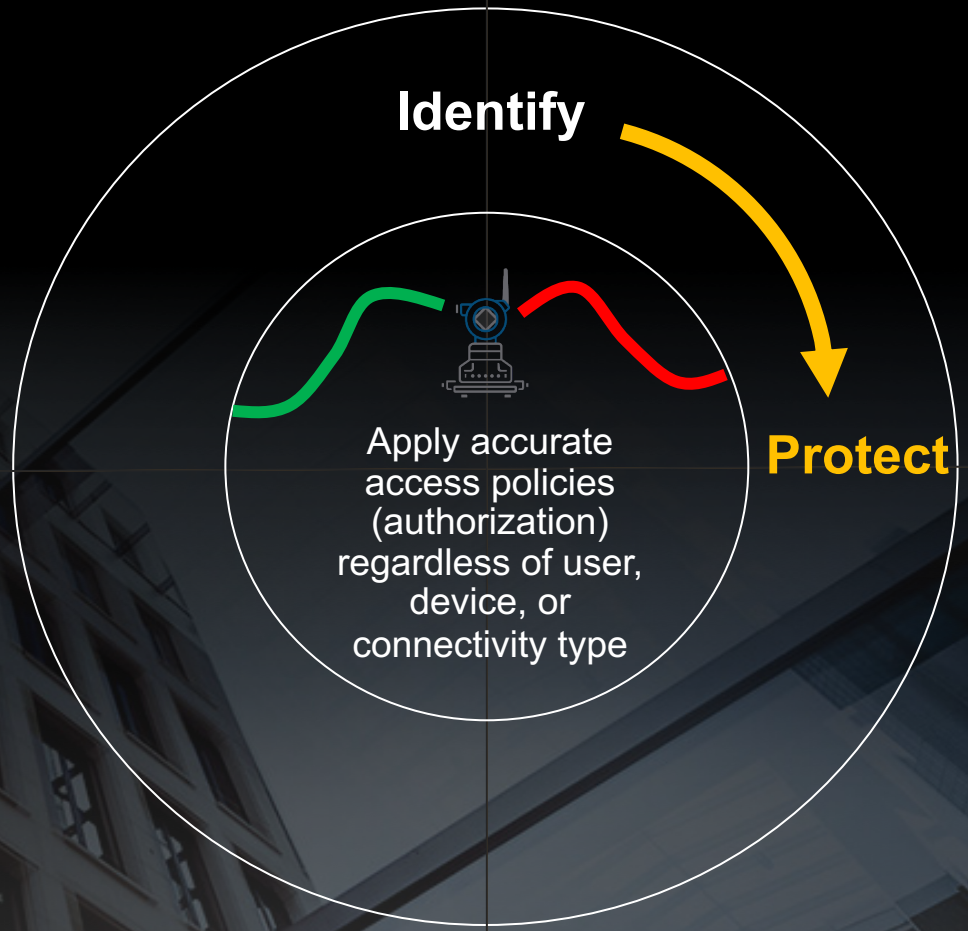
◂ Showing 1 of 1-92 records ▸ | Change Status | Show Configuration | Export | Show Logs | Close



Adaptive Trust in action

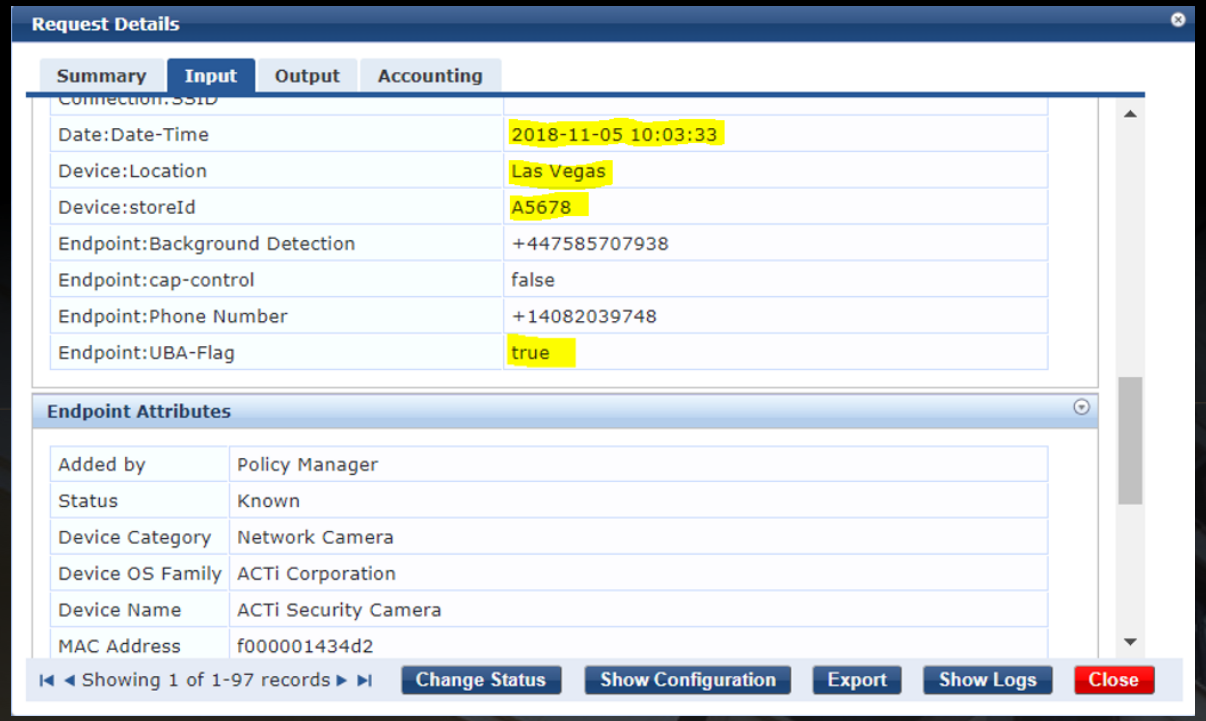
The Closed Loop approach to Security

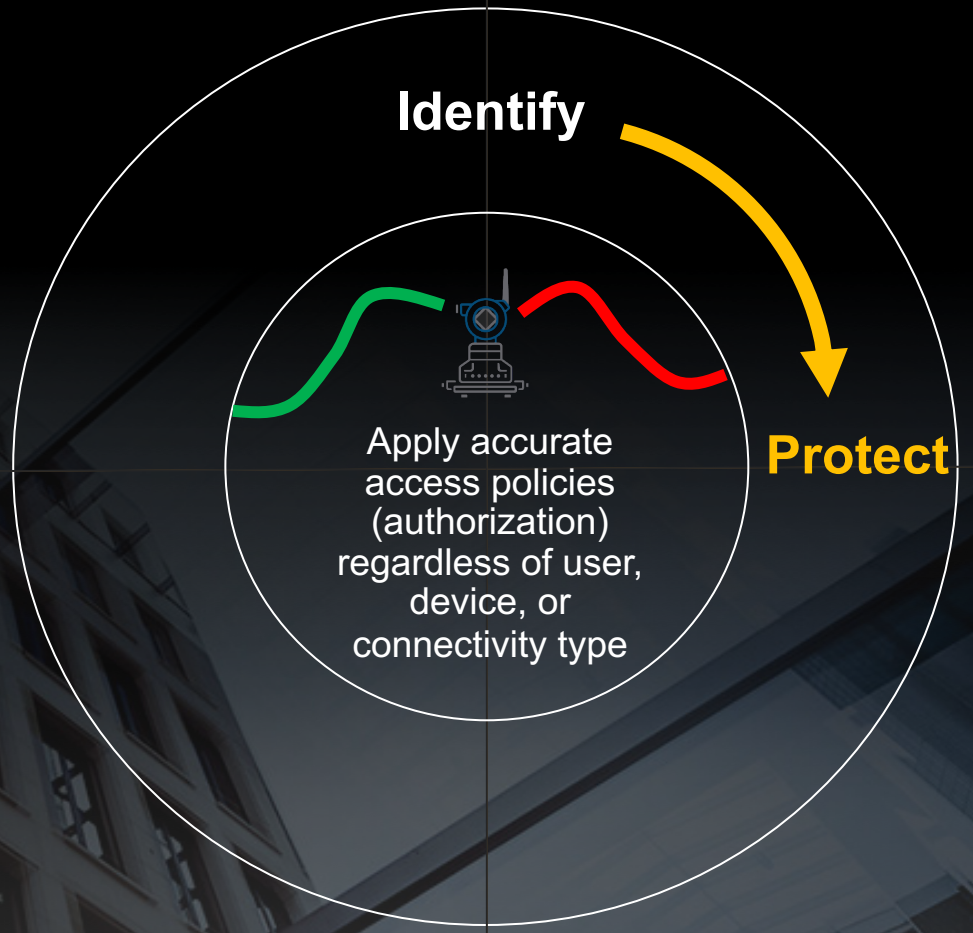




Adaptive Trust in action

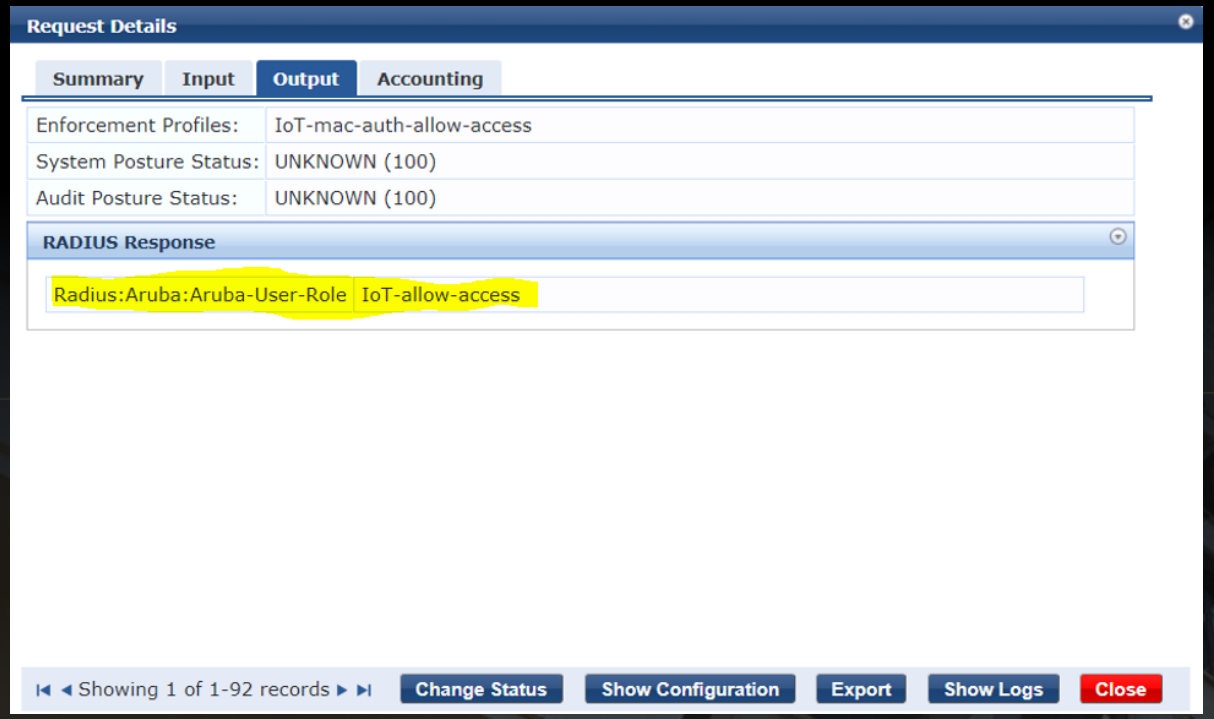
The Closed Loop approach to Security

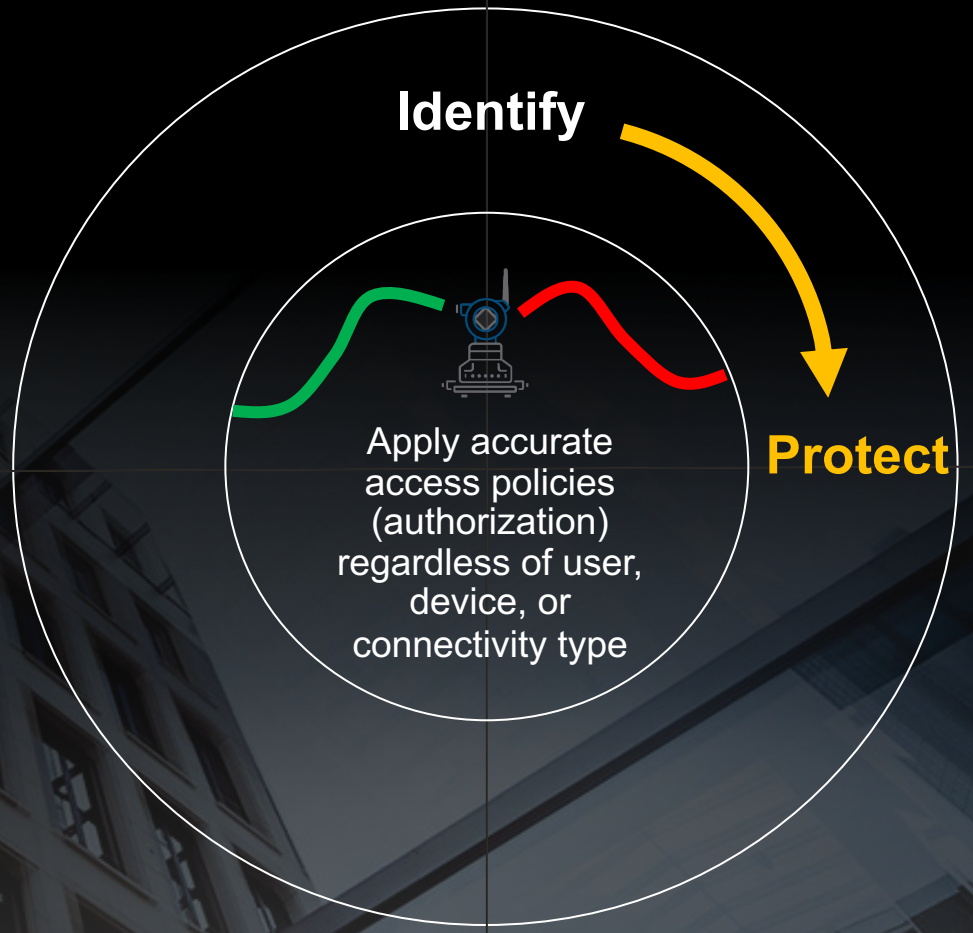




Adaptive Trust in action

The Closed Loop approach to Security

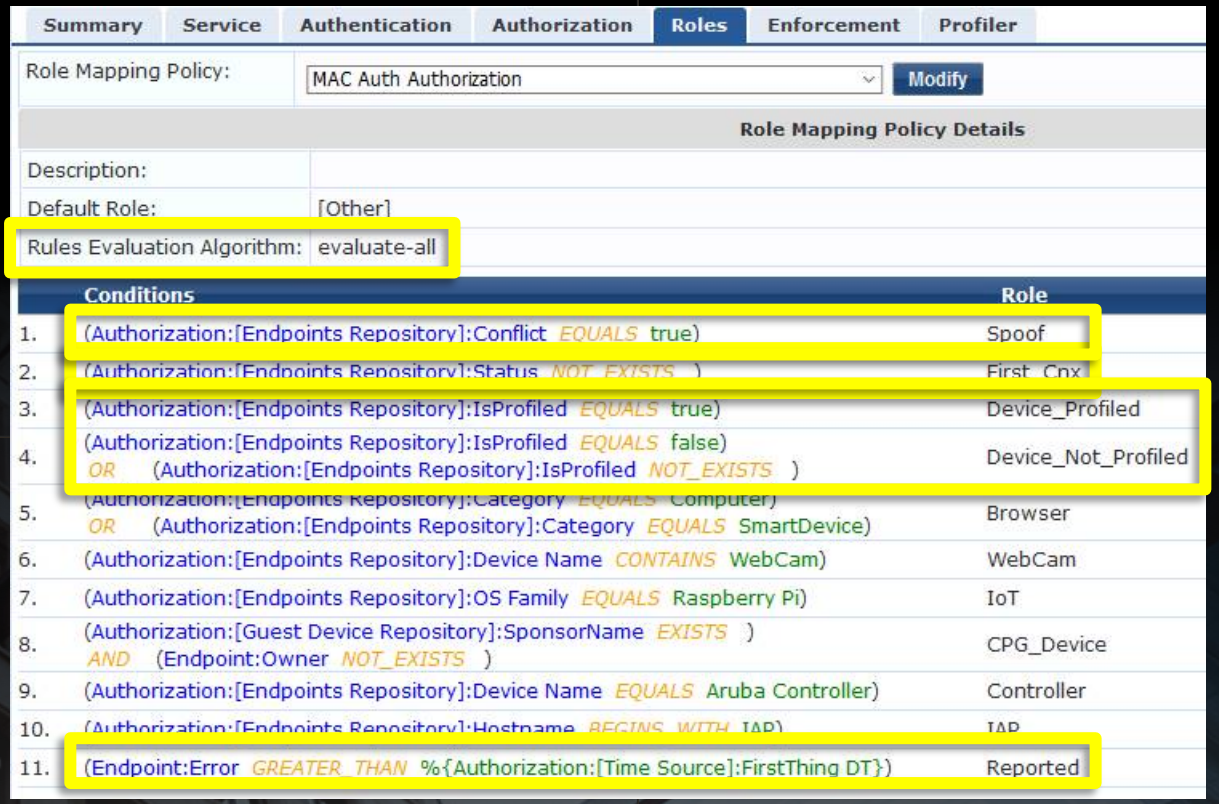




Dealing with the Unknowns

Applying decision making labels

- Have we seen it before?
- Has it been reported?
- Do we know what it is?
- Is it lying to me?



Adaptive Trust in action

Making the decisions!

- First attempt

Enforcement Policy Details

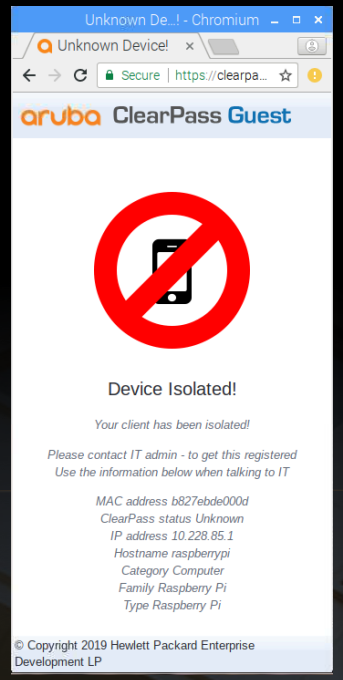
Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

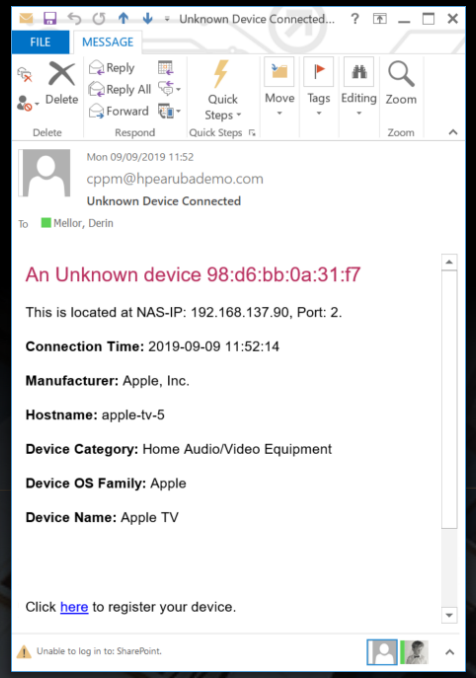
	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS Disabled)	DUR_Wired_Blocked, email - malicious device
2.	(Tips:Role EQUALS Spoof)	DUR_Wired_Blocked, email - wired spoof device
3.	(Tips:Role MATCHES_ALL First_Cnx	[Update Endpoint Known], Set Owner, DUR_Wired_Profile_portal
4.	(Tips:Role EQUALS First_Cnx)	DUR_Wired_Profile_portal
5.	(Tips:Role MATCHES_ALL Unknown Reported)	DUR_Wired_Unknown
6.	(Tips:Role EQUALS Unknown)	DUR_Wired_Unknown, email - wired unknown device, Reported
7.	(Tips:Role EQUALS Controller)	DUR_Wired_Controller, Full Scan
8.	(Tips:Role EQUALS IAP)	DUR_Wired_IAP, SNMP Scan, NMAP Scan
9.	(Tips:Role EQUALS Access Points)	DUR_Wired_AP-Basic, NMAP Scan
10.	(Tips:Role EQUALS Home Audio/Video Equipment)	DUR_Wired_AppleTV, NMAP Scan
11.	(Tips:Role EQUALS Guest)	DUR_Wired_Guest
12.	(Tips:Role EQUALS IoT)	DUR_Wired_IoT, NMAP Scan
13.	(Tips:Role EQUALS Printer)	DUR_Wired_Printer, SNMP Scan
14.	(Tips:Role EQUALS WebCam)	DUR_Wired_WebCam
15.	(Tips:Role EQUALS [Machine Authenticated])	DUR_Wired_Isolation
16.	(Tips:Role EQUALS [User Authenticated])	DUR_Wired_Guest_Reg

#	Request Timestamp	Source	NAS Name	NAS Port	Auth Method	Host MAC Address	Username	Service	Login Status	Enforcement Profiles
1.	2019/09/09 13:10:53	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	NMAP Scan, DUR_Wired_AppleTV
2.	2019/09/09 12:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Unknown
3.	2019/09/09 11:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	email - wired unknown device, Reported, DUR_Wired_Unknown
4.	2019/09/09 11:42:39	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Profile_portal

Adaptive Trust in action

Making the decisions!





Enforcement Policy Details

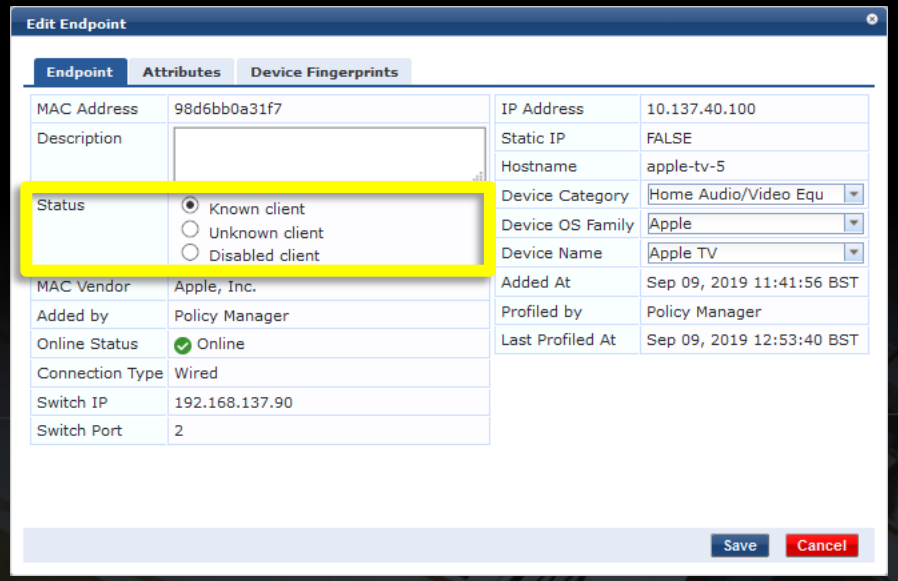
Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* Disabled)	DUR_Wired_Blocked, email - malicious device
2.	(Tips:Role *EQUALS* Spoof)	DUR_Wired_Blocked, email - wired spoof device
3.	(Tips:Role *MATCHES_ALL* First_Cnx CPG_Device)	[Update Endpoint Known], Set Owner, DUR_Wired_Profile_portal
4.	(Tips:Role *EQUALS* First_Cnx)	DUR_Wired_Profile_portal
5.	(Tips:Role *MATCHES_ALL* Unknown	DUR_Wired_Unknown
6.	(Tips:Role *EQUALS* Unknown)	DUR_Wired_Unknown, email - wired unknown device, Reported
7.	(Tips:Role *EQUALS* Controller)	DUR_Wired_Controller, Full Scan
8.	(Tips:Role *EQUALS* IAP)	DUR_Wired_IAP, SNMP Scan, NMAP Scan
9.	(Tips:Role *EQUALS* Access Points)	DUR_Wired_AP-Basic, NMAP Scan
10.	(Tips:Role *EQUALS* Home Audio/Video Equipment)	DUR_Wired_AppleTV, NMAP Scan
11.	(Tips:Role *EQUALS* Guest)	DUR_Wired_Guest
12.	(Tips:Role *EQUALS* IoT)	DUR_Wired_IoT, NMAP Scan
13.	(Tips:Role *EQUALS* Printer)	DUR_Wired_Printer, SNMP Scan
14.	(Tips:Role *EQUALS* WebCam)	DUR_Wired_WebCam
15.	(Tips:Role *EQUALS* [Machine Authenticated])	DUR_Wired_Isolation
16.	(Tips:Role *EQUALS* [User Authenticated])	DUR_Wired_Guest_Reg

#	Request Timestamp	Source	NAS Name	NAS Port	Auth Method	Host MAC Address	Username	Service	Login Status	Enforcement Profiles
1.	2019/09/09 13:10:53	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	NMAP Scan, DUR_Wired_AppleTV
2.	2019/09/09 12:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Unknown
3.	2019/09/09 11:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	email - wired unknown device, Reported, DUR_Wired_Unknown
4.	2019/09/09 11:42:39	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Profile_portal

Adaptive Trust in action

Making the decisions!



Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* Disabled)	DUR_Wired_Blocked, email - malicious device
2.	(Tips:Role *EQUALS* Spoof)	DUR_Wired_Blocked, email - wired spoof device
3.	(Tips:Role *MATCHES_ALL* First_Cnx CPG_Device)	[Update Endpoint Known], Set Owner, DUR_Wired_Profile_portal
5.	(Tips:Role *MATCHES_ALL* Unknown Reported)	DUR_Wired_Unknown
7.	(Tips:Role *EQUALS* Controller)	DUR_Wired_Controller, Full Scan
8.	(Tips:Role *EQUALS* IAP)	DUR_Wired_IAP, SNMP Scan, NMAP Scan
9.	(Tips:Role *EQUALS* Access Points)	DUR_Wired_AP-Basic, NMAP Scan
10.	(Tips:Role *EQUALS* Home Audio/Video Equipment)	DUR_Wired_AppleTV, NMAP Scan
11.	(Tips:Role *EQUALS* Guest)	DUR_Wired_Guest
12.	(Tips:Role *EQUALS* IoT)	DUR_Wired_IoT, NMAP Scan
13.	(Tips:Role *EQUALS* Printer)	DUR_Wired_Printer, SNMP Scan
14.	(Tips:Role *EQUALS* WebCam)	DUR_Wired_WebCam
15.	(Tips:Role *EQUALS* [Machine Authenticated])	DUR_Wired_Isolation
16.	(Tips:Role *EQUALS* [User Authenticated])	DUR_Wired_Guest_Reg

#	Request Timestamp	Source	NAS Name	NAS Port	Auth Method	Host MAC Address	Username	Service	Login Status	Enforcement Profiles
1.	2019/09/09 13:10:53	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	NMAP Scan, DUR_Wired_AppleTV
2.	2019/09/09 12:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Unknown
3.	2019/09/09 11:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	email - wired unknown device, Reported, DUR_Wired_Unknown
4.	2019/09/09 11:42:39	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Profile_portal

Adaptive Trust in action

Making the decisions!

Summary | Input | **Output** | Accounting

Enforcement Profiles:	NMAP Scan, DUR_Wired_AppleTV
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role	DUR_Wired_AppleTV-3162-31 class ipv4 DHCP match udp any any eq 67 exit class ipv4 DNS match udp any host 192.168.137.10 eq 53 exit class ipv4 NTP match udp any any eq 123 exit class ipv4 TCP3689 match tcp any any eq 3689 exit class ipv4 mDNS match udp any any eq 5353 exit aaa authorization user-role name AppleTV policy APPLE_TV reauth-period 3600 logoff-period 3600 vlan-name IoT exit
Session-Notify:Login Action	OnDemand NMAP Scan
Session-Notify:Server IP	localhost
Session-Notify:Server Type	HTTP

Enforcement Policy Details

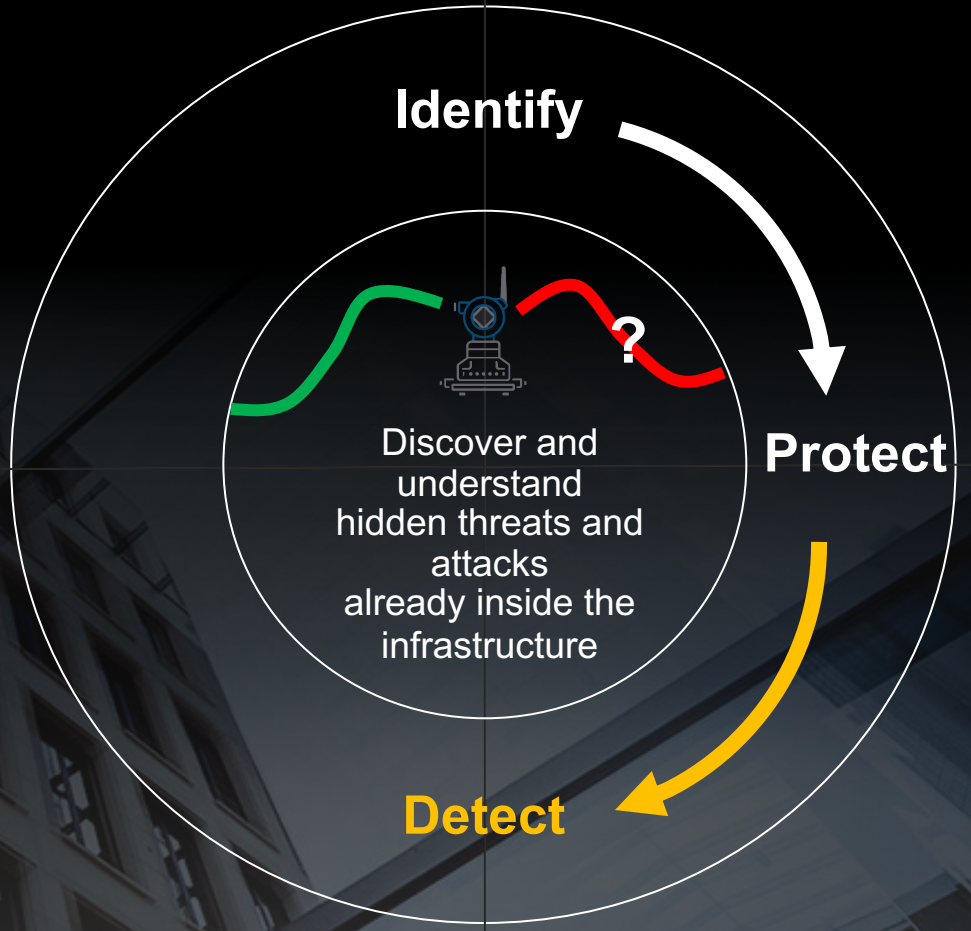
Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* Disabled)	DUR_Wired_Blocked, email - malicious device
2.	(Tips:Role *EQUALS* Spoof)	DUR_Wired_Blocked, email - wired spoof device
3.	(Tips:Role *MATCHES_ALL* First_Cnx CPG_Device)	[Update Endpoint Known], Set Owner, DUR_Wired_Profile_portal
4.	(Tips:Role *EQUALS* First_Cnx)	DUR_Wired_Profile_portal
5.	(Tips:Role *MATCHES_ALL* Unknown Reported)	DUR_Wired_Unknown
6.	(Tips:Role *EQUALS* Unknown)	DUR_Wired_Unknown, email - wired unknown device, Reported
7.	(Tips:Role *EQUALS* Controller)	DUR_Wired_Controller, Full Scan
8.	(Tips:Role *EQUALS* IAP)	DUR_Wired_IAP, SNMP Scan, NMAP Scan
10.	(Tips:Role *EQUALS* Home Audio/Video Equipment)	DUR_Wired_AppleTV, NMAP Scan
12.	(Tips:Role *EQUALS* IoT)	DUR_Wired_IoT, NMAP Scan
13.	(Tips:Role *EQUALS* Printer)	DUR_Wired_Printer, SNMP Scan
14.	(Tips:Role *EQUALS* WebCam)	DUR_Wired_WebCam
15.	(Tips:Role *EQUALS* [Machine Authenticated])	DUR_Wired_Isolation
16.	(Tips:Role *EQUALS* [User Authenticated])	DUR_Wired_Guest_Reg

#	Request Timestamp	Source	NAS Name	NAS Port	Auth Method	Host MAC Address	Username	Service	Login Status	Enforcement Profiles
1.	2019/09/09 13:10:53	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	NMAP Scan, DUR_Wired_AppleTV
2.	2019/09/09 12:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Unknown
3.	2019/09/09 11:52:14	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	email - wired unknown device, Reported, DUR_Wired_Unknown
4.	2019/09/09 11:42:39	RADIUS	Aruba-2930F-Local-Demo	2	MAC-AUTH	98d6bb0a31f7	98d6bb0a31f7	TeamX Wired MAC Auth DUR	ACCEPT	DUR_Wired_Profile_portal

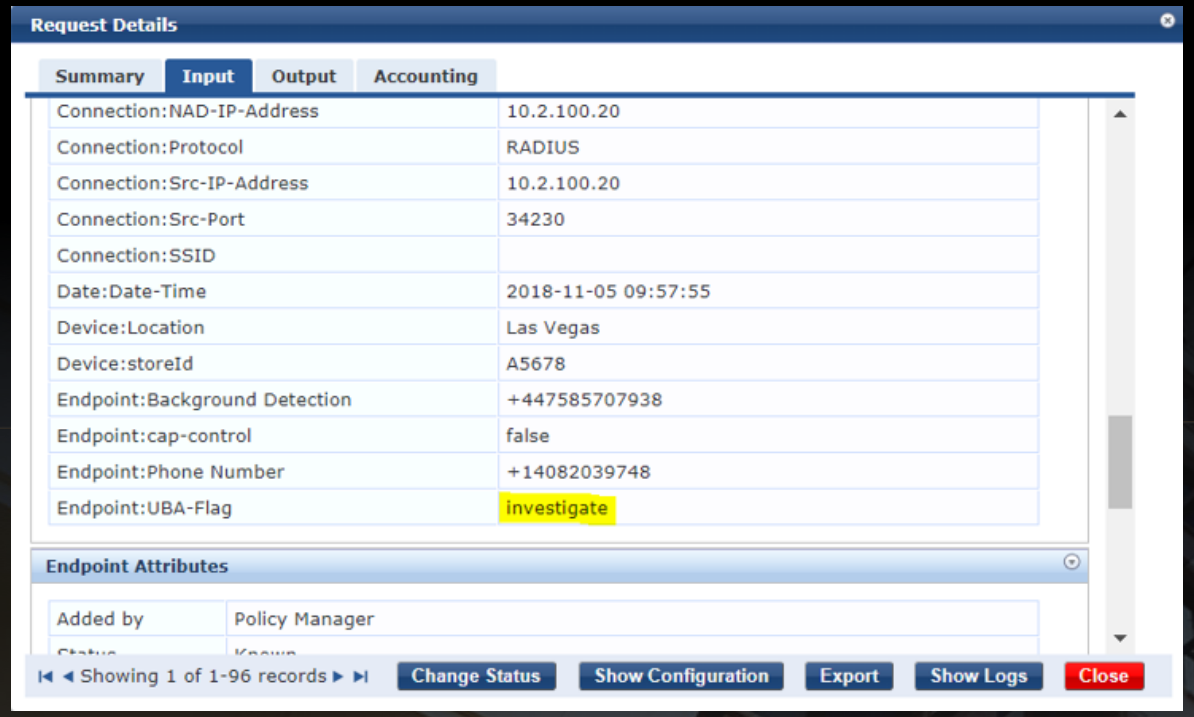
Adaptive Trust in action

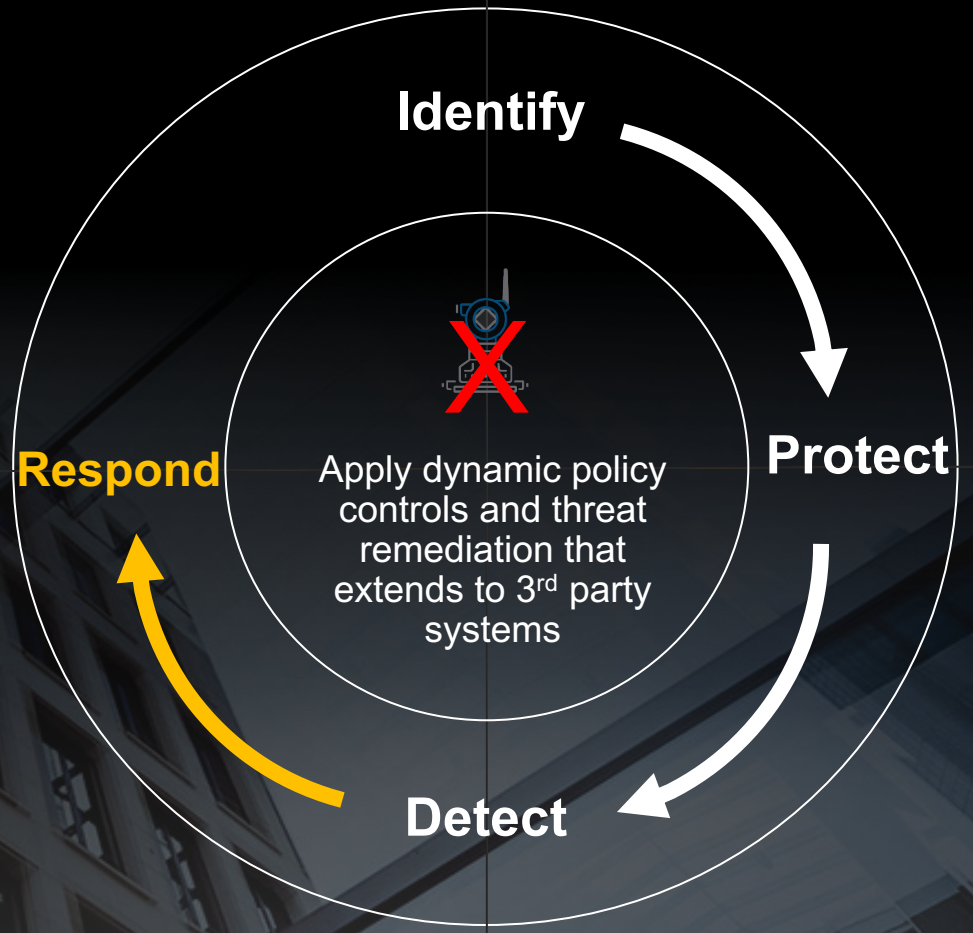
The Closed Loop approach to Security – More Context!



Adaptive Trust in action

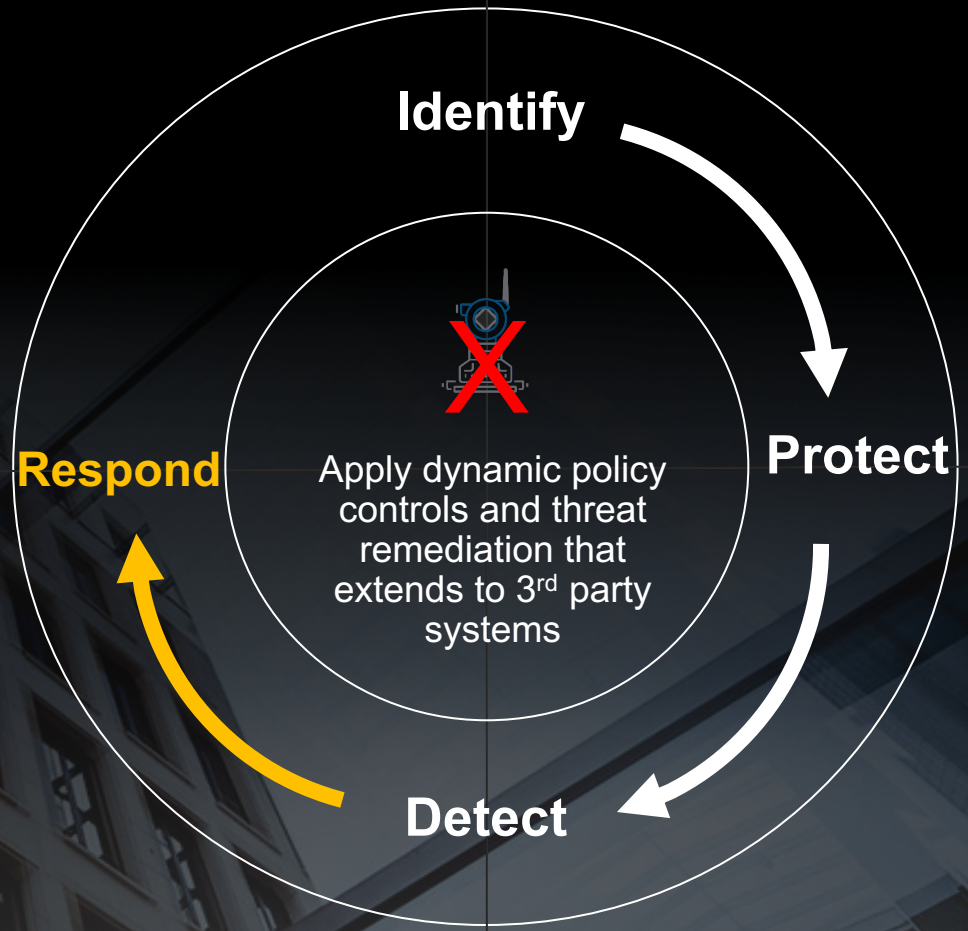
The Closed Loop approach to Security





Adaptive Trust in action

The Closed Loop approach to Security



Securely ready for the experiences to come!

- Visibility is only as good as the actions that follow!
- User Experience starts with Security Experience
- Security Experience depends on the Deployment and Operational Experience
- Make it more human!

aruba
a Hewlett Packard
Enterprise company

airheads

TECH TALK LIVE