

Eliminating the blind spots with ClearPass.

How visibility is the key to securing the experience

September 2019

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 - Outdated policies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

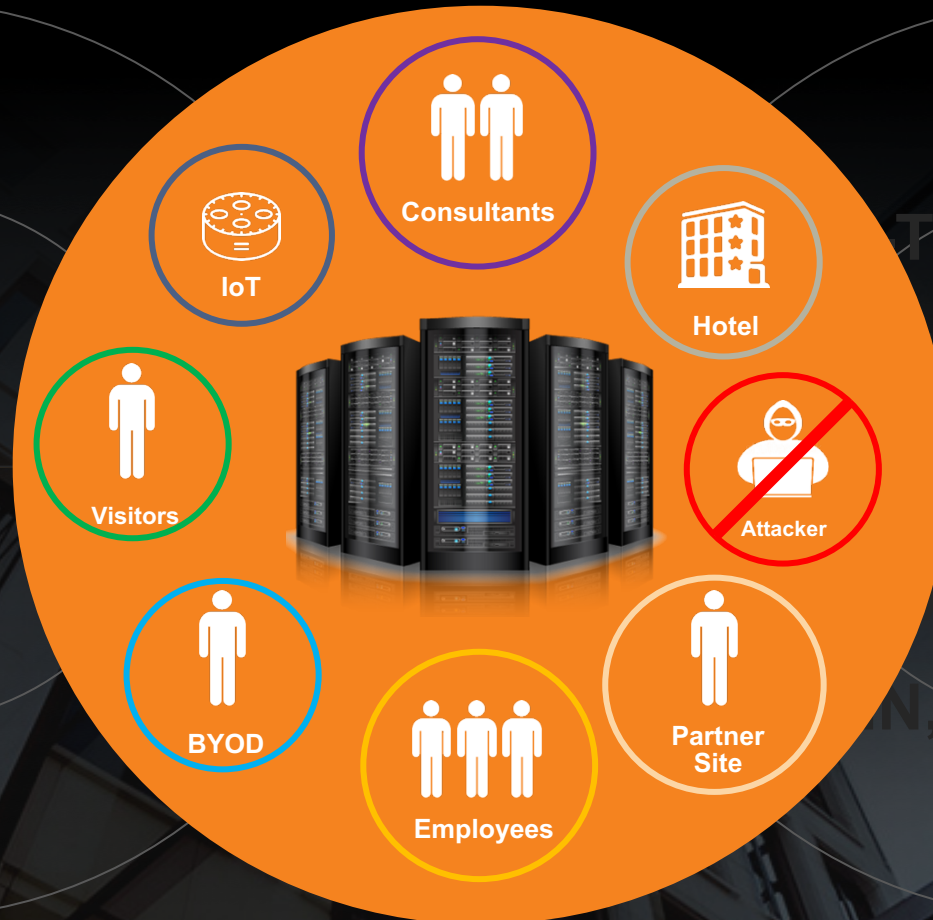
The untrusted LAN

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

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!



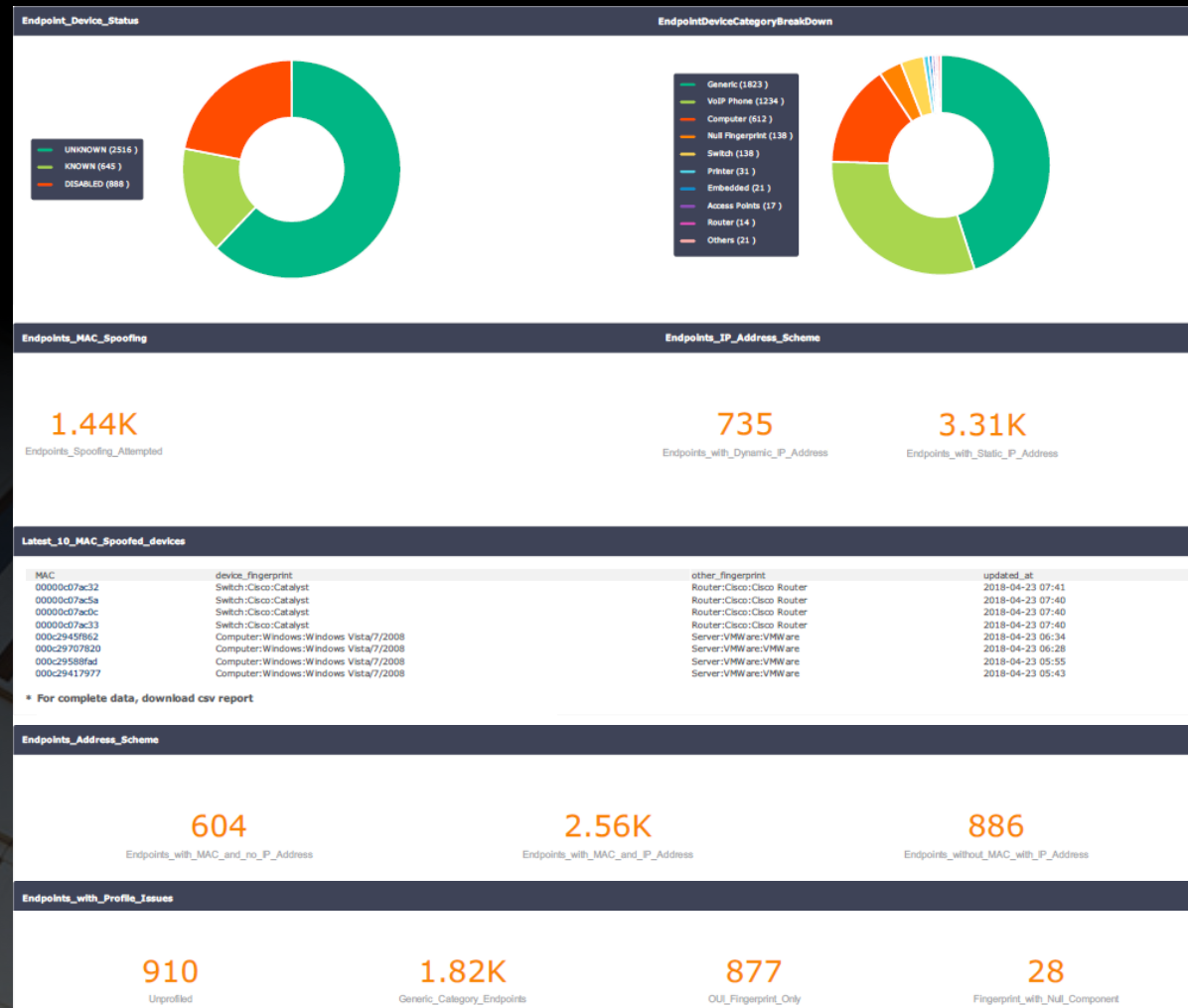
Device Visibility: ClearPass Policy Manager

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

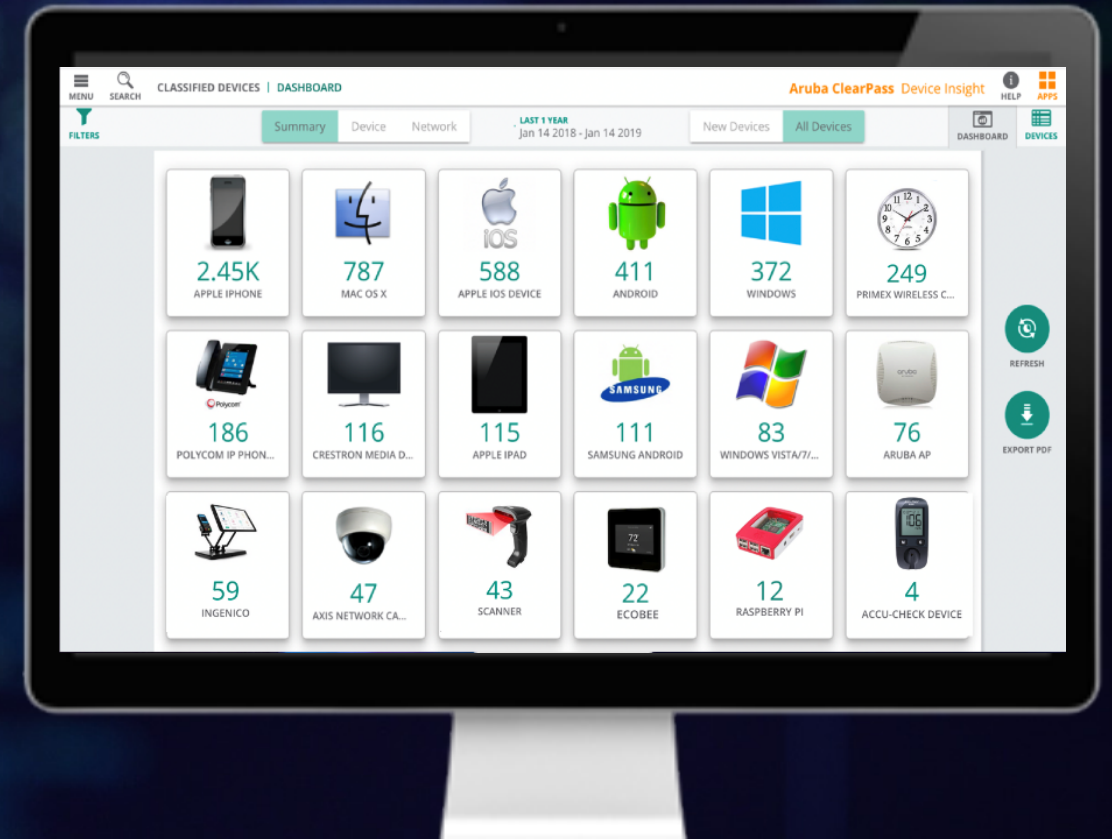


GENERIC
“WINDOWS” OR
“LINUX” DEVICE

CLEARPASS DEVICE INSIGHT

**ELIMINATES
BLIND SPOTS**

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



MAC / Vendor info

Port/Protocol

Static Attributes
(DHCP, User agent, SNMP info)

**MACHINE
LEARNING-
BASED
CLUSTERING
USING DPI**

**Communication
Frequency**

Destination IP

**Application
Communications**

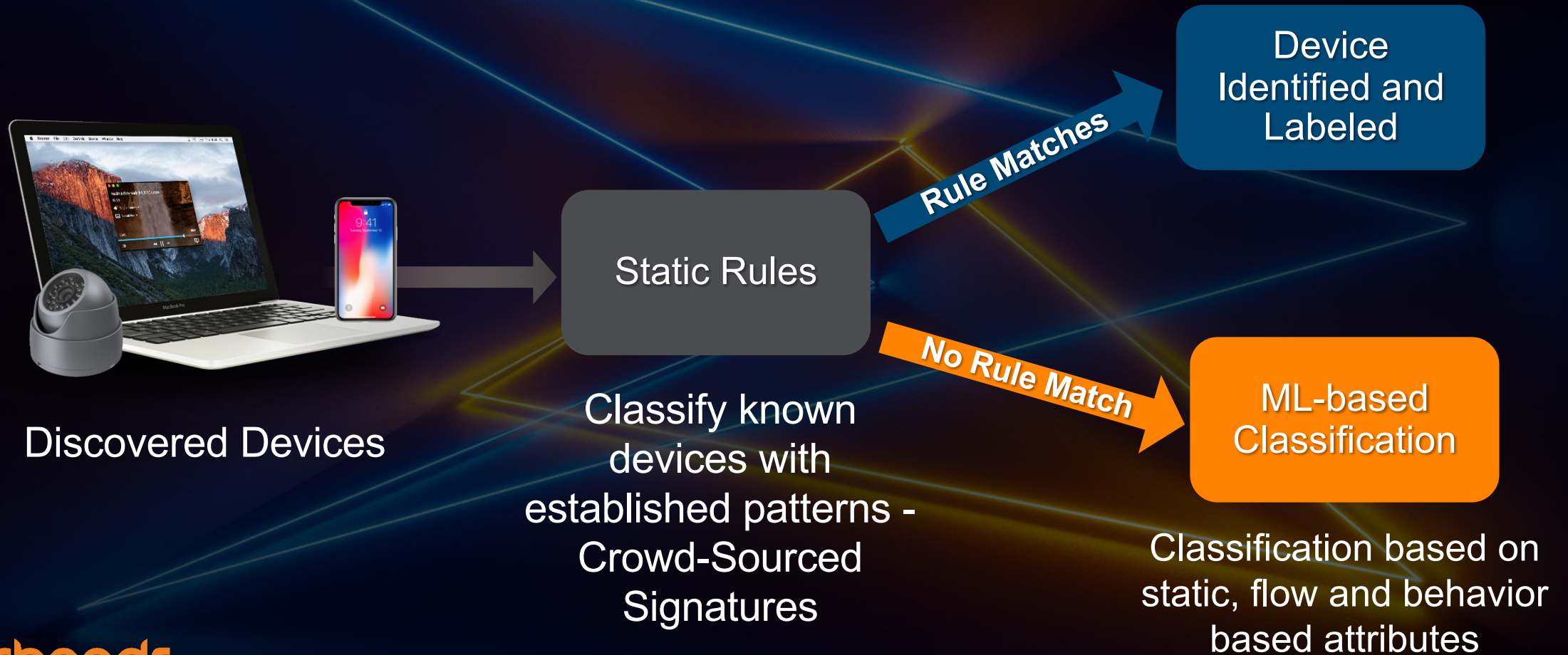
ARCHITECTURE OVERVIEW

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

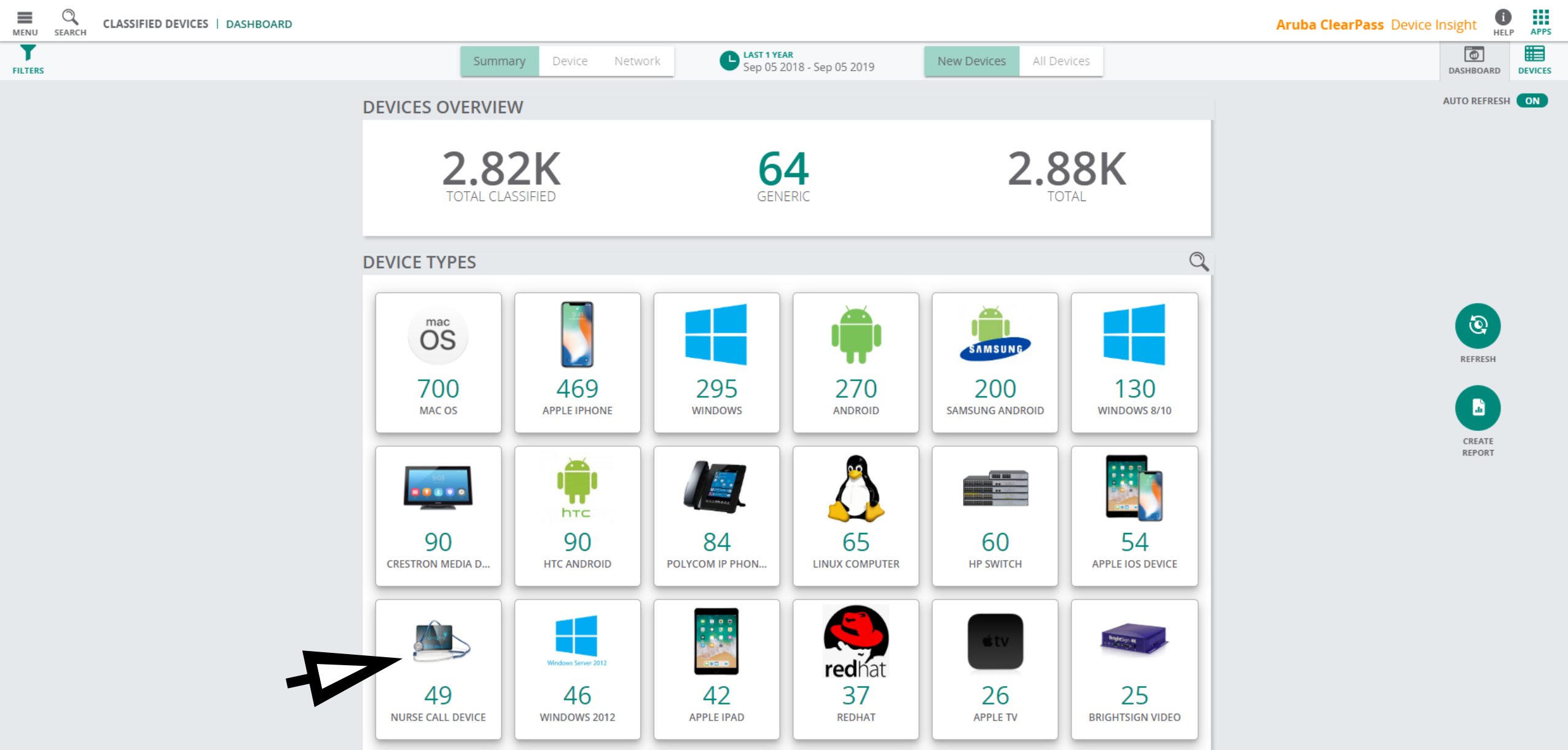
Through Deep Packet Inspection (DPI), device attributes are extracted and metadata is sent to the cloud for analysis



DEVICE CLASSIFICATION



ClearPass Device Insight – Accurate Classification



ClearPass Device Insight – Accurate Classification

MENU

SEARCH

DEVICES | LIST

Aruba ClearPass Device Insight

HELP

APPS

FILTERS

Summary

Device

Network

LAST 1 YEAR

Sep 05 2018 - Sep 05 2019














New Devices

All Devices

DASHBOARD

DEVICES

Devices (49)

MAC	IP ADDRESS	HOST NAME	MAC VENDOR	CATEGORY Medical Device	FAMILY Hillrom	Call Device	STATIC IP	ACCESS POI...	SEGMENT	SSID	USER NAME	STATUS	POSTURE ST...	NAD PORT	NAD IP
 001a6482b195	172.16.10.126		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Offline	UNKNOWN		
 001a6482b129	172.16.10.116		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Offline	UNKNOWN		
 001a6482b126	10.17.18.108		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Offline	UNKNOWN		
 001a6482b124	172.16.10.130		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		
 001a6482b167	172.16.10.138		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Offline	UNKNOWN		
 001a6482b113	172.16.10.121		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		
 001a6482b172	172.16.10.143		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		
 001a6482b134	10.17.18.128		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		
 001a6482b186	172.16.10.103		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		
 001a6482b165	10.17.18.119		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Offline	UNKNOWN		
 001a6482b185	10.17.18.144		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Offline	UNKNOWN		
 001a6482b158	10.17.18.123		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		
 001a6482b114	172.16.10.133		IBM Corp	Medical Device	Hillrom	Nurse Call Device	false		Segment for Switches/Server/ other devices			Online	UNKNOWN		

ClearPass Device Insight – Accurate Classification

001a6482b195 / 172.16.10.126

OFFLINE


First Seen: 5 months ago | Last Activity: 5 months ago | Updated At: 2 days ago

EXPORT PDF

HELP

CLOSE

DEVICE OVERVIEW



Posture Status

UNKNOWN

Status

Offline

IP Address

172.16.10.126

MAC Address

001a6482b195

Host Name

-

User Name

-

MAC Vendor

IBM Corp

Category

Medical Device

Family

Hillrom

Type

Nurse Call Device

INTERFACES

MAC ADDRESS	IP ADDRESS
001a6482b195	172.16.10.126

LOCATION

NAD IP

-

NAD Port

-

Segment

Segment for Switches/Server/other devices

Access Point

-

Wireless SSID

-

DEVICE ATTRIBUTES

DHCP Option55

1,6,12,15,26,28,42,100,121,249,3

DHCP Option60

udhcp 0.9.9-pre

DHCP Options

53,61,81,60,55

Application Group

business-systems.management
business-systems.network
collaboration.voip-video
media.photo-video

Application ID

dns
ntp
rtsp
sip
syslog

Destination Connection

10.170.117.154:123:udp
10.170.117.154:23010:udp
10.170.117.154:50010:udp
10.170.117.154:5060:udp
10.170.117.154:514:udp
201.12.123.31:80:udp
ahwapplinind690.linind.ds.sjhs.com:50010:udp
ahwapplinind690.linind.ds.sjhs.com:5060:udp

MAC OUI

001a64

Port

137, 30086, 30118, 30234, 3658, 4826, 4854, 5060

CLASSIFICATION RULE

Classified By System

DEVICE OVERVIEW

INTERFACES

LOCATION

DEVICE ATTRIBUTES

CLASSIFICATION RULE

NETWORK DIGEST

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.

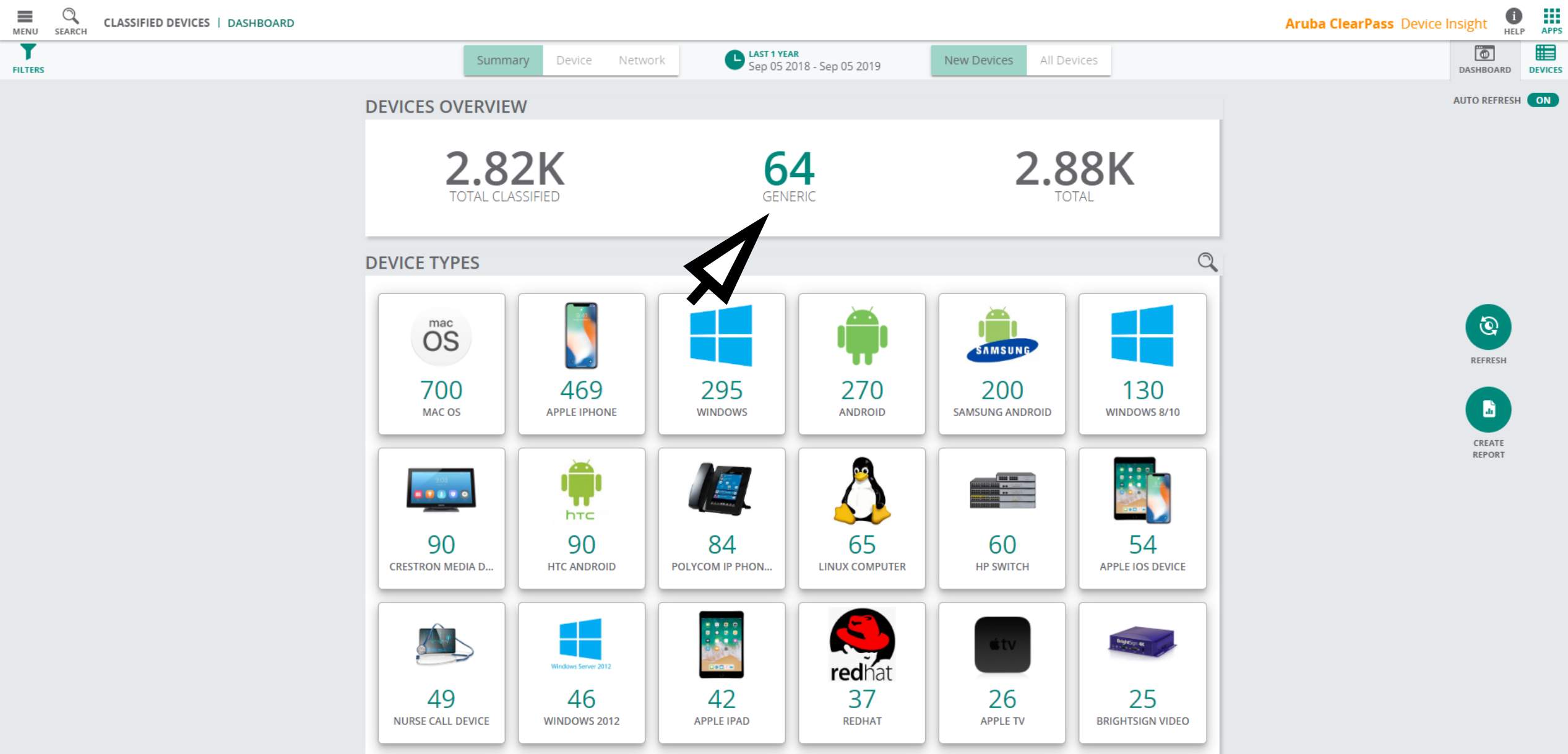
Comparative Attributes:

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

MENU

SEARCH

GENERIC DEVICES | DASHBOARD

Aruba ClearPass Device Insight

HELP

APPS

Device

Network

LAST 1 YEAR
Sep 05 2018 - Sep 05 2019

New Devices

All Devices

DASHBOARD

DEVICES

AUTO REFRESH **OFF**

CLUSTER-20

DHCP OPTION55 *

1,2,3,6

DHCP OPTIONS *

53,57,55,60,12,61,0

MAC VENDOR *

JK MICROSYSTEMS, INC.

DHCP OPTION12

RLNK-SW715R_D6_2C_14

DHCP OPTION60

RACKLINK

MAC OUI

DEVICE ATTRIBUTES THAT HELP IN GROUPING THEM INTO A DEVICE CLUSTER ARE MARKED WITH (*)

Classify Devices ▾

☐ ADD TO COMPARE

GENERIC DEVICES OVERVIEW

64

DEVICES

11

DEVICE CLUSTERS

7

MAC VENDORS

DEVICE CLUSTERS

Cluster-11 (32 Devices)
Hanwha Techwin Security Vietnam

Cluster-16 (10 Devices)
SAMSUNG TECHWIN CO.,LTD

Cluster-2 (6 Devices)
Avaya Inc

Cluster-17 (4 Devices)
Avaya Inc

Cluster-14 (3 Devices)
Microsoft Corporation

Cluster-6 (3 Devices)
Hanwha Techwin Security Vietnam

Cluster-8 (2 Devices)
Generic

Cluster-1 (1 Devices)
Microsoft Corporation

Cluster-20 (1 Devices)
JK Microsystems, Inc.

Cluster-5 (1 Devices)
JK Microsystems, Inc.

Cluster-7 (1 Devices)
Intel Corporate

SHOW DEVICES

CLEAR FILTERS

CREATE REPORT

RECLASSIFY DEVICES

COMPARE

ClearPass Device Insight – Generic to Granular

The screenshot displays the Aruba ClearPass Device Insight interface. The main dashboard shows a list of generic devices under 'CLUSTER-20'. A modal dialog titled 'Classify Devices using Rule' is open, allowing the user to create a rule by selecting conditions. The dialog has two tabs: 'EDIT CONDITIONS' and 'CREATE RULE'. The 'CREATE RULE' tab is active, showing a table of conditions with checkboxes for selection. A mouse cursor is pointing at the 'Next' button at the bottom of the dialog.

Aruba ClearPass Device Insight

GENERIC DEVICES | DASHBOARD

Device **Network** **LAST 1 YEAR** **Sep 05 2018 - Sep 05 2019** **New Devices** **All Devices**

CLUSTER-20

DHCP OPTION55 *

1,2,3,6

DHCP OPTIONS *

53,57,55,60,12,61,0

MAC VENDOR *

JK MICROSYSTEMS, INC.

DHCP OPTION12

RLNK-SW715R_D6_2C_14

DHCP OPTION60

RACKLINK

MAC OUI

DEVICE ATTRIBUTES THAT HELP IN GROUPING THEM INTO A DEVICE CLUSTER ARE MARKED WITH (*)

Classify Devices

☐ ADD TO COMPARE

Classify Devices using Rule

EDIT CONDITIONS **CREATE RULE**

DHCP Option55	MATCHES	<input checked="" type="checkbox"/>	1,2,3,6	+
DHCP Option60	MATCHES	<input type="checkbox"/>	RackLink	+
DHCP Options	MATCHES	<input type="checkbox"/>	53,57,55,60,12,61,0	+
DHCP Option12	MATCHES	<input type="checkbox"/>	RLNK-SW715R_D6_2C_14	+
MAC Vendor	MATCHES	<input checked="" type="checkbox"/>	JK microsystems, Inc.	+
Application ID	MATCHES	<input type="checkbox"/>	tcp	+
Destination Connection	MATCHES	<input checked="" type="checkbox"/>	54.39.13.155:80:tcp	+
MAC OUI	MATCHES	<input type="checkbox"/>	0090c2	+

Cancel **Next**

SHOW DEVICES

CLEAR FILTERS

CREATE REPORT

RECLASSIFY DEVICES

COMPARE

AUTO REFRESH **OFF**

ClearPass Device Insight – Generic to Granular

The screenshot displays the Aruba ClearPass Device Insight web interface. The main header includes a menu, search bar, and navigation tabs for 'GENERIC DEVICES' and 'DASHBOARD'. The top right corner shows the 'Aruba ClearPass Device Insight' logo, a help icon, and an 'APPS' icon. Below the header, there are tabs for 'Device' and 'Network', a date range selector for 'LAST 1 YEAR' (Sep 05 2018 - Sep 05 2019), and buttons for 'New Devices' and 'All Devices'. On the left side, there is a sidebar with a list of device attributes under 'CLUSTER-20', including DHCP OPTION55, DHCP OPTIONS, MAC VENDOR, DHCP OPTION12, DHCP OPTION60, and MAC OUI. A 'Classify Devices' button is visible at the bottom of this sidebar. The main content area is partially obscured by a modal dialog box titled 'Classify Devices using Rule'. This dialog has two tabs: 'EDIT CONDITIONS' and 'CREATE RULE'. It displays the following information: 'YOU HAVE SELECTED 3 CONDITIONS', Rule Name: 'JK Machines', Device Category: 'Embedded', Device Family: 'Windows', Device Type: 'Windows CE', and Device Image: 'Browse' (with a note to 'Upload an image for the device'). At the bottom of the dialog are four buttons: 'Cancel', 'Back', 'Save', and 'Save & Reclassify'. A large black arrow points to the 'Save & Reclassify' button. On the right side of the interface, there is a vertical sidebar with icons for 'SHOW DEVICES', 'CLEAR FILTERS', 'CREATE REPORT', 'RECLASSIFY DEVICES', and 'COMPARE'. The 'AUTO REFRESH' toggle is set to 'OFF'.

GENERIC DEVICES | DASHBOARD

Aruba ClearPass Device Insight

Device Network

LAST 1 YEAR
Sep 05 2018 - Sep 05 2019

New Devices All Devices

CLUSTER-20

DHCP OPTION55 *
1,2,3,6

DHCP OPTIONS *
53,57,55,60,12,61,0

MAC VENDOR *
JK MICROSYSTEMS, INC.

DHCP OPTION12
RLNK-SW715R_D6_2C_14

DHCP OPTION60
RACKLINK

MAC OUI

DEVICE ATTRIBUTES THAT HELP IN GROUPING THEM INTO A DEVICE CLUSTER ARE MARKED WITH (*)

Classify Devices

ADD TO COMPARE

Classify Devices using Rule

EDIT CONDITIONS CREATE RULE

YOU HAVE SELECTED 3 CONDITIONS

Rule Name
JK Machines

Device Category
Embedded

Device Family
Windows

Device Type
Windows CE

Device Image
Browse Upload an image for the device

Cancel Back Save Save & Reclassify

SHOW DEVICES

CLEAR FILTERS

CREATE REPORT

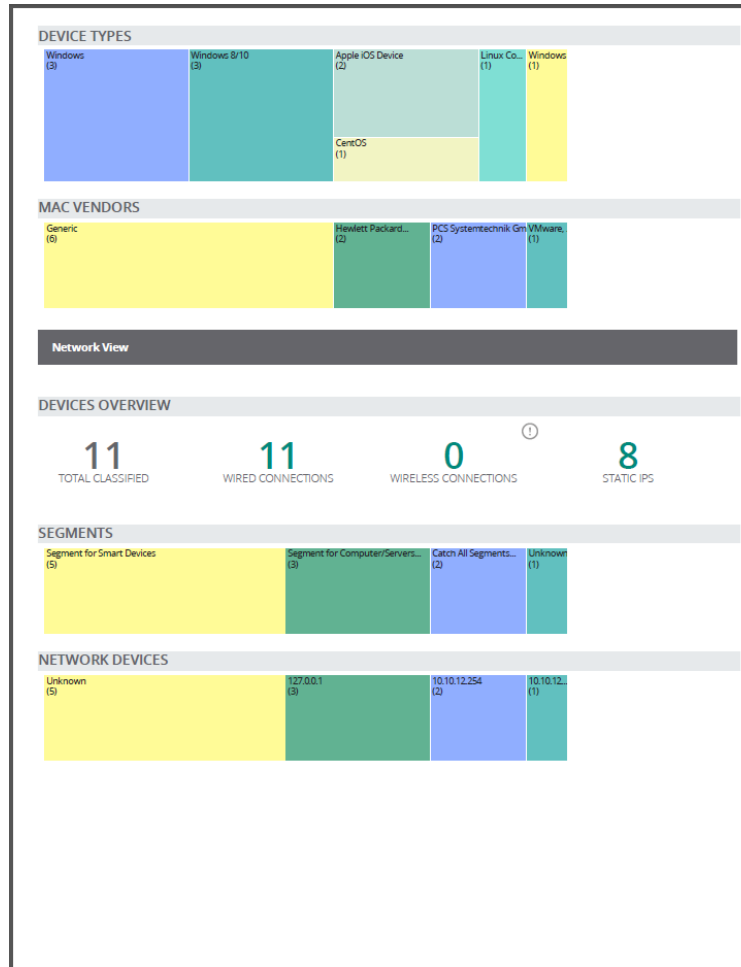
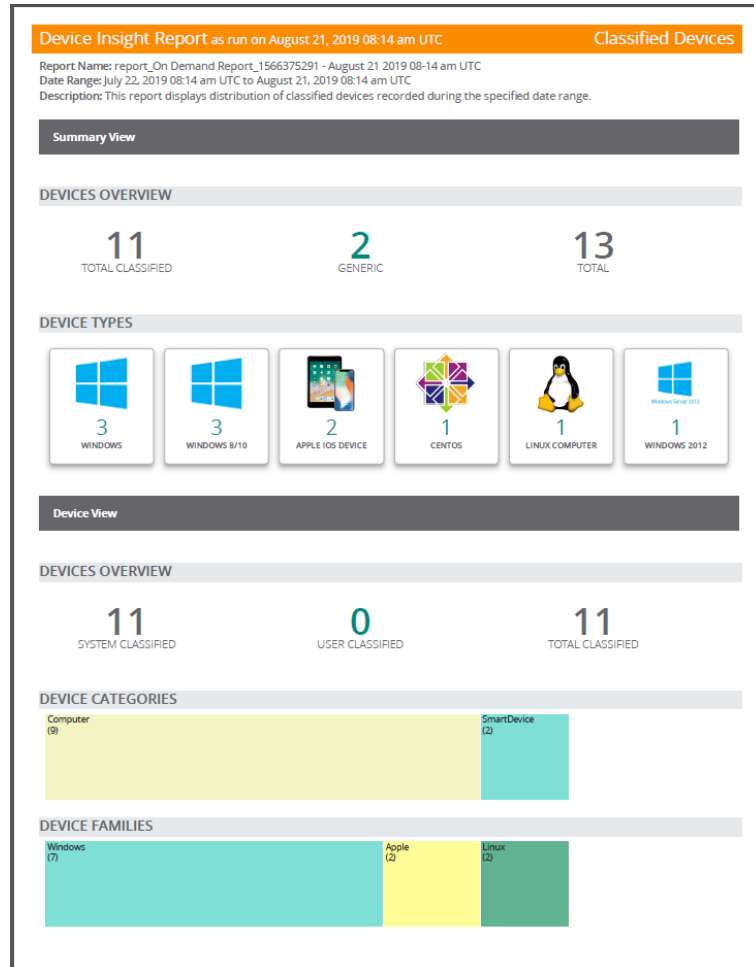
RECLASSIFY DEVICES

COMPARE

AUTO REFRESH OFF

Report on anything you can filter!

– Example: New “Unknowns”



MAC	IP Address	Host Name	MAC Vendor	Category	Family	Type	NAD IP	Status	NAD Port	Screen Point	Wireless	SSID	Device	Cluster	Segment	Feature Status
080c2be3d4d	10.10.12.132	PCSYSTEMTECH	VMware, Inc.	Computer	Windows	Windows 2012	10.10.12.255	TRUE	19	19	19	19	19	19	Segment for Computer/Servers	UNKNOWN
aa16147b57b	10.11.13.136		Generic	Computer	Windows	Windows		TRUE							Segment for Smart Devices	UNKNOWN
eeae5b2a27c	10.11.13.144		Generic	SmartDevice	Apple	Apple iOS Device		TRUE							Segment for Smart Devices	UNKNOWN
aa9f87f3561	10.11.13.187		Generic	Computer	Windows	Windows		TRUE							Segment for Smart Devices	UNKNOWN
00000000001	10.10.12.18	winbox-computer-1	Generic	Computer	Windows	Windows 8/10	127.0.0.1	FALSE							Segment for Smart Devices	UNKNOWN
0800276c4478	10.10.12.18		PCS Systemtechnik GmbH	Computer	Linux	Linux Computer	10.10.12.254	TRUE	19	19	19	19	19	19	Segment for Computer/Servers	UNKNOWN
0800276c4478	10.10.12.18	winbox-192.168.10.14	PCS Systemtechnik GmbH	Computer	Linux	CentOS	10.10.12.254	TRUE	19	19	19	19	19	19	Segment for Computer/Servers	UNKNOWN
aa16147b57b	10.11.13.144		Generic	SmartDevice	Apple	Apple iOS Device		TRUE							Segment for Smart Devices	UNKNOWN
0800276c4478	10.10.12.18	winbox-computer-1	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE							Catch All Segments	UNKNOWN
0800276c4478	10.10.12.18	winbox-computer-1	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19	19	19	19	19	19	Catch All Segments	UNKNOWN
0800276c4478	10.10.12.18	winbox-computer-1	Generic	Computer	Windows	Windows		TRUE							Segment for Smart Devices	UNKNOWN
0800276c4478	10.10.12.18	winbox-computer-1	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19	19	19	19	19	19	Catch All Segments	UNKNOWN
0800276c4478	10.10.12.18	winbox-computer-1	Hewlett Packard	Computer	Windows	Windows 8/10	127.0.0.1	FALSE	19	19	19	19	19	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



Edit Endpoint

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

ClearPass Device Insight – Enhancing Policy

Aruba ClearPass Device Insight
HELP APPS

MENU
 SEARCH

DEVICES | LIST

DASHBOARD
 DEVICES

MAC	IP ADDRESS	HOST NAME
x90a1d58733	10.100.46.163	
x7e78715b19	10.100.34.123	
58971ed440c1	193.58.106.93	UEN-GBPSL-F300UP AU01.eu.unilever.co
xab19bba3c8c	10.100.60.3	
xa09e09c03d3	10.100.36.235	
xa22552d77ae	10.100.49.82	
04d3b02ef487		PSLL108TDYPQ2
381c1a7281c1	193.58.106.134	UEN-GBPSL-FB00PL SS14.eu.unilever.co
xab8f8887742	10.100.93.5	
xabf25cfe6e6	10.100.46.125	
xaaac45ecb2c	10.100.33.70	
04d3b02ea0fe		PSLL10F312QQ2
3417ebdf7170		PSLWW72FZJ132
xaaa660242c7	10.100.64.191	
xa9c70c9ff2d	10.100.11.88	
xa425a70ed45	10.100.74.108	
xa2cfc16f395	10.100.72.223	
xa60676da683	10.100.39.191	
xa7422ca0808	10.100.32.120	
xad0b58b2769	10.100.81.156	
xa912bd0e0aa	10.100.60.145	
xa10388bae84	10.100.36.83	

xab19bba3c8c / 10.100.60.3
OFFLINE

OVERVIEW

LOCATION

ATTRIBUTES

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

Filter

Reclassify

Generate PDF

MENU

SEARCH

DEVICES | LIST

Aruba ClearPass Device Insight

HELPAPPS

FILTERSDASHBOARDDEVICES

Devices (1527)

MAC	IP ADDRESS	HOST NAME	NAD IP	STATUS
xa90a1d58733	10.100.46.163			Offline
xa7e78715b19	10.100.34.123			Offline
58971ed440c1	193.58.106.93	UEN-GBPSL-F300UP AU01.eu.unilever.co		Idle
xab19bba3c8c	10.100.60.3			Offline
xa09e09c03d3	10.100.36.235			Offline
xa22552d77ae	10.100.49.82			Offline
04d3b02ef487		PSLL108TDYPQ2		Offline
381c1a7281c1	193.58.106.134	UEN-GBPSL-FB00PL SS14.eu.unilever.co		Idle
xab8f8887742	10.100.93.5			Idle
xabf25cf6e6	10.100.46.125			Offline
xaaac45ecb2c	10.100.33.70			Offline
04d3b02ea0fe		PSLL10F312QQ2		Offline
3417ebdf7170		PSLWW72FZJ132		Offline
xaaa660242c7	10.100.64.191			Offline
xa9c70c9ff2d	10.100.11.88			Offline
xa425a70ed45	10.100.74.108			Offline
xa2cfc16f395	10.100.72.223			Offline
xa60676da683	10.100.39.191			Idle
xad0b58b2769	10.100.81.156			Offline
xa912bd0e0aa	10.100.60.145			Offline
xa10388bae84	10.100.36.83			Offline
3417ebd0f0d1		PSLWW7FQBTV22		Online

FILTER

MAC Vendor

MATCHES

Generic

+

User Agent

MATCHES

McAfee Agent

+

Application Group

MATCHES

business-systems.software-updat

+

Application ID

MATCHES ANY

mcafee

smb

+

Destination Connection

MATCHES ANY

159.239.78.4:445:tcp

159.239.78.4:8081:tcp

+

Add Filter

Search in Grid

Cancel

MENU

SEARCH

DEVICES | LIST

Aruba ClearPass Device Insight

HELPAPPS

FILTERSDASHBOARDDEVICES

Devices (1527)

MAC	IP ADDRESS	HOST NAME	NAD IP	STATUS
xa90a1d58733	10.100.46.163			Offline
xa7e78715b19	10.100.34.123			Offline
58971ed440c1	193.58.106.93	UEN-GBPSL-F300UP AU01.eu.unilever.co		Idle
xab19bba3c8c	10.100.60.3			Offline
xa09e09c03d3	10.100.36.235			Offline
xa22552d77ae	10.100.49.82			Offline
04d3b02ef487		PSLL108TDYPQ2		Offline
381c1a7281c1	193.58.106.134	UEN-GBPSL-FB00PL SS14.eu.unilever.co		Idle
xab8f8887742	10.100.93.5			Idle
xabf25cf6e6	10.100.46.125			Offline
xaaac45ecb2c	10.100.33.70			Offline
04d3b02ea0fe		PSLL10F312QQ2		Offline
3417ebdf7170		PSLWW72FZJ132		Offline
xaaa660242c7	10.100.64.191			Offline
xa9c70c9ff2d	10.100.11.88			Offline
xa425a70ed45	10.100.74.108			Offline
xa2cfc16f395	10.100.72.223			Offline
xa60676da683	10.100.39.191			Idle
xad0b58b2769	10.100.81.156			Offline
xa912bd0e0aa	10.100.60.145			Offline
xa10388bae84	10.100.36.83			Offline
3417ebd0f0d1		PSLWW7FQBTV22		Online

FILTER

MAC Vendor

MATCHES

Generic

+

User Agent

MATCHES

McAfee Agent

+

Application Group

MATCHES

business-systems.software-updat

+

Application ID

MATCHES ANY

mcafee

smb

+

Destination Connection

MATCHES ANY

159.239.78.4:445:tcp

159.239.78.4:8081:tcp

+

Add Filter

Search in Grid

Cancel

ClearPass Device Insight – Enhancing Policy

[illegible]

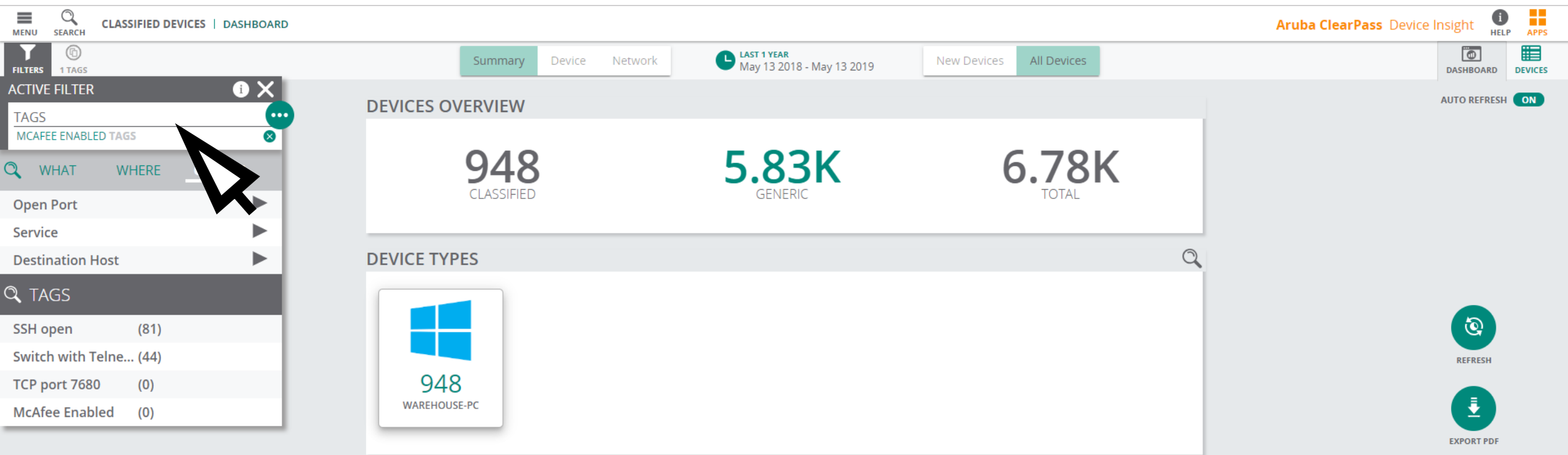
ClearPass Device Insight – Enhancing Policy

The screenshot displays the Aruba ClearPass Device Insight interface. A modal dialog is open in the center, titled "This tag will be applied to 6776 devices". The dialog contains a "Tag Name" field with the value "McAfee Enabled" and a "Description" field with the value "I'm worried about these devices". Below the description field are two buttons: "APPLY" and "CANCEL". A large black mouse cursor is pointing at the "APPLY" button.

The background interface shows a dashboard with a top navigation bar containing "MENU", "SEARCH", "DEVICES | LIST", and "Aruba ClearPass Device Insight". Below the navigation bar, there are tabs for "Summary", "Device", and "Network". A date range selector shows "LAST 1 YEAR" from "May 13 2018" to "May 13 2019". On the left side, there is a "FILTERS" panel with "2 OTHERS" and an "ACTIVE FILTER - Switch with Telnet ..." section. Below this, there are "OTHERS" filters including "MCAFFEE AGENT USER AGENT" and "MCAFFEE APPLICATION ID". There are also "WHAT" and "WHERE" filters, and a "TAGS" section with "SSH open (81)", "Switch with Teln... (44)", and "TCP port 7680 (0)".

The main content area is a table with columns: "HOST NAME", "TYPE", "NAD IP", and "STATUS". The table contains multiple rows of data, including "Warehouse-PC" and "Computer" types. On the right side of the table, there are two circular icons: a download icon and a refresh icon.

ClearPass Device Insight – Enhancing Policy



ClearPass Device Insight – Enhancing Policy

Aruba ClearPass Device Insight

MENU SEARCH DEVICES LIST DASHBOARD HELP APPS

Devices (1528)

MAC	IP ADDRESS	HOST NAME
x90a1d58733	10.100.46.163	
xa7e78715b19	10.100.34.123	
58971ed440c1	193.58.106.93	UEN-GBPSL-F300UP AU01.eu.unilever.co
xab19bba3c8c	10.100.60.3	
xa09e09c03d3	10.100.36.235	
xa22552d77ae	10.100.49.82	
04d3b02ef487		PSLL108TDYPQ2
381c1a7281c1	193.58.106.134	UEN-GBPSL-FB00PL SS14.eu.unilever.co
xab8f8887742	10.100.93.5	
xabf25cfe6e6	10.100.46.125	
xaaac45ecb2c	10.100.33.70	
04d3b02ea0fe		PSLL10F312QQ2
3417ebdf7170		PSLWW72FZJ132
xaaa660242c7	10.100.64.191	
xa9c70c9ff2d	10.100.11.88	
xa425a70ed45	10.100.74.108	
xa2cfc16f395	10.100.72.223	
xa60676da683	10.100.39.191	
xad0b58b2769	10.100.81.156	
xa912bd0e0aa	10.100.60.145	
xa10388bae84	10.100.36.83	
3417ebd0f0d1		PSLWW7FQBTV22

xab19bba3c8c / 10.100.60.3
OFFLINE

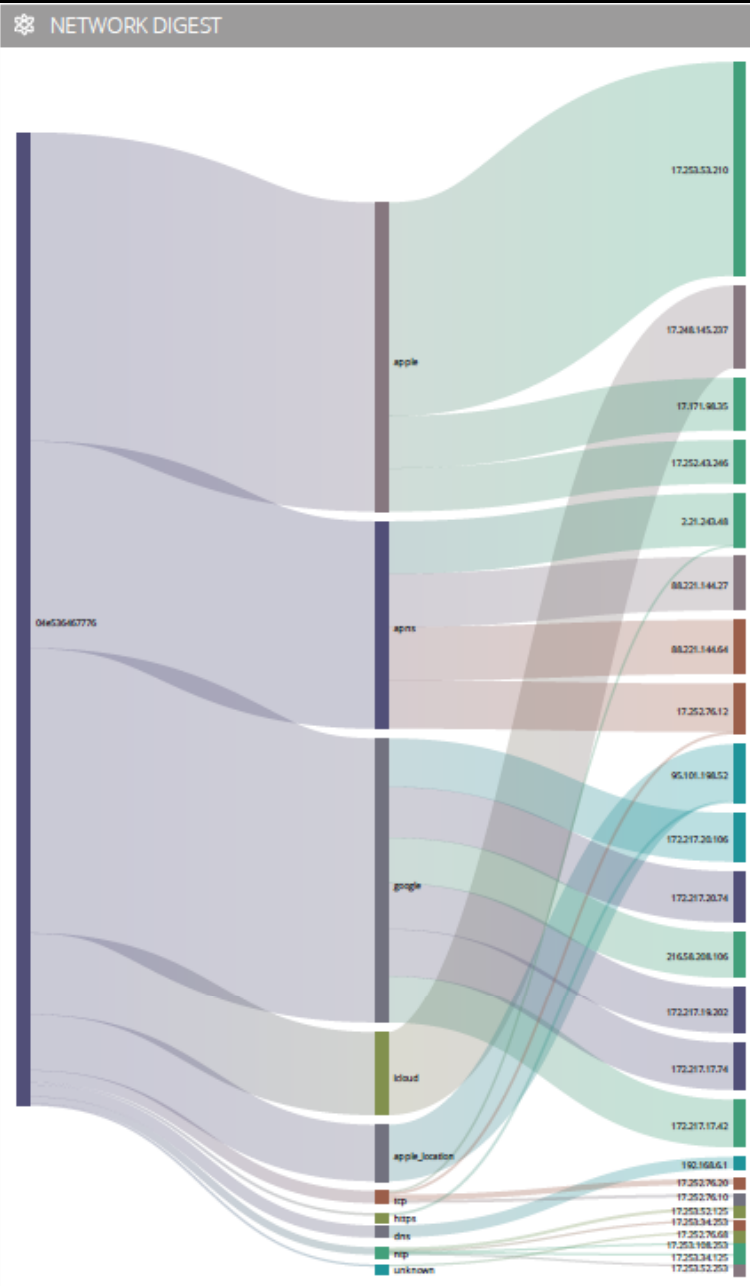
OVERVIEW	LOCATION	ATTRIBUTES
Host Name		
IP Address	10.100.60.3	
MAC Address	xab19bba3c8c	
MAC Vendor	Generic	
DEVICE CLASSIFICATION		
Category	Computer	
Family	Windows	
Type	Warehouse-PC	
MISCELLANEOUS		
Classified By	Device Cluster Labelling (cluster-33)	
First Seen	03-29-2019 02:11	
Last Activity	04-30-2019 13:35	
Updated At	05-13-2019 15:50	
TAGS		
MCAfee ENABLED		
Filter Reclassify Generate PDF		

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

EMM / MDM



PMS / IoT



Firewall



Network



Services



AuthN / MFA



Open, Multi-Vendor Security Framework

Messaging



Social Media



Logging



Deception



Endpoint



UEBA



Creating Access Policy Control

ClearPass Policy Manager Integrations



Configuration » Identity » Endpoints

Endpoints

This page automatically lists all authenticated endpoints. An endpoint device is an Internet-capable hardware device on a TCP/IP network (e.g. laptops, smart phones, tablets, etc.).

Filter: Added by contains

#	<input type="checkbox"/>	MAC Address ^	Hostname	Device Category	Device OS Family	Status	Profile
1.	<input type="checkbox"/>	0001e3112233		Programmable Logic Controller	SIEMENS AG	Known	Yes
2.	<input type="checkbox"/>	0001e3112234		Programmable Logic Controller	SIEMENS AG	Unknown	Yes
3.	<input type="checkbox"/>	0001e31123aa		Programmable Logic Controller	SIEMENS AG	Known	Yes
4.	<input type="checkbox"/>	004084112233		Unclassified by CyberX	HONEYWELL INTERNATIONAL HPS	Known	Yes
5.	<input type="checkbox"/>	004084112234		Unclassified by CyberX	HONEYWELL INTERNATIONAL HPS	Unknown	Yes
6.	<input type="checkbox"/>	008074021865		DCS Controller	FISHER CONTROLS	Known	Yes
7.	<input type="checkbox"/>	00c0723ffa3		Programmable Logic Controller	KNX LTD.	Unknown	Yes
8.	<input type="checkbox"/>	78a504c9b478					
9.	<input type="checkbox"/>	acfdce1221ee					
10.	<input type="checkbox"/>	acfdce12ffa0					
11.	<input type="checkbox"/>	c8d3ff123321					
12.	<input type="checkbox"/>	c8d3ff12ffa0					
13.	<input type="checkbox"/>	d806d1d5d6d7					
14.	<input type="checkbox"/>	ec68812a3c4d					
15.	<input type="checkbox"/>	f45433112233					

Endpoint	Attributes	Device Fingerprints
Attribute		Value
1.	cyberx_authorized	= true
2.	cyberx_engineeringStation	= false
3.	cyberx_firmware	= {additionalData=N/A, serial=N/A, routePath=N/A, model=N/A, version=11.3.0.3851.xx}
4.	cyberx_name	= 192.168.40.1
5.	cyberx_protocols	= DeltaV
6.	cyberx_type	= DCS Controller
7.	cyberx_vendor	= FISHER CONTROLS
8.	Click to add...	

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](#)

Identify



Discover/Profile and then authenticate users and devices connected to your network.

Adaptive Trust in action

The Closed Loop approach to Security

Request Details

Summary **Input** Output Accounting

Endpoint Attributes

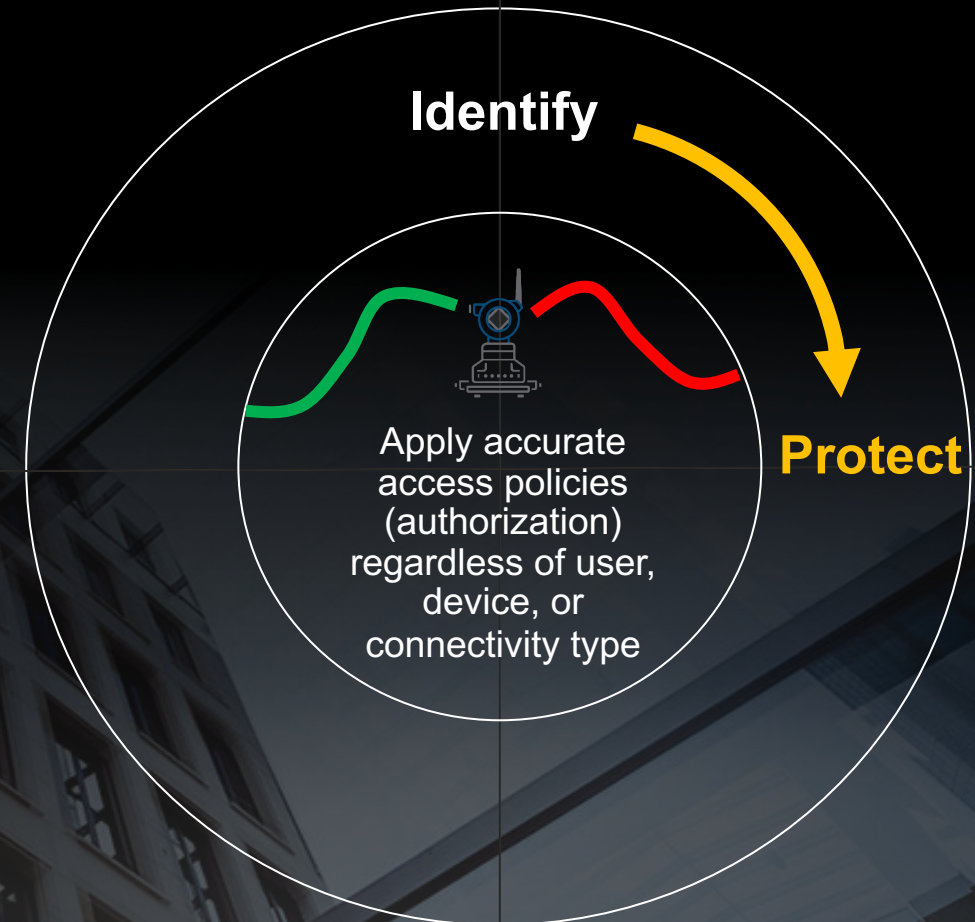
Added by	Policy Manager
Status	Known
Device Category	Network Camera
Device OS Family	ACTi Corporation
Device Name	ACTi Security Camera
MAC Address	f000001434d2
IP Address	10.2.100.234
Static IP	false
Hostname	ipcam-1434d2-mc200e2_200w_v0
Profile Conflict	false
Added Date	Oct 29, 2018 07:17:22 PDT
Updated Date	Nov 05, 2018 08:56:35 PST

Fingerprint Details -

fingerprint.host.mac_vendor [""]

Showing 1 of 1-92 records

Change Status Show Configuration Export Show Logs Close



Adaptive Trust in action

The Closed Loop approach to Security

Request Details

Summary Input Output Accounting

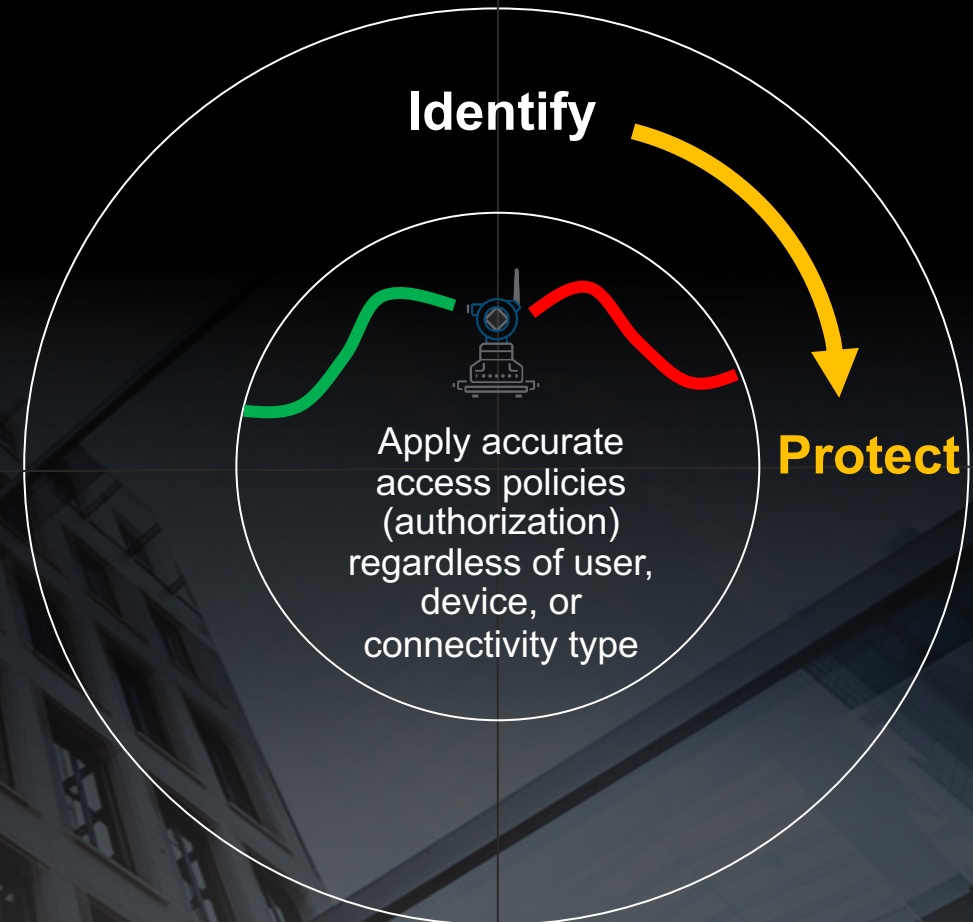
Connection:SSID	
Date:Date-Time	2018-11-05 10:03:33
Device:Location	Las Vegas
Device:storeId	A5678
Endpoint:Background Detection	+447585707938
Endpoint:cap-control	false
Endpoint:Phone Number	+14082039748
Endpoint:UBA-Flag	true

Endpoint Attributes

Added by	Policy Manager
Status	Known
Device Category	Network Camera
Device OS Family	ACTi Corporation
Device Name	ACTi Security Camera
MAC Address	f000001434d2

Showing 1 of 1-97 records

Change Status Show Configuration Export Show Logs Close



Adaptive Trust in action

The Closed Loop approach to Security

Request Details

Summary Input **Output** Accounting

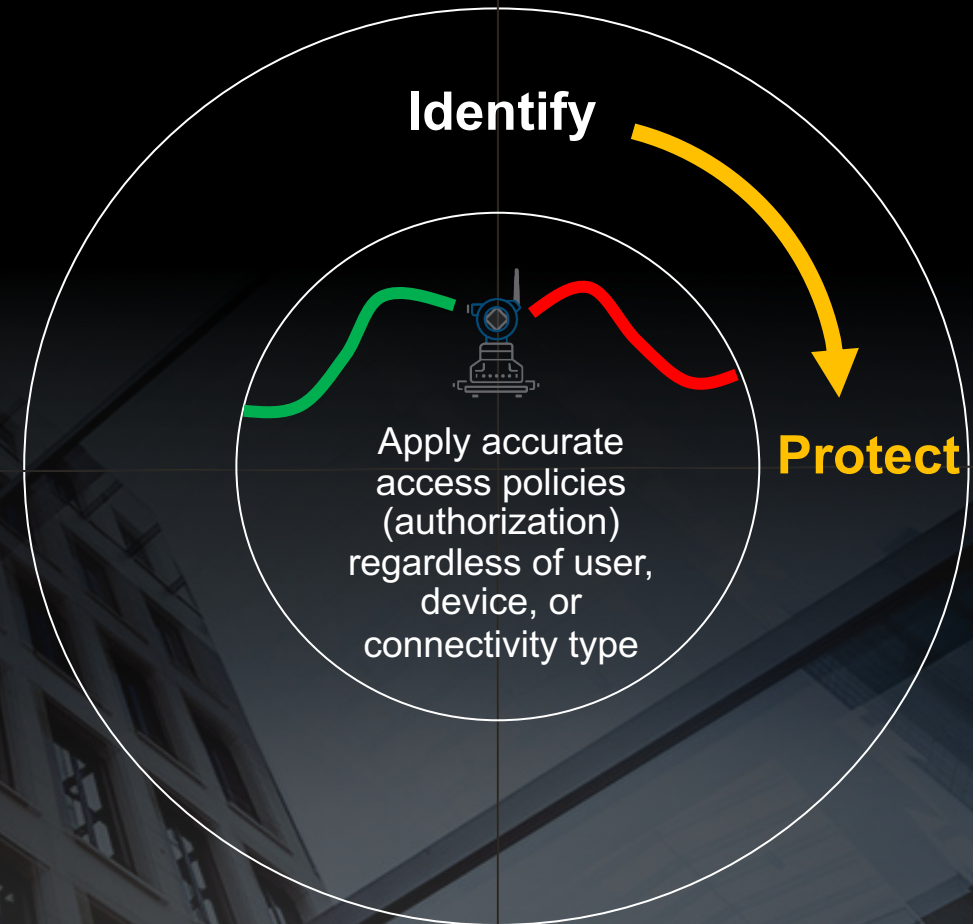
Enforcement Profiles:	IoT-mac-auth-allow-access
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role IoT-allow-access

Showing 1 of 1-92 records

Change Status Show Configuration Export Show Logs Close



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?

Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler
Role Mapping Policy:		MAC Auth Authorization			Modify	
Role Mapping Policy Details						
Description:						
Default Role:		[Other]				
Rules Evaluation Algorithm:		evaluate-all				
Conditions		Role				
1.	(Authorization:[Endpoints Repository]:Conflict EQUALS true)				Spoof	
2.	(Authorization:[Endpoints Repository]:Status NOT_EXISTS)				First Cnx	
3.	(Authorization:[Endpoints Repository]:IsProfiled EQUALS true)				Device_Profiled	
4.	(Authorization:[Endpoints Repository]:IsProfiled EQUALS false) OR (Authorization:[Endpoints Repository]:IsProfiled NOT_EXISTS)				Device_Not_Profiled	
5.	(Authorization:[Endpoints Repository]:Category EQUALS Computer) OR (Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)				Browser	
6.	(Authorization:[Endpoints Repository]:Device Name CONTAINS WebCam)				WebCam	
7.	(Authorization:[Endpoints Repository]:OS Family EQUALS Raspberry Pi)				IoT	
8.	(Authorization:[Guest Device Repository]:SponsorName EXISTS) AND (Endpoint:Owner NOT_EXISTS)				CPG_Device	
9.	(Authorization:[Endpoints Repository]:Device Name EQUALS Aruba Controller)				Controller	
10.	(Authorization:[Endpoints Repository]:Hostname BEGINS_WITH IAD)				IAD	
11.	(Endpoint:Error GREATER_THAN %{Authorization:[Time Source]:FirstThing DT})				Reported	

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 11:53:14	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!

Unknown Device! x

Secure | https://clearpa...

aruba ClearPass Guest

Device Isolated!

Your client has been isolated!

Please contact IT admin - to get this registered
Use the information below when talking to IT

MAC address b827ebde000d
 ClearPass status Unknown
 IP address 10.228.85.1
 Hostname raspberypi
 Category Computer
 Family Raspberry Pi
 Type Raspberry Pi

© Copyright 2019 Hewlett Packard Enterprise Development LP

Unknown Device Connected...

FILE MESSAGE

Mon 09/09/2019 11:52
 cprm@hpearubademo.com
 Unknown Device Connected
 To Mellor, Derin

An Unknown device 98:d6:bb:0a:31:f7

 This is located at NAS-IP: 192.168.137.90, Port: 2.

Connection Time: 2019-09-09 11:52:14

Manufacturer: Apple, Inc.

Hostname: apple-tv-5

Device Category: Home Audio/Video Equipment

Device OS Family: Apple

Device Name: Apple TV

 Click [here](#) to register your device.

Unable to log in to: SharePoint.

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!

Edit Endpoint

Endpoint Attributes Device Fingerprints

MAC Address	98d6bb0a31f7	IP Address	10.137.40.100
Description		Static IP	FALSE
		Hostname	apple-tv-5
Status	<input checked="" type="radio"/> Known client <input type="radio"/> Unknown client <input type="radio"/> Disabled client	Device Category	Home Audio/Video Equ
		Device OS Family	Apple
		Device Name	Apple TV
MAC Vendor	Apple, Inc.	Added At	Sep 09, 2019 11:41:56 BST
Added by	Policy Manager	Profiled by	Policy Manager
Online Status	Online	Last Profiled At	Sep 09, 2019 12:53:40 BST
Connection Type	Wired		
Switch IP	192.168.137.90		
Switch Port	2		

Save Cancel

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	
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!

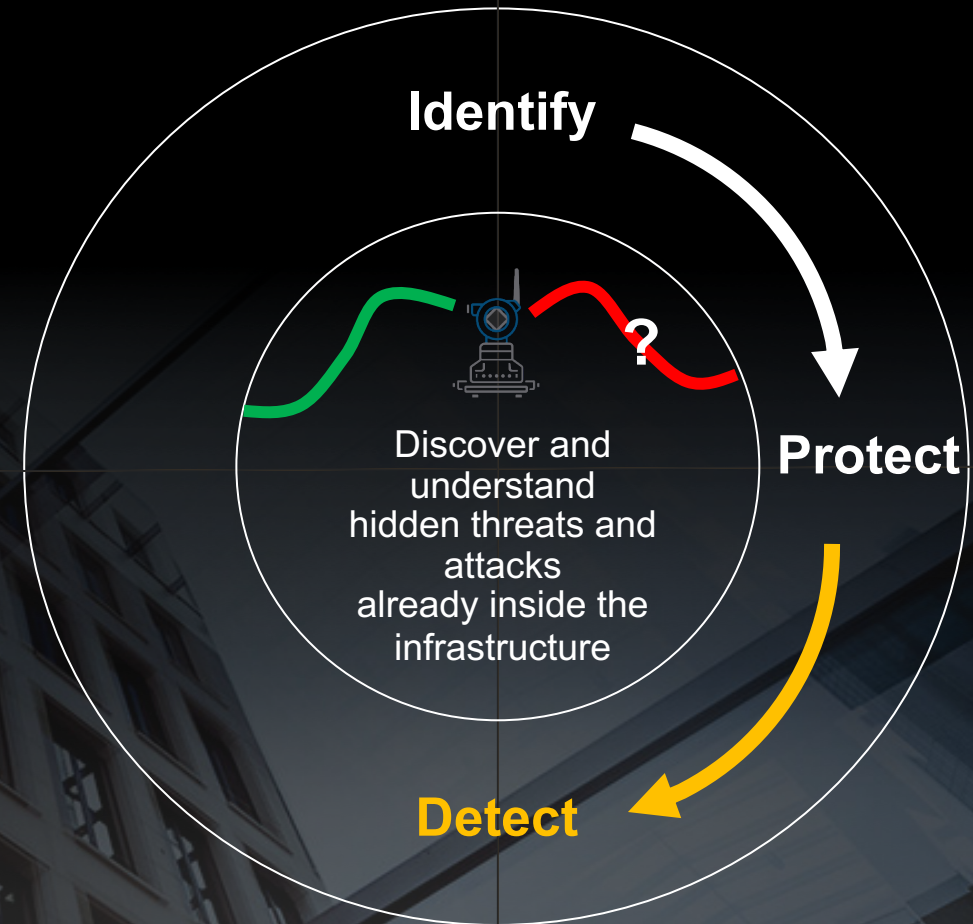
Summary	Input	Output	Accounting
Enforcement Profiles:	NMAP Scan, DUR_Wired_AppleTV		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role		DUR_Wired_AppleTV-3162-31 class ipv4 DHCP match udp any any eq 67 exit 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	
9. (Tips:Role EQUALS IAP Printer)	DUR_Wired_IAP_Printer, 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

The Closed Loop approach to Security – More Context!



Adaptive Trust in action

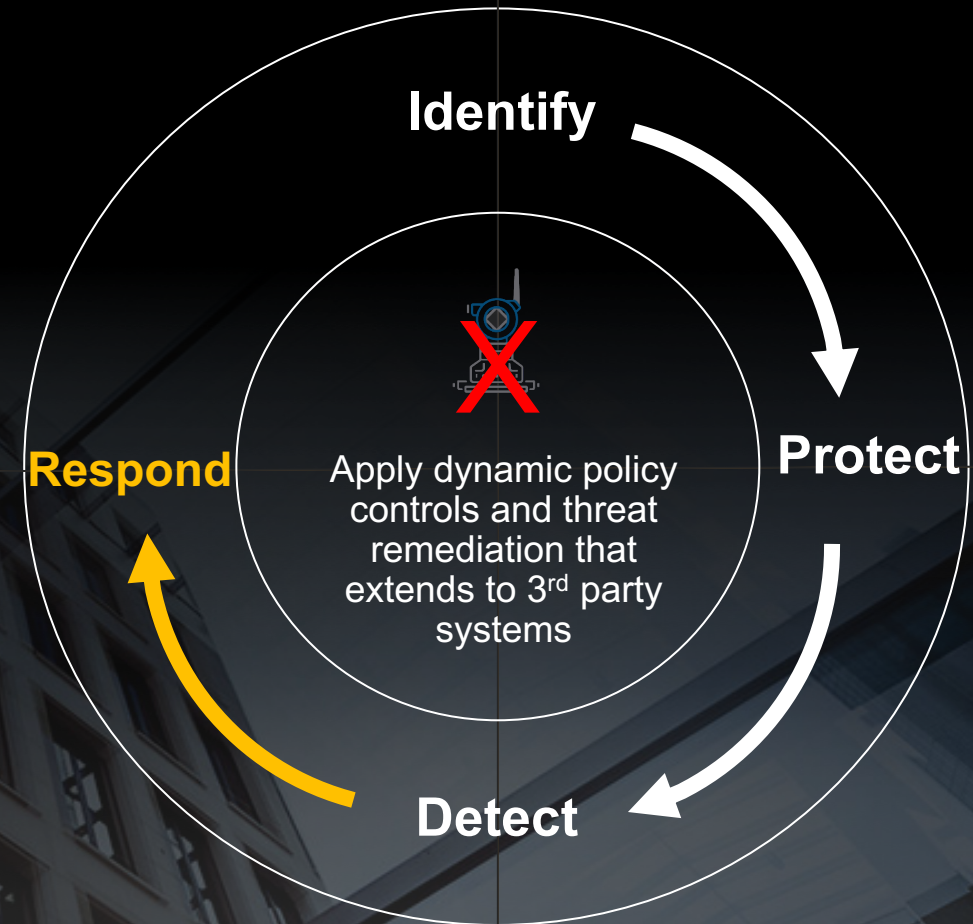
The Closed Loop approach to Security

Request Details	
Summary	Input
Connection:NAD-IP-Address	10.2.100.20
Connection:Protocol	RADIUS
Connection:Src-IP-Address	10.2.100.20
Connection:Src-Port	34230
Connection:SSID	
Date:Date-Time	2018-11-05 09:57:55
Device:Location	Las Vegas
Device:storeId	A5678
Endpoint:Background Detection	+447585707938
Endpoint:cap-control	false
Endpoint:Phone Number	+14082039748
Endpoint:UBA-Flag	investigate

Endpoint Attributes	
Added by	Policy Manager
Status	Known

Showing 1 of 1-96 records

Change Status Show Configuration Export Show Logs Close



Adaptive Trust in action

The Closed Loop approach to Security

Request Details

Summary Input **Output** Accounting

Enforcement Profiles: Send Quarantined Device Notification (Text to Speech), IoT-quarantine

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

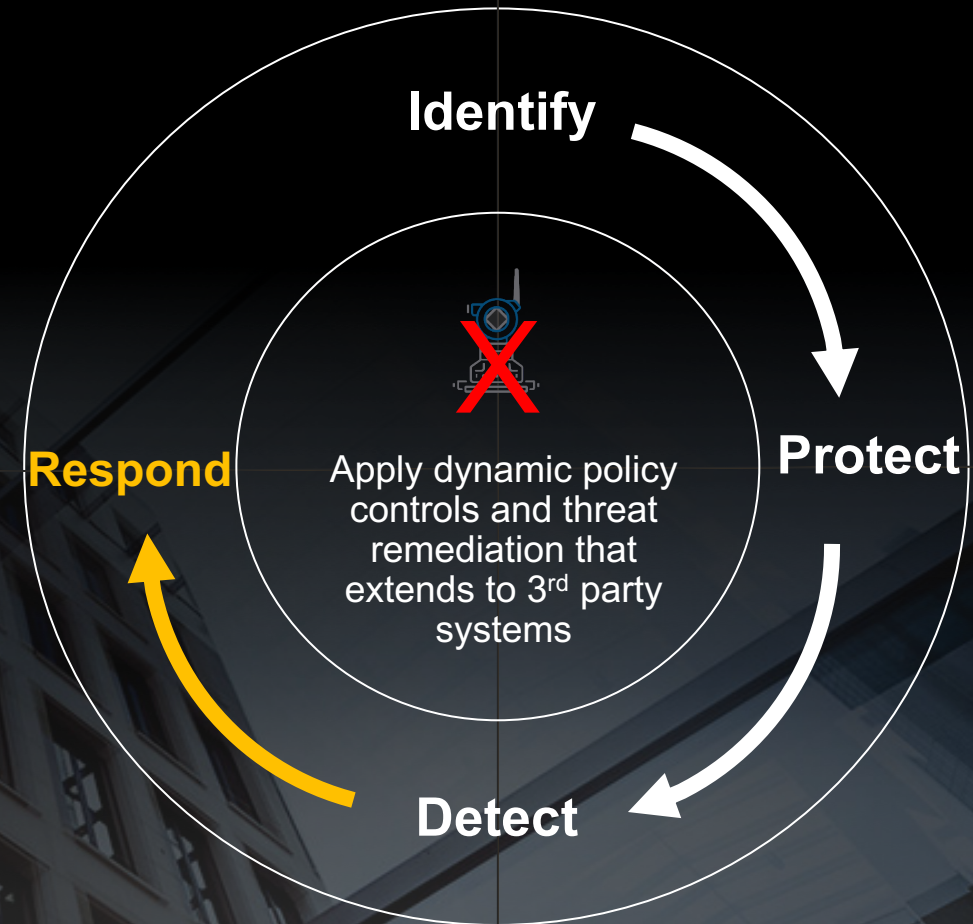
RADIUS Response

Action	3036
Radius:Aruba:Aruba-User-Role	IoT-quarantine
TargetServer	3023

Application Response

HTTP:Action	3036 [Send Compromised Device Notification (Text to Speech) (Generic HTTP)]
HTTP:TargetServer	3023 [api.twilio.com]

Showing 1 of 1-96 records | Change Status | Show Configuration | Export | Show Logs | Close



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!**

airheads

TECH TALK *LIVE*