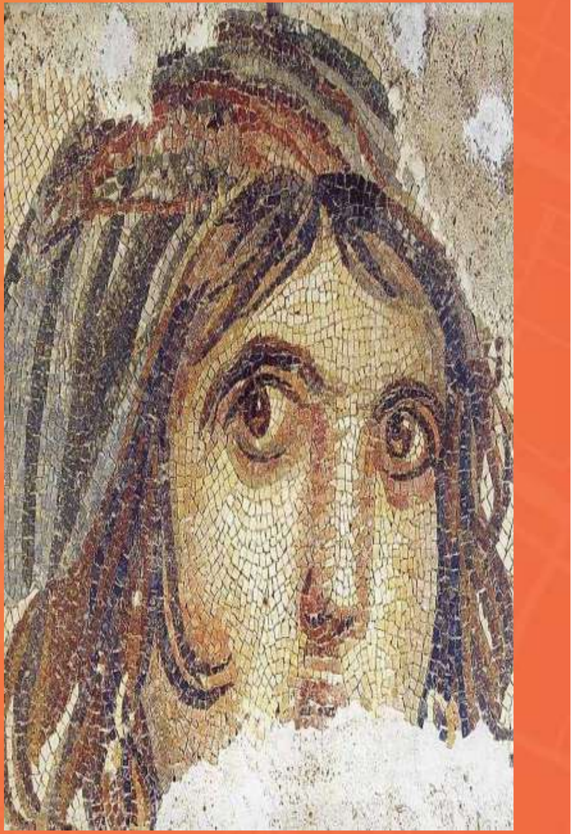
AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

ClearPass & IntroSpect Overview



Yasin FAKILI
yasin.fakili@hpe.com

06/12/2018 Gaziantep

#ArubaAirheads

Today’s Escalating Customer Challenges

Advanced attacks and unforeseen threats continue to plague customers

Lack of network and endpoint unified visibility hampers time to detect and remediate

Point solutions add to complexity and overloads security IT personnel

ClearPass at a Glance

VISIBILITY

- Know what's connected, connecting in your wired & wireless multivendor environment

aruba a Hewlett Packard Enterprise company · Hewlett Packard Enterprise · JUNIPER NETWORKS · BROCADE · CISCO · Extreme networks · ARISTA

CONTROL

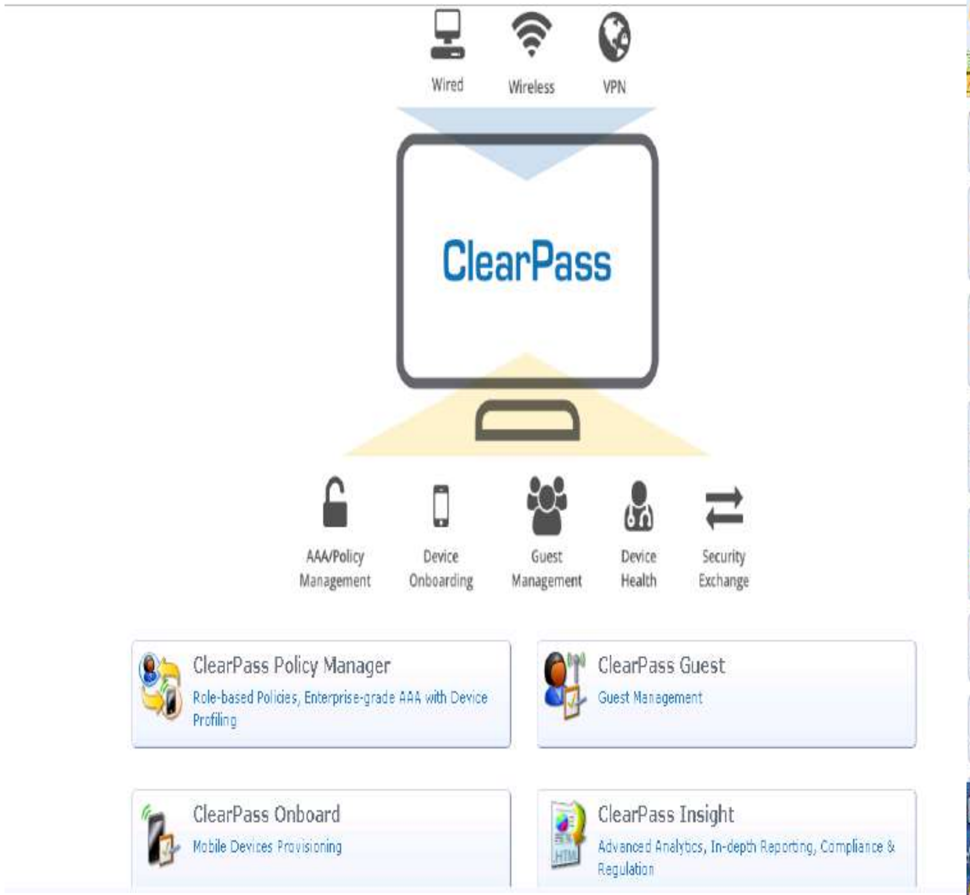
- Reduce risk and workload through Automation
- All devices are Authenticated or Authorized – NO UKNOWN DEVICES

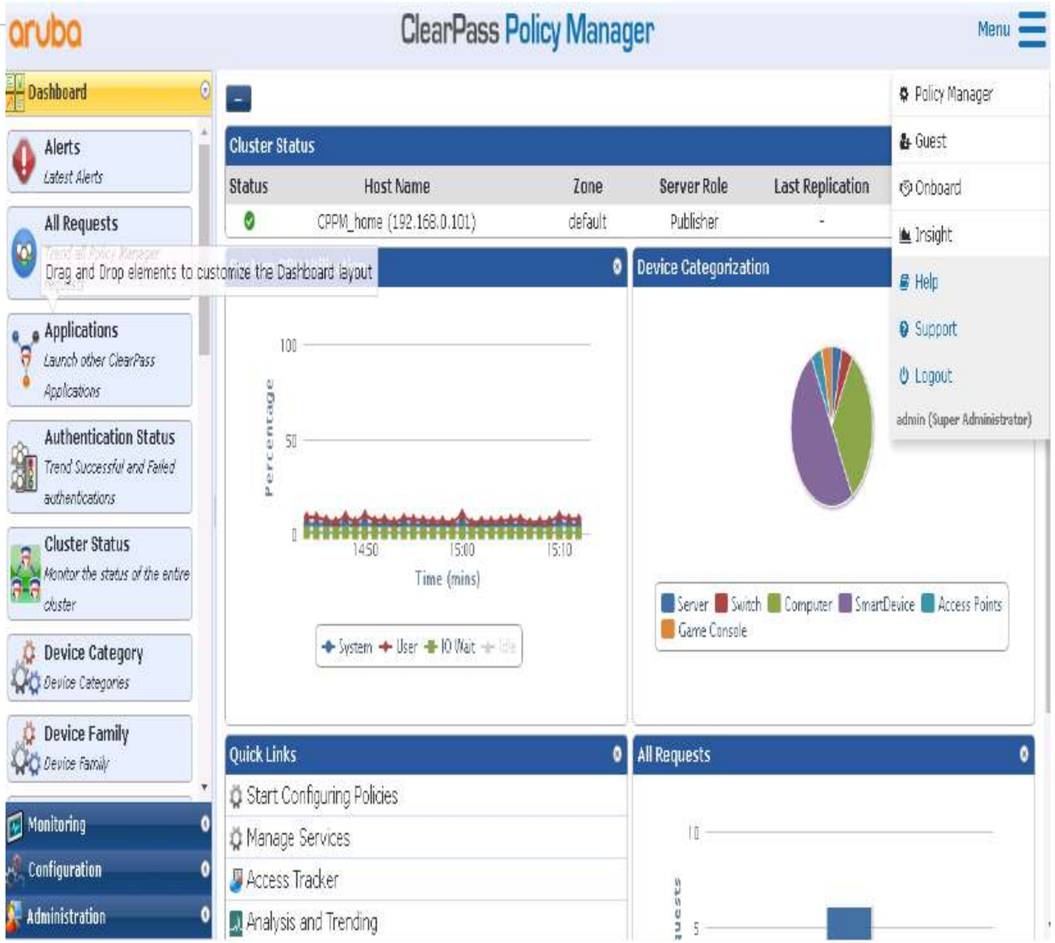
RESPONSE

- Adaptive response brokering best of breed security solutions

paloalto NETWORKS · splunk> · ArcSight · MobileIron · DUO · intel Security · Microsoft · Check Point SOFTWARE TECHNOLOGIES LTD.

ClearPass at a Glance





Drag and Drop elements to customize the Dashboard layout

Cluster Status

Status	Host Name	Zone	Server Role	Last Replication
✓	CPPM_home (192.168.0.101)	default	Publisher	-

Quick Links

- Start Configuring Policies
- Manage Services
- Access Tracker
- Analysis and Trending

ClearPass Policy Manager - What's Built-in!

Over 100+ Partners

Services

- Policy Engine
- 802.1X
- MAC Auth
- Guest
- TACACS+
- Profiling
- Context Database
- +100 RADIUS dictionaries

IT Tools

- Policy Simulation
- Access Tracking
- Template-based policy creation
- LDAP Browser
- Per Session Logs
- Advanced Reporting
- AirGroup

Bonjour/DLNA

Security Exchange

(3rd Party Integration)

- API's
- Syslog Feeds
- Extensions
- Ingress Events

paloalto NETWORKS

intel Security

Pluribus NETWORKS

MobileIron

Microsoft

DUO

servicenow

ClearPass Expandable Applications

Automated workflows

Enhanced security for BYOD and guests

Rules by user role and device types

Onboard

OnGuard

Understanding Connectivity Options

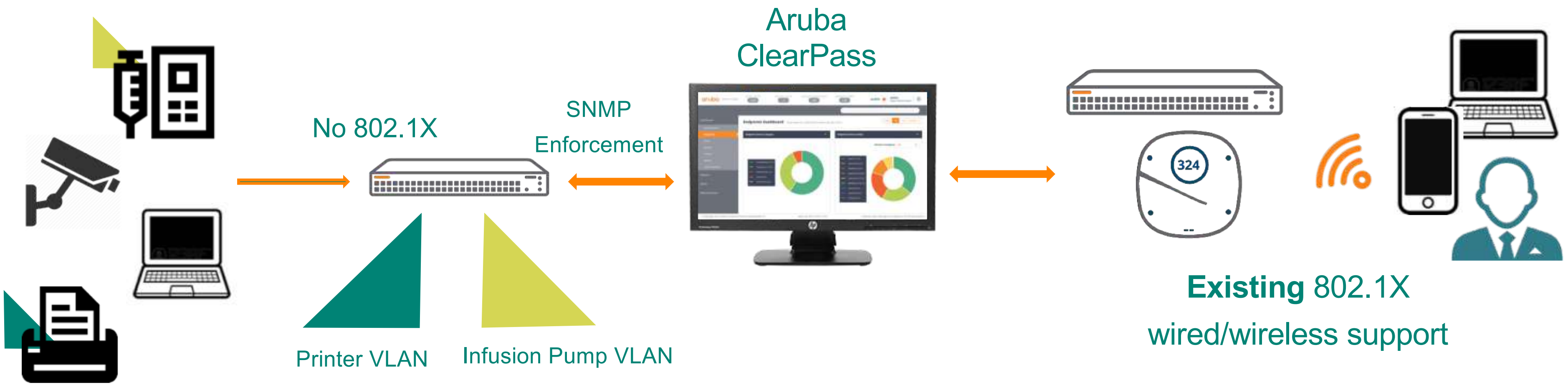
Customers want to **manage** what devices connect

Only some support .1X supplicants

50% of IoT may be wired

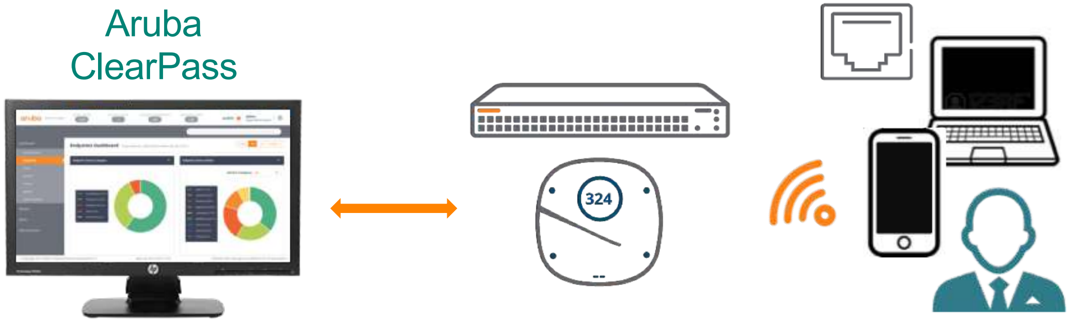
- ClearPass supports any customer Infrastructure and need

OnConnect for Wired Non-RADIUS Enforcement



- Built-in device-centric security for all non-AAA ready customers
- Easy to configure on legacy multivendor switches
- Leverages ClearPass profiling for wired/wireless - IoT, laptops, mobile phones.

Secure Connections: Authentication Before Access



Existing 802.1X
wired/wireless support

- Multivendor support for all 802.1X ready wired and wireless customers
- Secure encrypted wireless access
- Built-in ClearPass profiling - IoT, laptops, mobile phones
- Easy to use policy creation templates

Comprehensive Profiler Methods

Helps ensure accurate fingerprints

Passive Profiling

- DHCP Fingerprinting (MAC OUI & Certain Options)
  - AOS IF-MAP Interface, DHCP Relay or SPAN
- HTTP User-Agent
  - New! AOS IF-MAP Interface, SPAN, Guest and Onboard Workflows
- TCP Fingerprinting (SYN, SYN/ACK)
  - SPAN
- ARP
  - SPAN
- Cisco Device Sensor
- Netflow/IPFIX/sFlow New!
  - Identifies open ports

Active Profiling

- Windows Management Instrumentation (WMI)
- Nmap
- MDM/EMM
- SSH
- ARP Table
  - SNMP
- MAC/Interface Table
  - SNMP
- CDP/LLDP Table
  - SNMP

Sources of Usable Context

Device Profiling

- Samsung SM-G950U
- Android
- “Jons-Galaxy”

EMM/MDM

- Personally owned
- Registered
- OS up-to-date

- Hansen, Jon [Sales]
- MDM enabled = true
- In-compliance = true

- Hansen, Jon [Sales]
- Title – COO
- Dept – Executive office
- City – London

Identity Stores

Microsoft Active Directory
Office 365
MySQL
okta
G Suite
Ping Identity
OASIS STANDARD SAML
OAUTH 2

Enforcement Points

- Location – Bldg 10
- Floor – 3
- Bandwidth – 10Mbps

Adaptive Policy Using Device Ownership

Enterprise Laptop

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet and Intranet

SAP

ORACLE

Lync

box

Exchange

BYOD Phone

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet Only

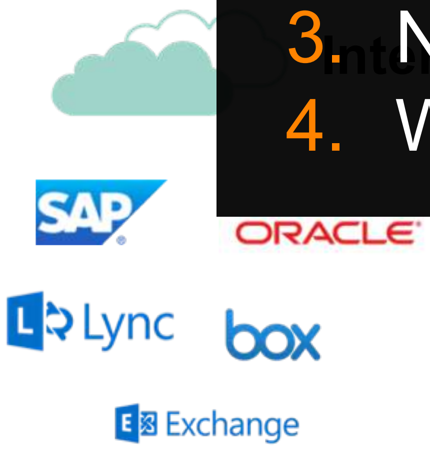
Adaptive Policy Using Device Ownership

Enterprise Laptop

Authentication → EAP-TLS

SSID → CORP-SECURE

Internet and Intranet



BYOD Phone

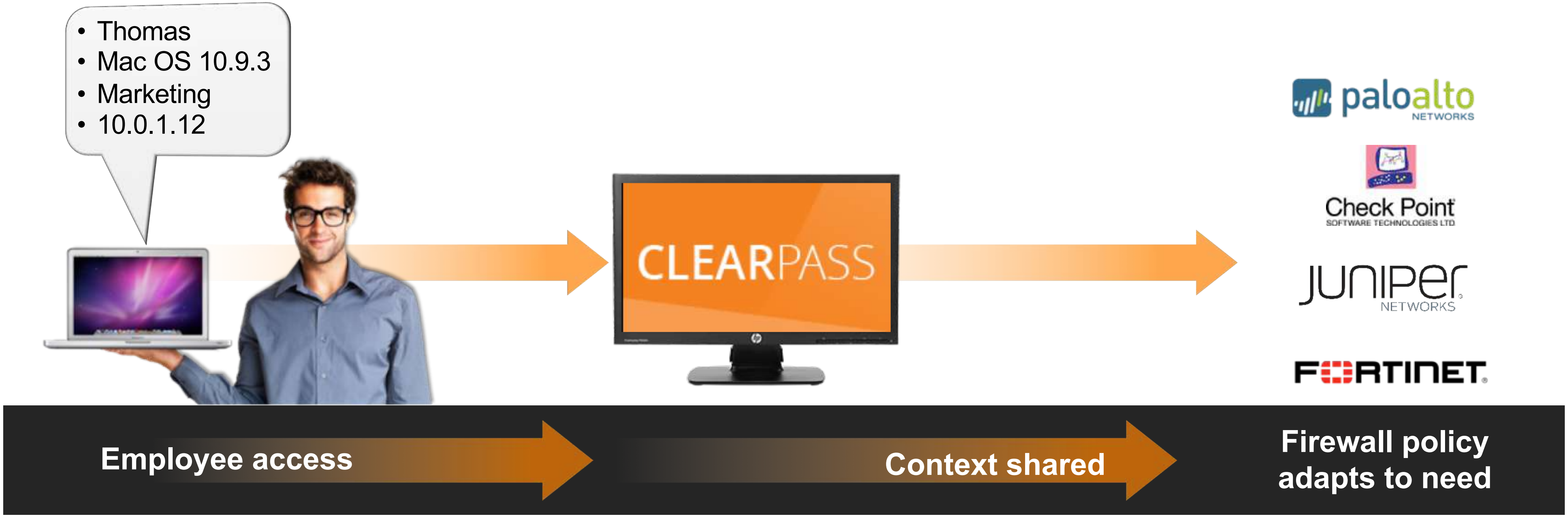
Authentication → EAP-TLS

SSID → CORP-SECURE

Internet Only

1. Uses same identity store and EAP type
2. Leverages profiling and owner data
3. No need for separate SSIDs
4. Works at the office and over VPN

Adaptive Trust Context Sharing



- Thomas
- Mac OS 10.9.3
- Marketing
- 10.0.1.12

Employee access

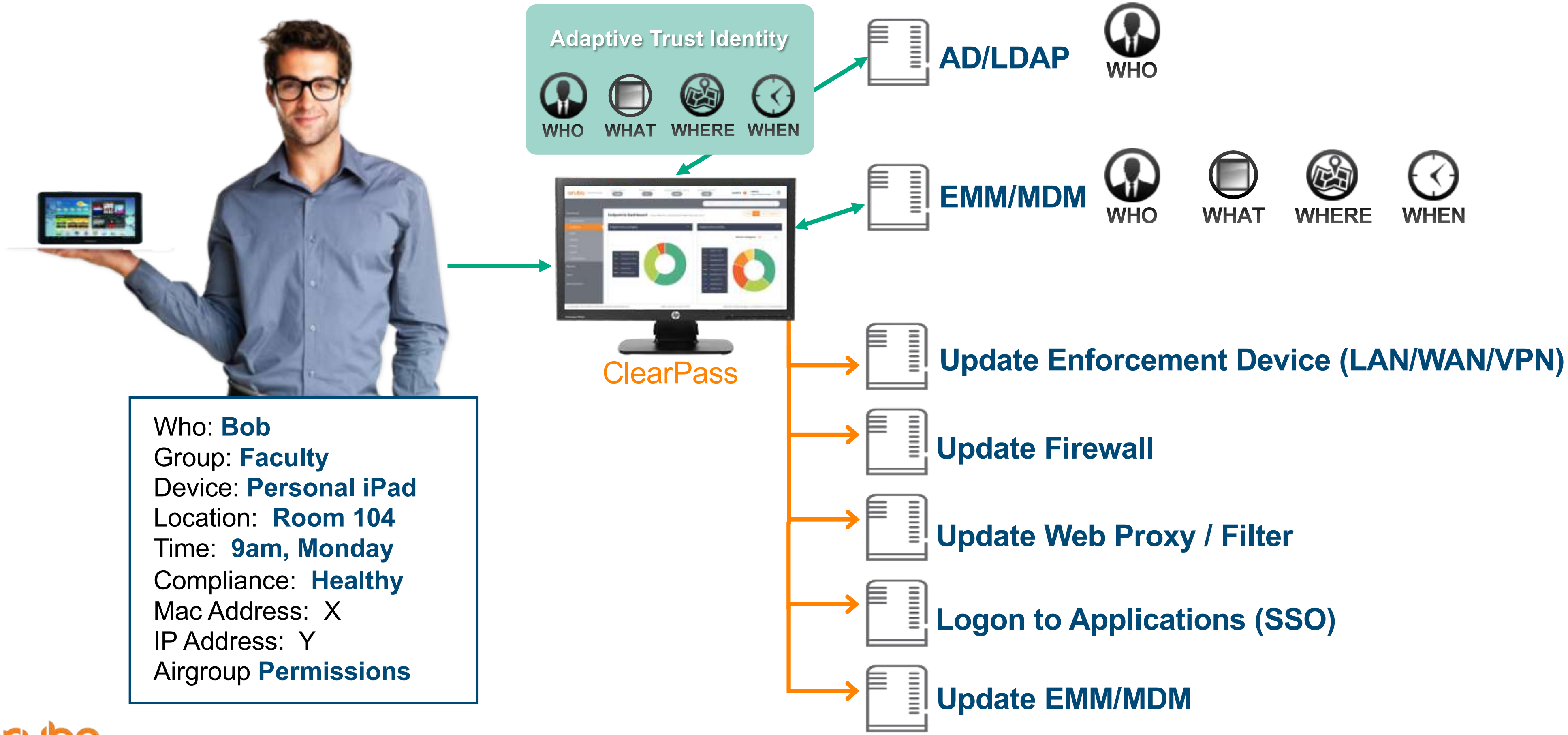
Context shared

Firewall policy adapts to need

Works with AD, LDAP, ClearPass dB, SQL dB

No agents/clients required

Security and Usability Coordination



Adaptive Trust Identity

ClearPass

AD/LDAP

EMM/MDM

Update Enforcement Device (LAN/WAN/VPN)

Update Firewall

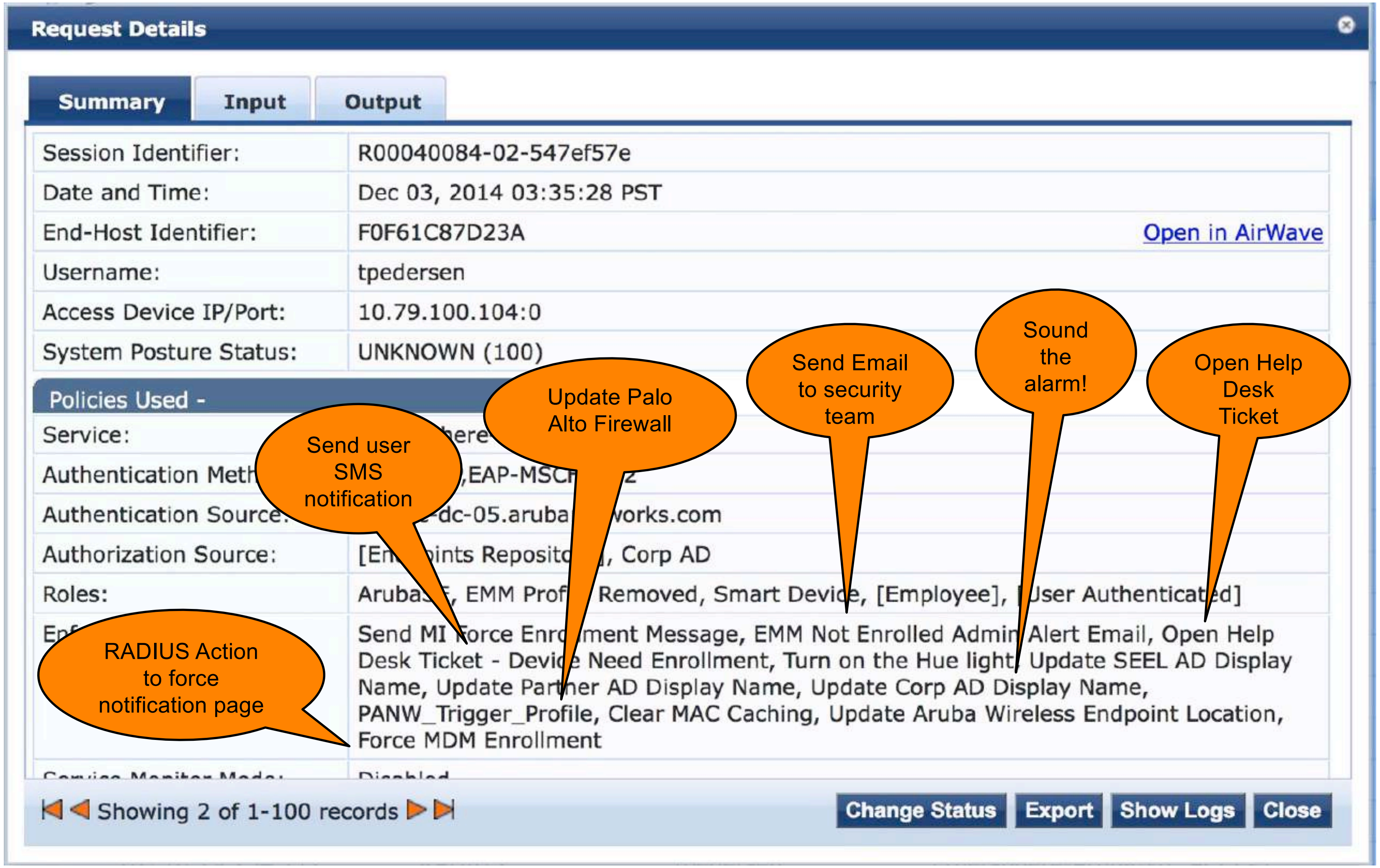
Update Web Proxy / Filter

Logon to Applications (SSO)

Update EMM/MDM

Who: **Bob**
Group: **Faculty**
Device: **Personal iPad**
Location: **Room 104**
Time: **9am, Monday**
Compliance: **Healthy**
Mac Address: X
IP Address: Y
Airgroup **Permissions**

Service Chaining Example



Session Identifier:	R00040084-02-547ef57e
Date and Time:	Dec 03, 2014 03:35:28 PST
End-Host Identifier:	F0F61C87D23A
Username:	tpedersen
Access Device IP/Port:	10.79.100.104:0
System Posture Status:	UNKNOWN (100)
Service:	here
Authentication Meth	,EAP-MSCH 2
Authentication Source:	-dc-05.aruba works.com
Authorization Source:	[En oints Reposito], Corp AD
Roles:	Aruba F, EMM Prof Removed, Smart Device, [Employee], [User Authenticated]
En	Send MI Force Enrollment Message, EMM Not Enrolled Admin Alert Email, Open Help Desk Ticket - Device Need Enrollment, Turn on the Hue light, Update SEEL AD Display Name, Update Partner AD Display Name, Update Corp AD Display Name, PANW_Trigger_Profile, Clear MAC Caching, Update Aruba Wireless Endpoint Location, Force MDM Enrollment
Service Monitor Mode:	Disabled

Send user SMS notification

Update Palo Alto Firewall

Send Email to security team

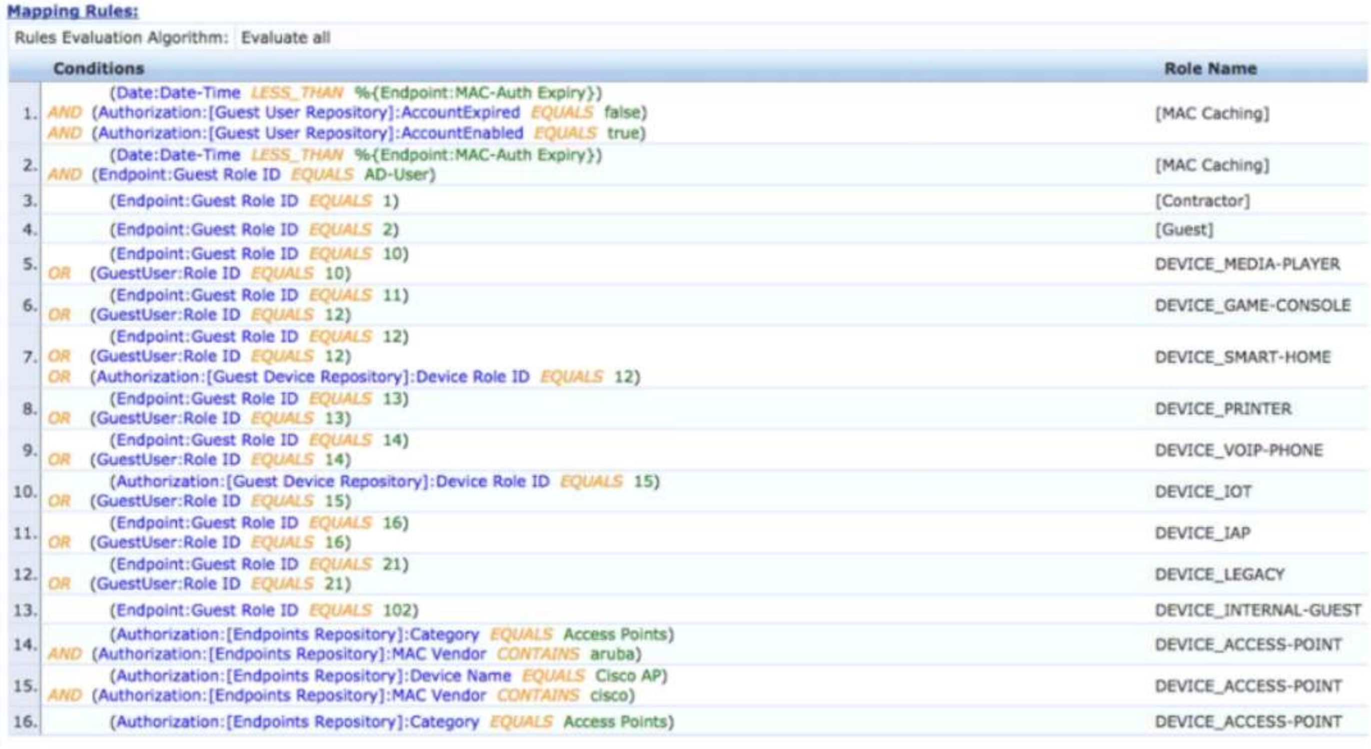
Sound the alarm!

Open Help Desk Ticket

RADIUS Action to force notification page

Role Mapping

- Can be simple or complex

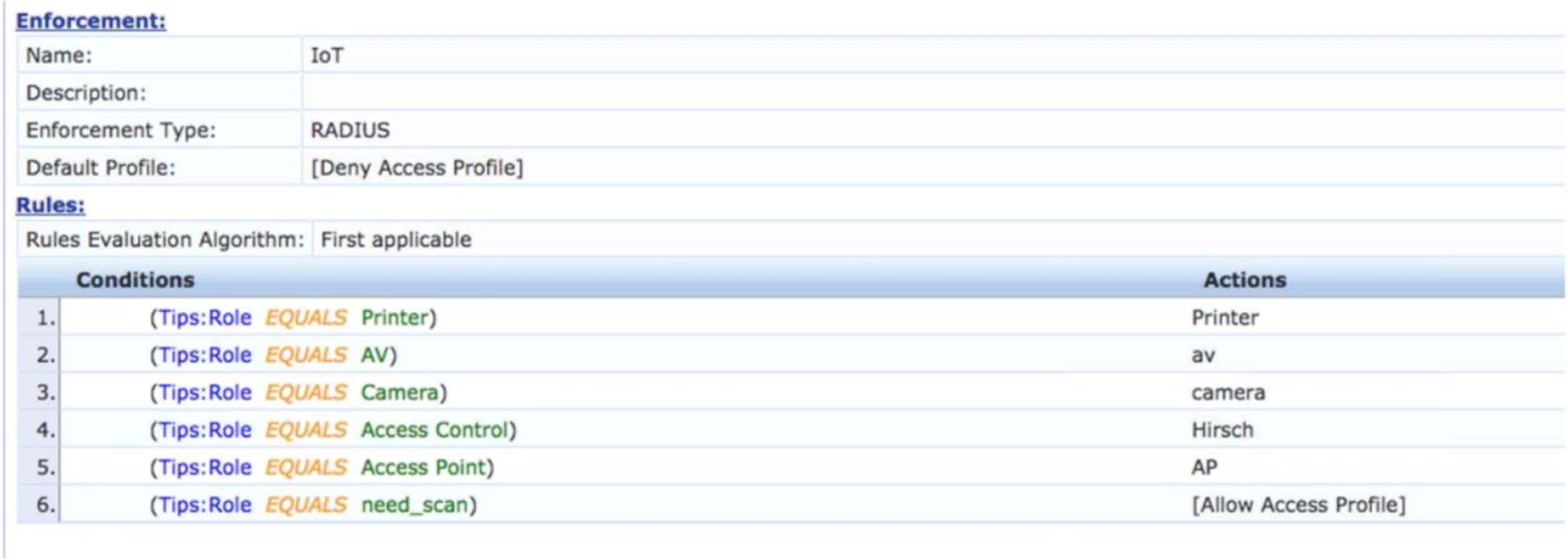


Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

	Conditions	Role Name
1.	(Date:Date-Time LESS_THAN %{Endpoint:MAC-Auth Expiry}) AND (Authorization:[Guest User Repository]:AccountExpired EQUALS false) AND (Authorization:[Guest User Repository]:AccountEnabled EQUALS true)	[MAC Caching]
2.	(Date:Date-Time LESS_THAN %{Endpoint:MAC-Auth Expiry}) AND (Endpoint:Guest Role ID EQUALS AD-User)	[MAC Caching]
3.	(Endpoint:Guest Role ID EQUALS 1)	[Contractor]
4.	(Endpoint:Guest Role ID EQUALS 2)	[Guest]
5.	(Endpoint:Guest Role ID EQUALS 10) OR (GuestUser:Role ID EQUALS 10)	DEVICE_MEDIA-PLAYER
6.	(Endpoint:Guest Role ID EQUALS 11) OR (GuestUser:Role ID EQUALS 12)	DEVICE_GAME-CONSOLE
7.	(Endpoint:Guest Role ID EQUALS 12) OR (GuestUser:Role ID EQUALS 12) OR (Authorization:[Guest Device Repository]:Device Role ID EQUALS 12)	DEVICE_SMART-HOME
8.	(Endpoint:Guest Role ID EQUALS 13) OR (GuestUser:Role ID EQUALS 13)	DEVICE_PRINTER
9.	(Endpoint:Guest Role ID EQUALS 14) OR (GuestUser:Role ID EQUALS 14)	DEVICE_VOIP-PHONE
10.	(Authorization:[Guest Device Repository]:Device Role ID EQUALS 15) OR (GuestUser:Role ID EQUALS 15)	DEVICE_IOT
11.	(Endpoint:Guest Role ID EQUALS 16) OR (GuestUser:Role ID EQUALS 16)	DEVICE_IAP
12.	(Endpoint:Guest Role ID EQUALS 21) OR (GuestUser:Role ID EQUALS 21)	DEVICE_LEGACY
13.	(Endpoint:Guest Role ID EQUALS 102)	DEVICE_INTERNAL-GUEST
14.	(Authorization:[Endpoints Repository]:Category EQUALS Access Points) AND (Authorization:[Endpoints Repository]:MAC Vendor CONTAINS aruba)	DEVICE_ACCESS-POINT
15.	(Authorization:[Endpoints Repository]:Device Name EQUALS Cisco AP) AND (Authorization:[Endpoints Repository]:MAC Vendor CONTAINS cisco)	DEVICE_ACCESS-POINT
16.	(Authorization:[Endpoints Repository]:Category EQUALS Access Points)	DEVICE_ACCESS-POINT

Enforcement



Enforcement:

Name:	IoT
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* Printer)	Printer
2.	(Tips:Role *EQUALS* AV)	av
3.	(Tips:Role *EQUALS* Camera)	camera
4.	(Tips:Role *EQUALS* Access Control)	Hirsch
5.	(Tips:Role *EQUALS* Access Point)	AP
6.	(Tips:Role *EQUALS* need_scan)	[Allow Access Profile]

Why ClearPass Guest?

Any industry, any # of guests

Only secure guest app in industry

Any device, any network vendor

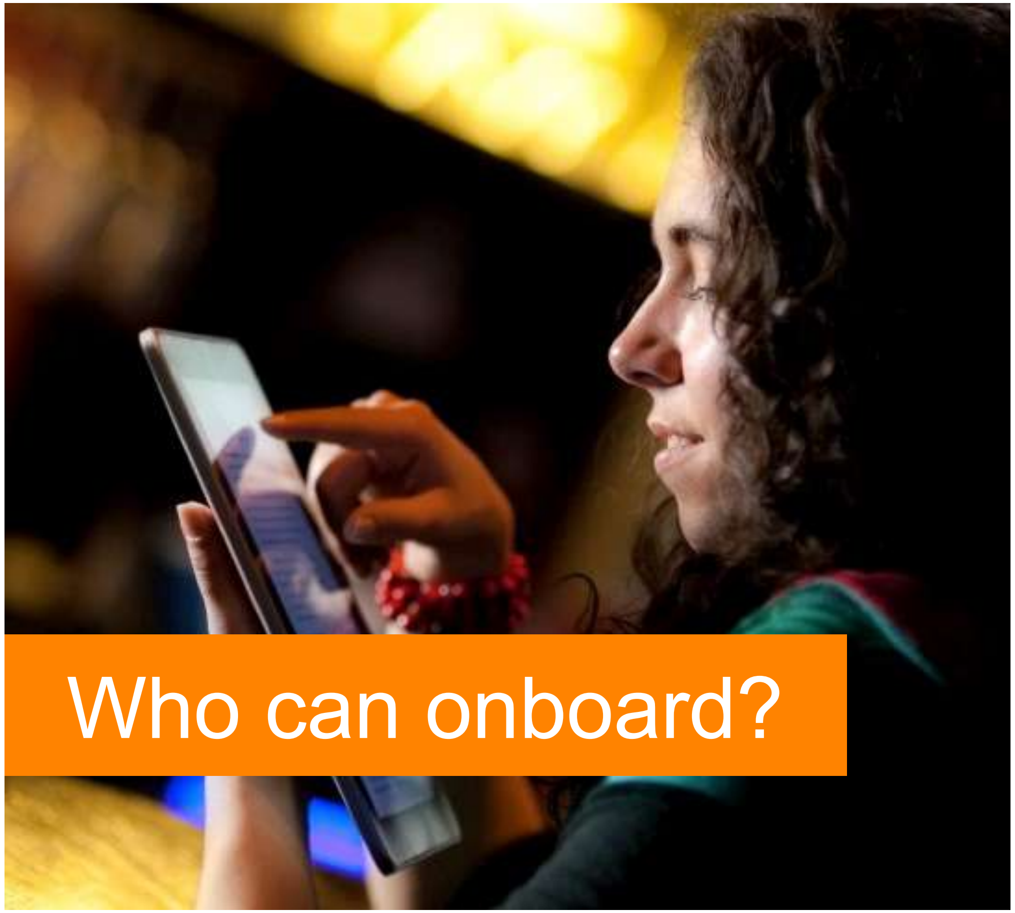
Internet / managed Intranet

Self-service / sponsor / social

Portal fits phone, laptop, tablet

aruba
a Hewlett Packard Enterprise company

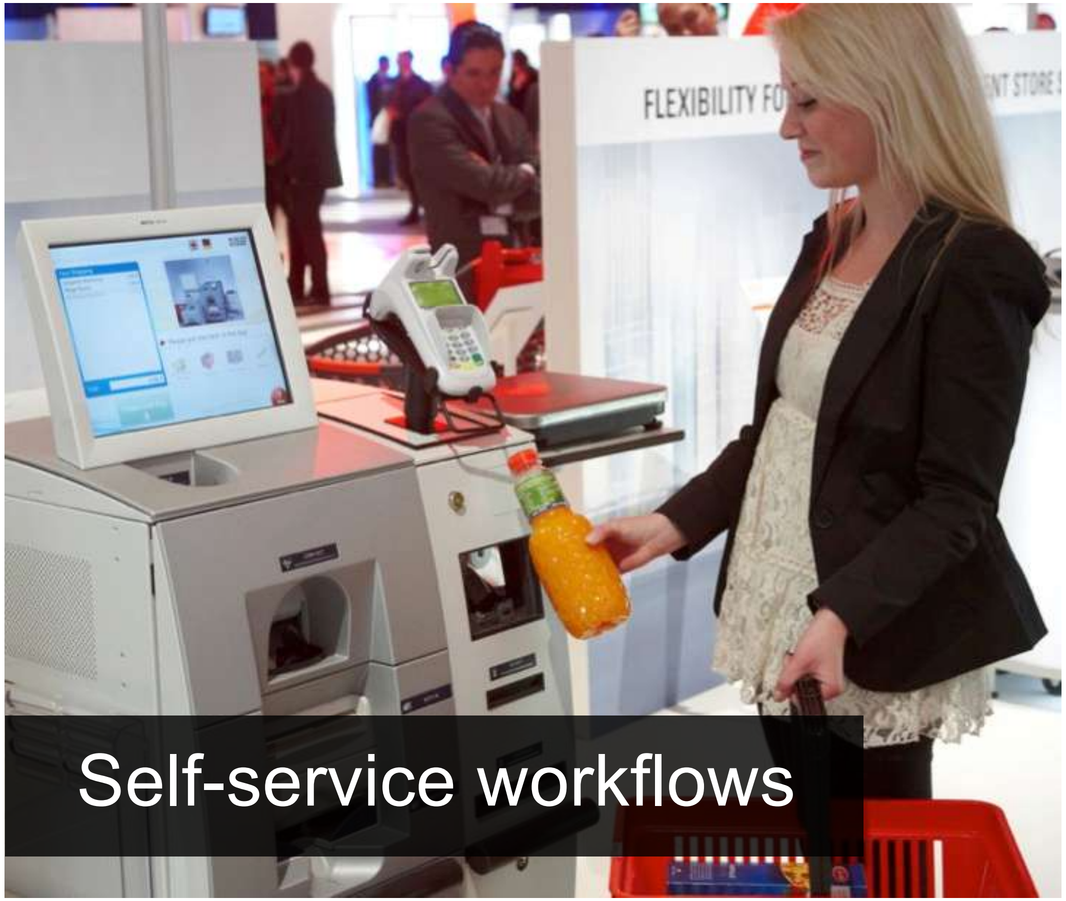
Managing Personal Devices



- User owned
- Replaced often
- Access from anywhere
- Android, iOS, Windows
- Work & personal use

aruba
a Hewlett Packard Enterprise company

Why ClearPass Onboard?



Self-service workflows

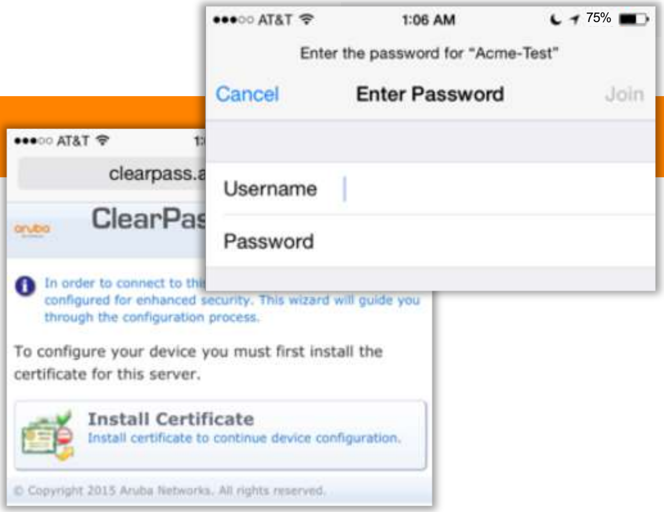
- Automated configuration: Network settings and certs
- Built-in certificate authority (CA): Including user and device data
- Can include in MDM/EMM workflows
- Add security without increasing IT workload or user frustration

Authentication Using Unique Device Certificates

1 User’s device redirected to portal

2 User enters AD credentials to start onboard

3 Automatically places user on proper network segment



●●●○○ AT&T 1:06 AM 75%

Enter the password for “Acme-Test”

Cancel Enter Password Join

Username

Password

●●●○○ AT&T 1:

clearpass.a

aruba ClearPas

In order to connect to th configured for enhanced security. This wizard will guide you through the configuration process.

To configure your device you must first install the certificate for this server.

Install Certificate

Install certificate to continue device configuration.

© Copyright 2015 Aruba Networks. All rights reserved.

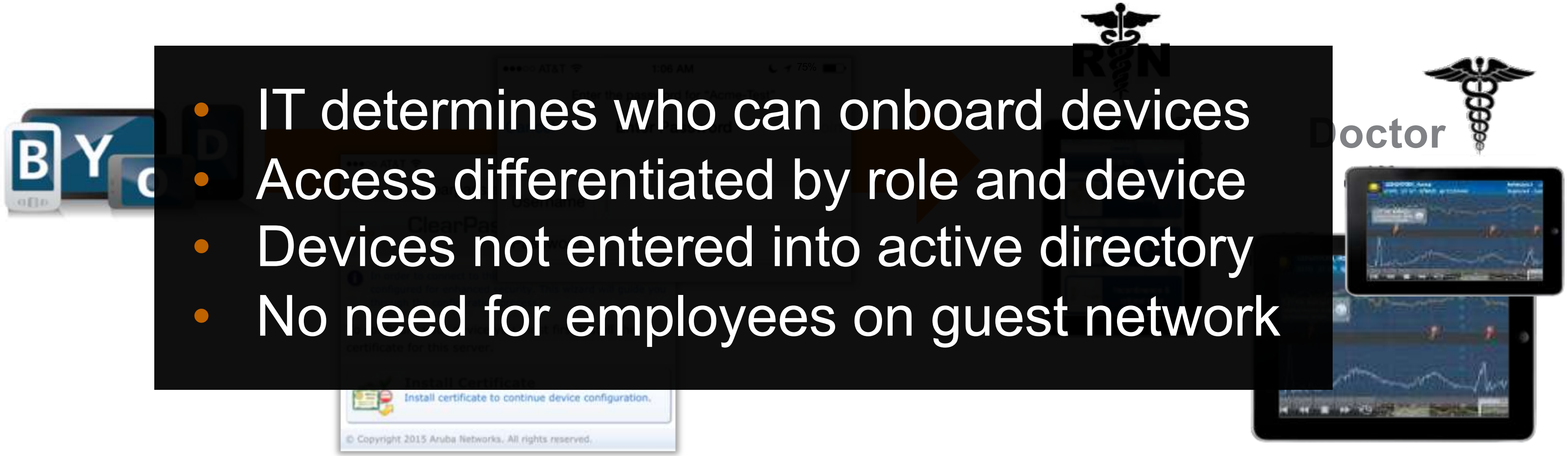
Easy → Secure → No Passwords

Authentication Using Unique Device Certificates

1 User's device redirected to portal

2 User enters AD credentials to start onboard

3 Automatically places user on proper network segment


B Y O D
RN
Doctor
ClearPass
Install Certificate
Install certificate to continue device configuration.
© Copyright 2015 Aruba Networks. All rights reserved.

- IT determines who can onboard devices
- Access differentiated by role and device
- Devices not entered into active directory
- No need for employees on guest network

Easy → Secure → No Passwords

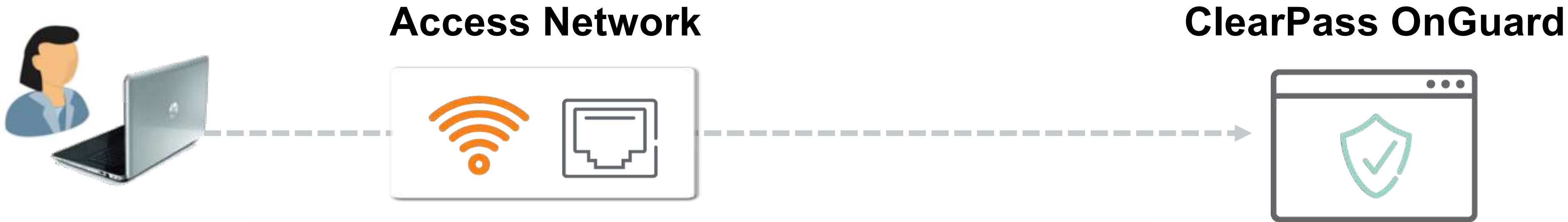
aruba
a Hewlett Packard Enterprise company

Why ClearPass OnGuard?

Endpoint Health

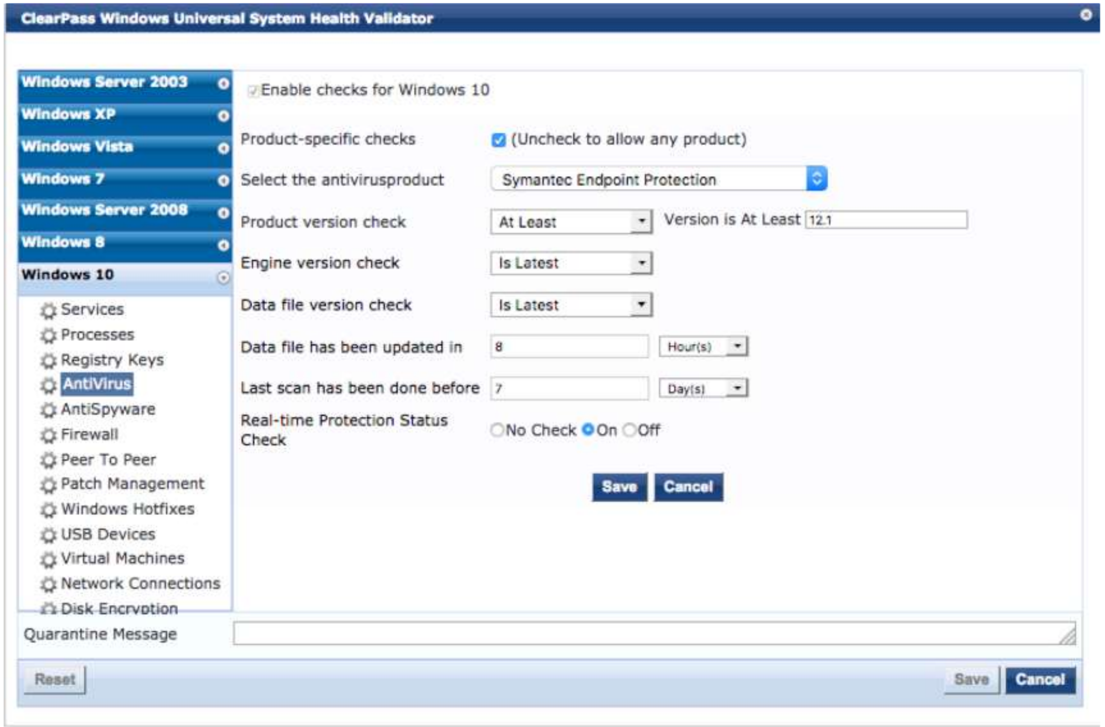
- Check health before network access
- Multiple operating systems supported
- Persistent and dissolvable agents
- Can also be used with BYOD workflows

Automate Device Health Checking



Access Network

ClearPass OnGuard



ClearPass Windows Universal System Health Validator

- Windows Server 2003
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2008
- Windows 8
- Windows 10
  - Services
  - Processes
  - Registry Keys
  - AntiVirus
  - AntiSpyware
  - Firewall
  - Peer To Peer
  - Patch Management
  - Windows Hotfixes
  - USB Devices
  - Virtual Machines
  - Network Connections
  - Disk Encryption

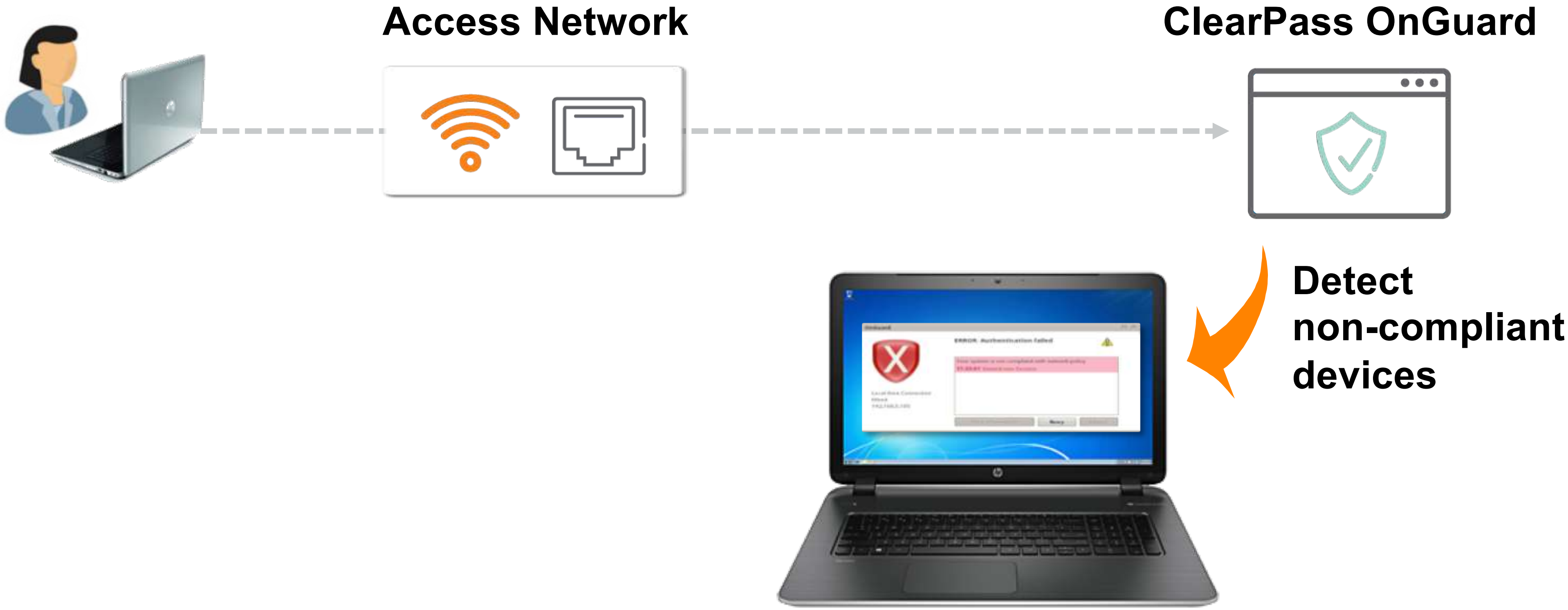
☑ Enable checks for Windows 10

Product-specific checks	☑ (Uncheck to allow any product)
Select the antivirusproduct	Symantec Endpoint Protection
Product version check	At Least — Version is At Least 12.1
Engine version check	Is Latest
Data file version check	Is Latest
Data file has been updated in	8 Hour(s)
Last scan has been done before	7 Day(s)
Real-time Protection Status Check	○ No Check ● On ○ Off

Quarantine Message

Detect non-compliant devices

Automate Device Health Checking



ERROR: Authentication failed
Your system is not compliant with network policy
Retry

Access Network

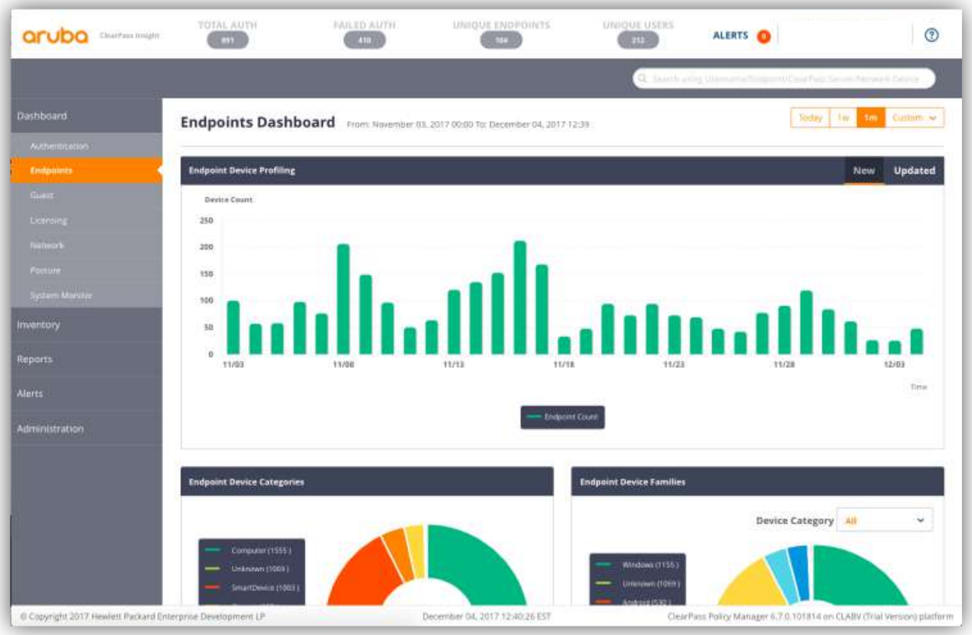
ClearPass OnGuard

Detect non-compliant devices

Block access to network resources across wired, wireless & remote

ClearPass Reporting Using Insight

- One stop shop for all your reporting needs
- New Inventory dashboard
  - Customizable inventory view of all learned devices
- New custom alerting options and filters
  - Improves the ability for ClearPass to proactively notify admins/users of certain events
- Ability to import/export report templates
  - Allows admins to create any template they want without needing a feature enhancement.
- Emailed reports now include the HTML version of the report as well as the raw CSV



Endpoints Dashboard From: November 03, 2017 00:00 To: December 04, 2017 12:39

© Copyright 2017 Hewlett Packard Enterprise Development LP December 04, 2017 12:40:26 EST ClearPass Policy Manager 6.7.0.101814 on CLABV (Trial Version) platform

aruba
a Hewlett Packard Enterprise company

ClearPass 6.7 Licensing

Subscription Or Perpetual	OnGuard (Endpoint Health/Posture)	Onboard (BYOD/CA)	• Sold as 100, 500, 1K, 2500, 5K, 10K • Perpetual and 1/3/5* year Subscription based offerings
Subscription Or Perpetual	Access (802.1X, MAC-Auth, Guest, TACACS+, OnConnect, Endpoint Profiling & Security Exchange)		• Sold as 100, 500, 1K, 2500, 5K, 10K • Perpetual and 1/3/5 year Subscription based offerings
Perpetual	VM Appliance / Hardware Appliances		• Sold as Small, Medium, Large Sizes (HW) • Perpetual VM license

Why ClearPass

Multivendor & 3rd Party integration

User-experience driven applications

Scalability and cost advantages

Business oriented policy services
– building blocks, roles, troubleshooting tools

aruba
a Hewlett Packard
Enterprise company

aruba
a Hewlett Packard Enterprise company

AIRHEADS meetup

IntroSpect

User and Entity Behavior Analytics

06/12/2018 Gaziantep

#ArubaAirheads

INTROSPECT UEBA
User and Entity Behavior Analytics

Uses advanced behavioral analytics

to discover and understand

hidden threats and attacks

already inside the infrastructure

KEY FEATURES

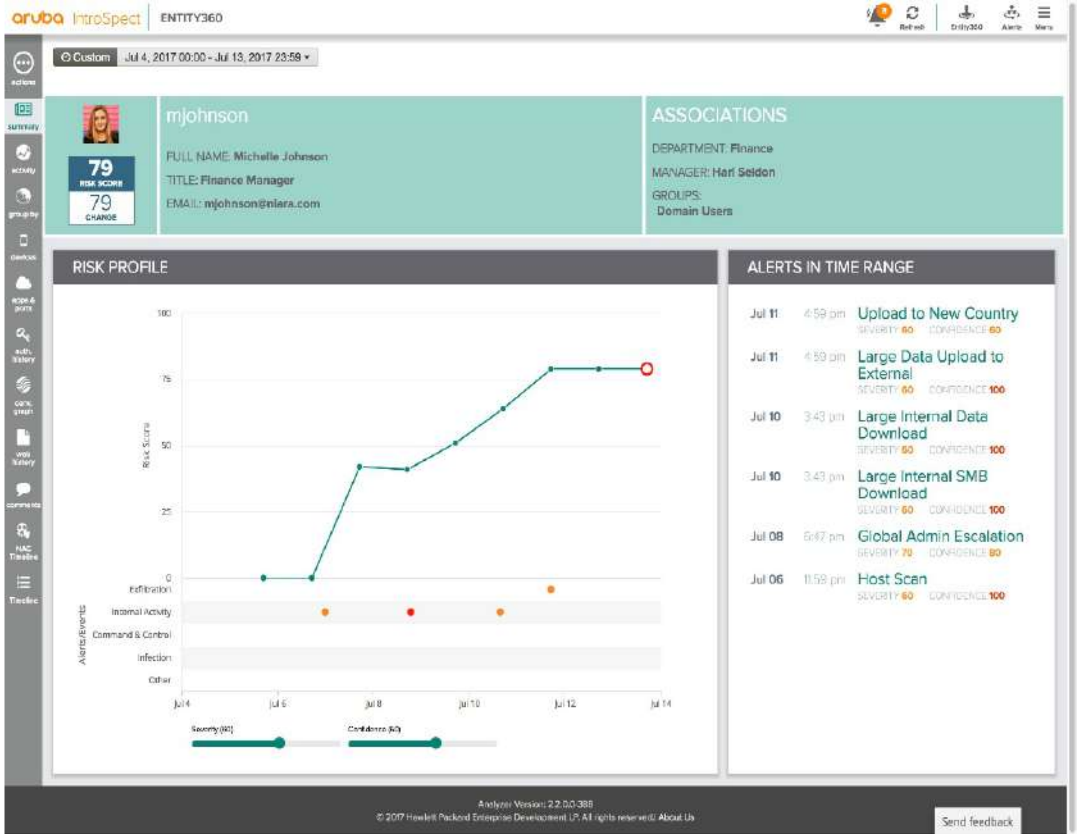
Continuous behavior monitoring

AI-powered attack detection

Threat prioritization

Rapid incident investigation

Multi-vendor integrations



Jul 4, 2017 00:00 - Jul 13, 2017 23:59

mjohnson

FULL NAME: Michelle Johnson

TITLE: Finance Manager

EMAIL: mjohnson@niara.com

ASSOCIATIONS

DEPARTMENT: Finance

MANAGER: Hari Seldon

GROUPS:
Domain Users

ALERTS IN TIME RANGE

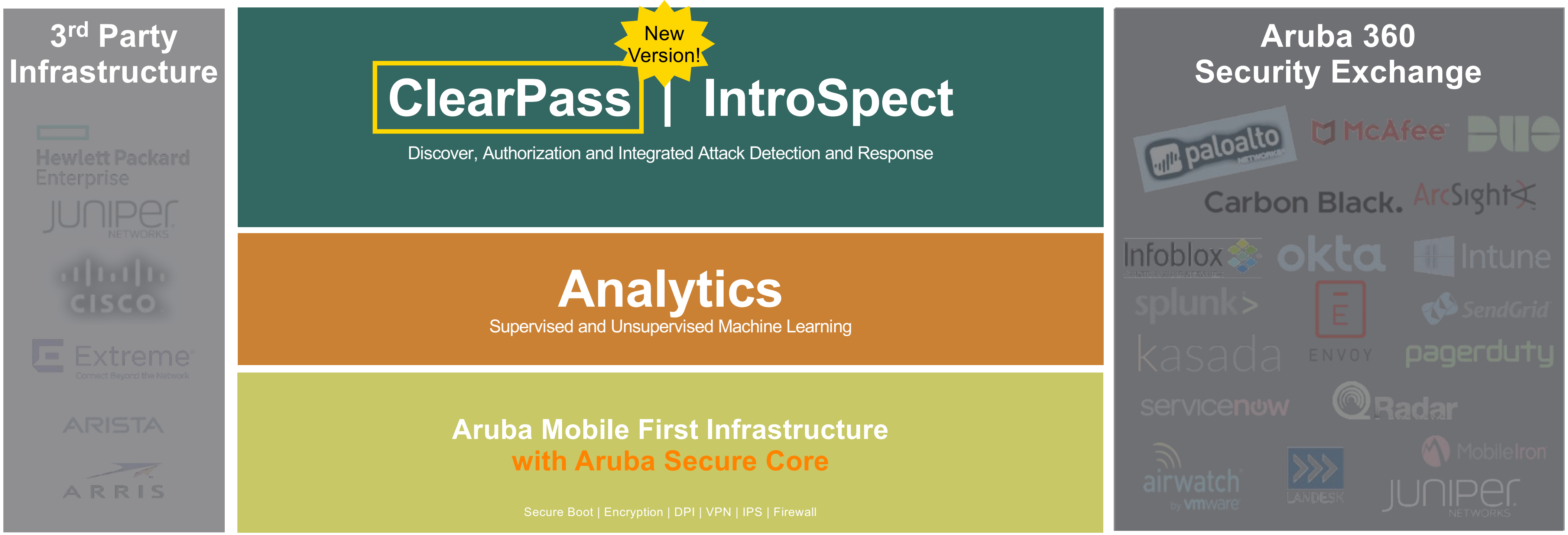
Jul 11	4:59 pm	Upload to New Country SEVERITY 60 CONFIDENCE 60
Jul 11	4:59 pm	Large Data Upload to External SEVERITY 60 CONFIDENCE 100
Jul 10	3:43 pm	Large Internal Data Download SEVERITY 60 CONFIDENCE 100
Jul 10	3:43 pm	Large Internal SMB Download SEVERITY 60 CONFIDENCE 100
Jul 08	6:47 pm	Global Admin Escalation SEVERITY 70 CONFIDENCE 80
Jul 06	11:59 pm	Host Scan SEVERITY 60 CONFIDENCE 100

Analyzer Version: 2.2.0.0-388
© 2017 Hewlett Packard Enterprise Development LP. All rights reserved. About Us

aruba
a Hewlett Packard
Enterprise company

INTRODUCING THE ARUBA 360 SECURE FABRIC

Open, Analytics-driven Security for the Mobile, Cloud, and IoT Era



3rd Party Infrastructure

New Version!

ClearPass | IntroSpect

Discover, Authorization and Integrated Attack Detection and Response

Analytics

Supervised and Unsupervised Machine Learning

Aruba Mobile First Infrastructure with Aruba Secure Core

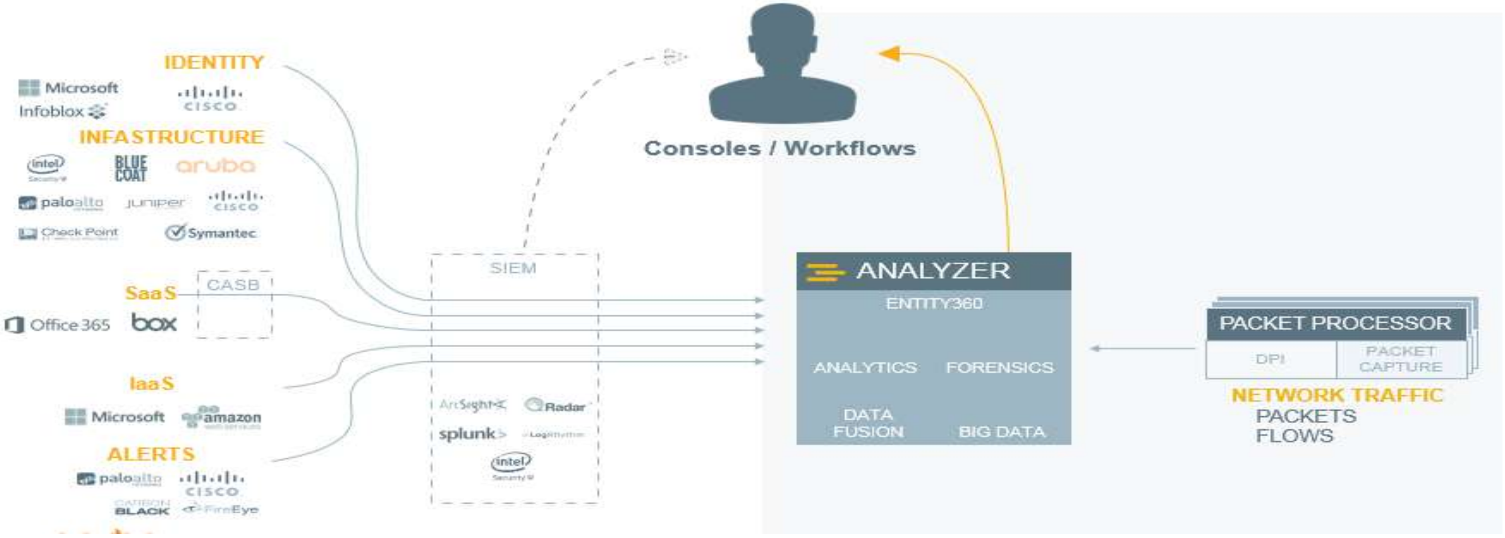
Secure Boot | Encryption | DPI | VPN | IPS | Firewall

Aruba 360 Security Exchange

a Hewlett Packard Enterprise company

360° active cyber protection and secure access
from the edge, to the core, to the cloud—for any network

SOLUTION – INTEGRATED WITH SECURITY ECOSYSTEM



Point #1: consumes exhaust data

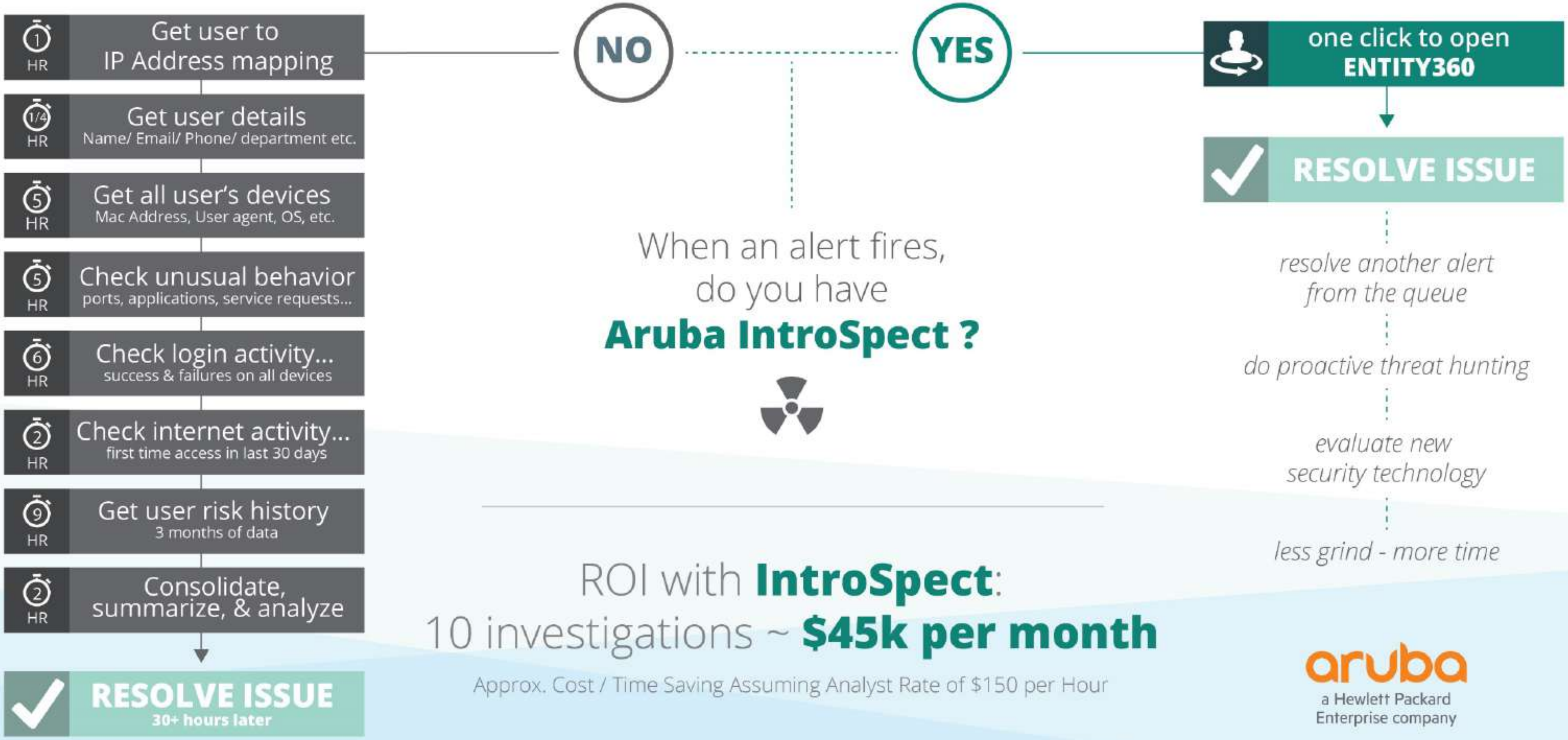
Point #2: SIEM/log management.

Point #3: can be deployed on site or in the cloud

aruba
a Hewlett Packard
Enterprise company

HOW TO INVESTIGATE AN ALERT

brought to you by Aruba, a Hewlett Packard Enterprise company



When an alert fires,
do you have
Aruba IntroSpect ?

NO

1 HR — Get user to IP Address mapping

1/4 HR — Get user details
Name/ Email/ Phone/ department etc.

5 HR — Get all user's devices
Mac Address, User agent, OS, etc.

5 HR — Check unusual behavior
ports, applications, service requests...

6 HR — Check login activity...
success & failures on all devices

2 HR — Check internet activity...
first time access in last 30 days

9 HR — Get user risk history
3 months of data

2 HR — Consolidate, summarize, & analyze

✓ **RESOLVE ISSUE**
30+ hours later

YES

one click to open
ENTITY360

✓ **RESOLVE ISSUE**

resolve another alert from the queue

do proactive threat hunting

evaluate new security technology

less grind - more time

ROI with **IntroSpect**:
10 investigations ~ **$45k per month**

Approx. Cost / Time Saving Assuming Analyst Rate of $150 per Hour

aruba
a Hewlett Packard Enterprise company

IntroSpect Summary

Diverse Data Sources

FOR

Analytics + Forensics

SUPPORTING

Attack Detection + Incident Investigation

ALL IN A

Self-Contained Solution + Open Platform

AVAILABLE

Streamlined for Aruba Networks + Scaled for Enterprise UEBA

AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

Thank You