AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

IntroSpect
User and Entity Behavior Analytics (UEBA) & ClearPass

29/06/2018

#ArubaAirheads

AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

IntroSpect

#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

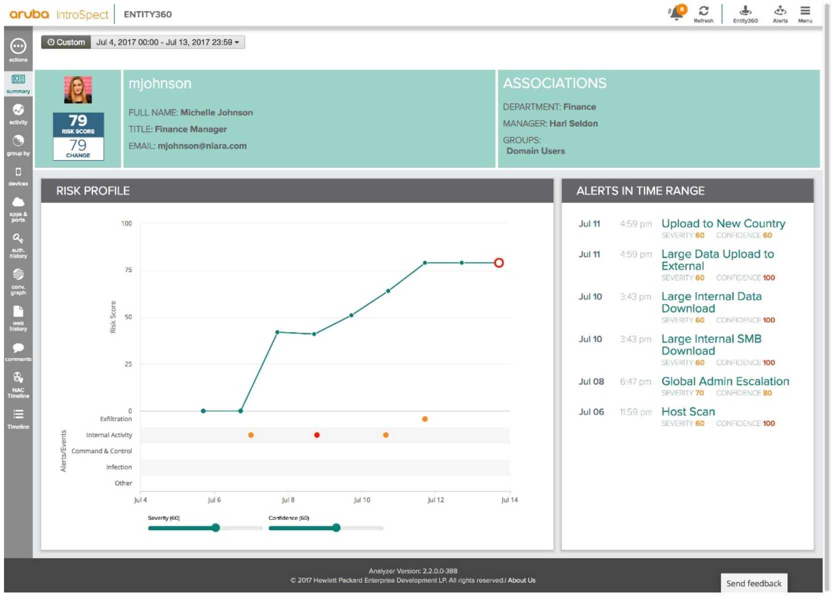
Continuous behavior monitoring

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

MACHINE LEARNING TO
SECURE THE ENTERPRISE FROM THE INSIDE

IntroSpect

Machine-learned user and entity
behavioral analytics for enterprise security

Visibility

Monitoring

Policy
Enforcement

CLEARPASS
POLICY MANAGER

New Attack Environment: No Walls, New Threats

ATTACKERS

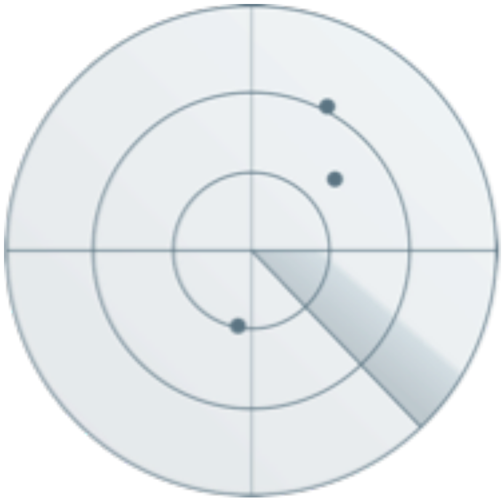
ARE QUICKLY INNOVATING & ADAPTING

BATTLEFIELD

WITH IOT AND CLOUD, SECURITY IS BORDERLESS

Current Security Defenses Falling Short

+



CURRENT PREVENTION & DETECTION NOT STOPPING TARGETED ATTACKS

MANAGEMENT SYSTEMS NOT KEEPING UP

IntroSpect Addresses Two Key Security Challenges

ATTACKS AND RISKY BEHAVIORS

on the inside

One of the main goals of external adversaries is to gain access to legitimate internal credentials to advance their assault.

EFFICIENCY AND EFFECTIVENESS

of the security team

80% of these breaches are more likely to take months and years to detect rather than weeks or less

Source: Verizon 2017 Data Breach Investigations Report

Automated Detection of Threats Inside the Organization

ATTACKS AND RISKY BEHAVIORS

on the inside

Comprehensive Visibility

Machine learning-Based Attack Detection

Enterprise Scale

Attacks on the Inside Utilizing Legitimate Credentials

COMPROMISED

40 million credit cards were stolen from Target's severs

STOLEN CREDENTIALS

MALICIOUS

Edward Snowden stole more than 1.7 million classified documents

INTENDED TO LEAK INFORMATION

NEGLIGENT

DDoS attack from 10M+ hacked home devices took down major websites

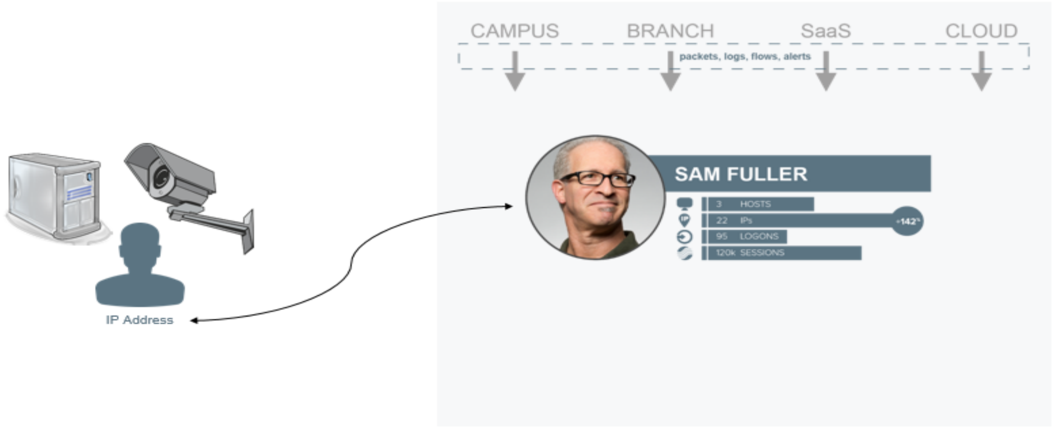
ALL USED THE SAME PASSWORD

IntroSpect

- **User and Entity**: This refers to the product's ability to track the behavior and risk score of anything with an IP address, including Users, Systems and Devices.
- **Behavior Analytics:** Because the most potent and damaging attacks are designed to use legitimate credentials from compromised users or devices, detection requires new types of artificial intelligence-based analytics that look for small changes in behavior that are often indicative of attacks that have moved inside the network

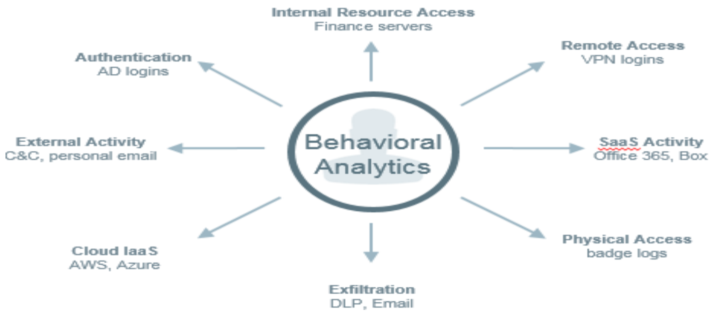
IntroSpect

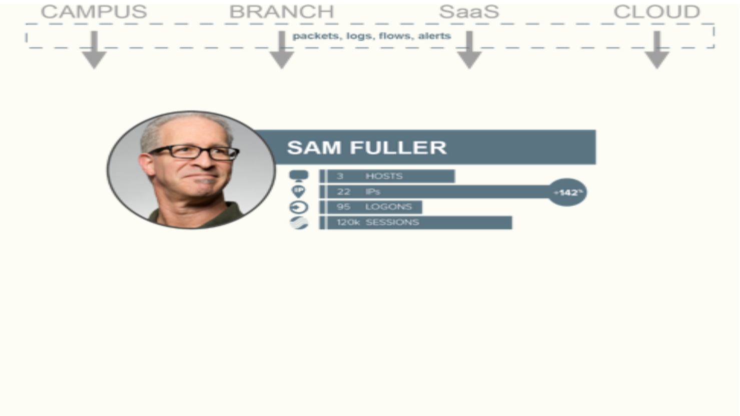
The Start: User/Entity View of Events



- IntroSpect aggregates all the data from the IT ecosystem
- puts it in the context of an entity

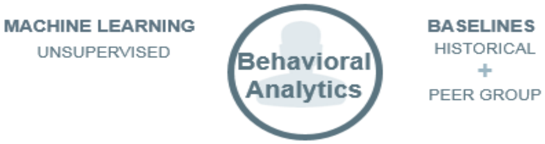
Behavior – Many Different Dimensions

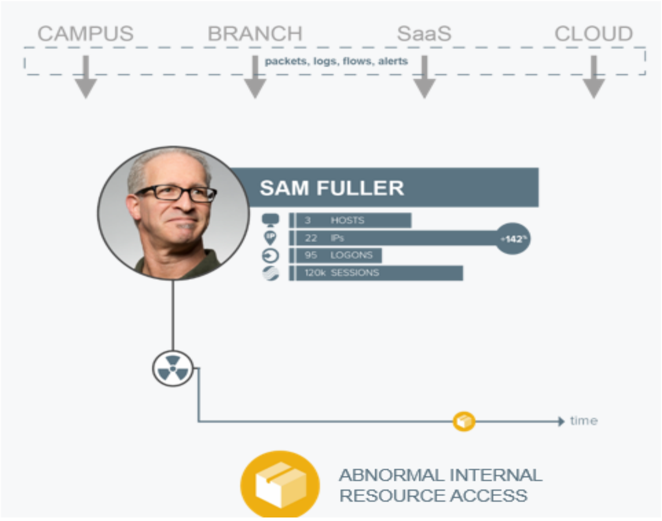




- IntroSpect can aggregate and analyze everything from network packets to general IT logs to third party alerts, our machine learning models have a complete view of user or device behavior
- build **behavioral “baselines”** for all entities

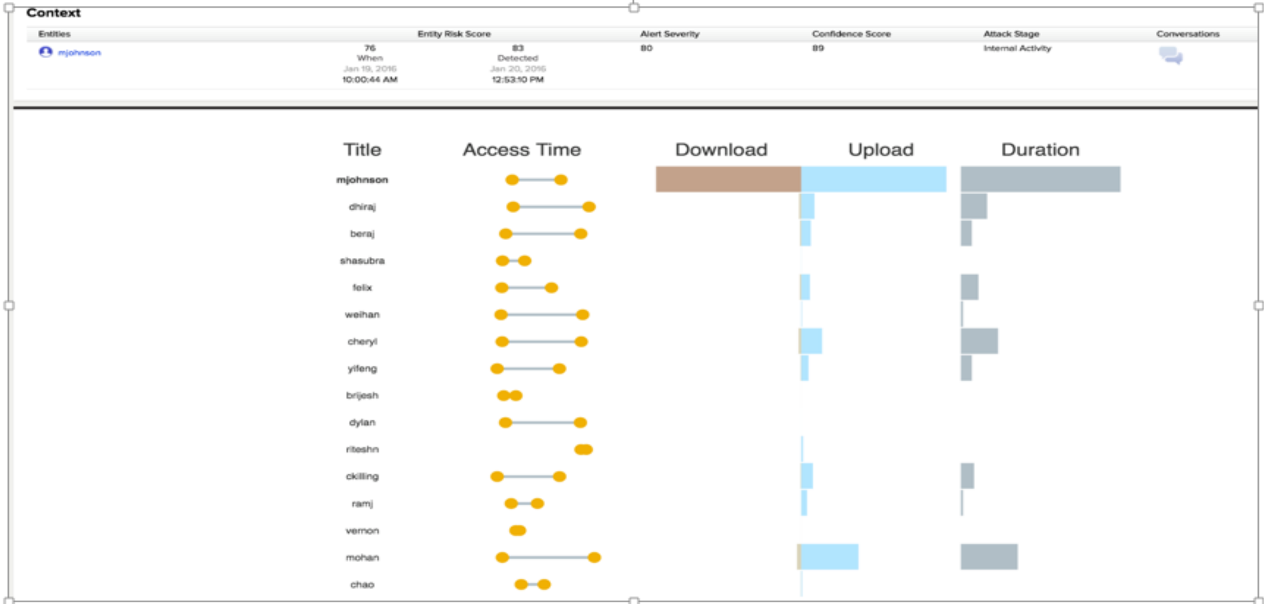
Basics of Behavioral Analytics





behavioral anomaly detection is known as **Unsupervised Machine Learning**

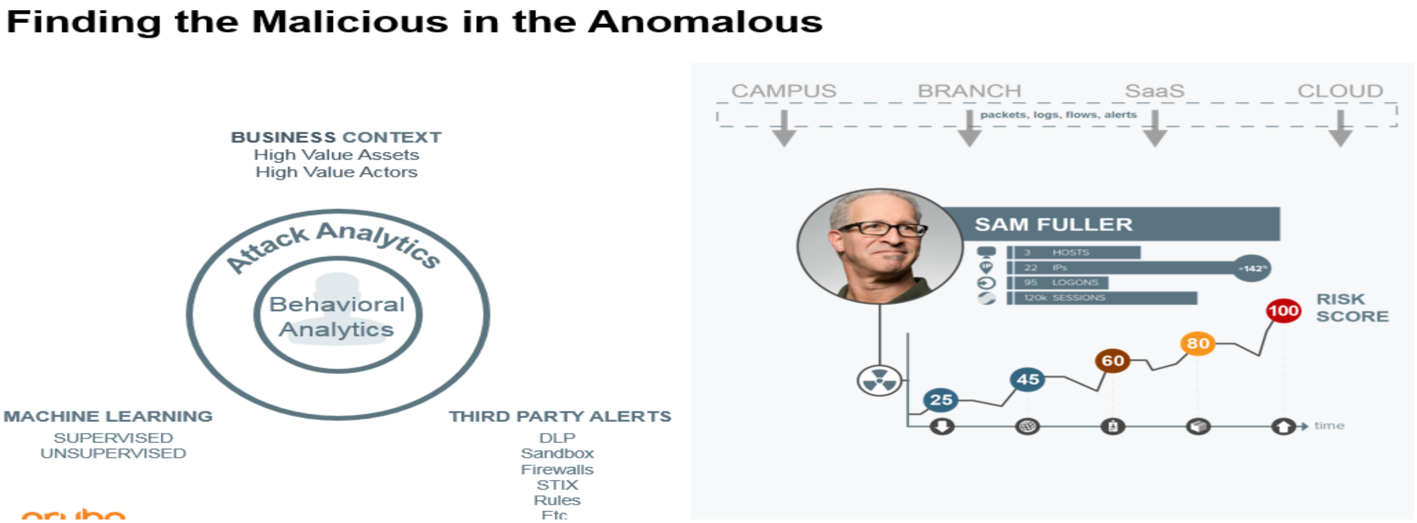
Peer Baseline Anomaly



Context

Entities	Entity Risk Score		Alert Severity	Confidence Score	Attack Stage	Conversations
mjohnson	76 When Jan 19, 2016 10:00:44 AM	83 Detected Jan 20, 2016 12:53:10 PM	80	89	Internal Activity	

No doubt about it. That’s 100% anomalous behavior



Finding the Malicious in the Anomalous

BUSINESS CONTEXT
High Value Assets
High Value Actors

Attack Analytics

Behavioral Analytics

MACHINE LEARNING
SUPERVISED
UNSUPERVISED

THIRD PARTY ALERTS
DLP
Sandbox
Firewalls
STIX
Rules
Etc

How do you know if the behavior is malicious?

Supervised Machine Learning

Force Multiplier for Security Analysts

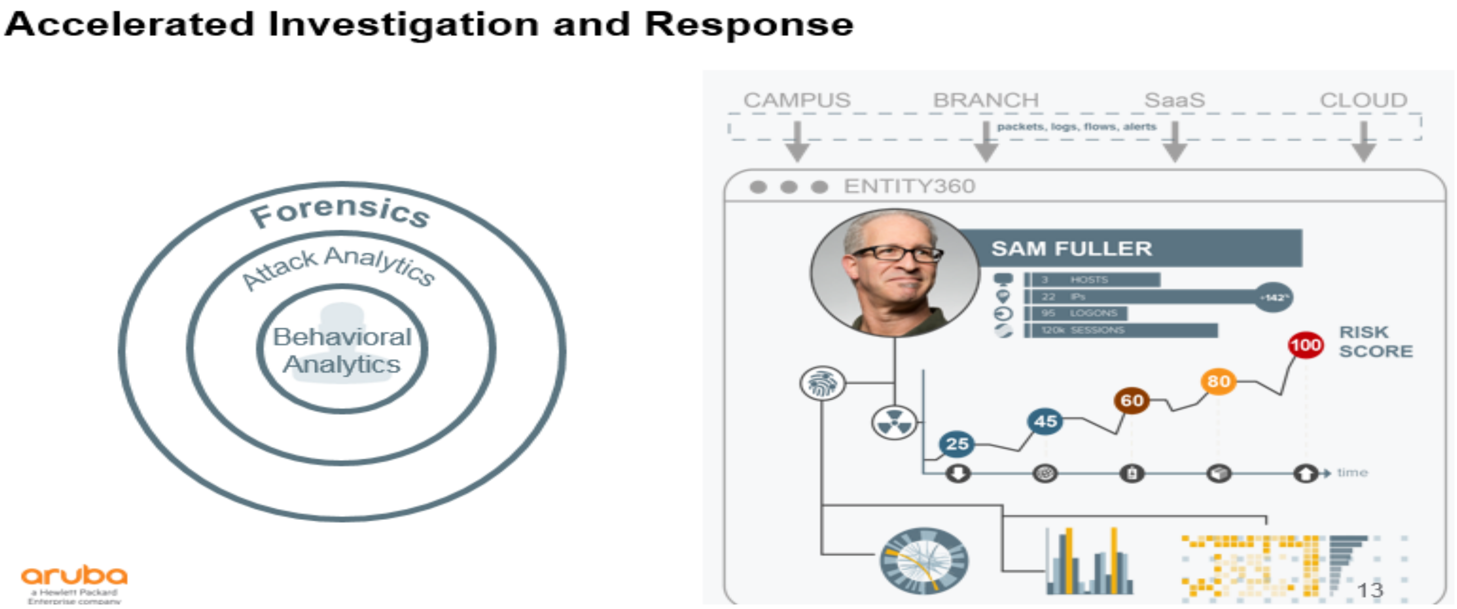
BREAKTHROUGH ROI
for Incident Investigation
and Threat Hunting

Consolidated Data Access

Rapid Decision-Making and Action

Seamless ClearPass Integration

IntroSpect’s second key value proposition is using analytics as a “force multiplier “



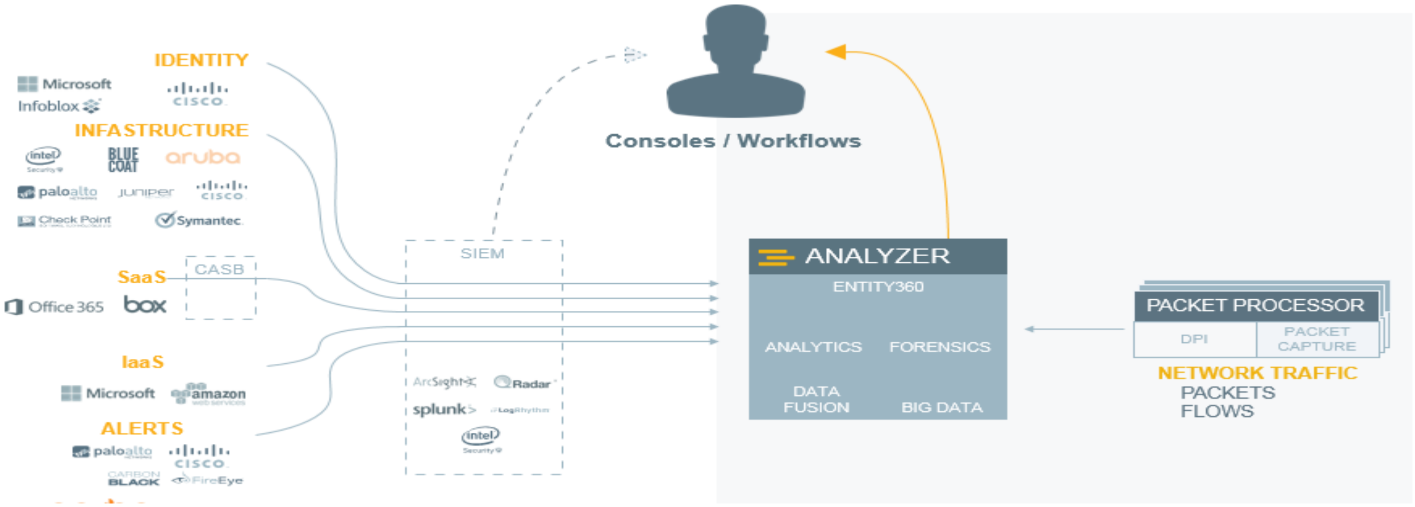
Accelerated Investigation and Response

The heart of this value proposition is **IntroSpect's Entity360** profile

DEMO

AIRHEADS meetup

SOLUTION – INTEGRATED WITH SECURITY ECOSYSTEM



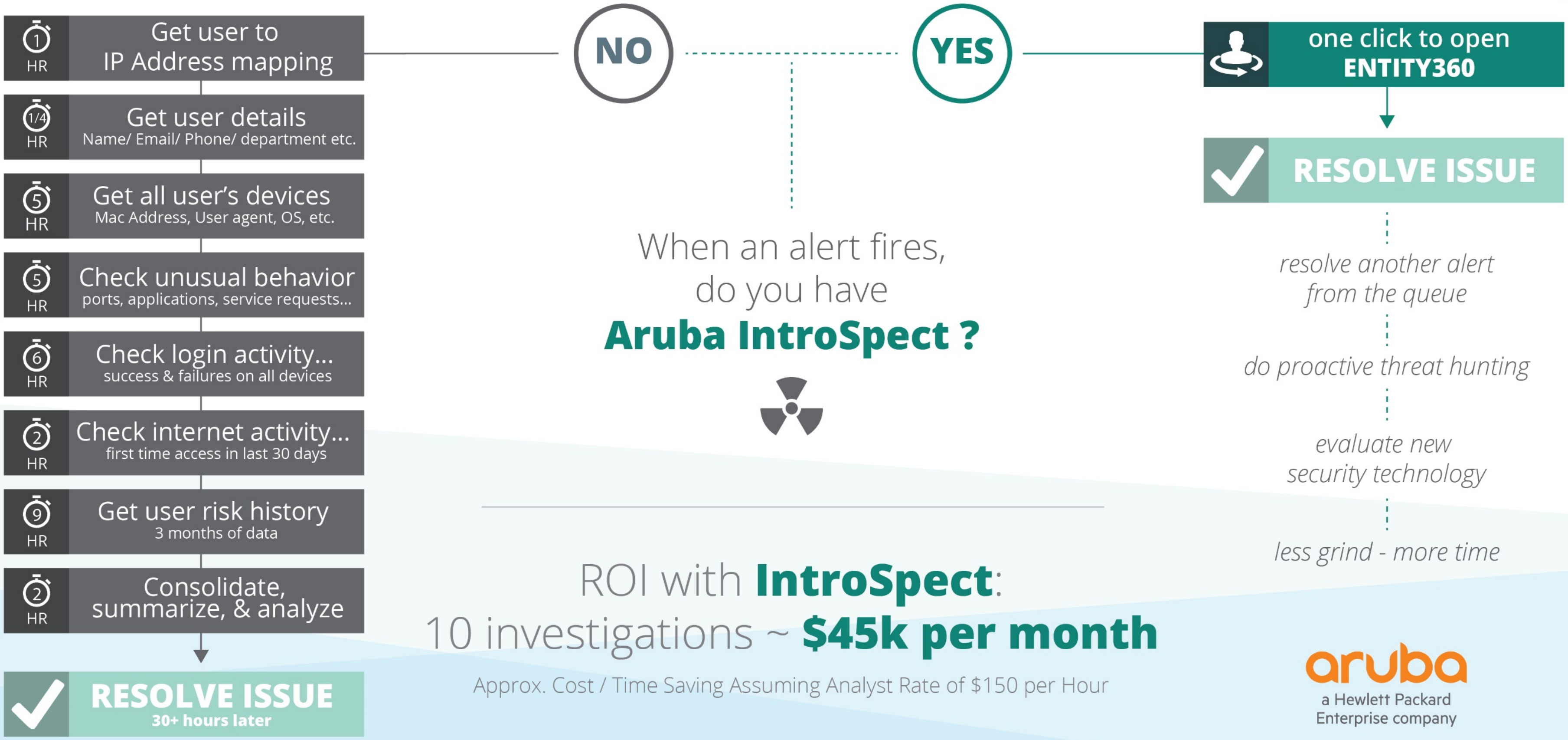
Point #1: consumes exhaust data

Point #2: SIEM/log management.

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

HOW TO INVESTIGATE AN ALERT

brought to you by Aruba, a Hewlett Packard Enterprise company



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

NO

YES

When an alert fires,
do you have
Aruba IntroSpect ?

one click to open
ENTITY360

RESOLVE ISSUE

*resolve another alert
from the queue*

do proactive threat hunting

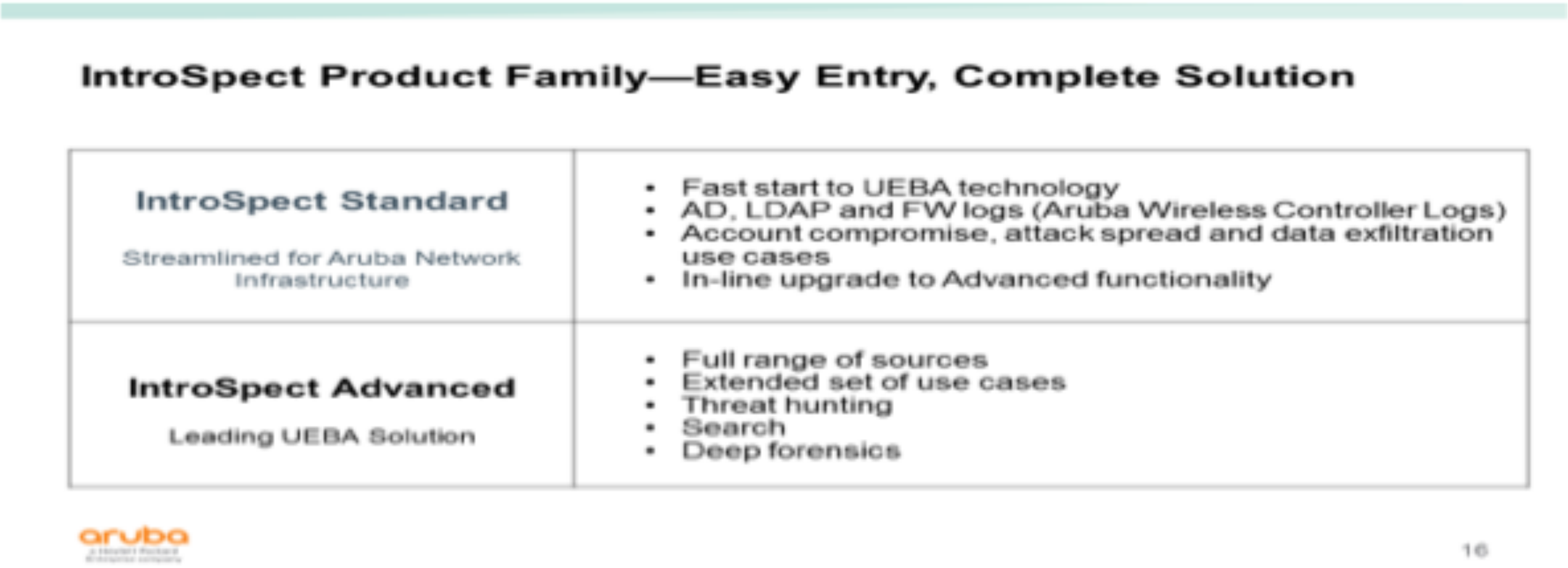
*evaluate new
security technology*

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 Product Family—Easy Entry, Complete Solution

IntroSpect Standard Streamlined for Aruba Network Infrastructure	• Fast start to UEBA technology • AD, LDAP and FW logs (Aruba Wireless Controller Logs) • Account compromise, attack spread and data exfiltration use cases • In-line upgrade to Advanced functionality
IntroSpect Advanced Leading UEBA Solution	• Full range of sources • Extended set of use cases • Threat hunting • Search • Deep forensics

Differentiation

Comprehensive visibility	• Packets, flows, logs • No blind spots
Most extensive attack analytics	• 100+ supervised and unsupervised machine learning models • Adaptive learning • Extensible models (new use cases, data sources) • Business context in risk score
Accelerated Investigations and Response	• Integrated forensics • Seamless ClearPass integration
Deployment ease	• Flexible: on-premise or cloud • Ingest data natively or from SIEM, log management, packet broker solutions
Quick Start, Enterprise Scale	• Standard Edition tuned for Aruba networks • Tens of data sources, hundreds of behavioral models across tens of thousands of users

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

ClearPass Integration

#ArubaAirheads

Different Network Elements Must Work Together

Holistic approach for access control, regardless of location, time, device, transport

Real-time sharing of context provides visibility for accurate policy enforcement

Tightly integrated workflows between security protection tools for efficiency and speed

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

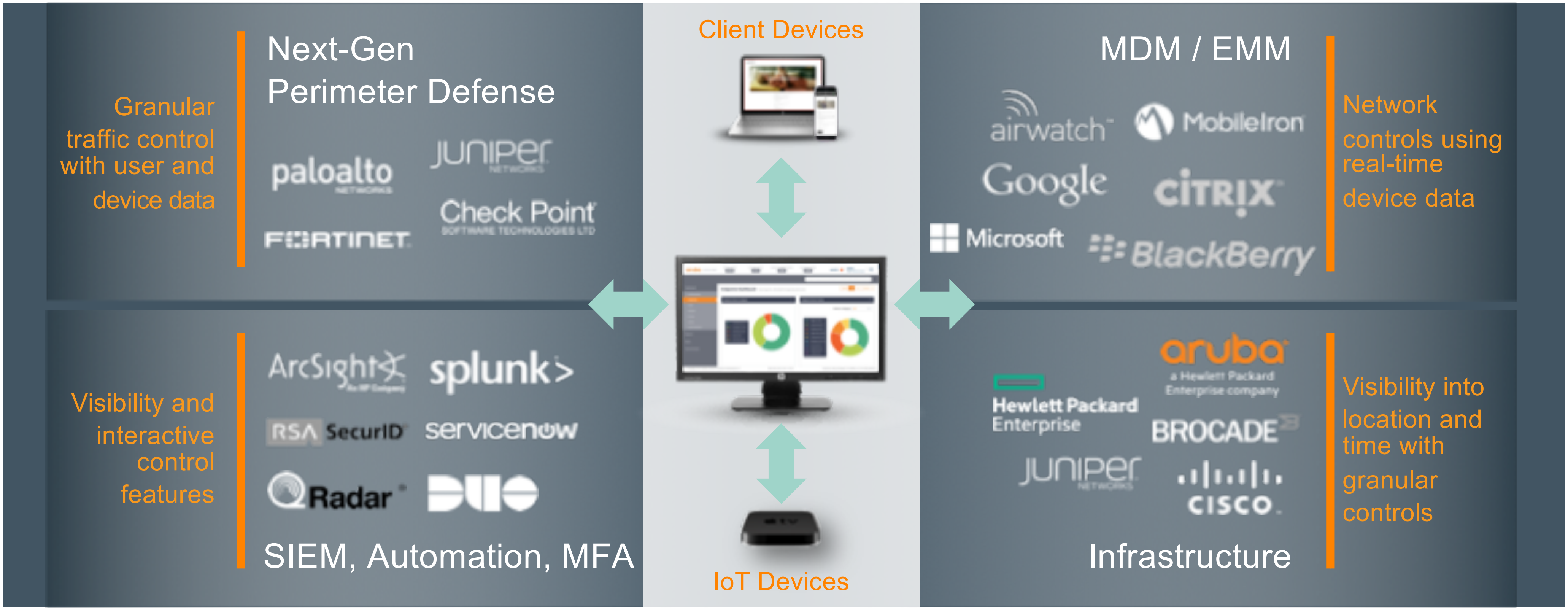
- Reduce risk and workload through Automation
- All devices are Authenticated or Authorized – NO UKNOWN DEVICES

RESPONSE

- Adaptive response brokering best of breed security solutions

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

ClearPass Exchange Continues to Grow



Next-Gen Perimeter Defense

Granular traffic control with user and device data

Client Devices

MDM / EMM

Network controls using real-time device data

SIEM, Automation, MFA

Visibility and interactive control features

IoT Devices

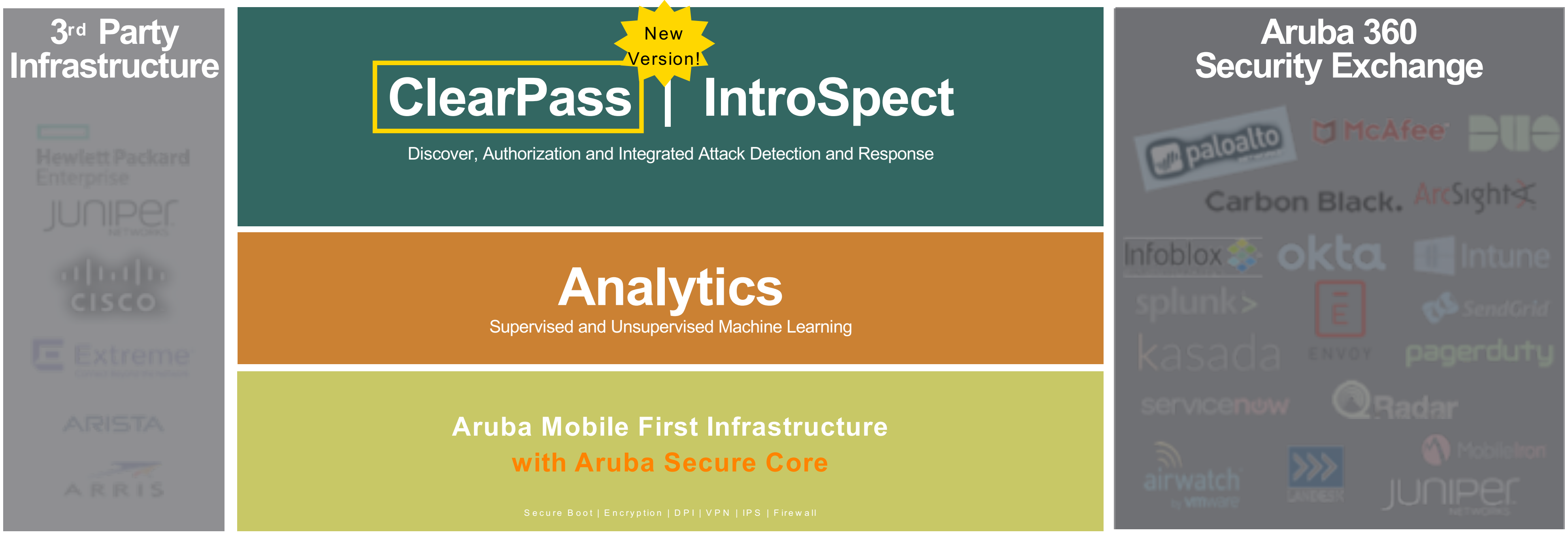
Infrastructure

Visibility into location and time with granular controls

aruba a Hewlett Packard Enterprise company
Hewlett Packard Enterprise
BROCADE
JUNIPER NETWORKS
cisco

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

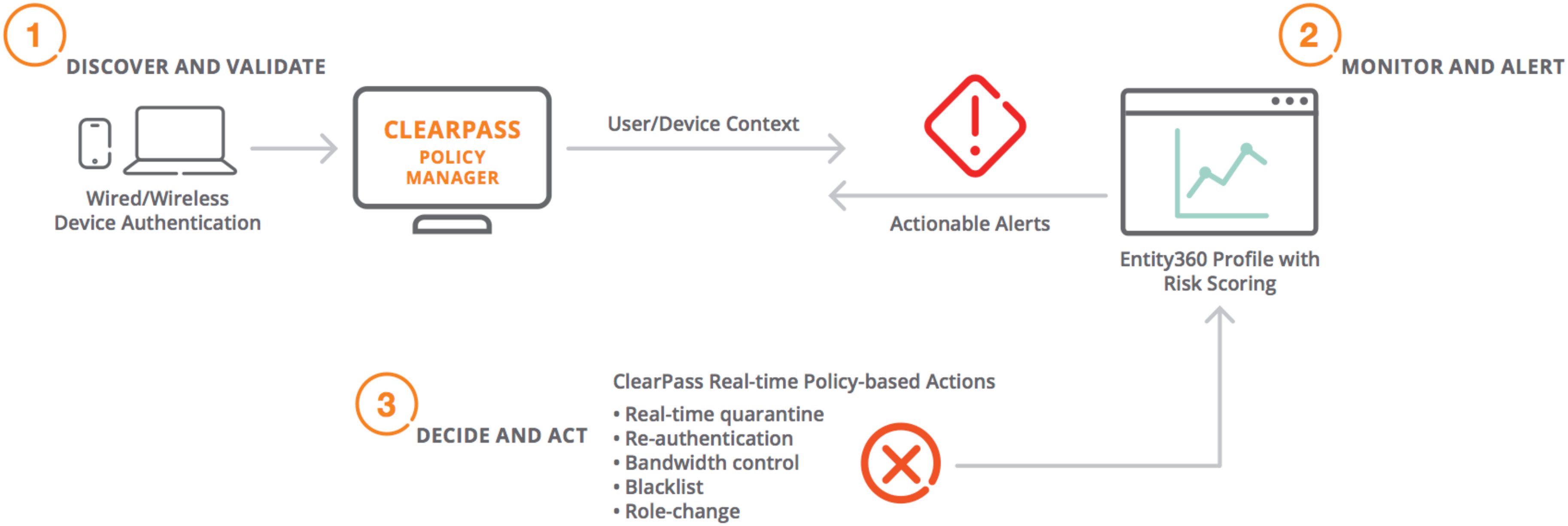
Secure Boot | Encryption | DPI | VPN | IPS | Firewall

Aruba 360 Security Exchange

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

360° PROTECTION

CLEARPASS + UEBA



1 DISCOVER AND VALIDATE

Wired/Wireless
Device Authentication

CLEARPASS
POLICY
MANAGER

User/Device Context

Actionable Alerts

2 MONITOR AND ALERT

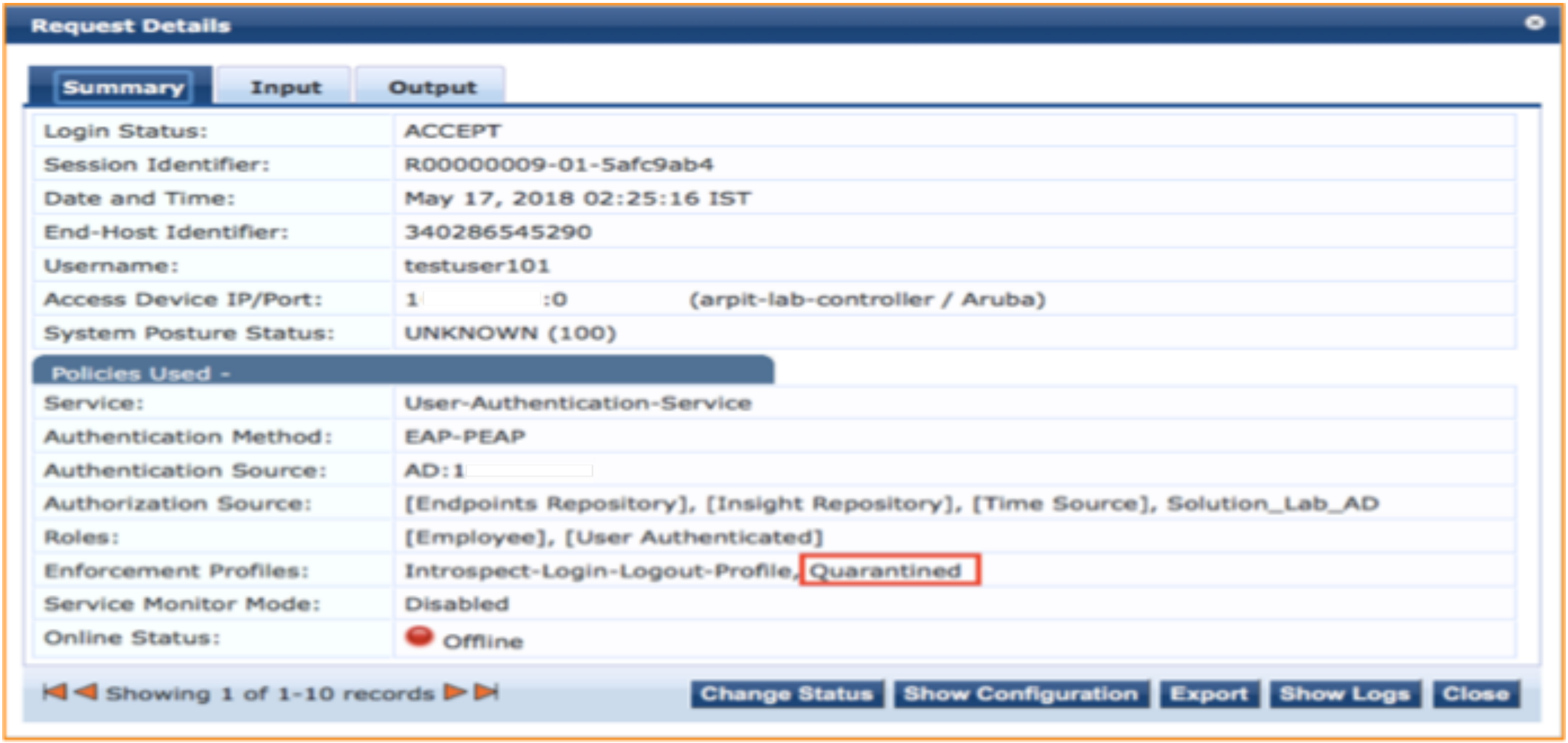
Entity360 Profile with
Risk Scoring

3 DECIDE AND ACT

ClearPass Real-time Policy-based Actions

- Real-time quarantine
- Re-authentication
- Bandwidth control
- Blacklist
- Role-change

Access Tracker result



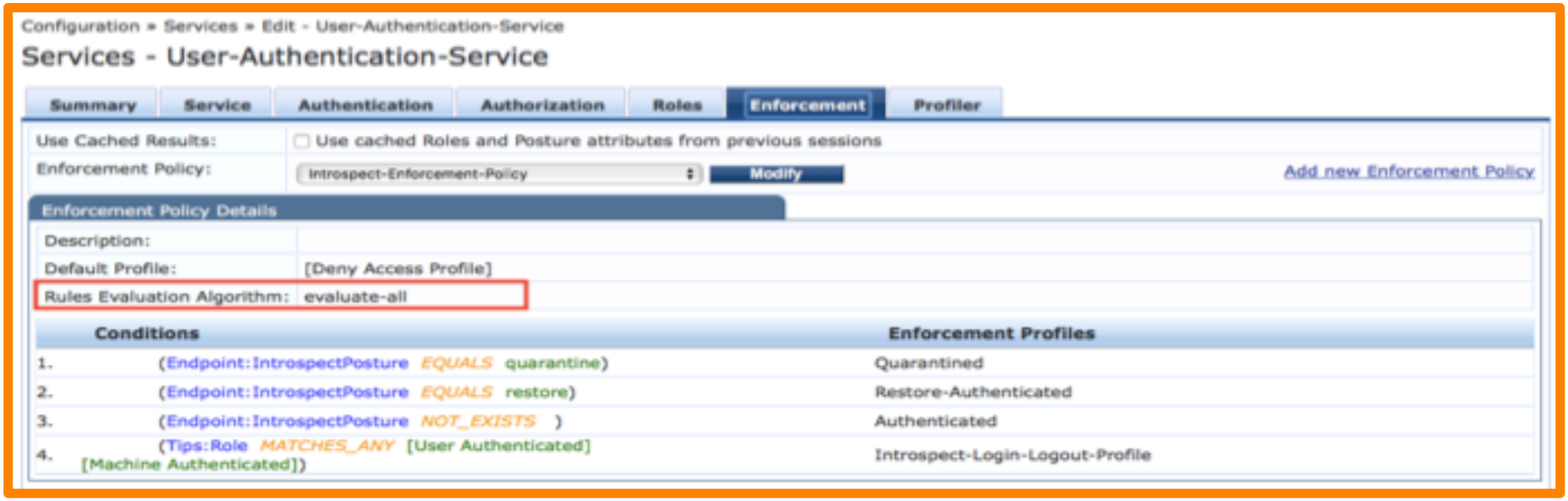
Login Status:	ACCEPT
Session Identifier:	R00000009-01-5afc9ab4
Date and Time:	May 17, 2018 02:25:16 IST
End-Host Identifier:	340286545290
Username:	testuser101
Access Device IP/Port:	1[redacted]:0 (arpit-lab-controller / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	User-Authentication-Service
Authentication Method:	EAP-PEAP
Authentication Source:	AD:1[redacted]
Authorization Source:	[Endpoints Repository], [Insight Repository], [Time Source], Solution_Lab_AD
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	Introspect-Login-Logout-Profile, Quarantined
Service Monitor Mode:	Disabled
Online Status:	● Offline

Showing 1 of 1-10 records

Enforcement Policy for RADIUS-based Authentication Service



Configuration » Services » Edit - User-Authentication-Service

Services - User-Authentication-Service

Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Introspect-Enforcement-Policy

Enforcement Policy Details

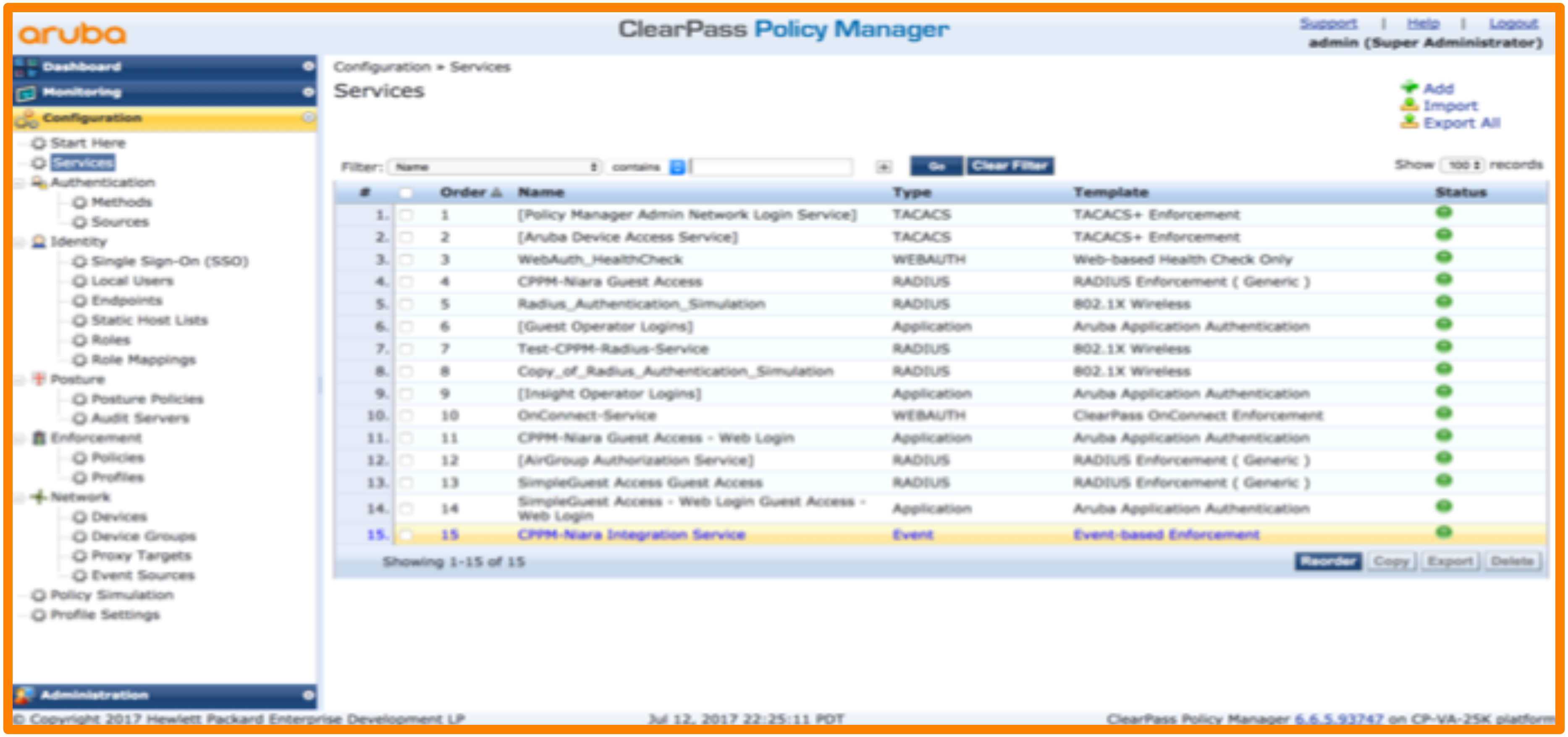
Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

	Conditions	Enforcement Profiles
1.	(Endpoint:IntrospectPosture *EQUALS* quarantine)	Quarantined
2.	(Endpoint:IntrospectPosture *EQUALS* restore)	Restore-Authenticated
3.	(Endpoint:IntrospectPosture *NOT_EXISTS*)	Authenticated
4.	(Tips:Role *MATCHES_ANY* [User Authenticated] [Machine Authenticated])	Introspect-Login-Logout-Profile

Create an Event-based Service



Configuration ▸ Services

Services

Filter: Name contains

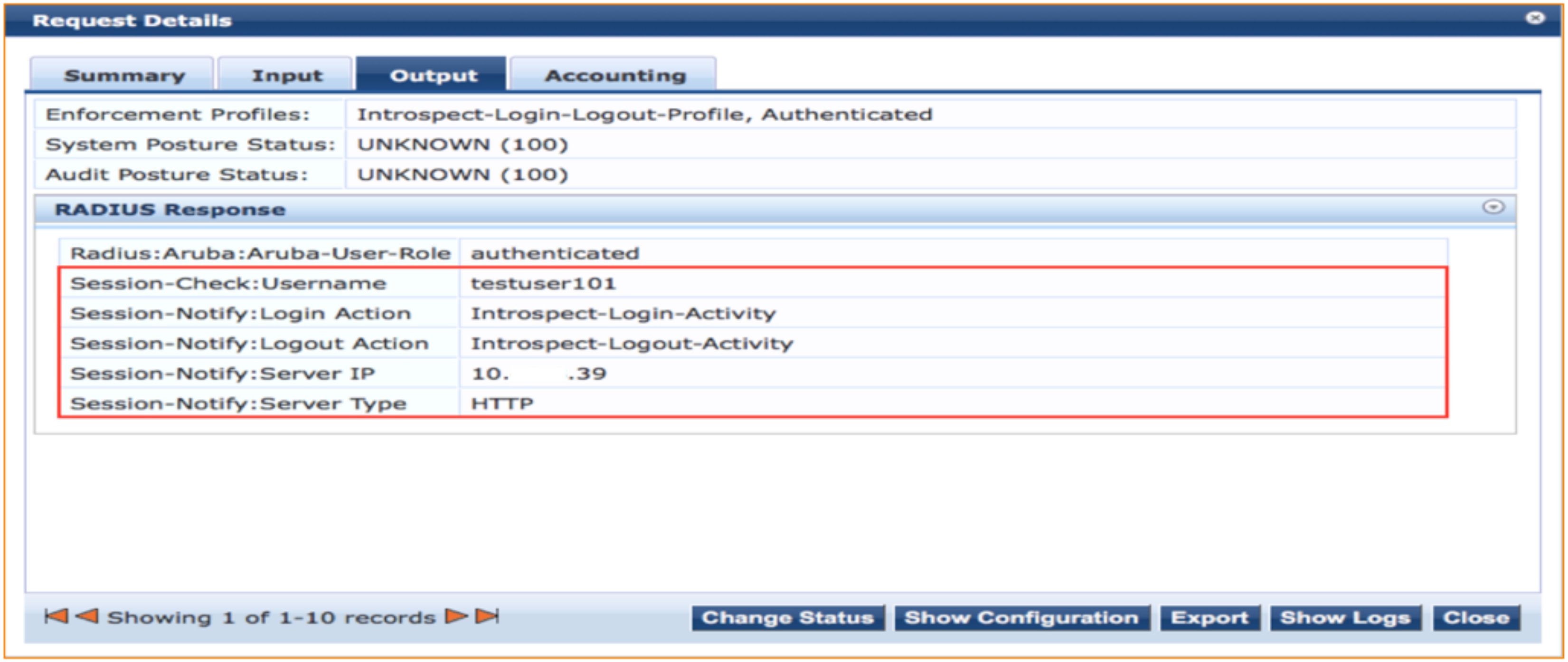
Show 100 records

#	□	Order ▲	Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	□	2	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
3.	□	3	WebAuth_HealthCheck	WEBAUTH	Web-based Health Check Only	●
4.	□	4	CPPM-Niara Guest Access	RADIUS	RADIUS Enforcement (Generic)	●
5.	□	5	Radius_Authentication_Simulation	RADIUS	802.1X Wireless	●
6.	□	6	[Guest Operator Logins]	Application	Aruba Application Authentication	●
7.	□	7	Test-CPPM-Radius-Service	RADIUS	802.1X Wireless	●
8.	□	8	Copy_of_Radius_Authentication_Simulation	RADIUS	802.1X Wireless	●
9.	□	9	[Insight Operator Logins]	Application	Aruba Application Authentication	●
10.	□	10	OnConnect-Service	WEBAUTH	ClearPass OnConnect Enforcement	●
11.	□	11	CPPM-Niara Guest Access - Web Login	Application	Aruba Application Authentication	●
12.	□	12	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
13.	□	13	SimpleGuest Access Guest Access	RADIUS	RADIUS Enforcement (Generic)	●
14.	□	14	SimpleGuest Access - Web Login Guest Access - Web Login	Application	Aruba Application Authentication	●
15.	□	15	CPPM-Niara Integration Service	Event	Event-based Enforcement	●

Showing 1-15 of 15

© Copyright 2017 Hewlett Packard Enterprise Development LP Jul 12, 2017 22:25:11 PDT ClearPass Policy Manager 6.6.5.93747 on CP-VA-25K platform

Access Tracker result



Enforcement Profiles:	Introspect-Login-Logout-Profile, Authenticated
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	authenticated
Session-Check:Username	testuser101
Session-Notify:Login Action	Introspect-Login-Activity
Session-Notify:Logout Action	Introspect-Logout-Activity
Session-Notify:Server IP	10. .39
Session-Notify:Server Type	HTTP

aruba
a Hewlett Packard
Enterprise company

AIRHEADS meetup

Thank You