

Network Security

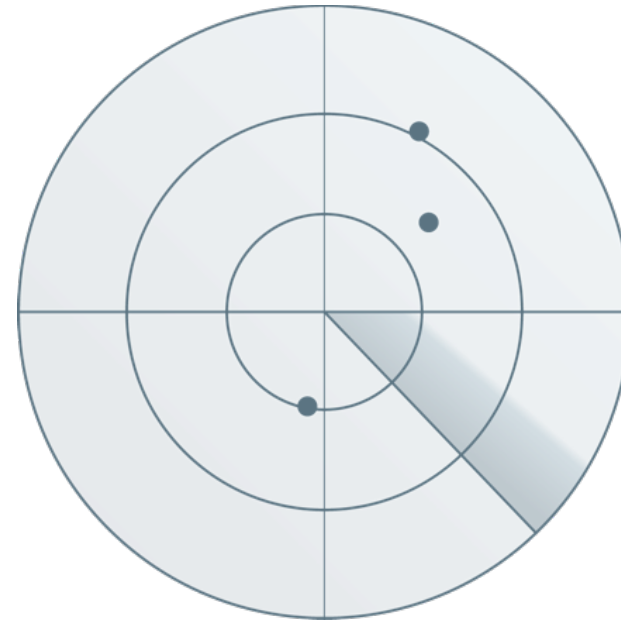
ClearPass, Device Insight, UEBA, Dynamic Segmentation

Herman Robers – Aruba EMEA Security CSE
19 September 2019

Agenda

- **Aruba 360 Secure Fabric**
 - Intro, overview, context
 - Architecture
 - Components
 - UEBA (IntroSpect)
- **Live demo's**
 - Colorless ports, Profiling
 - Dynamic Segmentation

Current Security Defenses Falling Short



**CURRENT PREVENTION & DETECTION
NOT STOPPING TARGETED ATTACKS**

**MANAGEMENT SYSTEMS
NOT KEEPING UP**

New Attack Environment: No Walls, New Threats



ATTACKERS

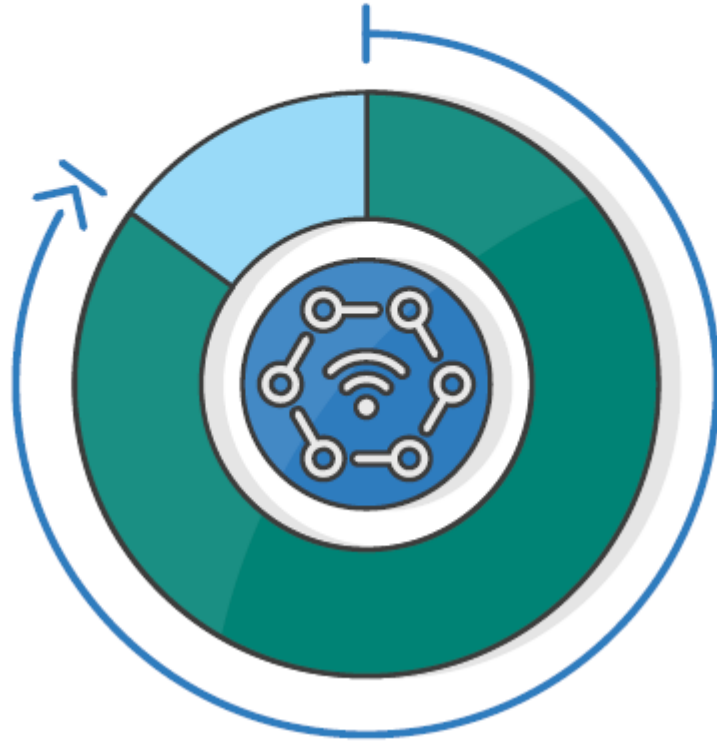
ARE QUICKLY INNOVATING &
ADAPTING



BATTLEFIELD

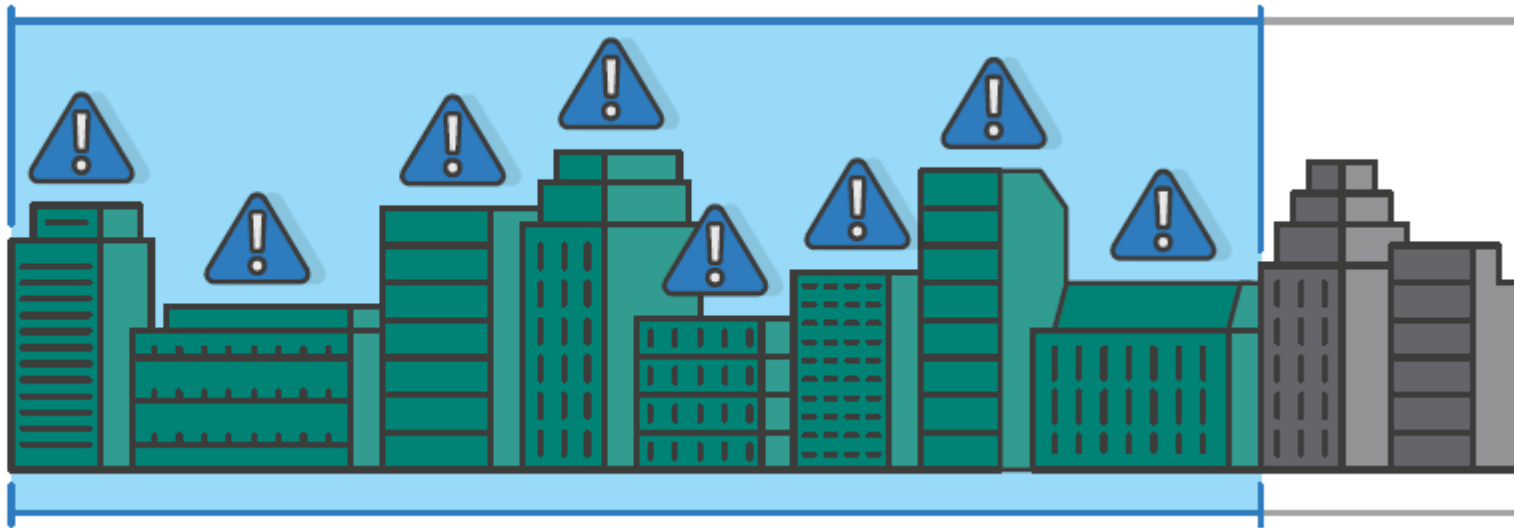
WITH IOT AND CLOUD, SECURITY
IS BORDERLESS

You already have IoT...



85% of businesses
will implement IoT in
their networks by 2019.²

Security breaches actually happen...



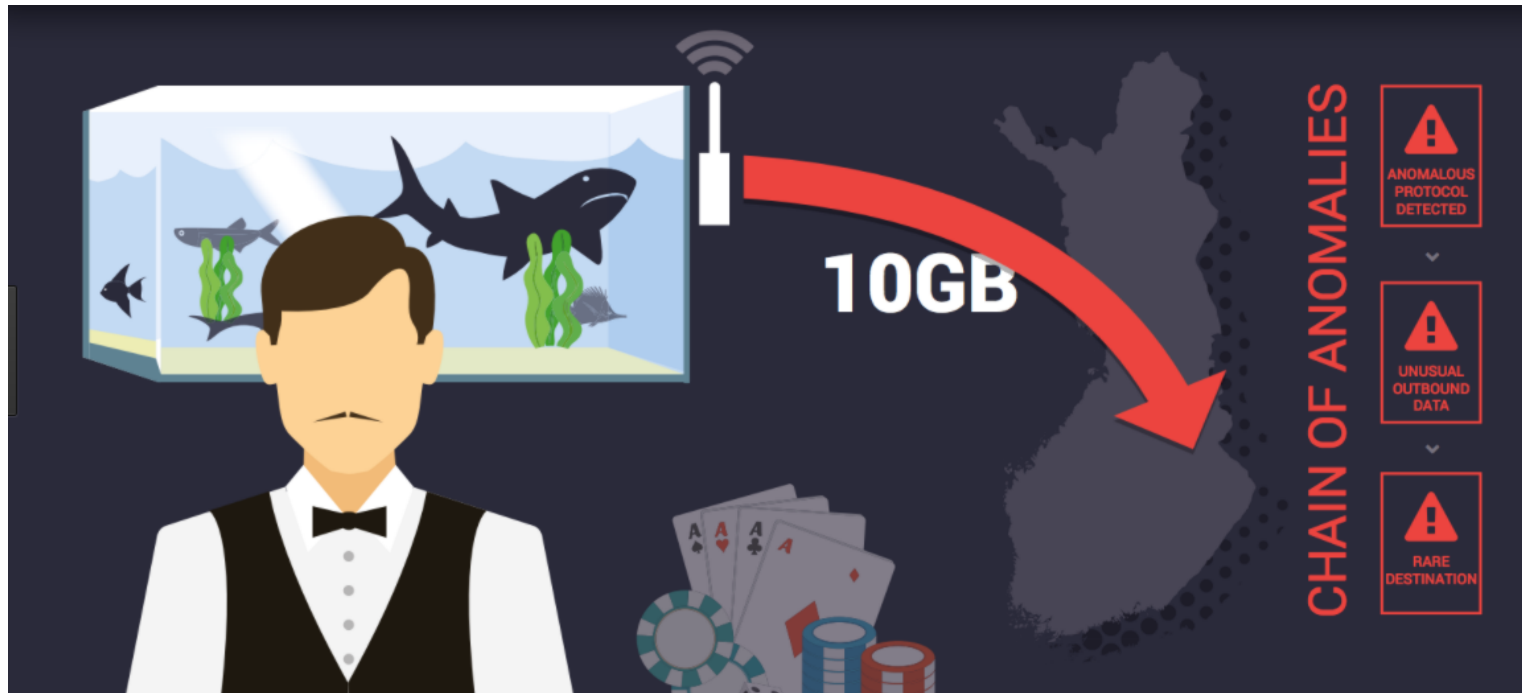
**8 out of 10
organizations**
have experienced
an IoT-related
security breach.³

For example....



**8 out of 10
organizations**
have experienced
an IoT-related
security breach.³

...another example...

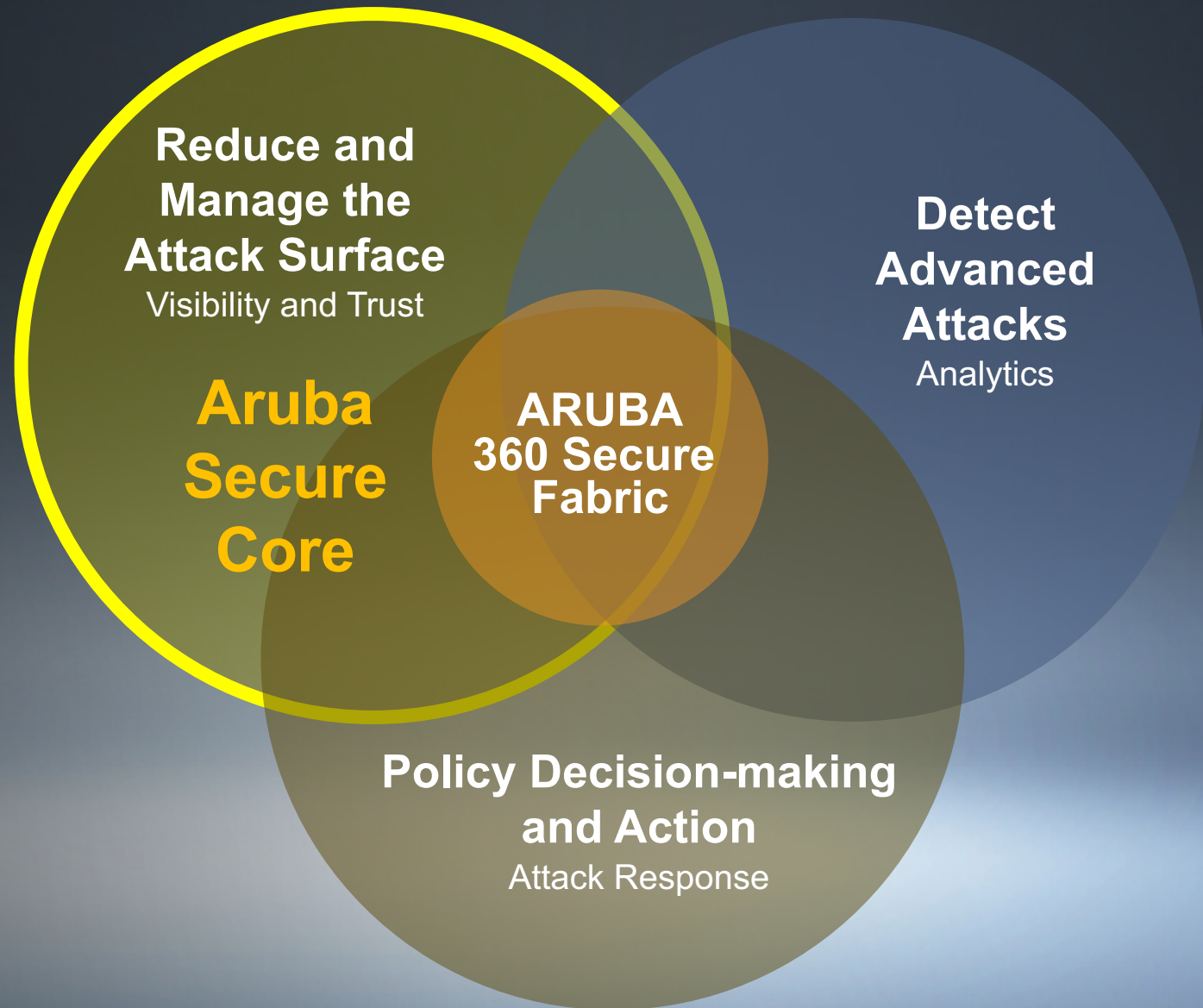


8 out of 10 organizations have experienced an IoT-related security breach.³

THE NEW SECURITY IMPERATIVE

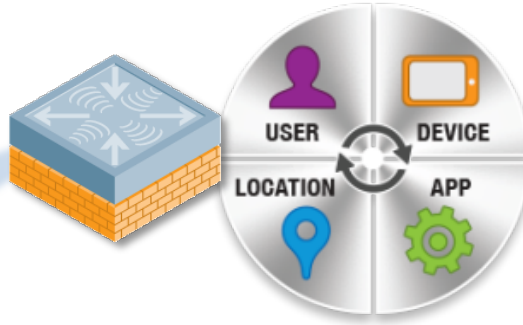


THE NEW SECURITY IMPERATIVE



Role based access networking

ROLE BASED ACCESS
NETWORKING



Role Based Access Firewall
(for WLAN, LAN & VPN)

Device context:
User, device,
location, time,
application

Role Based
access



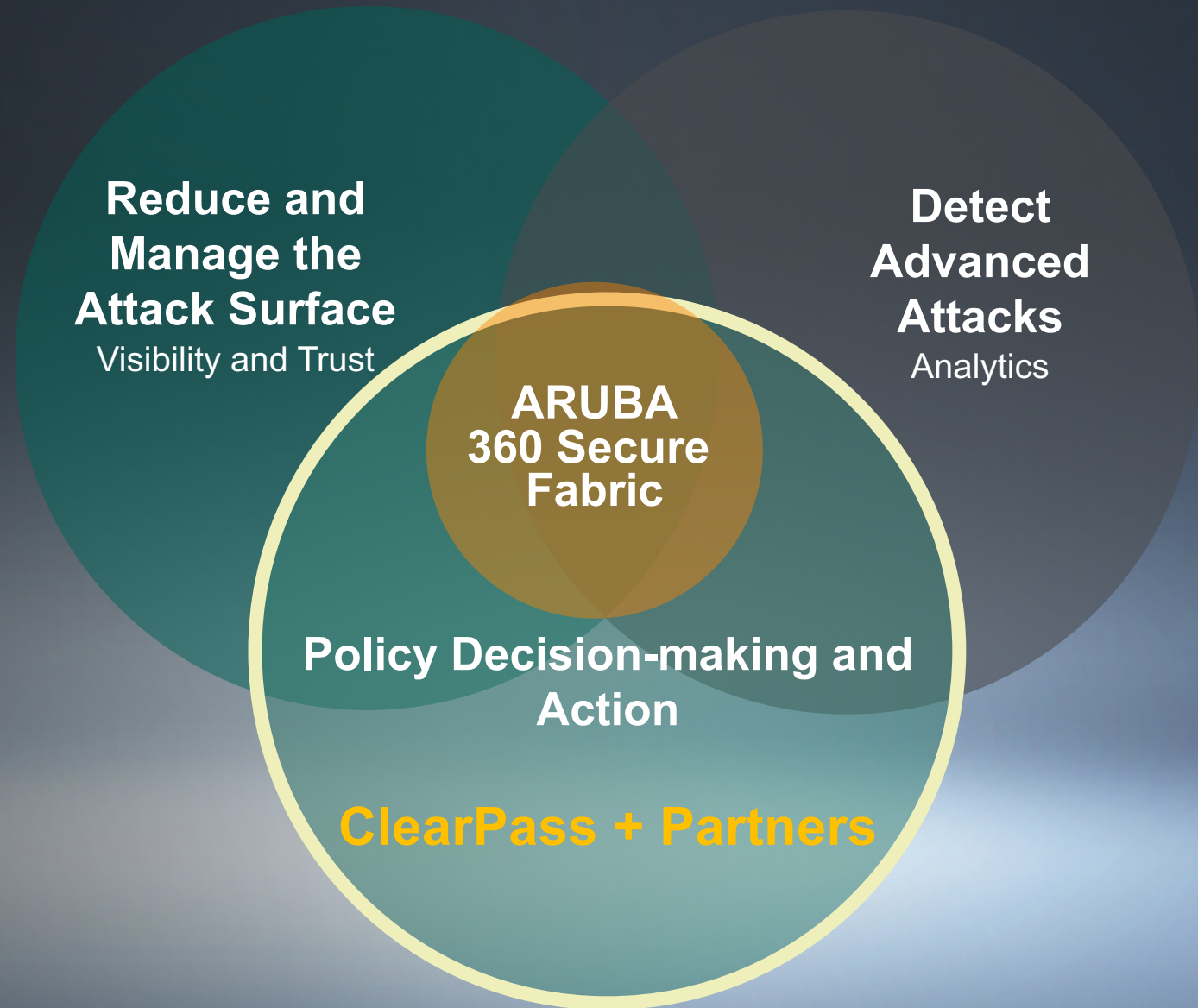
Visibility: AppRF™

Stateful
firewall
rules

QoS
flow-based

VLAN

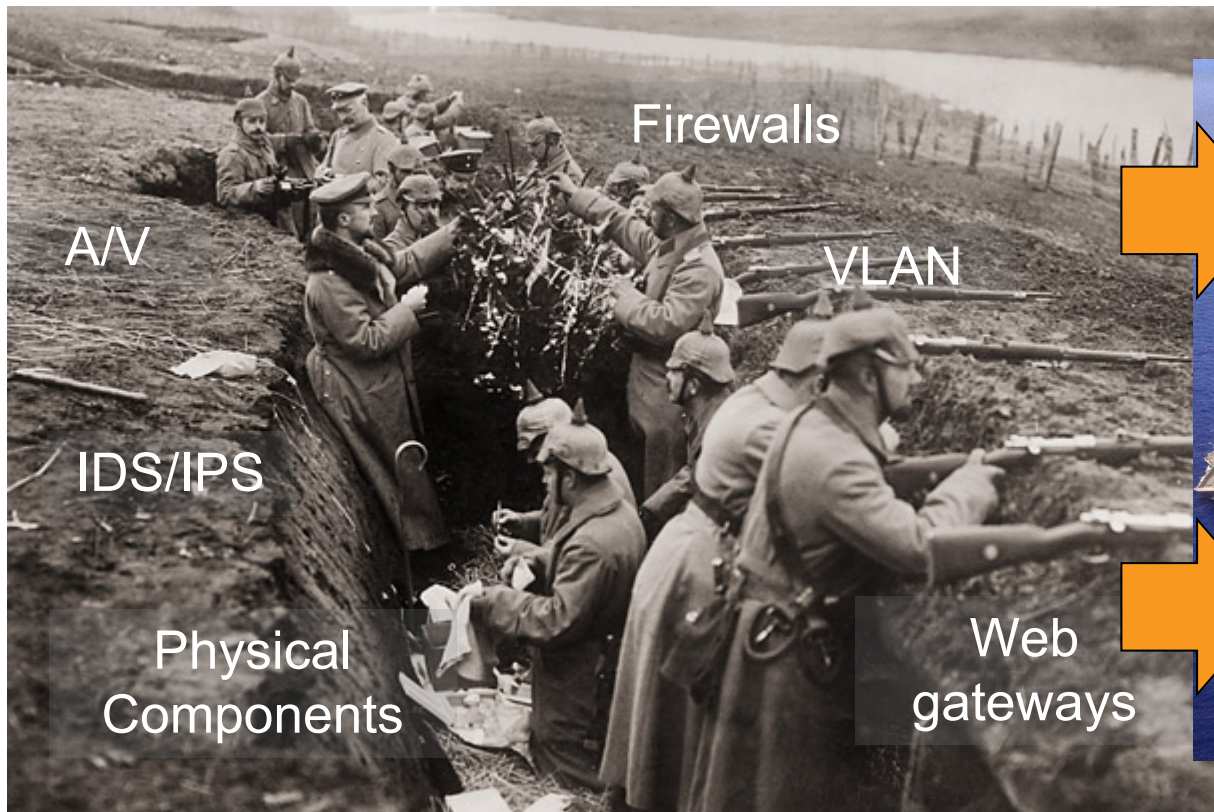
THE NEW SECURITY IMPERATIVE



Time for a New Mobility Defense Model

Static Perimeter Defense

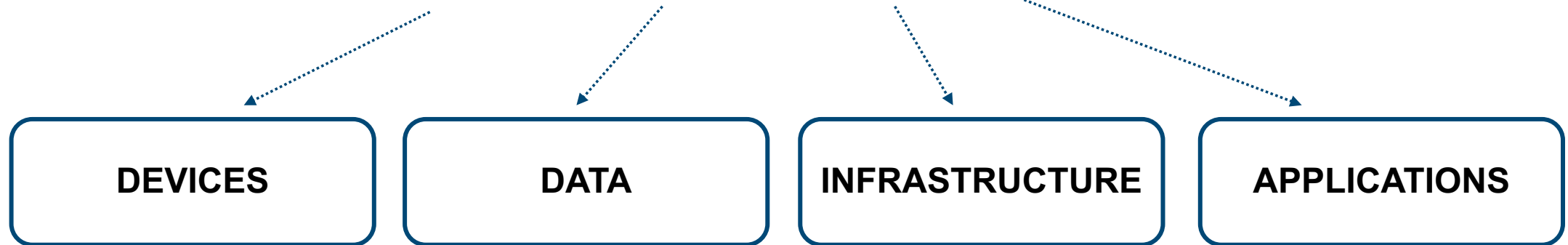
Adaptive Trust – Zero Tolerance



What does ClearPass do to help?



Defines **WHO** and **WHAT DEVICES** can connect to:



Identify – Enforce – Protect

A Secure Enterprise: Identify Everything

Contractor



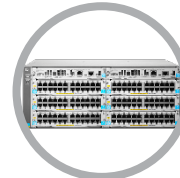
IoT



Headless



Employee BYOD



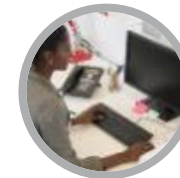
Infrastructure



Visitor

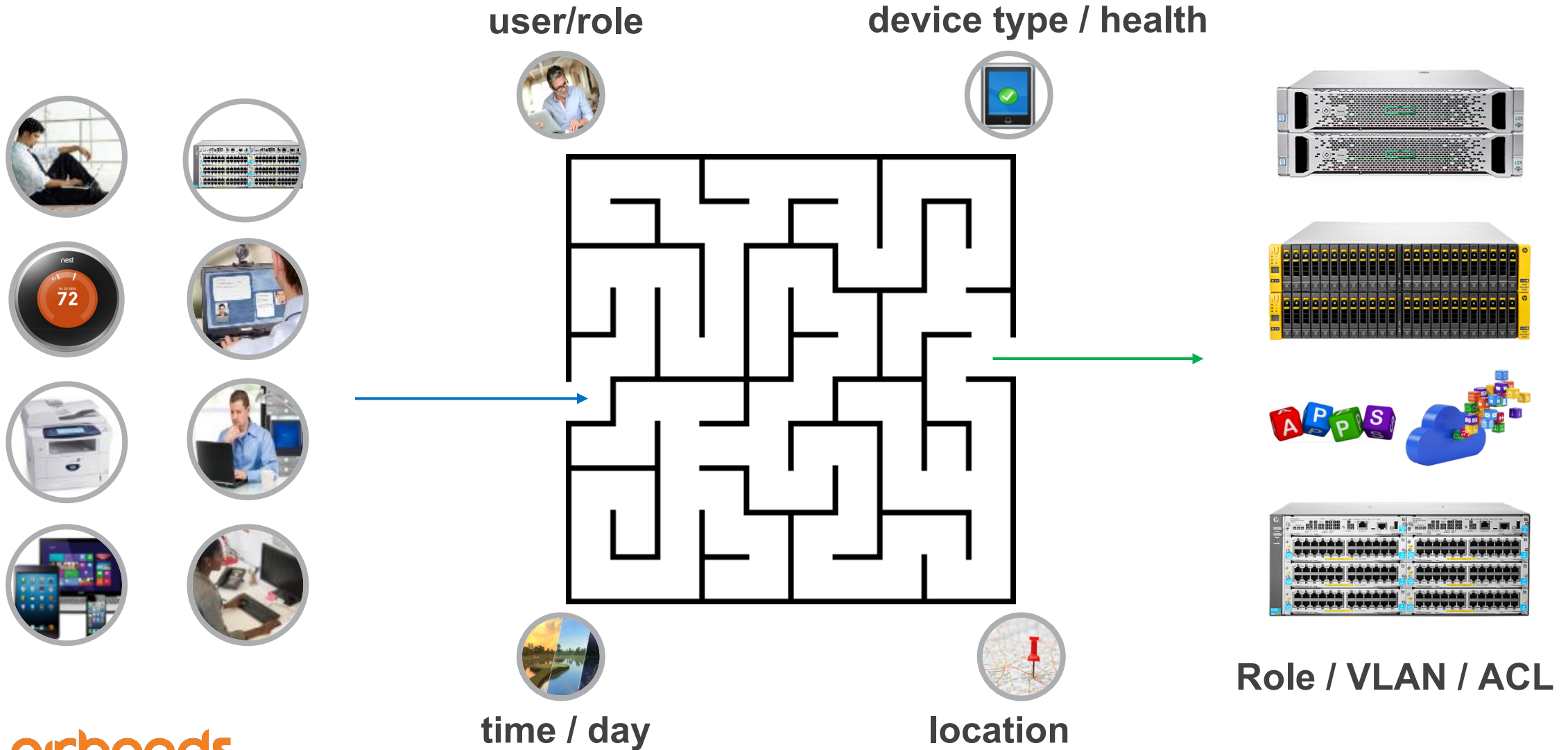


Administrator

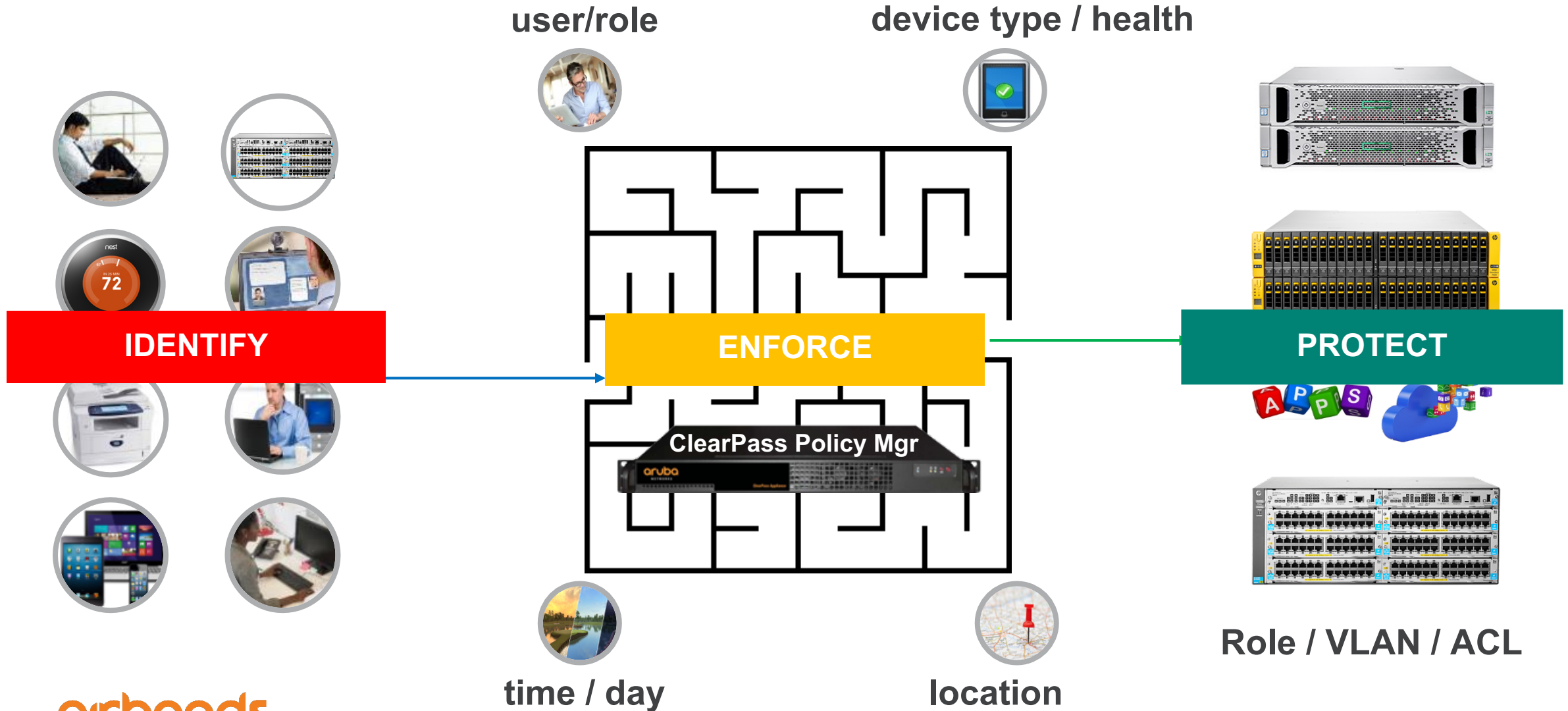


Employee

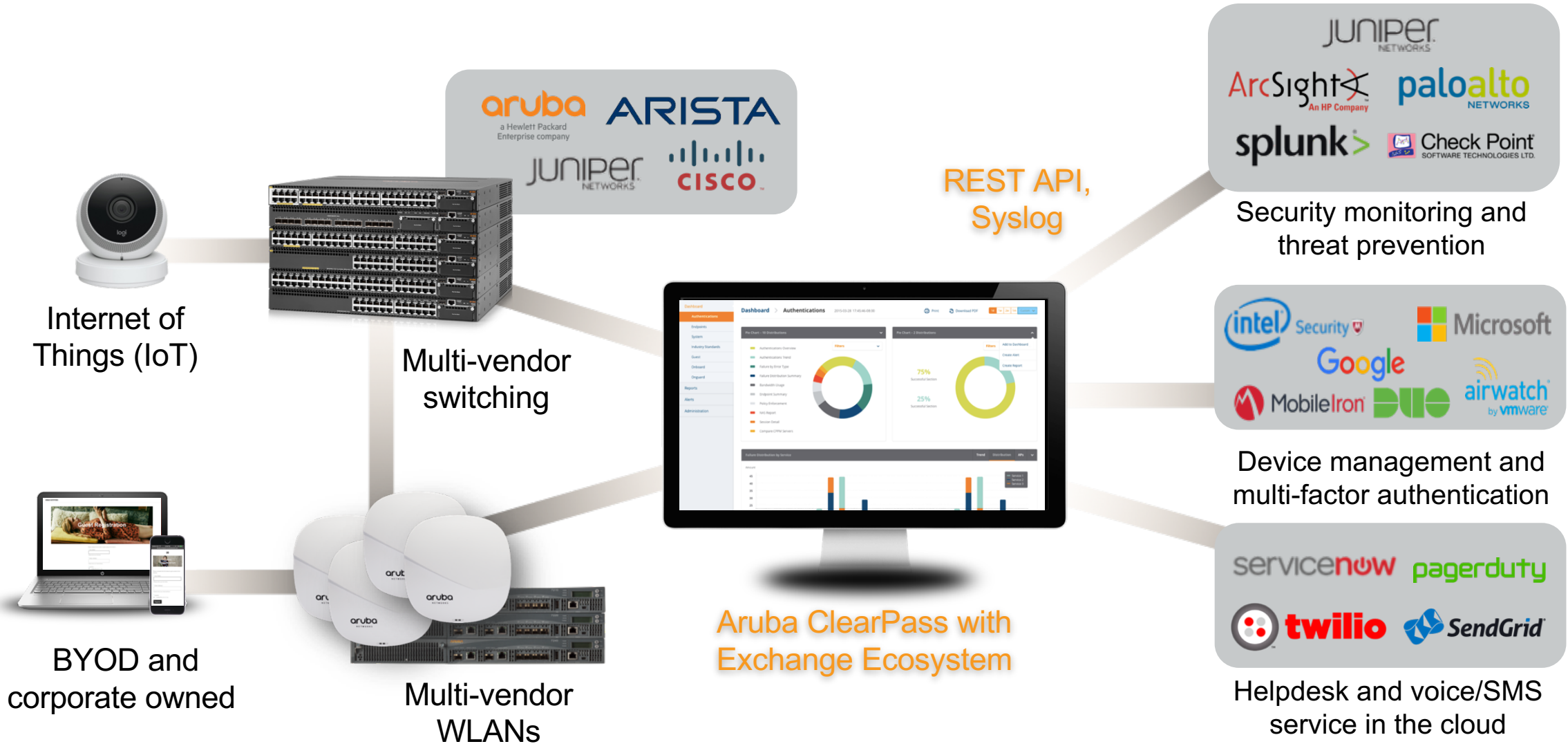
Enforce a Per Device Policy



Enforce A Per Device Policy



ClearPass Exchange: End to End Controls



Wired Colorless Ports

Plug in any device into any switch port

Understanding Connectivity Options

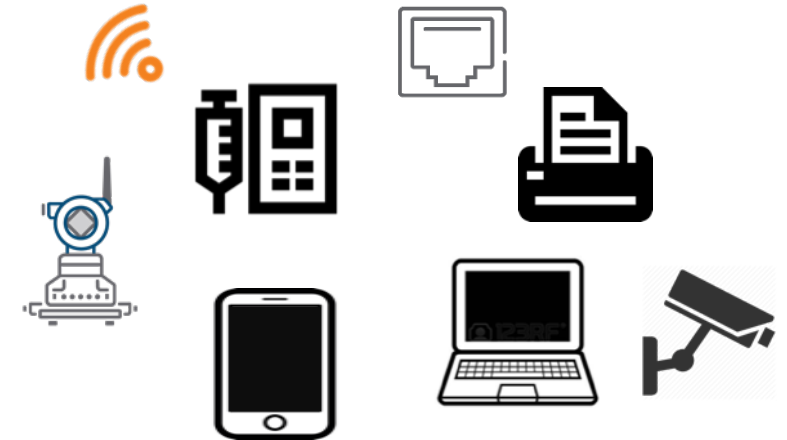
Customers want to **manage**
what devices connect



Only some support .1X
suplicants

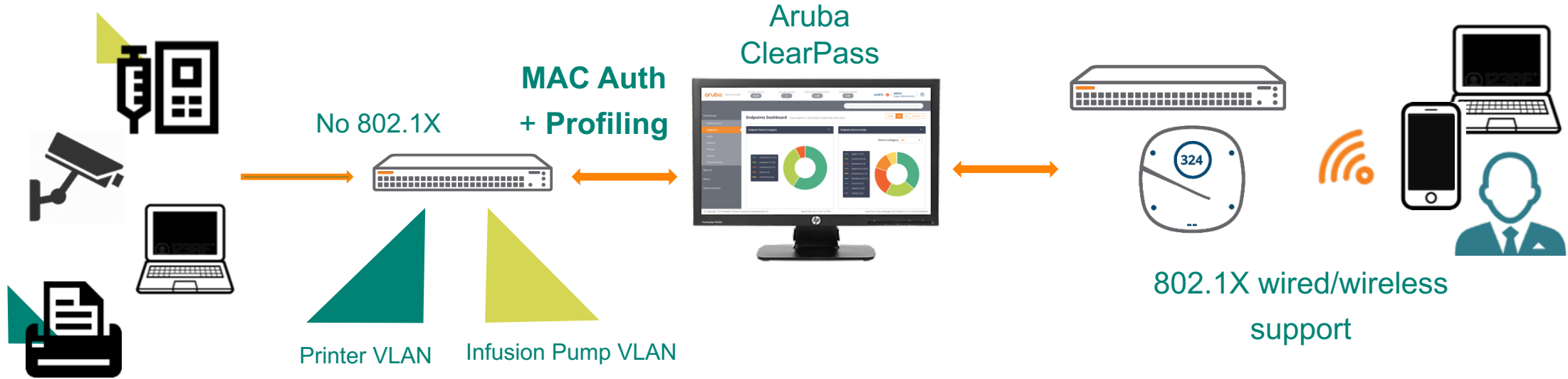


50% of IoT may be
wired



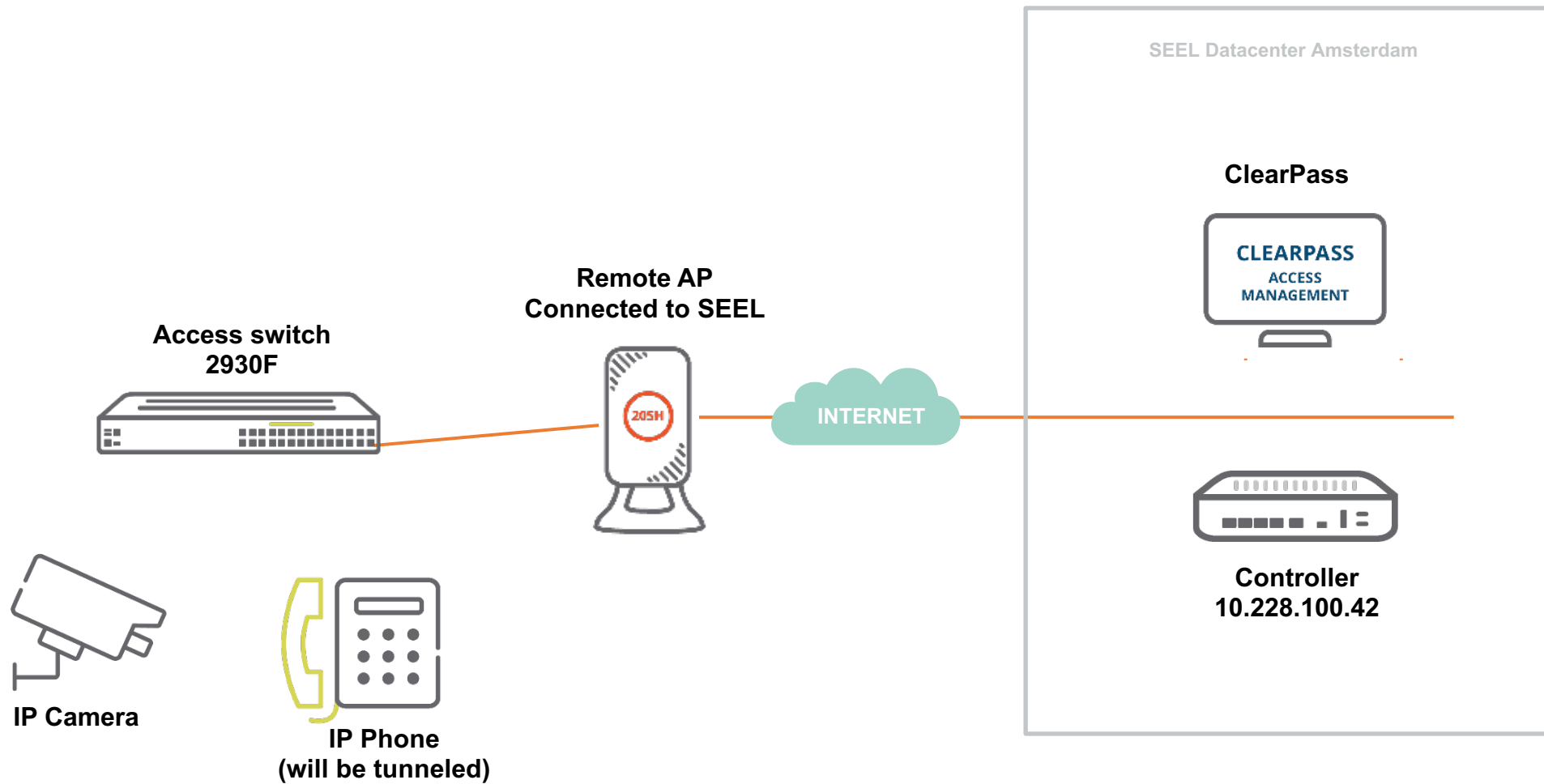
- ClearPass supports any customer Infrastructure and need

802.1X + MAC Auth + Profiling => Colorless ports

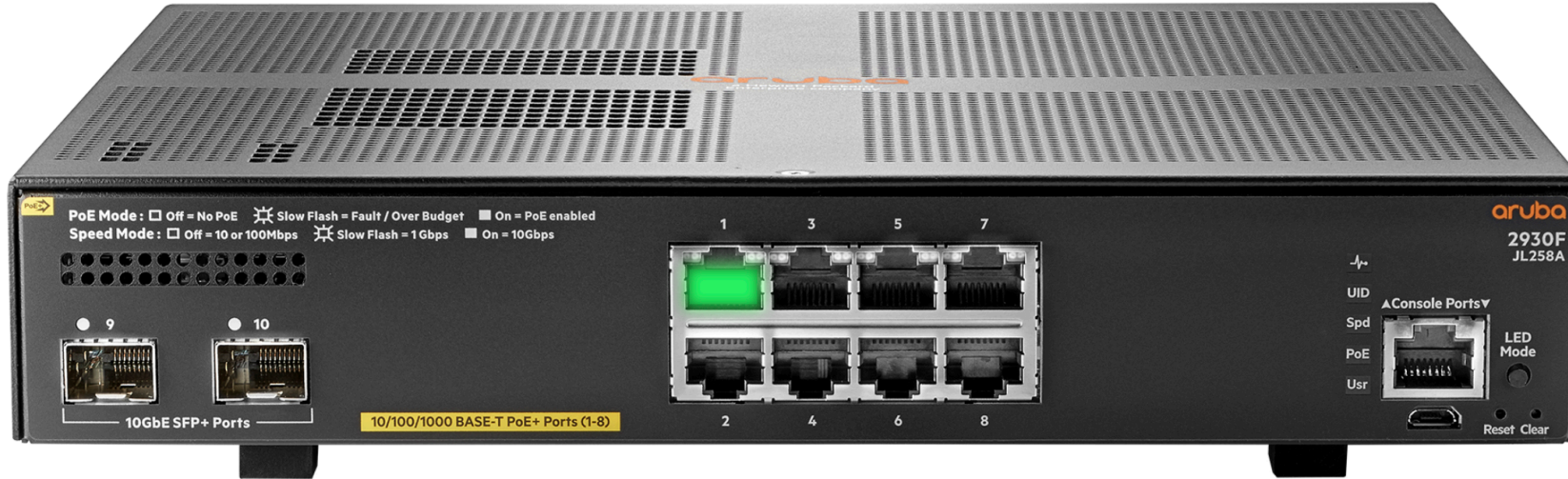


- Use 802.1X whenever possible
- Fallback to MAC authentication for non 802.1X capable devices
- Leverages ClearPass profiling for wired/wireless - IoT, laptops, mobile phones.















Demo lab setup



Demo: Plug in an IP Camera



Port Color per Role Assigned

	Network Uplink		Multiple Roles
	DS_IOT_SW		DS_USER_SW
	Secure_1x		Guest_BYOD
	Guest_Selfreg		Infrastructure
	AppleTV		VOIP_Phone
	Network_Camera		Headless
	Quarantine		Disabled

Demo: Plug in an IP Camera

The screenshot displays the Aruba ClearPass Policy Manager interface. The left sidebar shows the navigation menu with 'Monitoring' selected. The main content area is titled 'Request Details' and contains a table with request information. A red box highlights the 'End-Host Identifier' field, which shows the MAC address '00-88-01-12-4e-c6' and the device name '(Network Camera / Kingcam / Kingcam IP Camera)'. Another red box highlights the 'Enforcement Profiles' field, which lists several profiles including 'AOSS_Endpoint-Update', 'IS_DemoAN-Update', 'IS_SandboxAN-Update', 'IS360_DemoAN-Update', and 'NETWORK-CAMERA'. The bottom of the interface shows a pagination bar indicating 'Showing 1 of 1-20 records' and buttons for 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

Request Details

Summary	Input	Output	Accounting	Alerts
Login Status:	ACCEPT			
Session Identifier:	R000026ec-06-5d822040			
Date and Time:	Sep 18, 2019 05:17:04 PDT			
End-Host Identifier:	00-88-01-12-4e-c6 (Network Camera / Kingcam / Kingcam IP Camera)			
Username:	008801124ec6			
Access Device IP/Port:	10.228.80.95:3			
Access Device Name:	SEEL-AOSS-Demo-robers@hpe.com			
System Posture Status:	UNKNOWN (100)			
Policies Used -				
Service:	Wired MAC - AOSS			
Authentication Method:	MAC-AUTH			
Authentication Source:	None			
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Onboard Devices Repository], [Time Source]			
Roles:	1568809024, AMS-AOSS, DEVICE_NETWORK-CAMERA, Kingcam, Kingcam IP Camera,			
Enforcement Profiles:	AOSS_Endpoint-Update, IS_DemoAN-Update, IS_SandboxAN-Update, IS360_DemoAN-Update, NETWORK-CAMERA			

Showing 1 of 1-20 records | Change Status | Show Configuration | Export | Show Logs | Close

Demo: Plug in an IP Camera

Request Details

SummaryInput**Output**AccountingAlerts

RADIUS Response

Endpoint:Device Type	Network Camera
Endpoint:Display Name	Kingcam IP Camera
Endpoint>Last_Known_Location	SEEL-AOSS-Demo-robers@hpe.com:3
Radius:Hewlett-Packard-Enterprise:HPE-CPPM-Role	NETWORK_CAMERA-3162-2 class ipv4 DNS match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53 exit class ipv4 DHCP match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67 exit class ipv4 IP-ANY-ANY match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit policy user HEADLESS class ipv4 DHCP action permit class ipv4 DNS action permit

◀ ◀ Showing 1 of 1-20 records ▶ ▶

Change Status

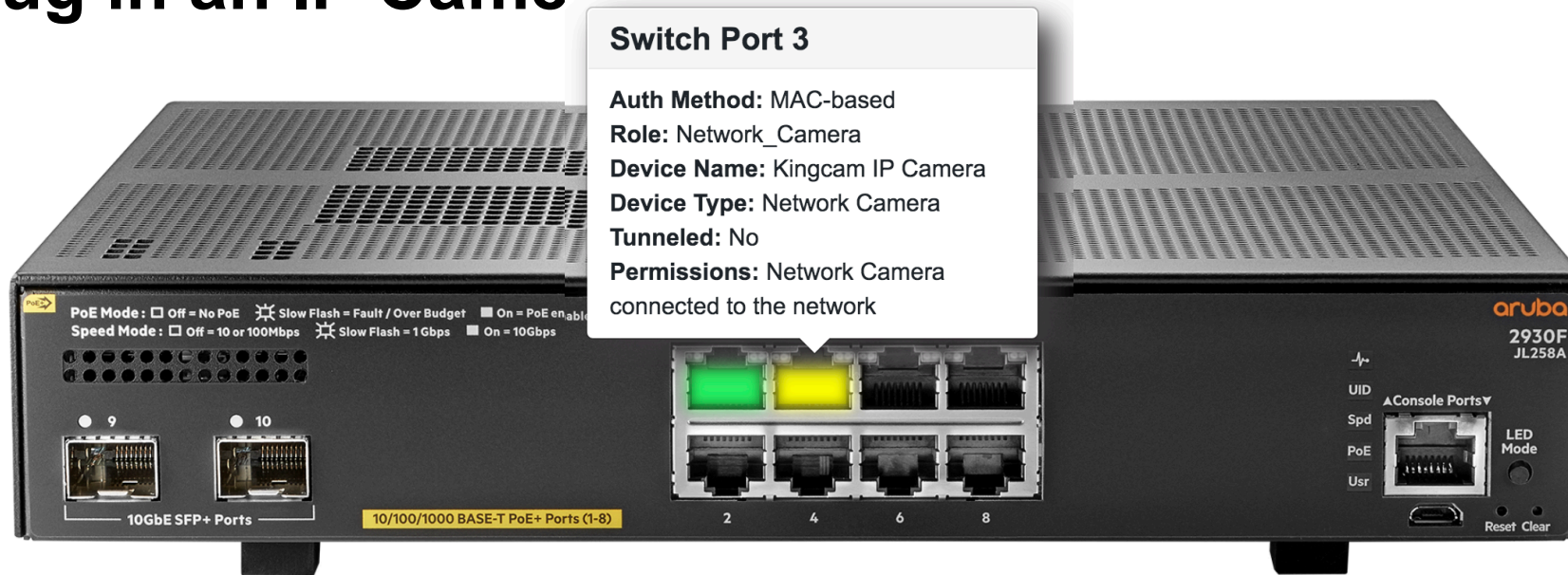
Show Configuration

Export















Show Logs

Close

Demo: Plug in an IP Camera



Port Color per Role Assigned

	Network Uplink		Multiple Roles
	DS_IOT_SW		DS_USER_SW
	Secure_1x		Guest_BYOD
	Guest_Selfreg		Infrastructure
	AppleTV		VOIP_Phone
	Network_Camera		Headless
	Quarantine		Disabled

Demo: Plug in an IP Camera

```
SEEL-AOSS-Demo-robers@hpe.com# show port-access clients
```

Downloaded user roles are preceded by *

```
SEEL-AOSS-Demo-robers@hpe.com# show port-access clients 3 detailed
```

Port Access Client Port Access Client Status Detail

Port	Client No	Client Base Details :
-----	-----	
3	008801124	Port : 3 Client Status : authenticated Client Name : 008801124ec6 MAC Address : 008801-124ec6 IP : 10.228.87.3

Authentication Type : mac-based
Session Time : 617 seconds
Session Timeout : 5160 seconds

```
SEEL-AOSS-Demo-ro
```

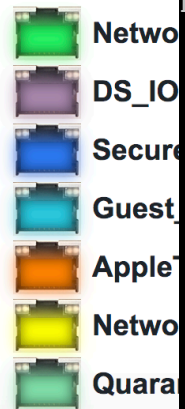
Auth Order : Not Set
Auth Priority : Not Set
LMA Fallback : Disabled

Downloaded user roles are preceded by *

User Role Information

Name	: *NETWORK_CAMERA-3162-2
Type	: downloaded
Reauthentication Period (seconds)	: 5160
Cached Reauth Period (seconds)	: 0
Logoff Period (seconds)	: 300
Untagged VLAN	: 3012
Tagged VLANs	:
Captive Portal Profile	:
Policy	: HEADLESS_NETWORK_CAMERA-3162-2

Port Color p



Benefits of colorless ports

Simplified user experience

- It just works in the eyes of the end user!

Increased visibility

- See and know what is on your network

Increased security

- Network automatically applies the correct policy

Simplified switch configuration

- All access ports are configured the same

ClearPass Device Insight

Introducing ClearPass Device Insight



Full-Spectrum Visibility
through DPI-based discovery
and profiling techniques

Unknown Device Classification
using advanced Machine Learning

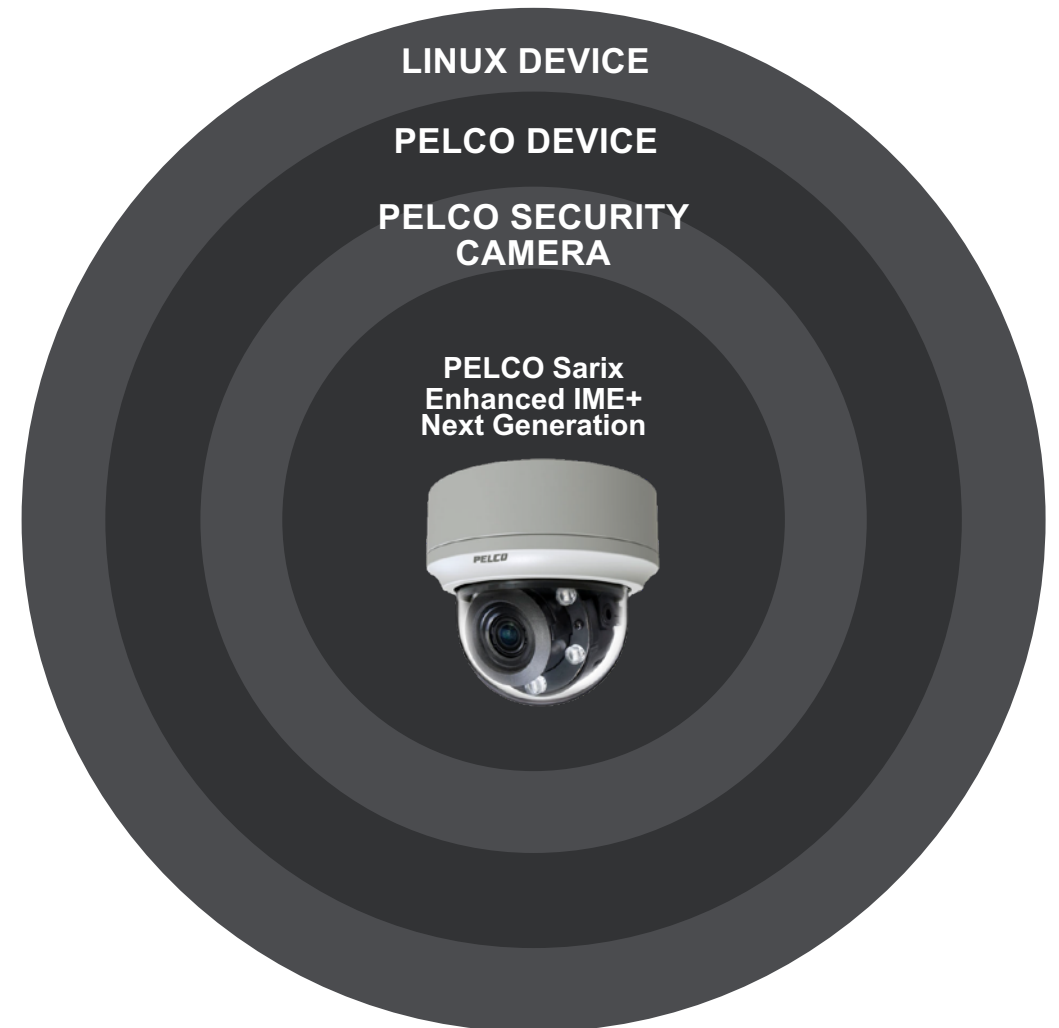
Seamless Integration
ClearPass Policy Manager enables
enforcement and segmentation

CLEARPASS DEVICE INSIGHT: FROM GENERIC TO GRANULAR

Before Device Insight, understanding specifics around generic “Windows Devices” is difficult

Device Insight delivers additional context via DPI and ML

The End Result: Deep intelligence around the nature and attributes of each device



ClearPass Device Insight Architecture

ClearPass Policy Manager Capabilities + Deep Packet Inspection +
Machine Learning + Nice UI

Deep Packet Inspection

Device Attributes

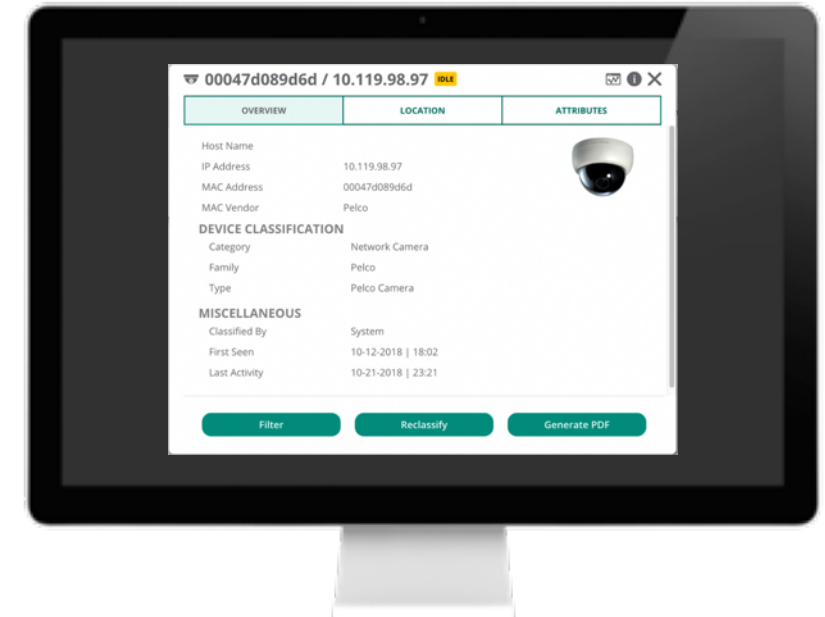
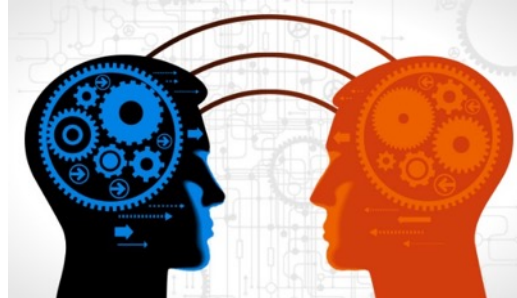
IP/MAC Address

Communication Patterns

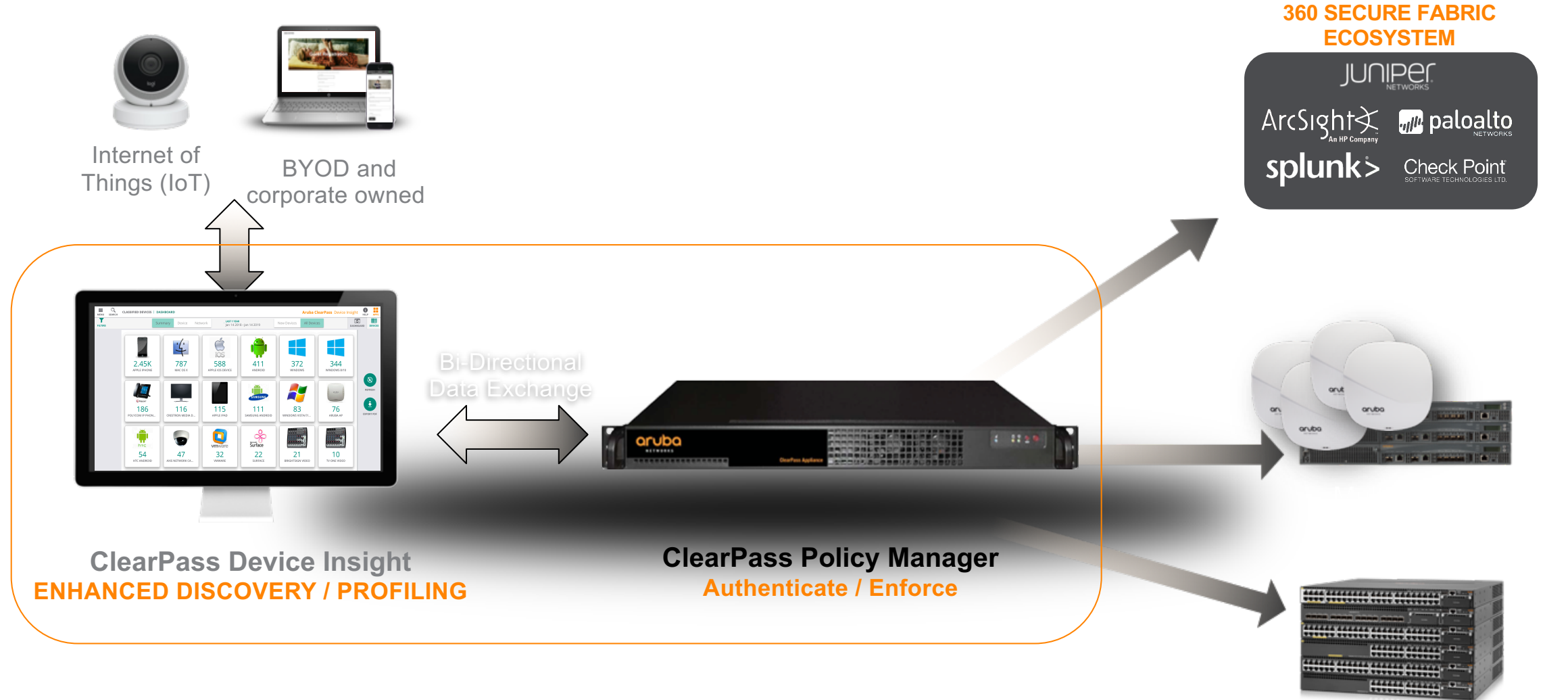
Applications

Communication Frequency

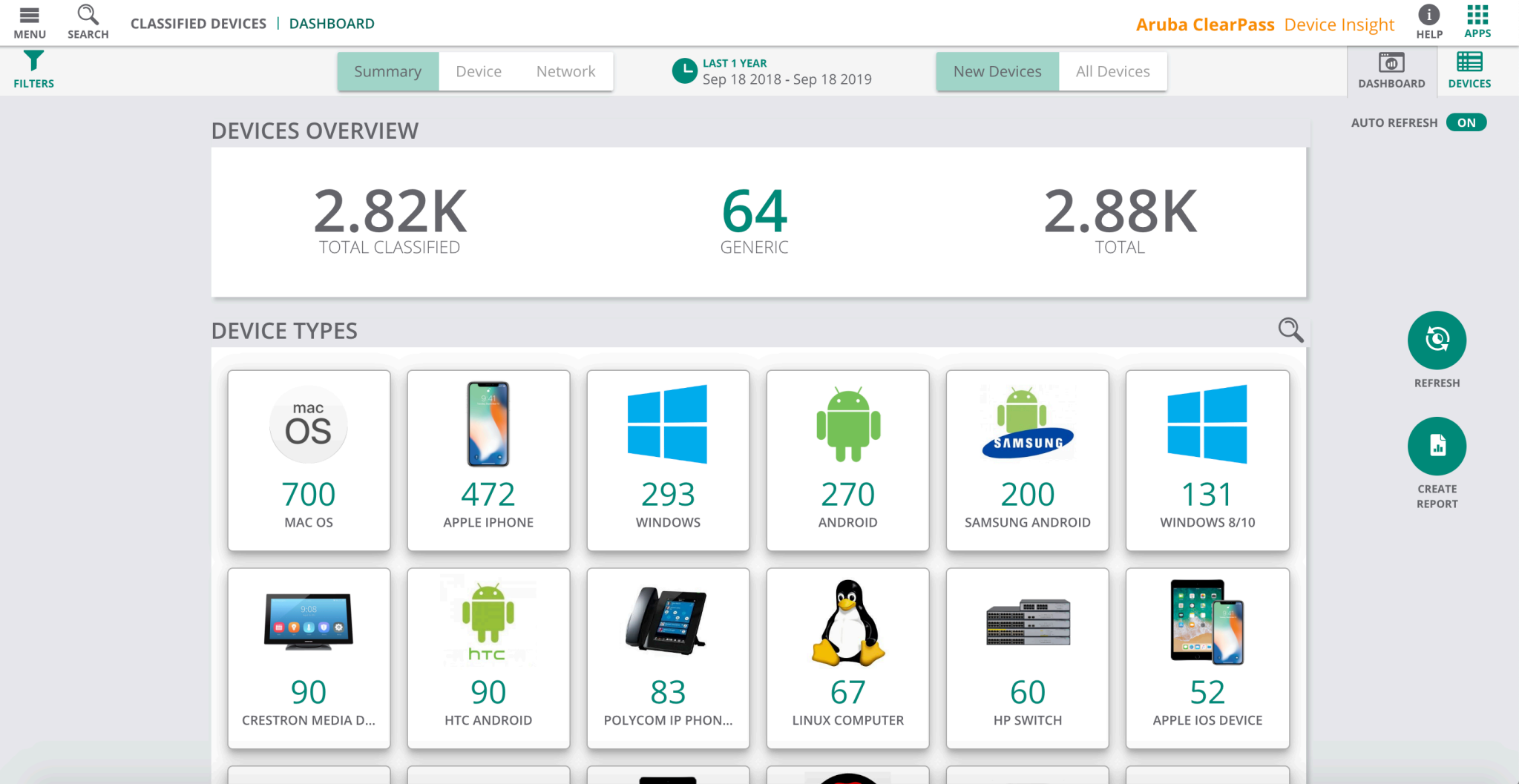
MACHINE LEARNING



Device Insight meet Policy Manager



Device Insight Demo



Device Insight Demo

GENERIC DEVICES

DASHBOARD

Aruba ClearPass

Device Insight

HELP

APPS

Device

Network

LAST 1 YEAR

Sep 18 2018 - Sep 18 2019

New Devices

All Devices

DASHBOARD

DEVICES

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

AUTO REFRESH

ON

SHOW DEVICES

REFRESH

CREATE REPORT

RECLASSIFY DEVICES

COMPARE

Device Insight Demo

MENU

SEARCH

DEVICES | LIST

FILTERS

Devices (1)

MAC	IP ADDRESS
347e5c345aec	192.168.5.11

347e5c345aec / 192.168.5.11

OVERVIEW

LOCATION

Host Name

SonosZP

IP Address

192.168.5.11

MAC Address

347e5c345aec

MAC Vendor

Sonos, Inc.

User Name

SonosZP

DEVICE CLASSIFICATION

Category

Home Audio

Family

Sonos

Type

Sonos

MISCELLANEOUS

Classified By

System

First Seen

08-06-2019

Last Activity

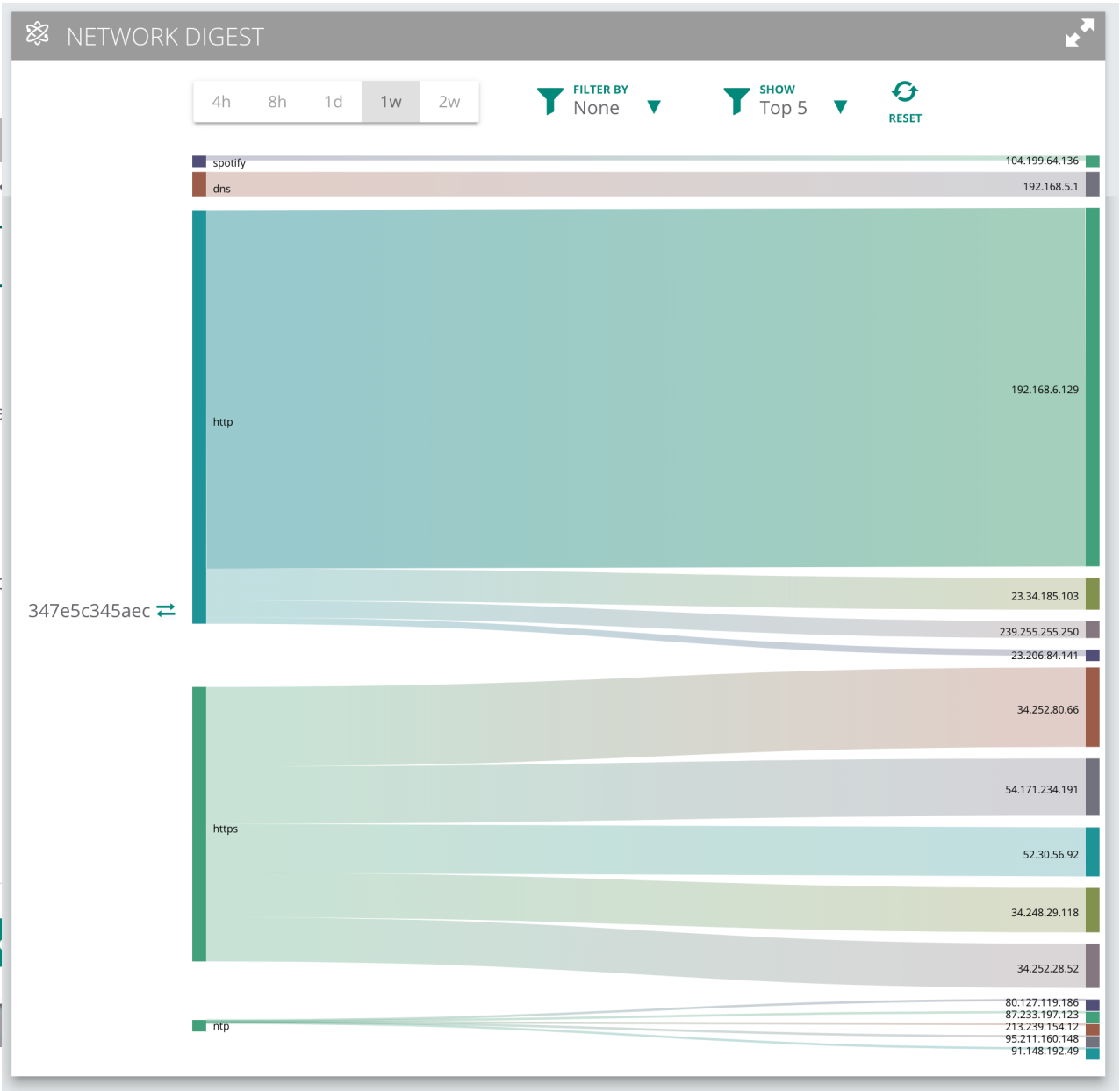
09-18-2019

Updated At

09-18-2019

Filter

Reset



When ClearPass Policy Manager? When ClearPass Device Insight?

ClearPass Policy Manager

- When you are happy with ClearPass and it's profiling capabilities
- When you need to do Enforcement anyway

Basic profiling built-in

Works best combined with enforcement

ClearPass Device Insight

- When you don't have ClearPass Policy Manager
- If you just want to know what is on the network
- If you don't need (or don't want) Enforcement
- If you prefer Cloud Applications over On-Premise solutions
- If you need the Traffic Insights to enhance the profiling quality (many IOT/OT systems).

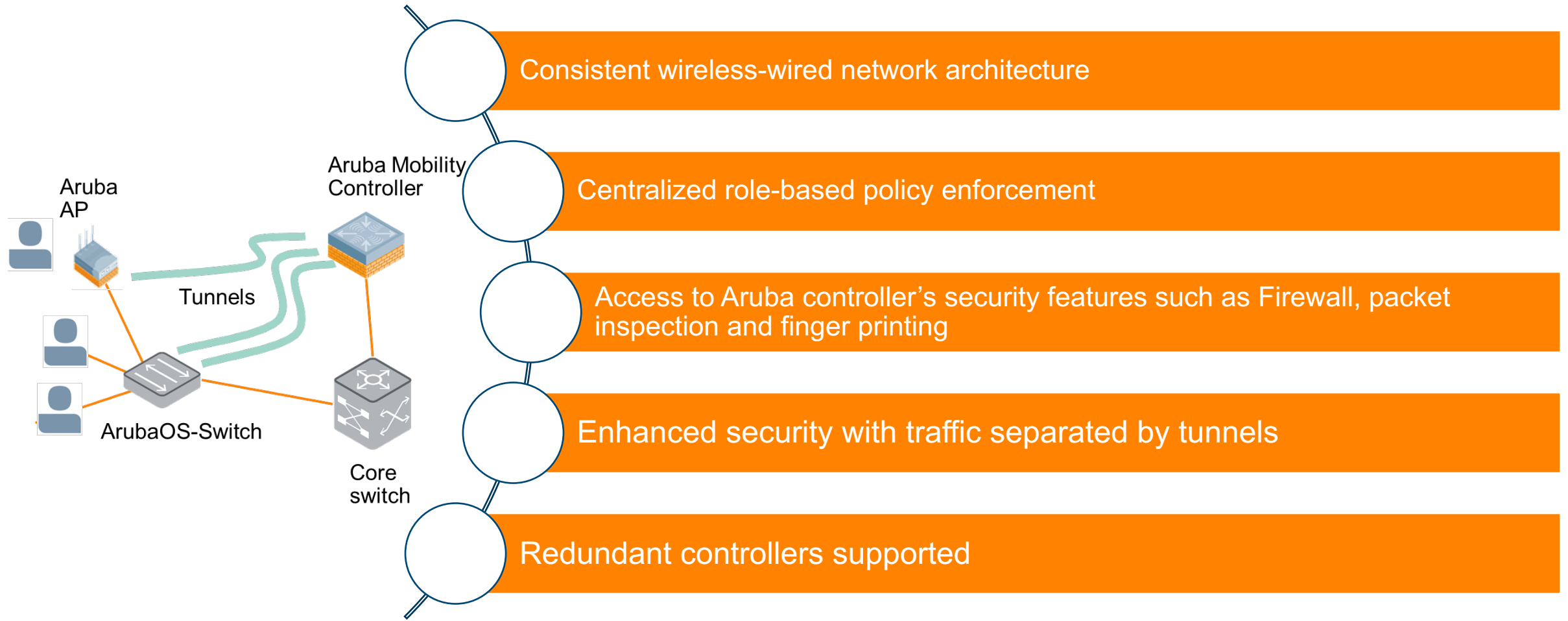
Advanced profiling capabilities

Easier and faster to set up

Dynamic Segmentation

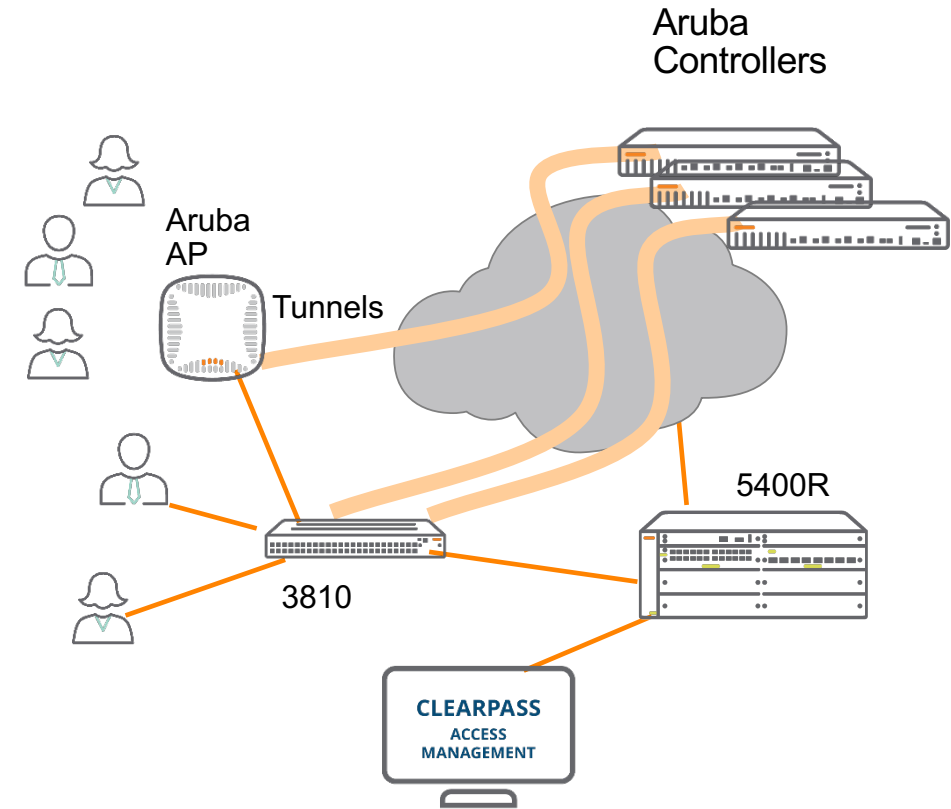
Make your switch a wired access point

Tunneled Node (Port based): unified policy enforcement for wired and wireless clients



Per User Tunneled Node

- Secured and flexible control of access layer
 - With ClearPass or switch configuration, only traffic from a specific user/device role is sent to the mobility controller
 - Policies (e.g., QoS, ACL, rate-limit) can be enforced at Tunneled Node ports or at the controller
- Access to Controller's applications
 - Users can access Controller's applications such as stateful firewall and AppRF
- Higher availability and scalability
 - Load balance to multiple controllers for high scalability
 - Stateful failover to standby management module for high availability
- Support on 5400R/v3, 3810, and 2930F/M
- Support on AOS 8.1 or later in the controllers



Policy source and enforcement for different scenarios

Scenario	Datapath & Policy Enforcement
Colorless ports with dACL	Local switch
Colorless ports with Role based access	Local switch
Port based tunnel (PBT)	Mobility controller
User based tunnel (UBT)	Switch (local) / Controller (tunneled)

Downloadable roles (ArubaOS 16.05)

- Starting ArubaOS 16.05, Downloadable user roles are supported with ClearPass 6.7.0+
- This feature allow you to define the role content in ClearPass instead of local on the switch
- ArubaOS for wireless supports Downloadable roles for a while already.
- Pro's for central defined roles (ClearPass):
No need to go in each switch/controller if roles need to be defined, or changed.
- Pro's for local defined roles:
Easier to make role content location specific (example: floor VLAN, location VLANs)
Fewer moving parts
- You have both options available in your toolkit.

Policy/role
Content

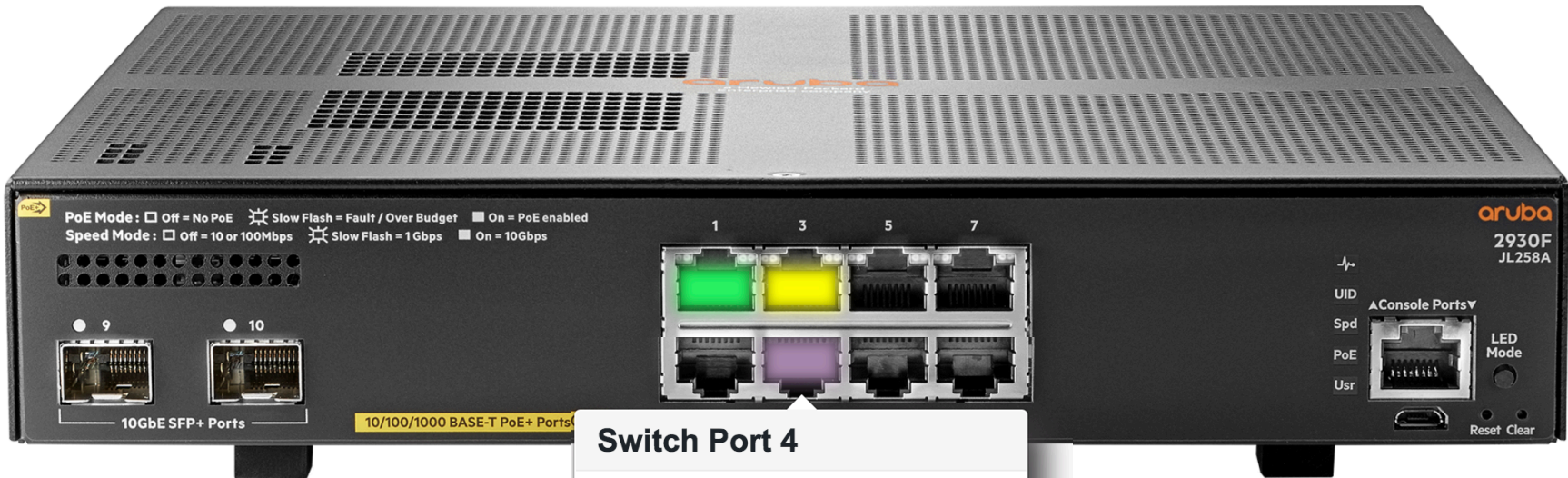
ClearPass

Local switch















Mobility controller

Switch (local) /
Controller
(tunneled)

Demo Tunneled Node



Port Color per Role Assigned

	Network Uplink		Multiple Roles
	DS_IOT_SW		DS_USER_SW
	Secure_1x		Guest_BYOD
	Guest_Selfreg		Infrastructure
	AppleTV		VOIP_Phone
	Network_Camera		Headless
	Quarantine		Disabled








Switch Port 4

Auth Method: MAC-based
Role: DS_IOT_SW
Device Name: Yealink/Tiptel IP Phone
Device Type: VoIP Phone
Tunneled: Yes
Cluster: N/A
Controller: 10.228.100.42
Role on Controller:
*DS_IOT_CTR-3150-4
Permissions: Tunneled IoT device

Demo Tunneled Node



Port Color per Role Assignment

	Network Uplink
	DS_IOT_SW
	Secure_1x
	Guest_Selfreg
	AppleTV
	Network_Camera
	Quarantine

```
SEEL-AOSS-Demo-robers@hpe.com# show port-access clients 4 detailed
```

Port Access Client Status Detail

Client Base Details :

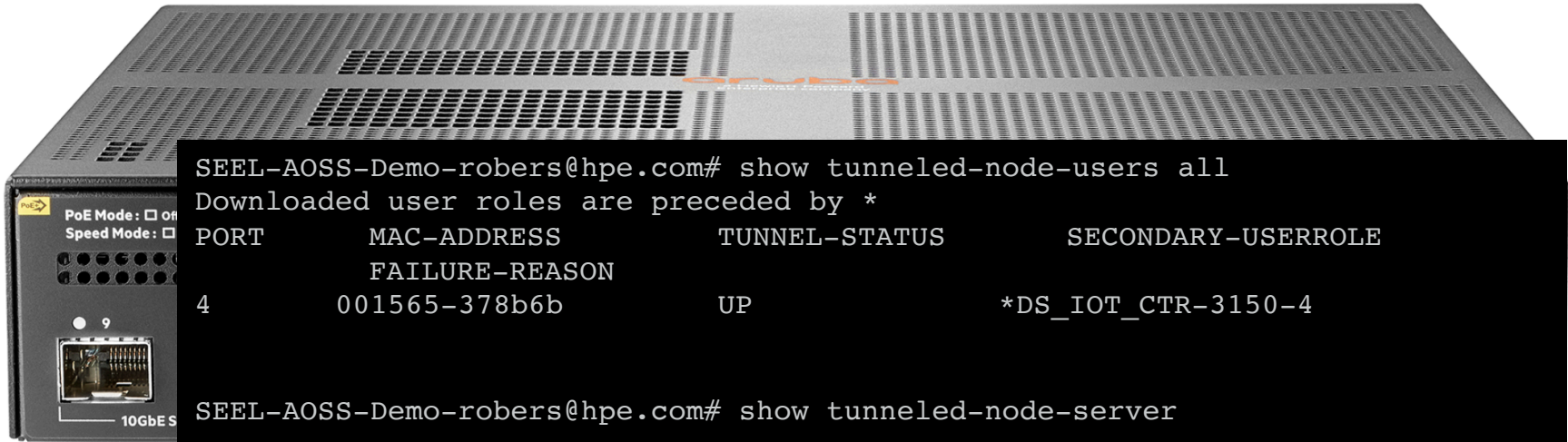
Port	: 4	Authentication Type	: mac-based
Client Status	: authenticated	Session Time	: 156 seconds
Client Name	: 001565378b6b	Session Timeout	: 0 seconds
MAC Address	: 001565-378b6b		
IP	: 10.228.91.4		
Auth Order	: Not Set		
Auth Priority	: Not Set		
LMA Fallback	: Disabled		

Downloaded user roles are preceded by *

User Role Information

Name	: *DS_IOT_SW-3148-12
Type	: downloaded
Reauthentication Period (seconds)	: 0
Cached Reauth Period (seconds)	: 0
Logoff Period (seconds)	: 300
Untagged VLAN	: 1000
Tagged VLANs	:
Captive Portal Profile	:
Policy	:
Tunnelednode Server Redirect	: Enabled
Secondary Role Name	: *VSA
Device Attributes	: Disabled

Demo Tunneled Node



SEEL-AOSS-Demo-robers@hpe.com# show tunneled-node-users all

Downloaded user roles are preceded by *

PORT	MAC-ADDRESS	TUNNEL-STATUS	SECONDARY-USERROLE
	FAILURE-REASON		
4	001565-378b6b	UP	*DS_IOT_CTR-3150-4

SEEL-AOSS-Demo-robers@hpe.com# show tunneled-node-server











Tunneled Node Server Information

State	: Enabled
Primary Controller	: 10.228.100.42
Backup Controller	:
Keepalive Interval (seconds)	: 8
Mode	: Role-based
Vlan-Mode	: vlan-extend-disable
Reserved-Vlan	: 1000

*DS_IOT_CTR-3150-4

Permissions: Tunneled IoT device

Port Color per Role Assignment

	Network Uplink		DS_IOT_SW
	Secure_1x		Guest_Selfreg
	AppleTV		VOIP_Phone
	Network_Camera		Headless
	Quarantine		Disabled

Demo Tunneled Node

aruba

MOBILITY CONTROLLER
AMS-WLC-02

ACCESS POINTS

3 8

CLIENTS

0 1

ALERTS

1

herman.robbers@hpe.com

Mobility Master: 10.228.30.80

Search

Dashboard

Overview

Infrastructure

Traffic Analysis

Services

Configuration

Diagnostics

Maintenance

← 1 Client

4 WLANs

343 MB

5 Radios

Wired Clients 1

NAME ▲	IP ADDRESS	ROLE	CONNECTED TO	AGE	RX BYTES	TX BYTES
001565378b6b	10.228.91.4	DS_IOT_CTR-3150-4	SEEL-AOSS-Demo-ro...	8m 24s	6.60 k	0

Guest_Selfreg

AppleTV

Network_Camera

Quarantine

Infrastructure

VOIP_Phone

Headless

Disabled

Controller: 10.228.100.42

Role on Controller:

*DS_IOT_CTR-3150-4

Permissions: Tunneled IoT device

Dynamic Segmentation benefits

Simplified network setup and operations

- Operate your wired like your wireless network

Unified policies across wired and wireless

Increased Security by Client isolation

- Individual tunnel per client, even client-to-client traffic is firewalled

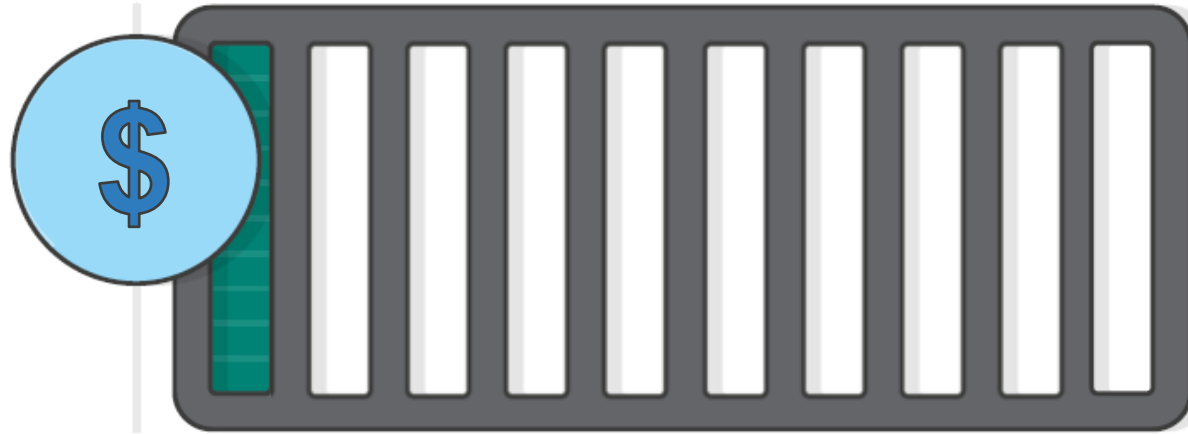
Flexible where needed with per user tunneled node

- Decide during network association if traffic needs to be switch locally or tunneled and processed centrally

Now the device are connected

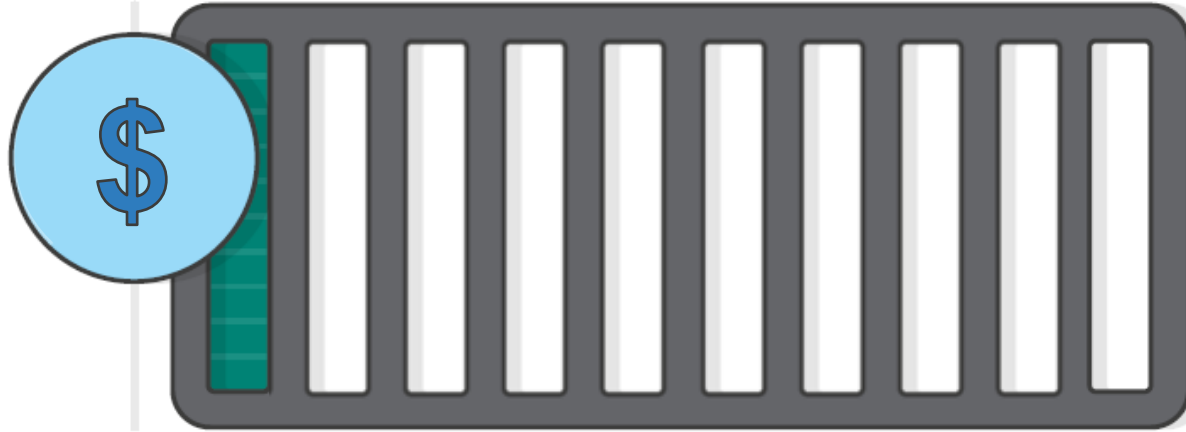
What if devices become malicious?

Where are we placing our bets?



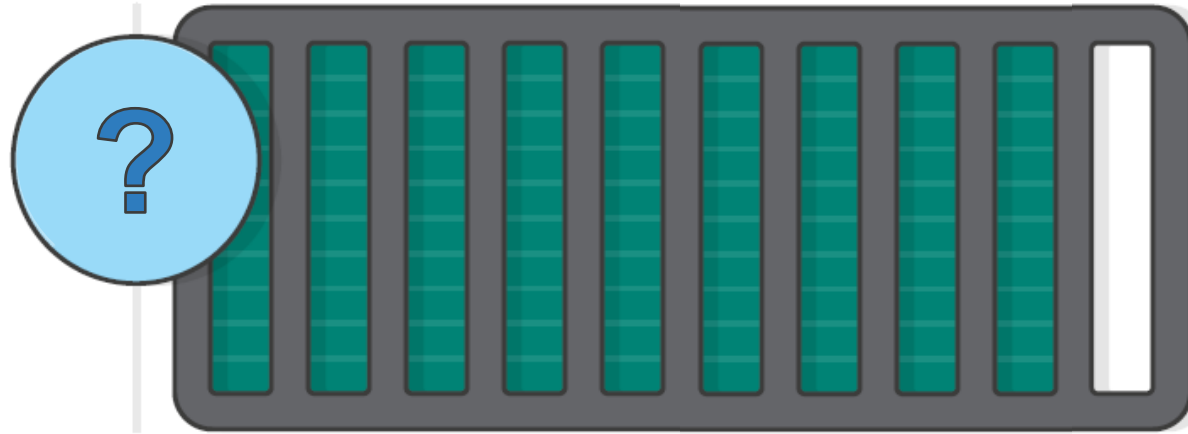
- Organizations spend an average of 5.6% (between 1 and 13%) of the overall IT budget on IT security and risk management. (Gartner Dec. 2016)
- Average consolidated cost of a breach = \$4 Million (Ponemon Institute 2016)

Where are we placing our bets?

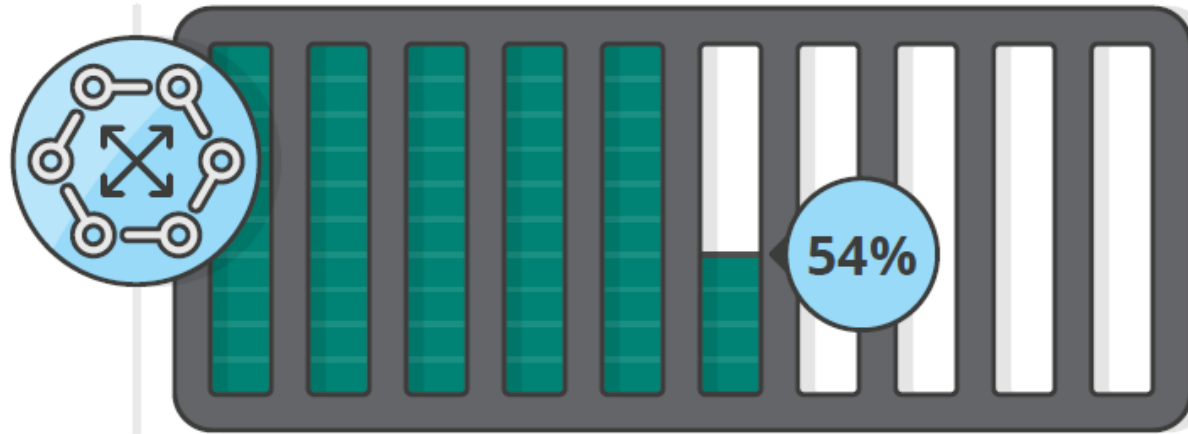


- **Perimeter Defense (Firewalls, IPS etc)**
 - **Endpoint Security**
 - **Log Management**
- **Vulnerability Management**

What about the Security team?

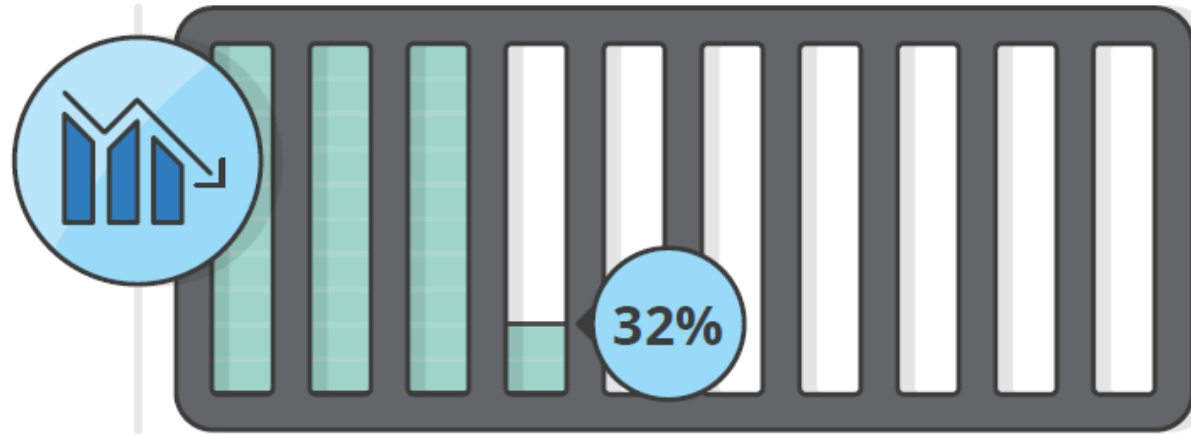


What about the Security team?



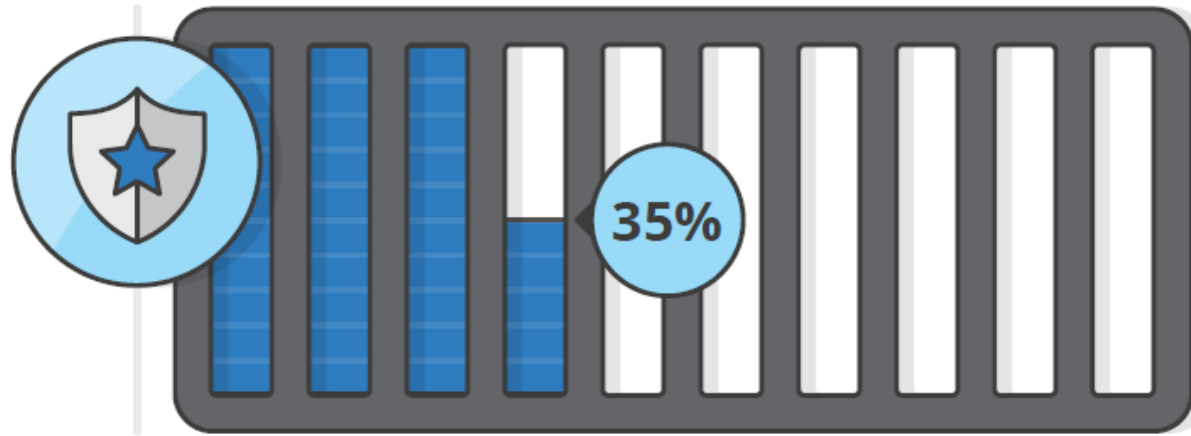
Most say the cybersecurity skills shortage has increased workloads, overloaded analysts.

What about the Security team?



Nearly 1/3 reported increased sustained workload, introducing errors, making the situation worse.

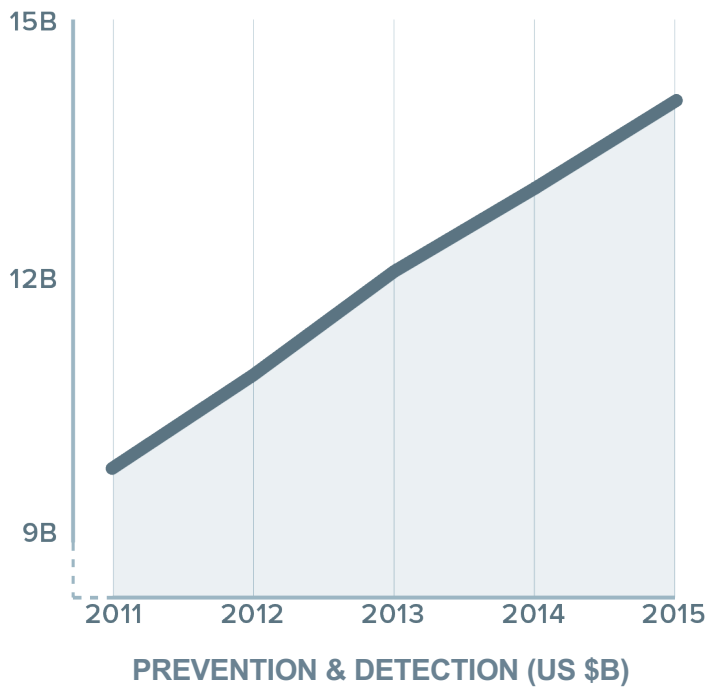
What about the Security team?



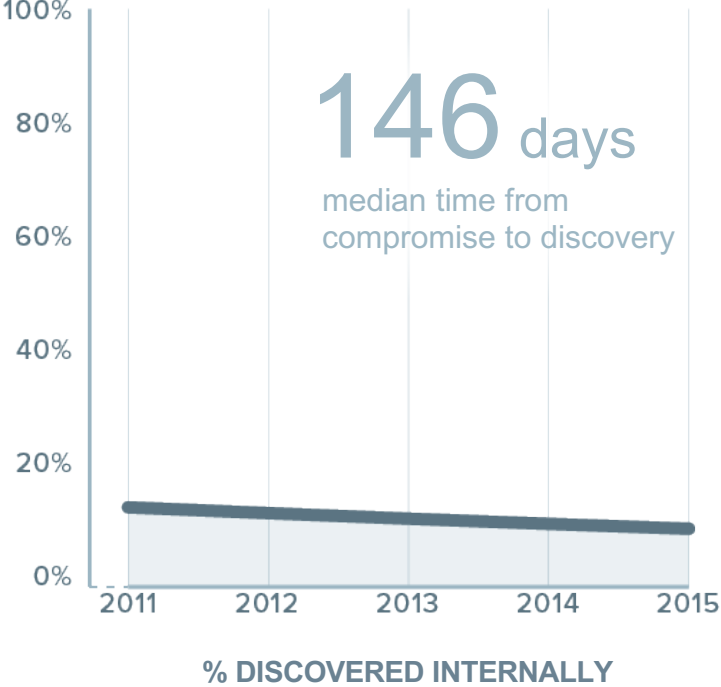
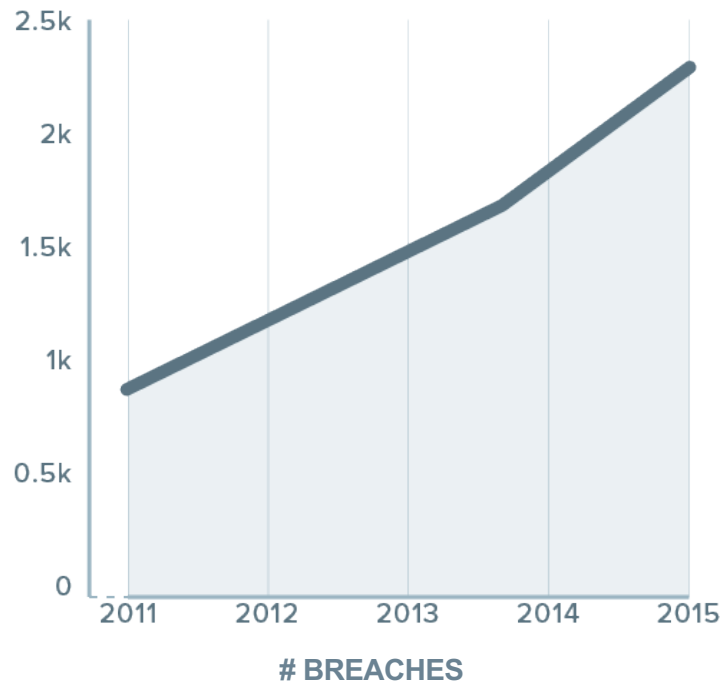
Over 1/3 can't utilize security technologies to their full potential, decreasing effectiveness.

The Security gap

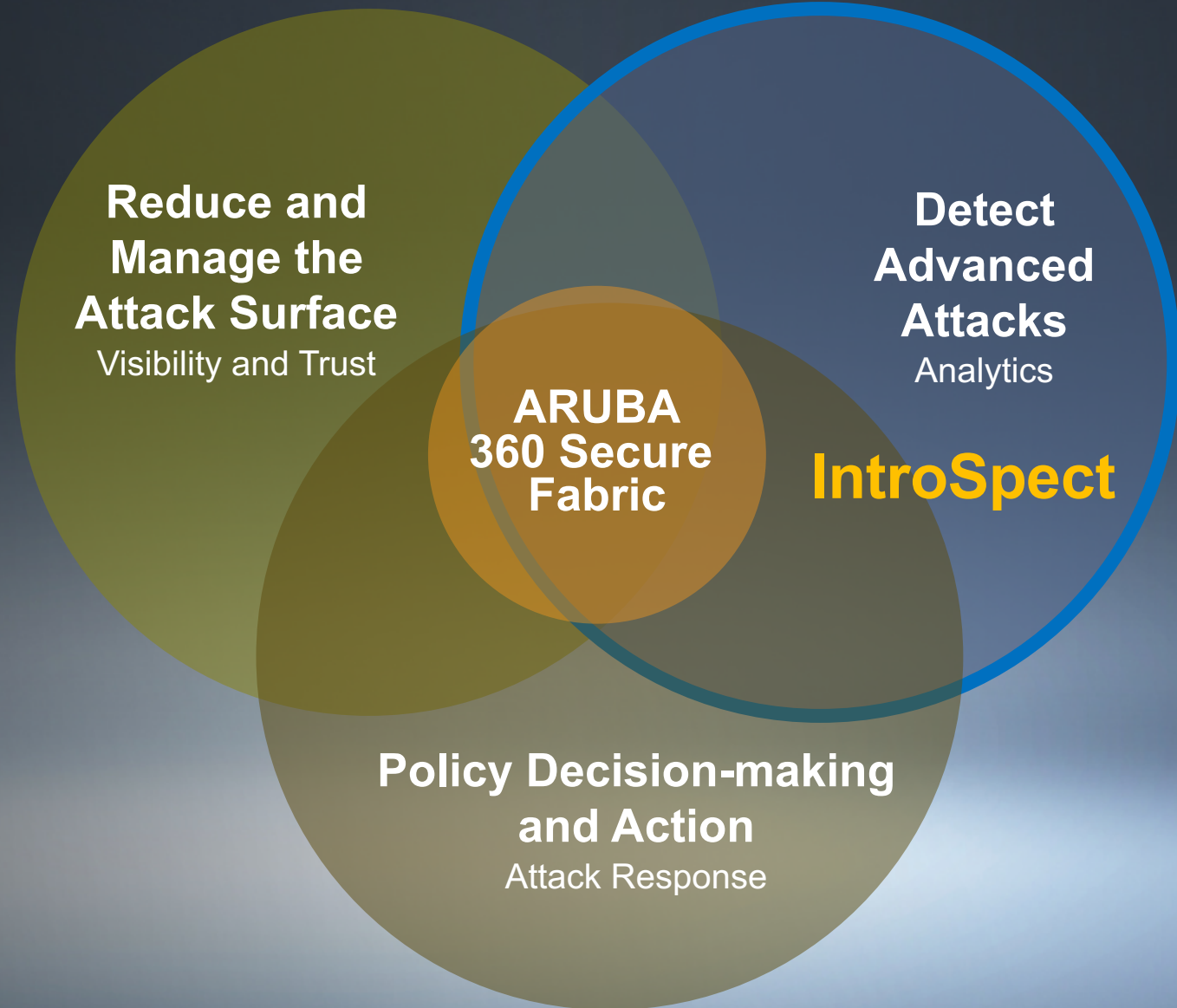
SECURITY SPEND



DATA BREACHES



THE NEW SECURITY IMPERATIVE



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

Attacks on the Inside Utilizing Legitimate Credentials



COMPROMISED

40 million credit cards were stolen from Target's servers



MALICIOUS

Edward Snowden stole more than 1.7 million classified documents



NEGLIGENT

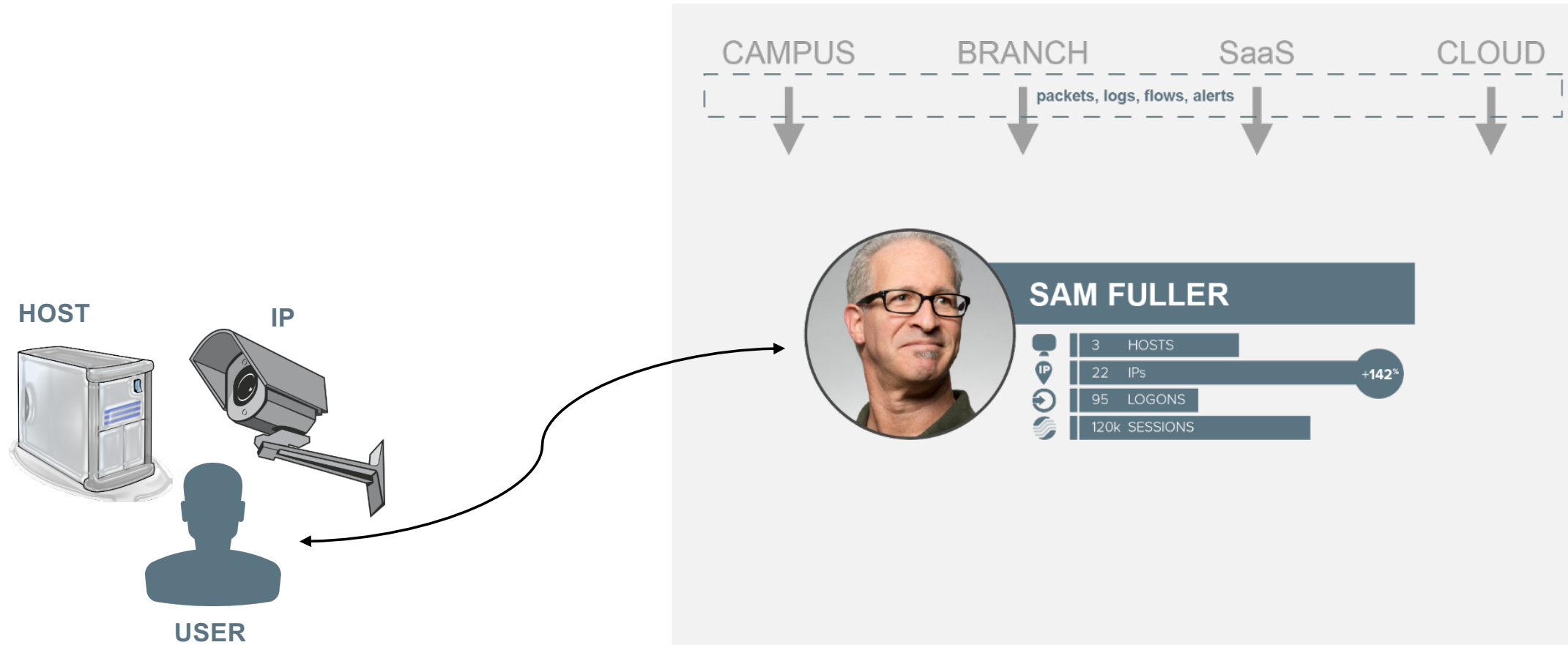
DDoS attack from 10M+ hacked home devices took down major websites

STOLEN CREDENTIALS

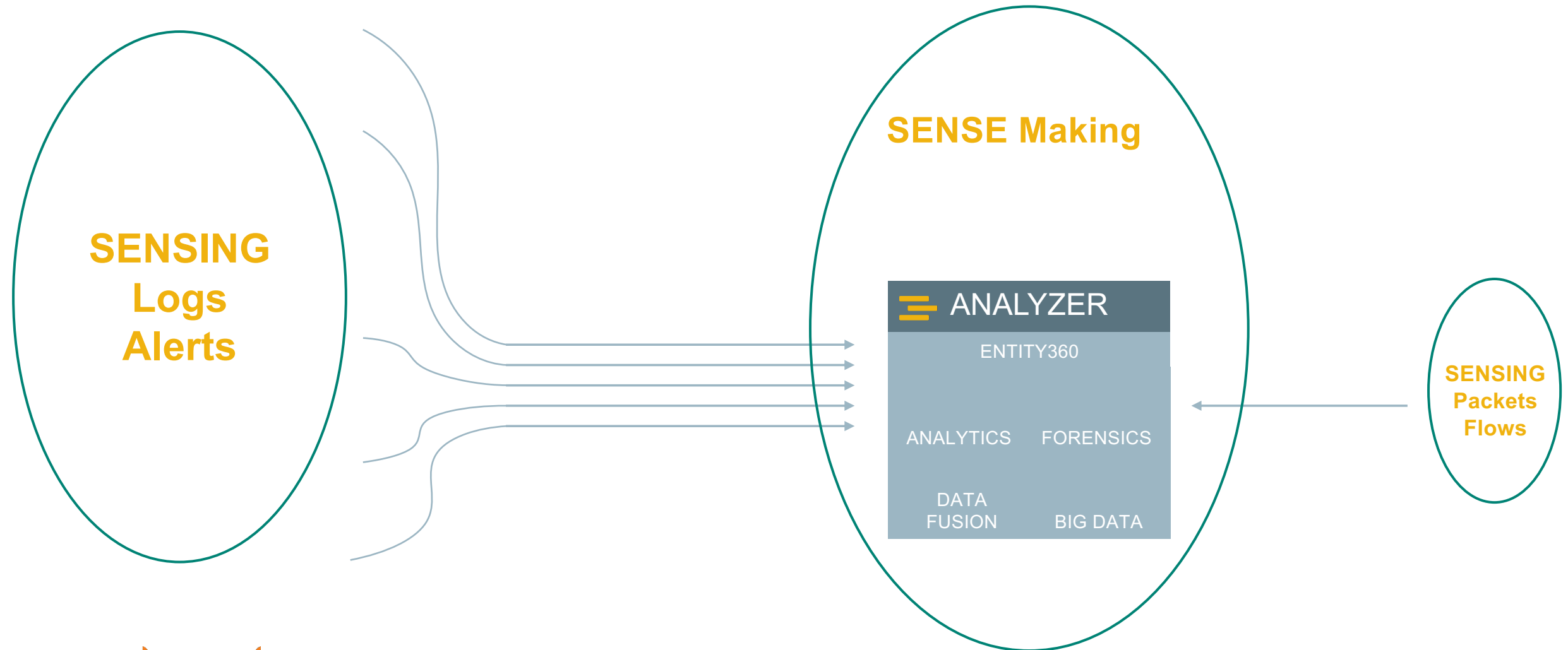
INTENDED TO LEAK INFORMATION

ALL USED THE SAME PASSWORD

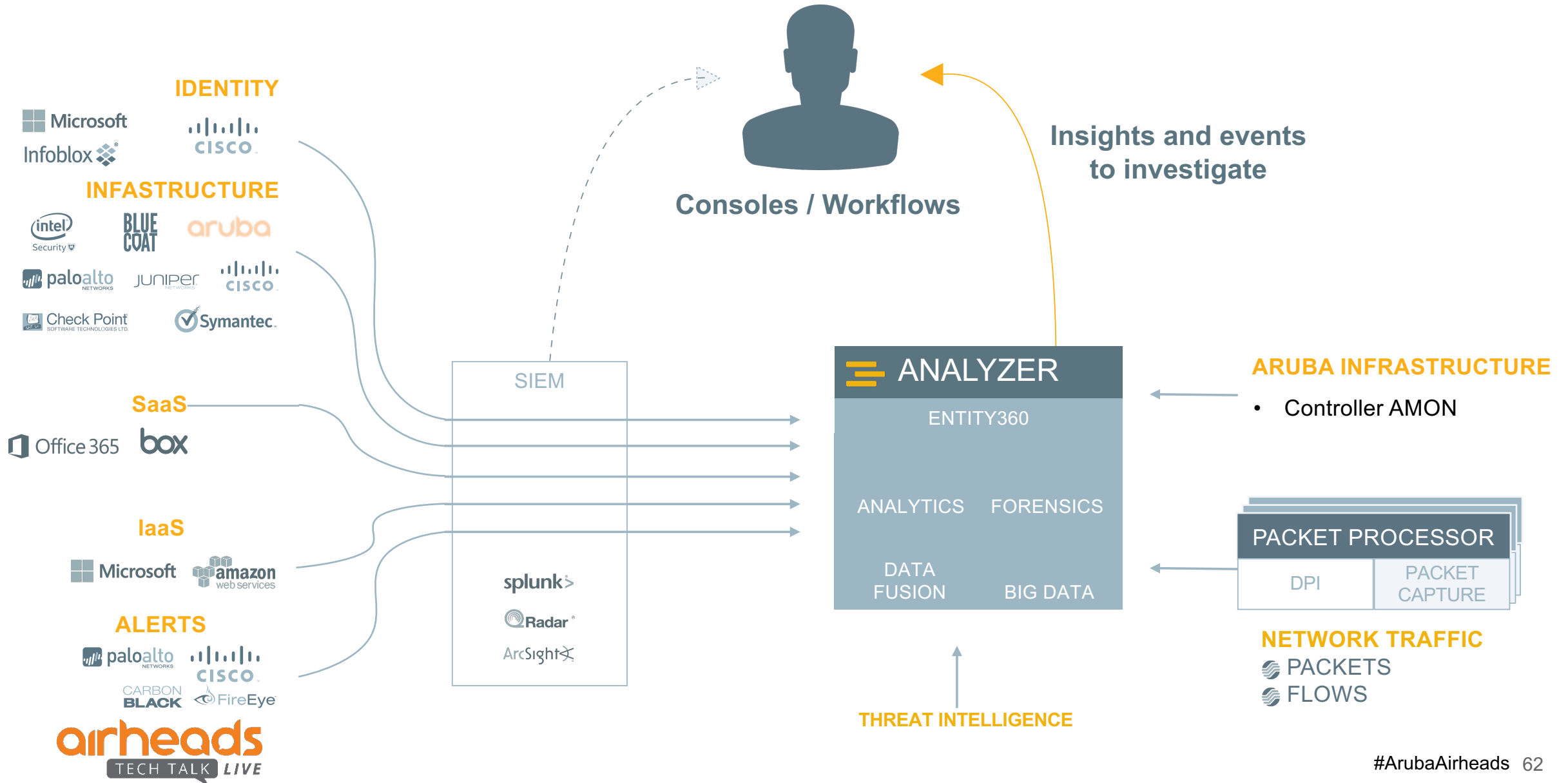
The Start: User/Entity View of Events



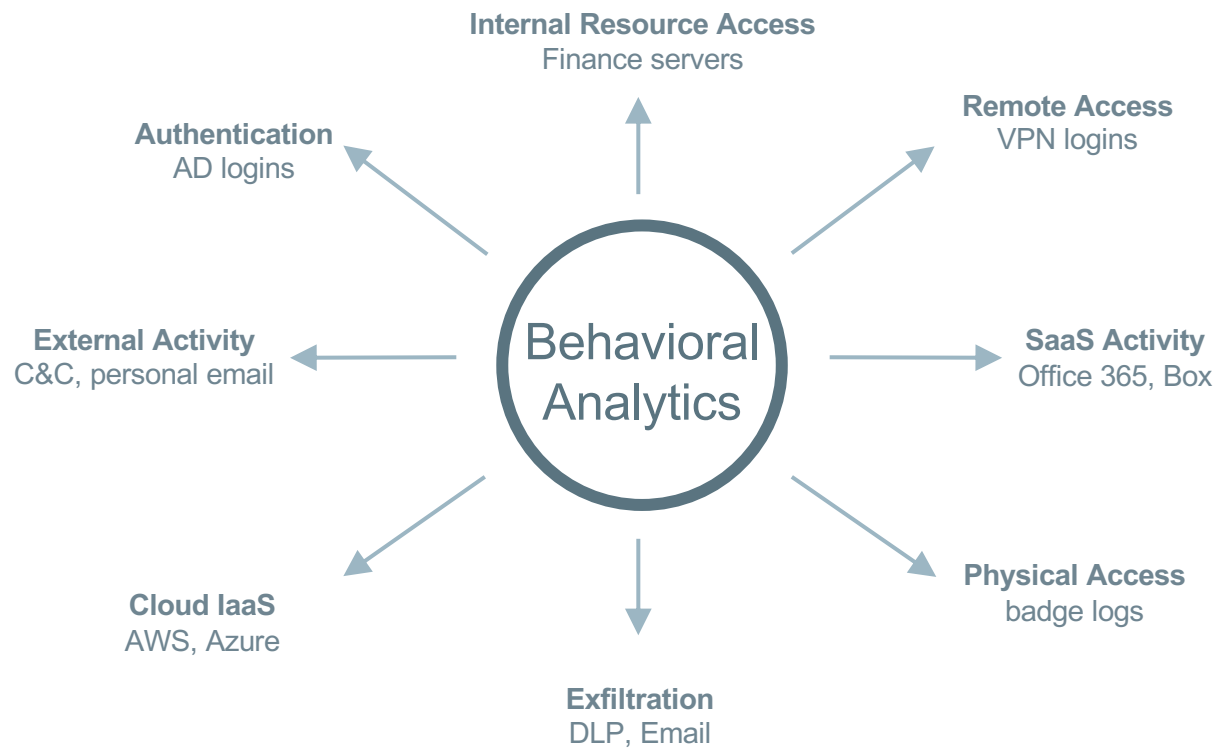
Introspect Solution - at a glance



SOLUTION – INTEGRATED WITH SECURITY ECOSYSTEM



Behavior – Many Different Dimensions



SAM FULLER

	3 HOSTS
	22 IPs +142%
	95 LOGONS
	120k SESSIONS

Basics of Behavioral Analytics

MACHINE LEARNING
UNSUPERVISED



BASELINES
HISTORICAL
+
PEER GROUP



SAM FULLER

	3 HOSTS	
	22 IPs	+142%
	95 LOGONS	
	120k SESSIONS	

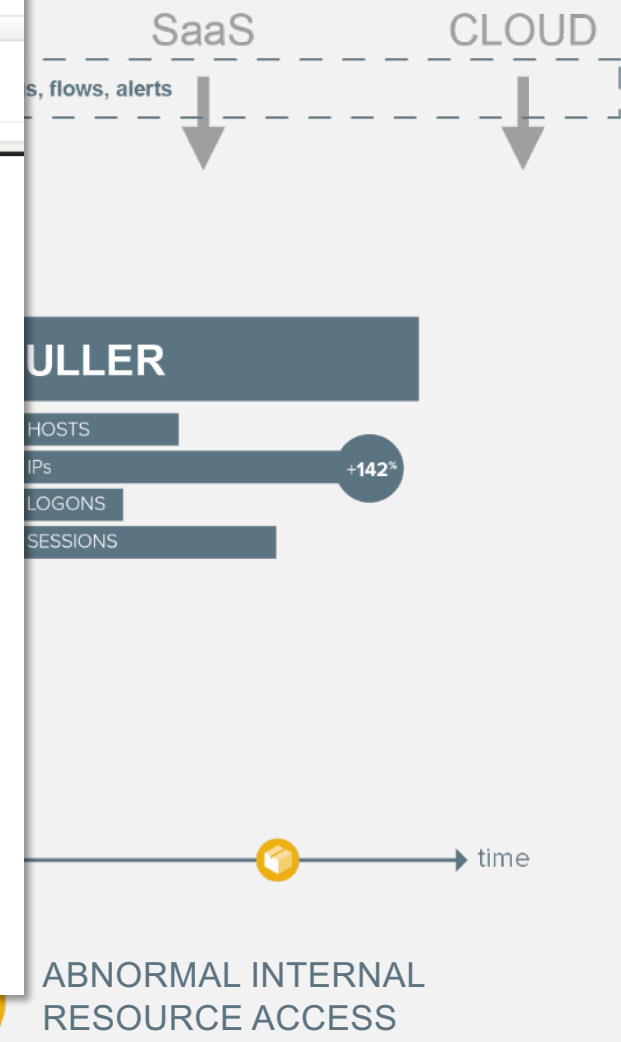


time

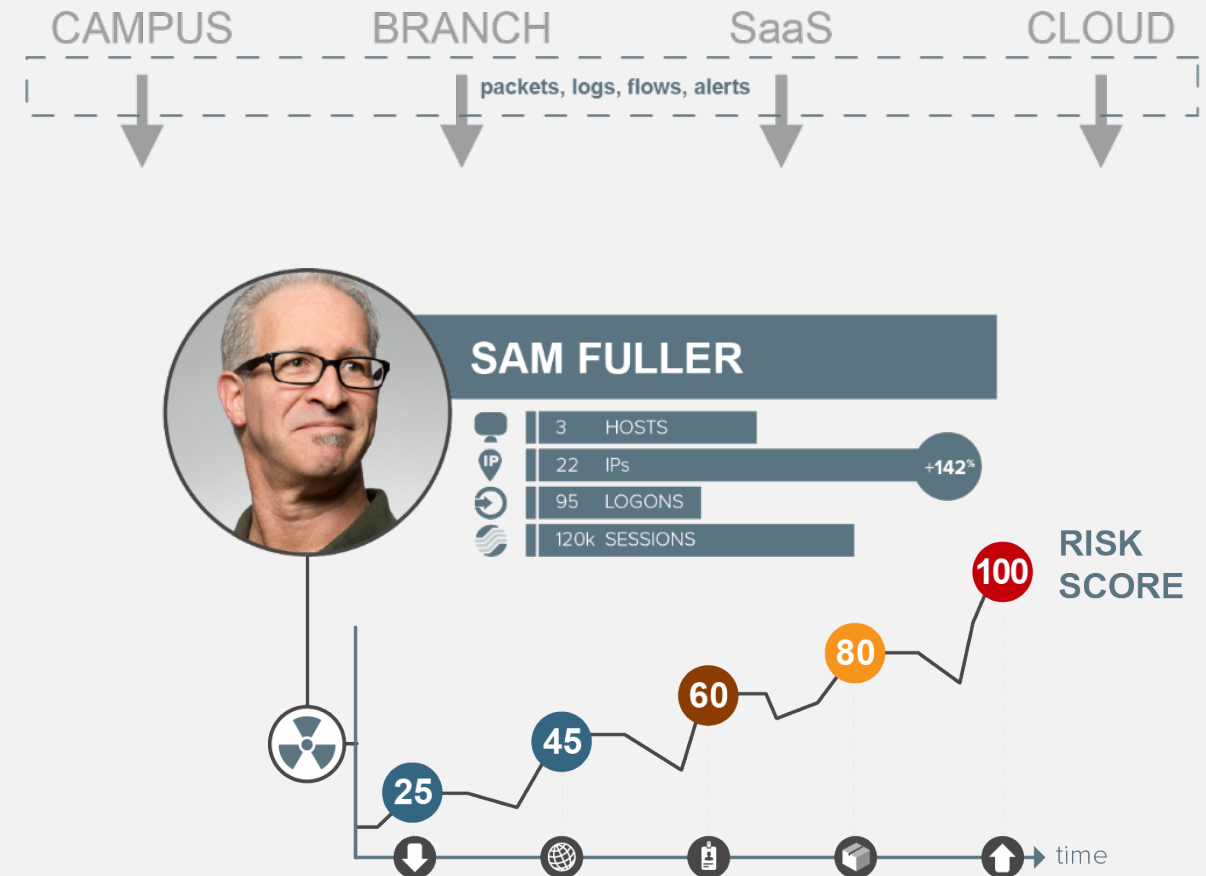


ABNORMAL INTERNAL
RESOURCE ACCESS

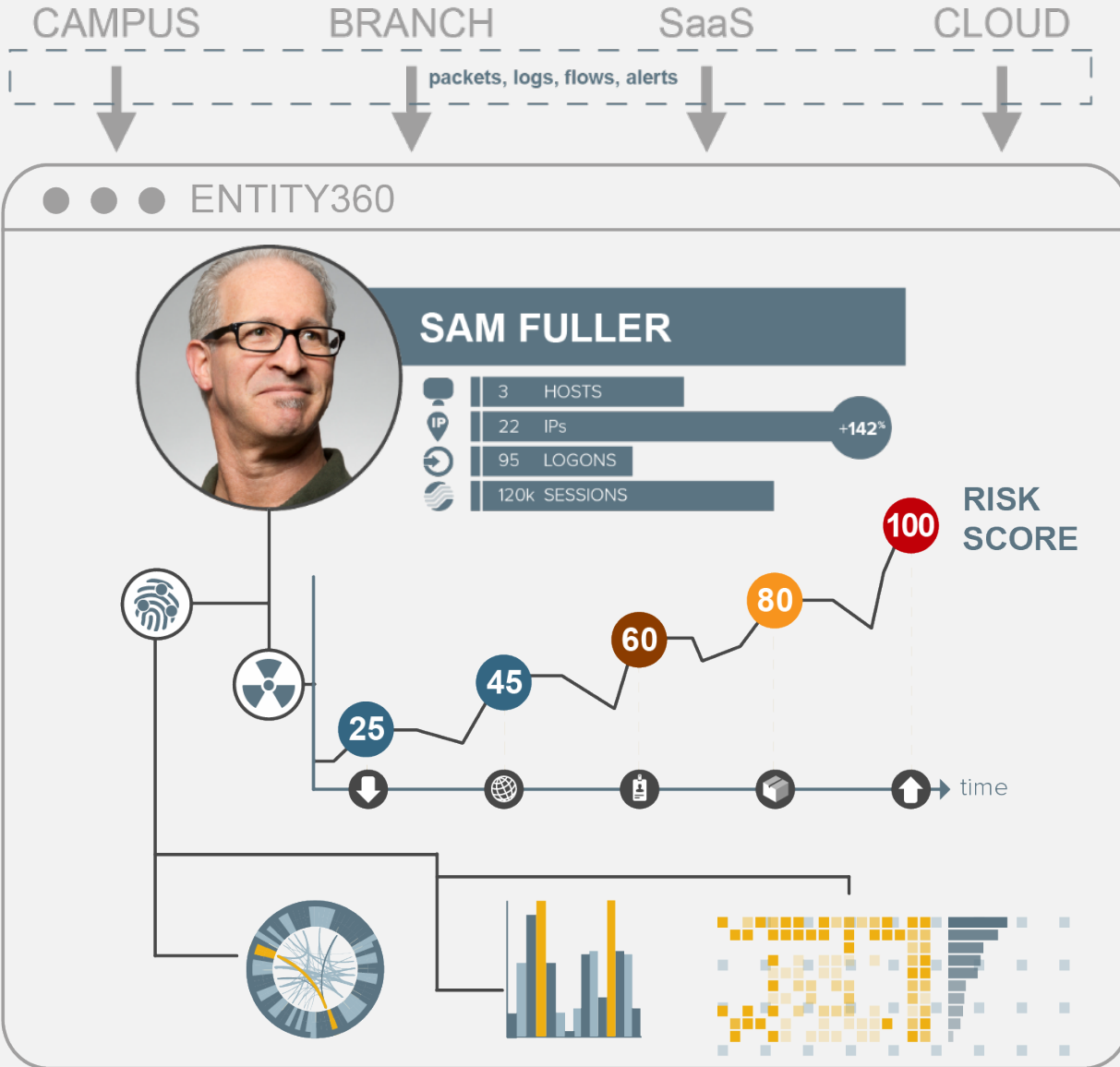
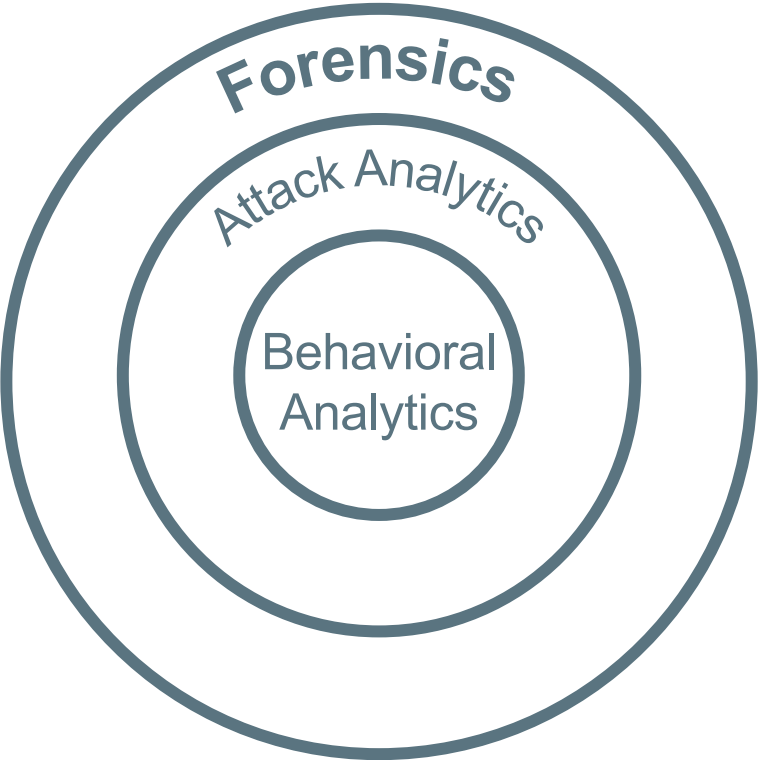
Peer Baseline Anomaly



Finding the Malicious in the Anomalous



Accelerated Investigation and Response



Introspect Analyzer Deployment Options



2RU Appliance



1RU Scale Out



Customer
Public/Hybrid Cloud
(AWS)



ClearPass + IntroSpect = 360° Protection

1. Detect and Authorize

Wired/Wireless
Device Authentication

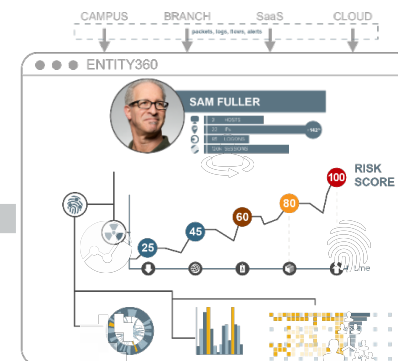


**ClearPass
Policy Manager**

User/Device
Context

Change network
access

IntroSpect UEBA



Entity360 Profile
with Risk Scoring

2. Monitor and Alert

3. Decide and Act

ClearPass Real-time Policy-based Actions

- Real-time quarantine,
- Re-authentication
- Bandwidth Control
- Blacklist



For who? High Value Assets, SOC efficiency

CHALLENGE

INTROSPECT SOLUTION



F50 Financial

- Monitoring privileged user activity
- Improve SOC efficiency

- Behavioral analytics on AD, email, VPN, network
- FireEye alert context for investigations



Legal

- Concerned about **IP** theft
- Lacking user-level visibility and profiling

- Behavioral analytics
- User-level visibility



High Tech

- Security analytics initiative to supplement existing SIEM and detection systems

- User Behavior Analytics
- Splunk integration



F50 Insurance

- Alert white noise and overwhelmed SOC
- Splunk not delivering value

- DLP and DNS Analytics
- SOC efficiency through machine intelligence



F50 High Tech

- **High Value asset** protection

- Behavioral analytics for insider activity to high value assets
- User activity association with key assets

IntroSpect Summary

Diverse Data Sources

FOR

Analytics + Forensics

SUPPORTING

Attack Detection + Incident Investigation

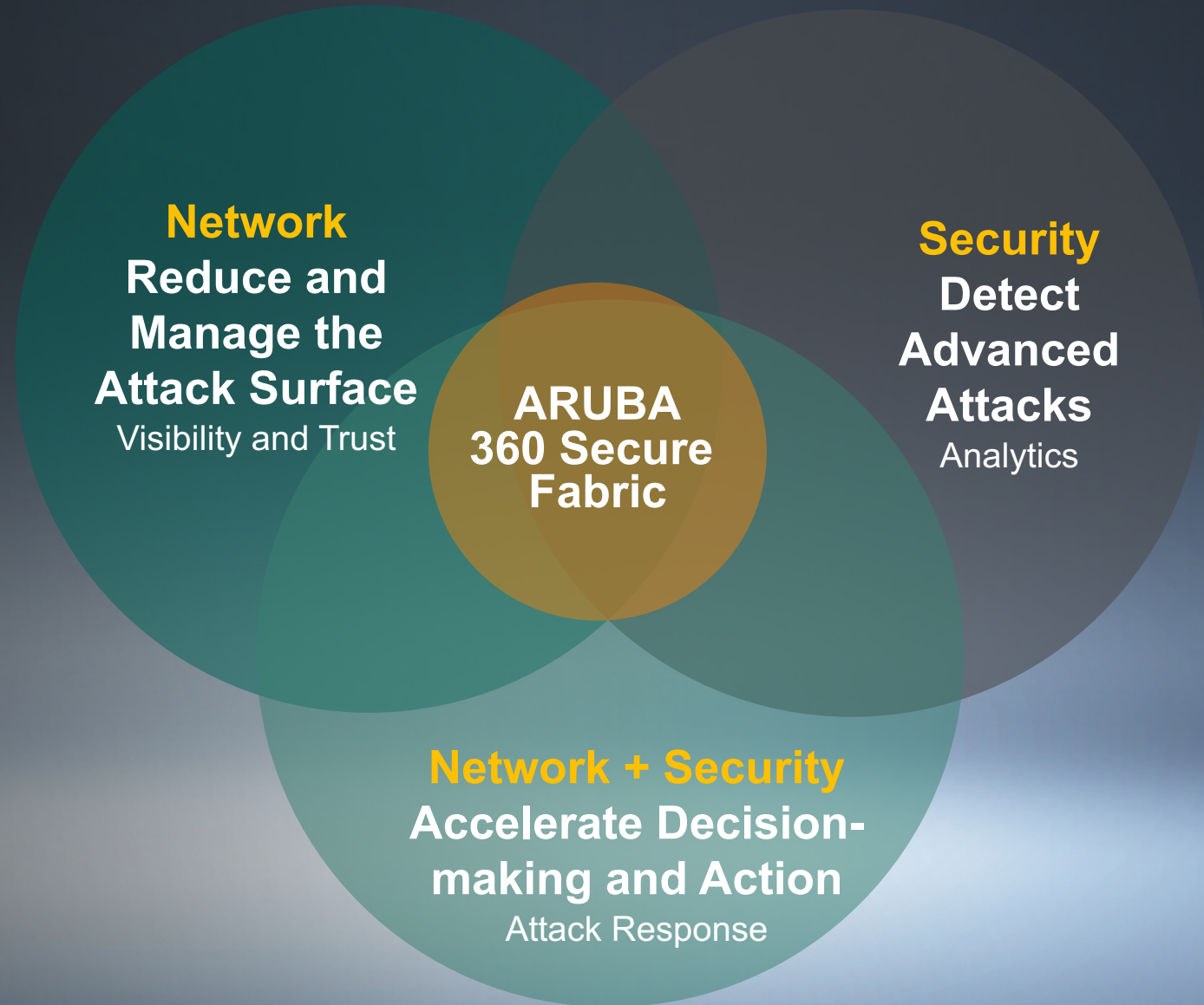
ALL IN A

Self-Contained Solution + Open Platform

AVAILABLE

Streamlined for Aruba Networks + Scaled for Enterprise UEBA

THE NEW SECURITY IMPERATIVE



airheads

TECH TALK *LIVE*