



AIRHEADS

meetup

aruba
a Hewlett Packard
Enterprise company

Colorless Ports & Micro Segmentation for wired networks

Aruba 360 Secure Fabric live in action!

15 februari 2018

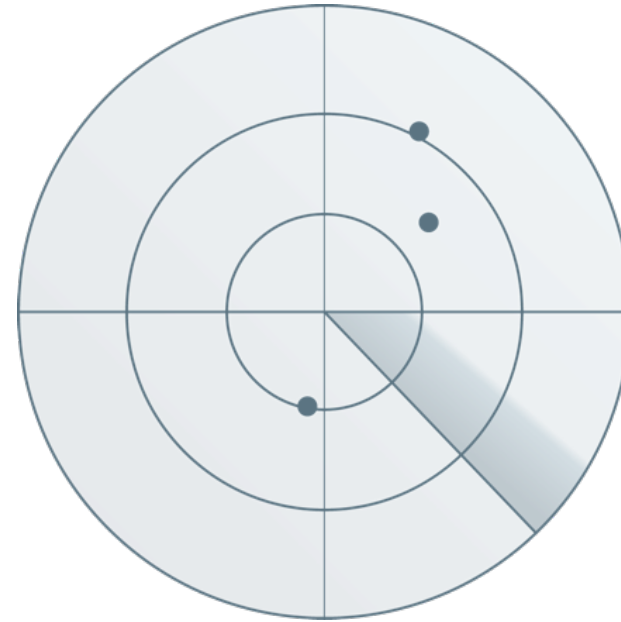
Herman Robers EMEA Consulting Systems Engineer Security

#ArubaAirheads

Agenda

- Aruba 360 Secure Fabric
 - Intro, overview, context
- Wired Colorless ports
 - Architecture
 - Components
 - Per port tunneled node
 - Per user tunneled node
- Live demo
 - Colorless ports, 802.1X, MAC, Profiling
 - Per user tunneled node
- Q&A

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

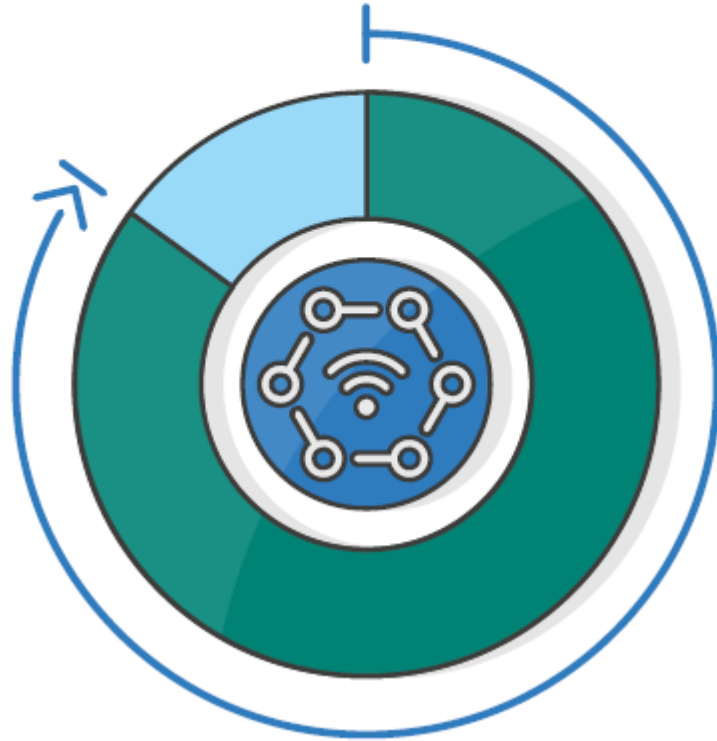
ARE QUICKLY INNOVATING &
ADAPTING



BATTLEFIELD

WITH IOT AND CLOUD, SECURITY
IS BORDERLESS

You already have IoT...



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

...it got worse



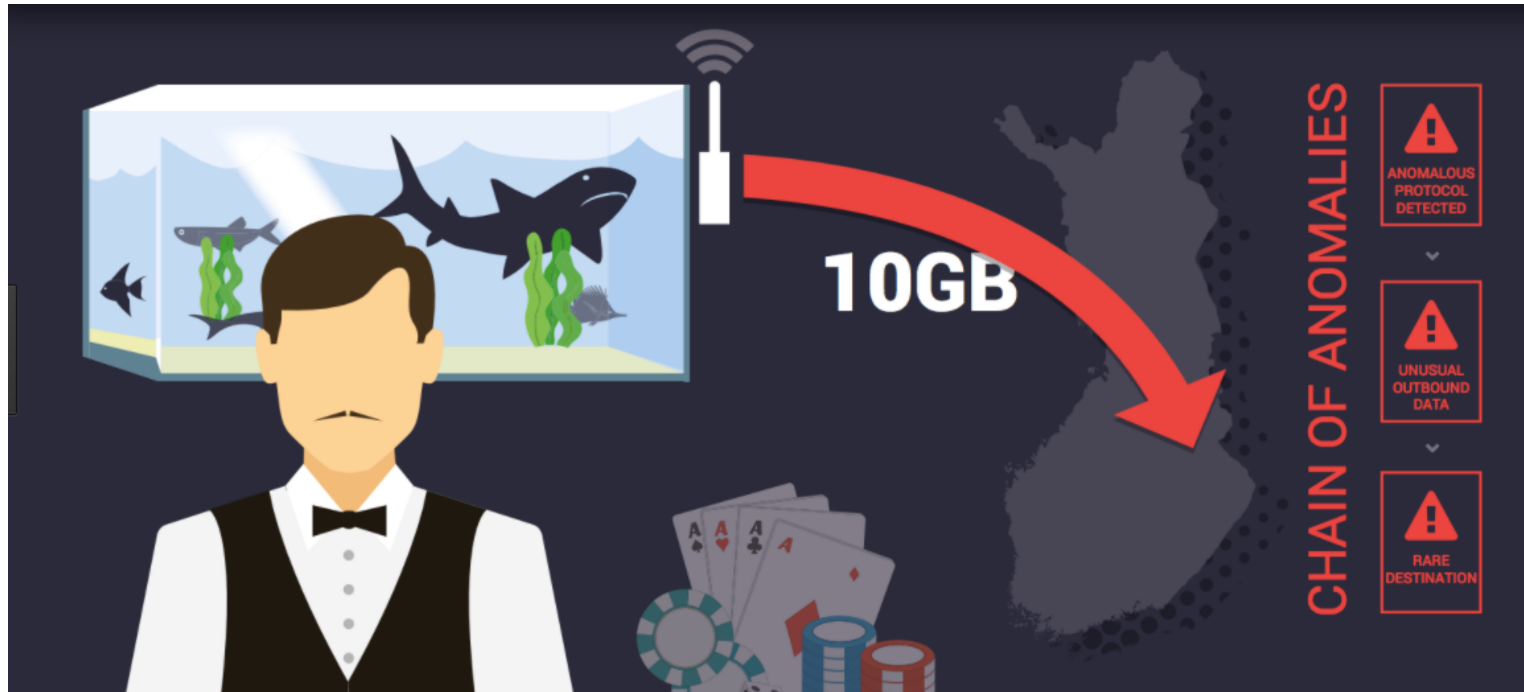
**8 out of 10
organizations**
have experienced
an IoT-related
security breach.³

...it got worse



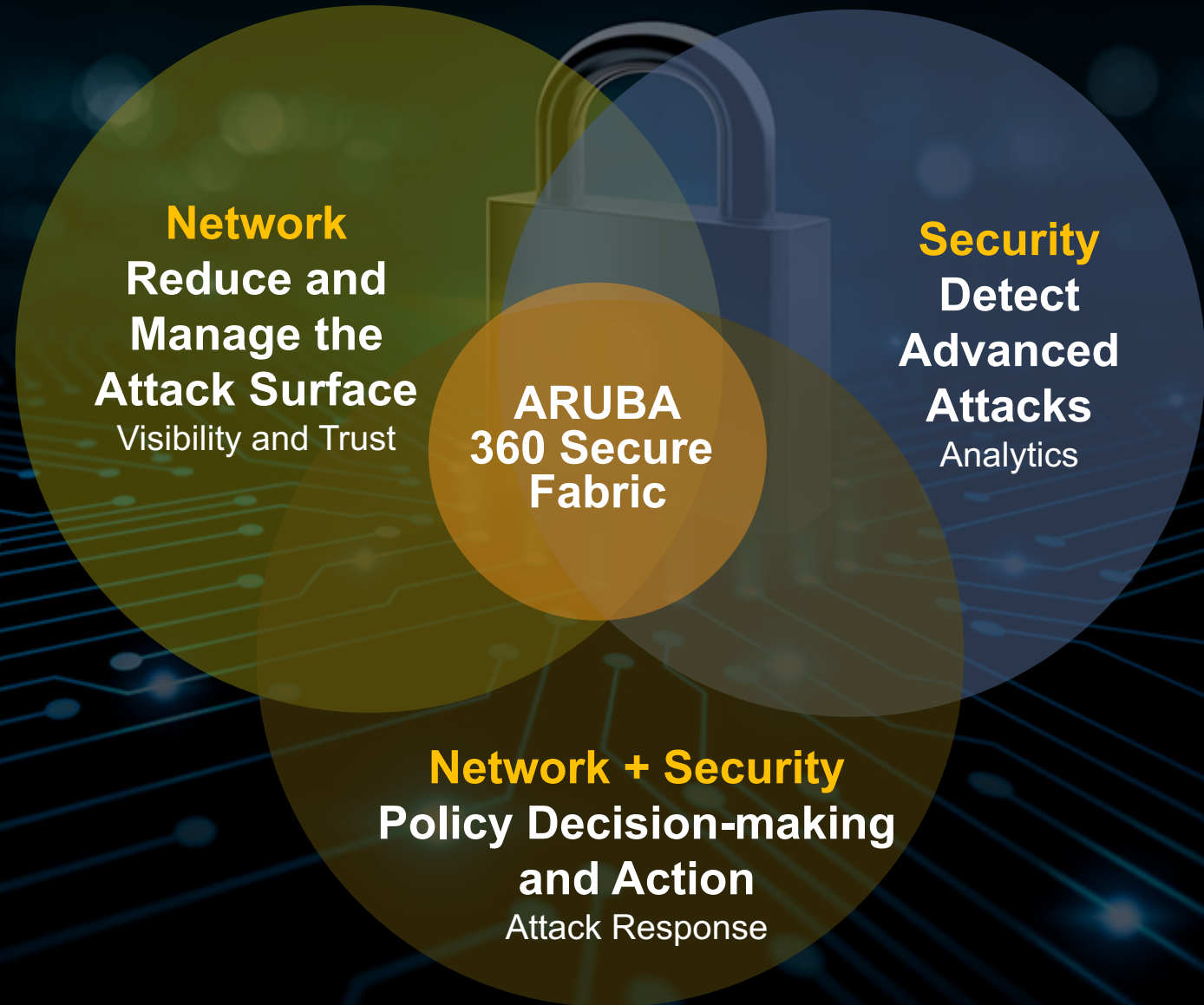
**8 out of 10
organizations**
have experienced
an IoT-related
security breach.³

...it got worse

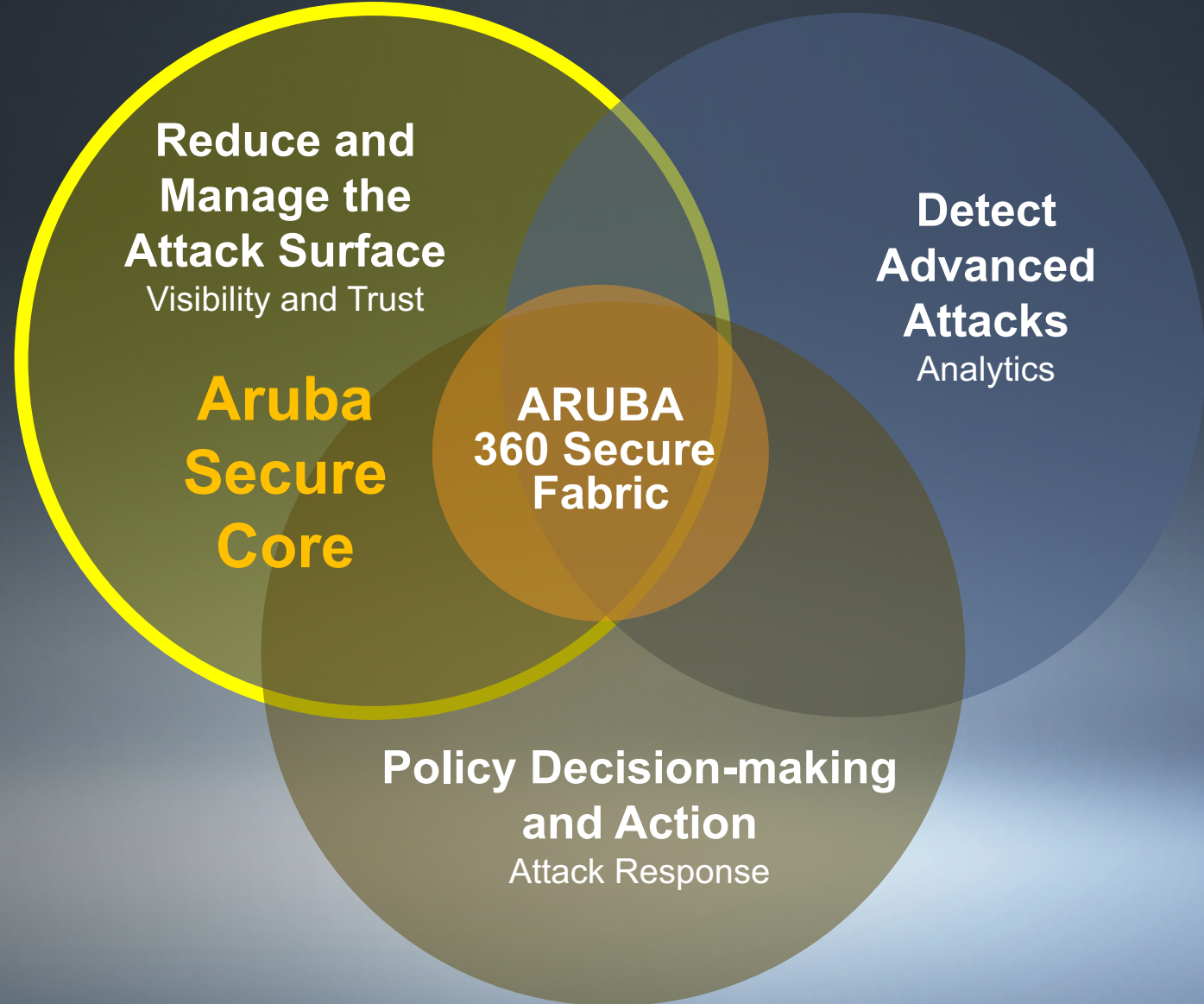


8 out of 10 organizations have experienced an IoT-related security breach.³

THE NEW SECURITY IMPERATIVE

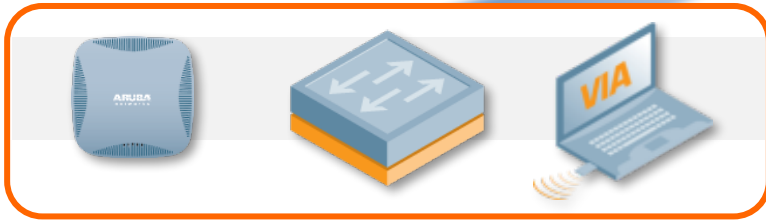
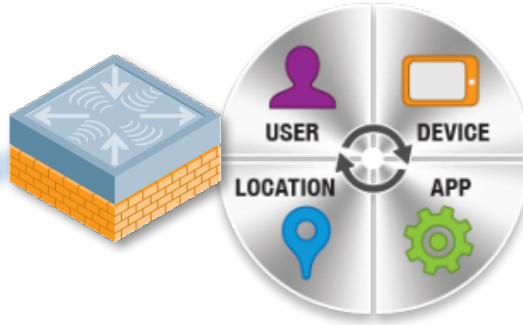


THE NEW SECURITY IMPERATIVE



Role based access networking

ROLE BASED ACCESS
NETWORKING



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

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

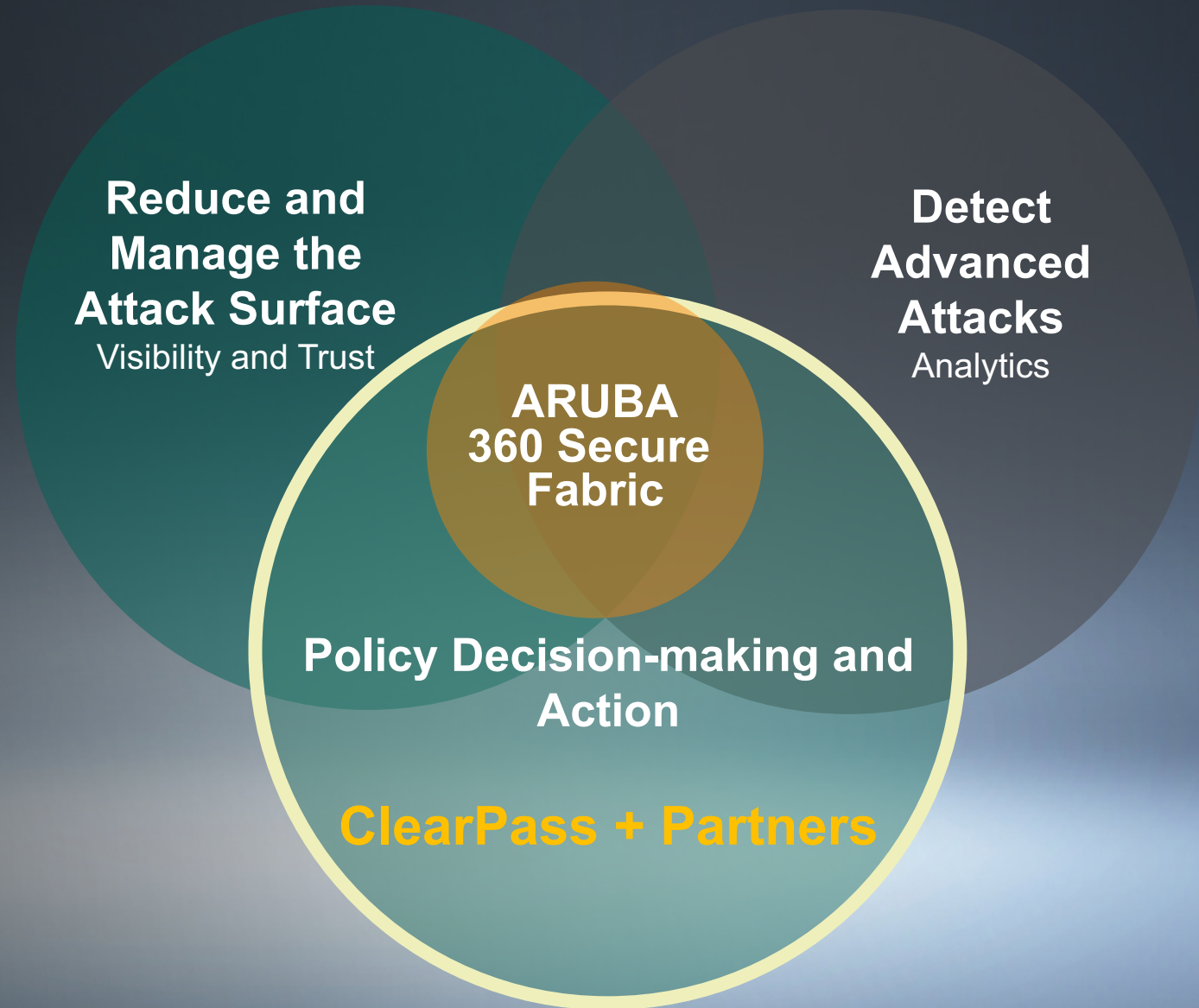
Role Based
access

Firewall
rules

QoS
flow-based

VLAN

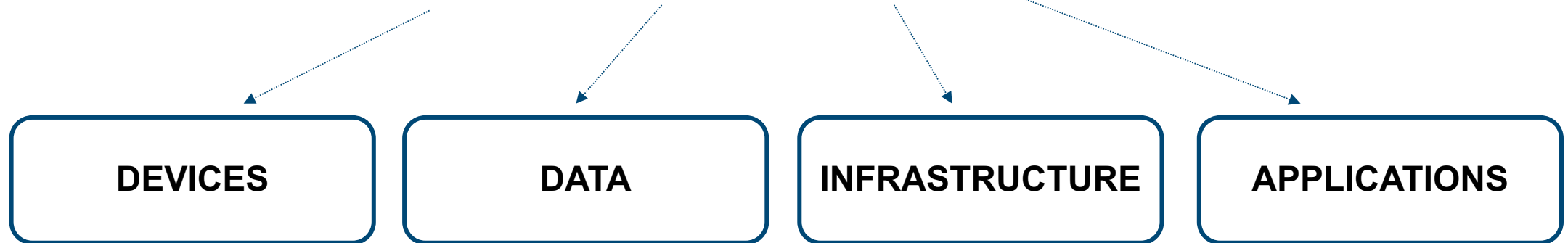
THE NEW SECURITY IMPERATIVE



What does ClearPass do to help?



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

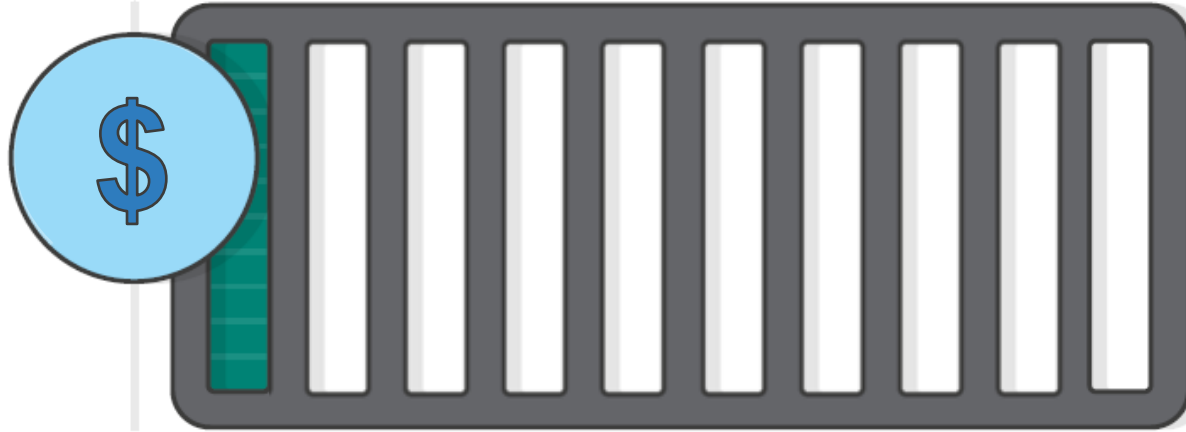


Identify – Enforce – Protect

ClearPass Exchange: End to End Controls

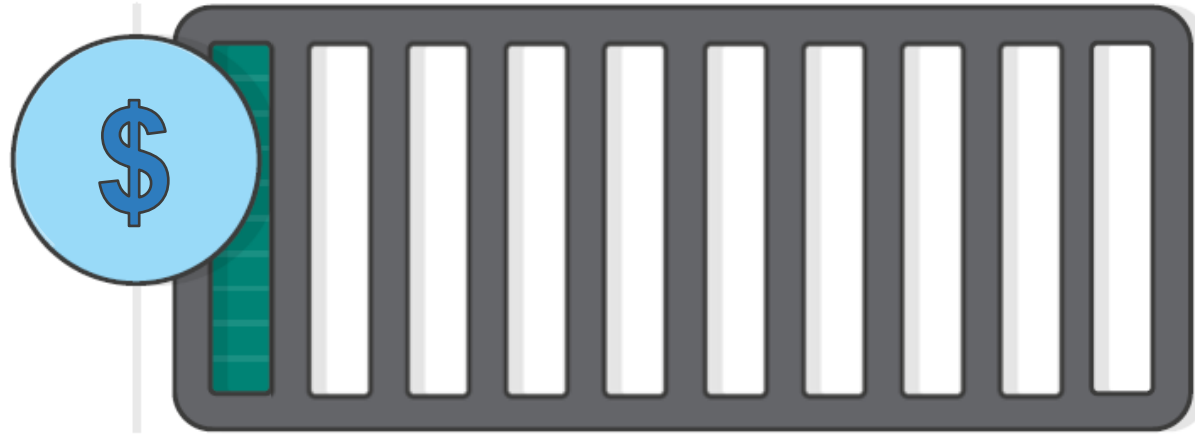


Where are we placing our bets?



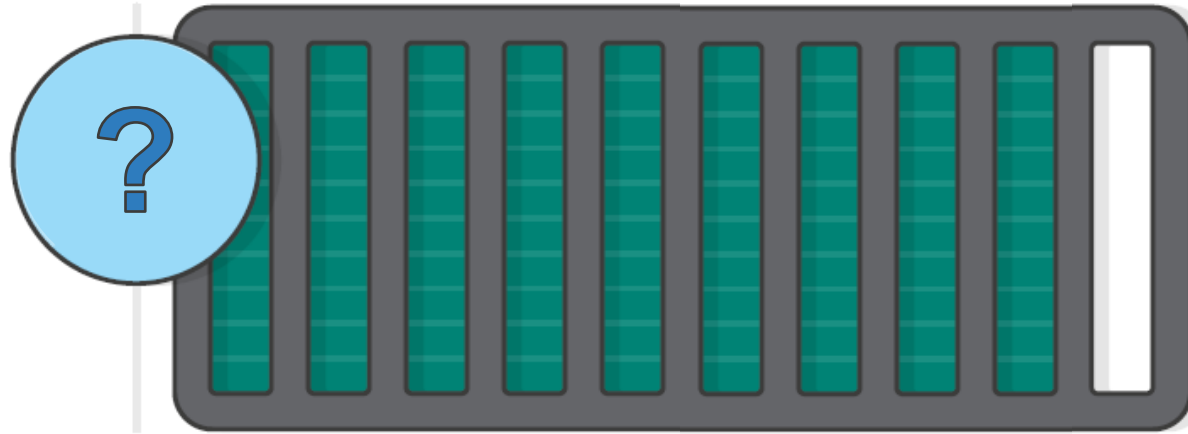
- Organizations spend an average of 5.6% (between 1 and 13%) of the overall IT budget on IT security and risk management. (Gartner Dec. 2016)
- Average consolidated cost of a breach = \$4 Million (Ponemon Institute 2016)

Where are we placing our bets?

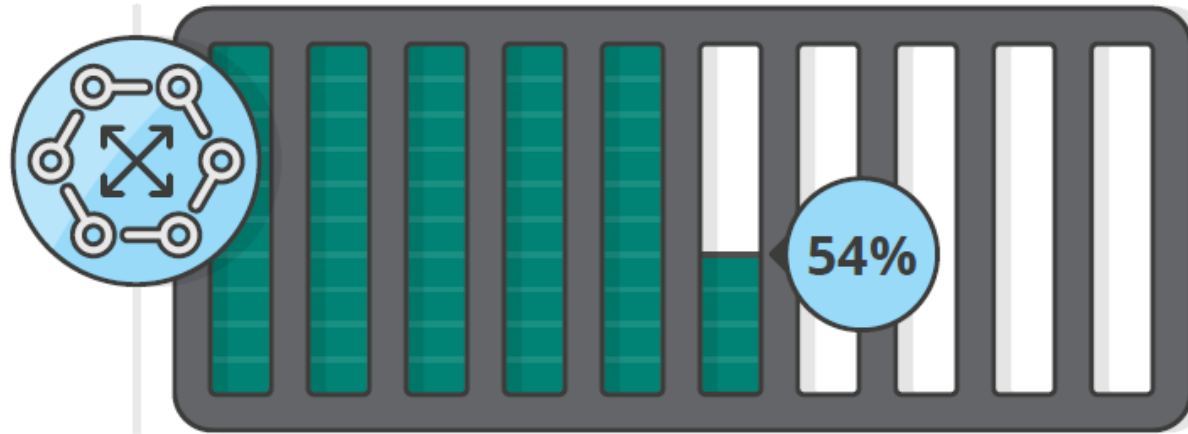


- **Perimeter Defense (Firewalls, IPS etc)**
 - **Endpoint Security**
 - **Log Management**
- **Vulnerability Management**

What about the Security team?

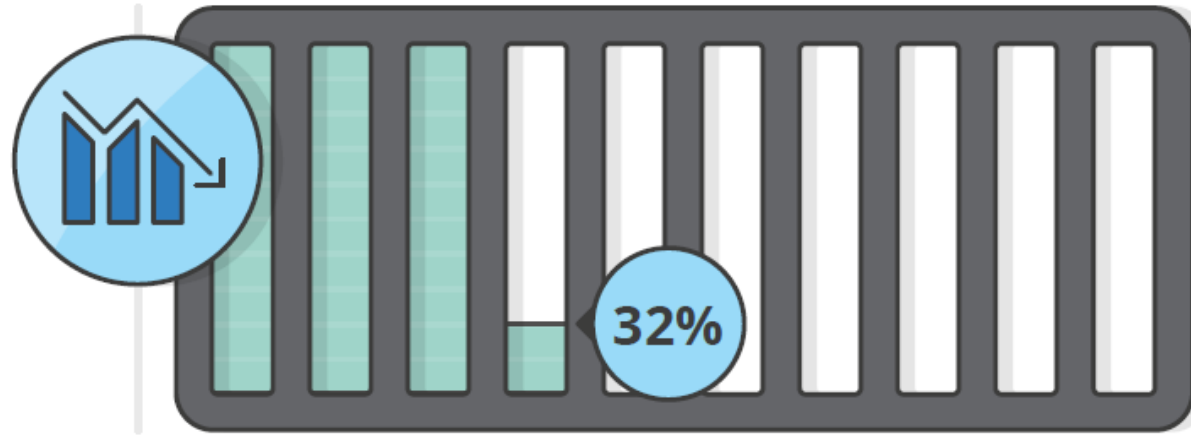


What about the Security team?



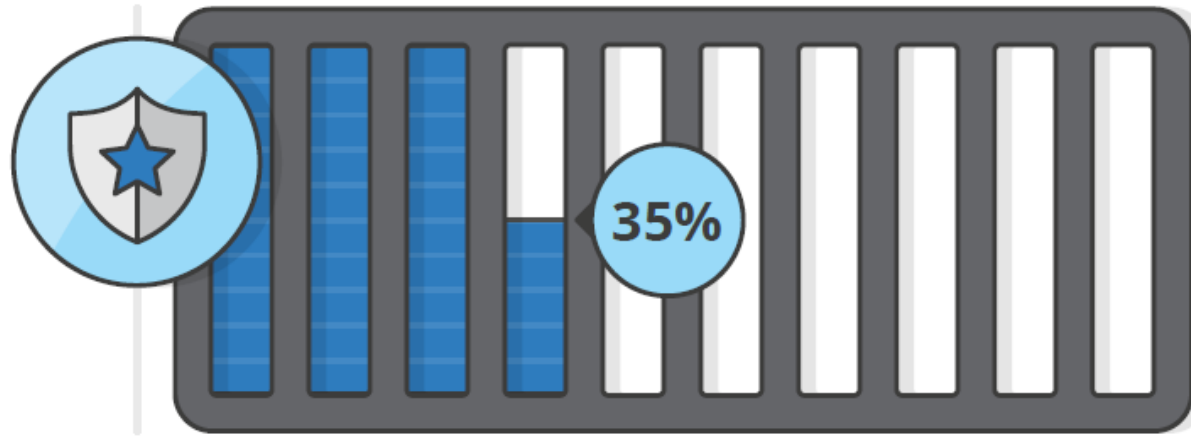
Most say the cybersecurity skills shortage has increased workloads, overloaded analysts.

What about the Security team?



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

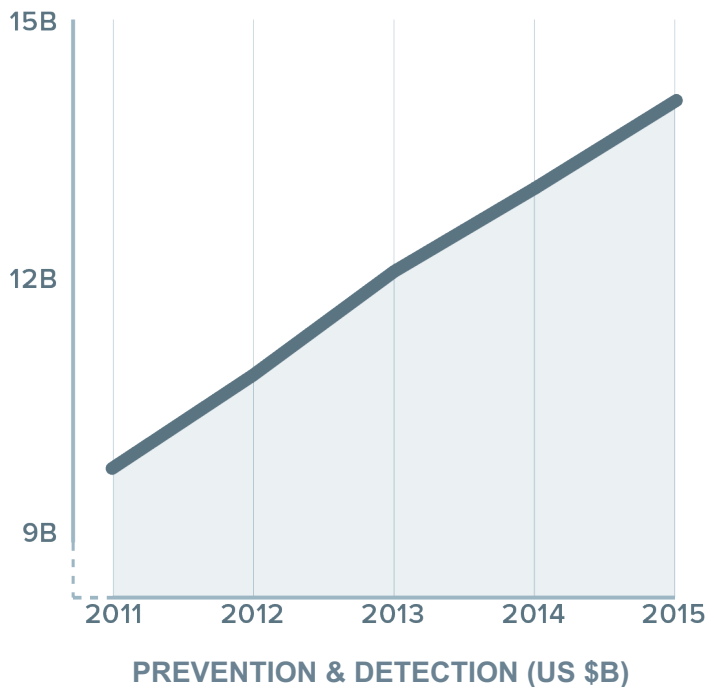
What about the Security team?



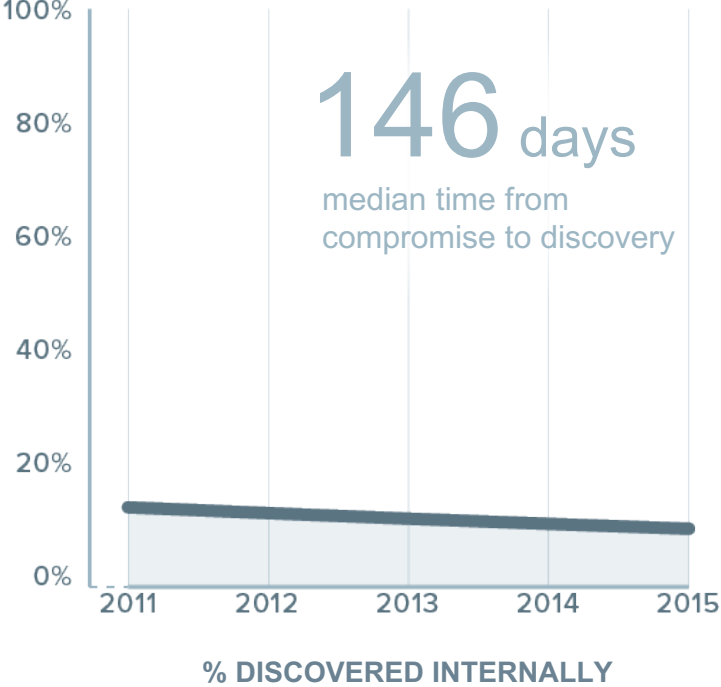
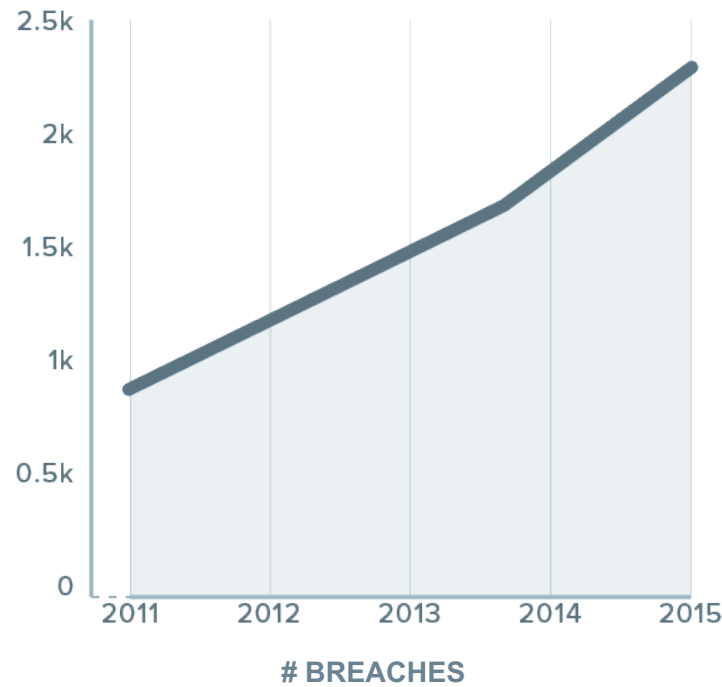
Over 1/3 can't utilize security technologies to their full potential, decreasing effectiveness.

The Security gap

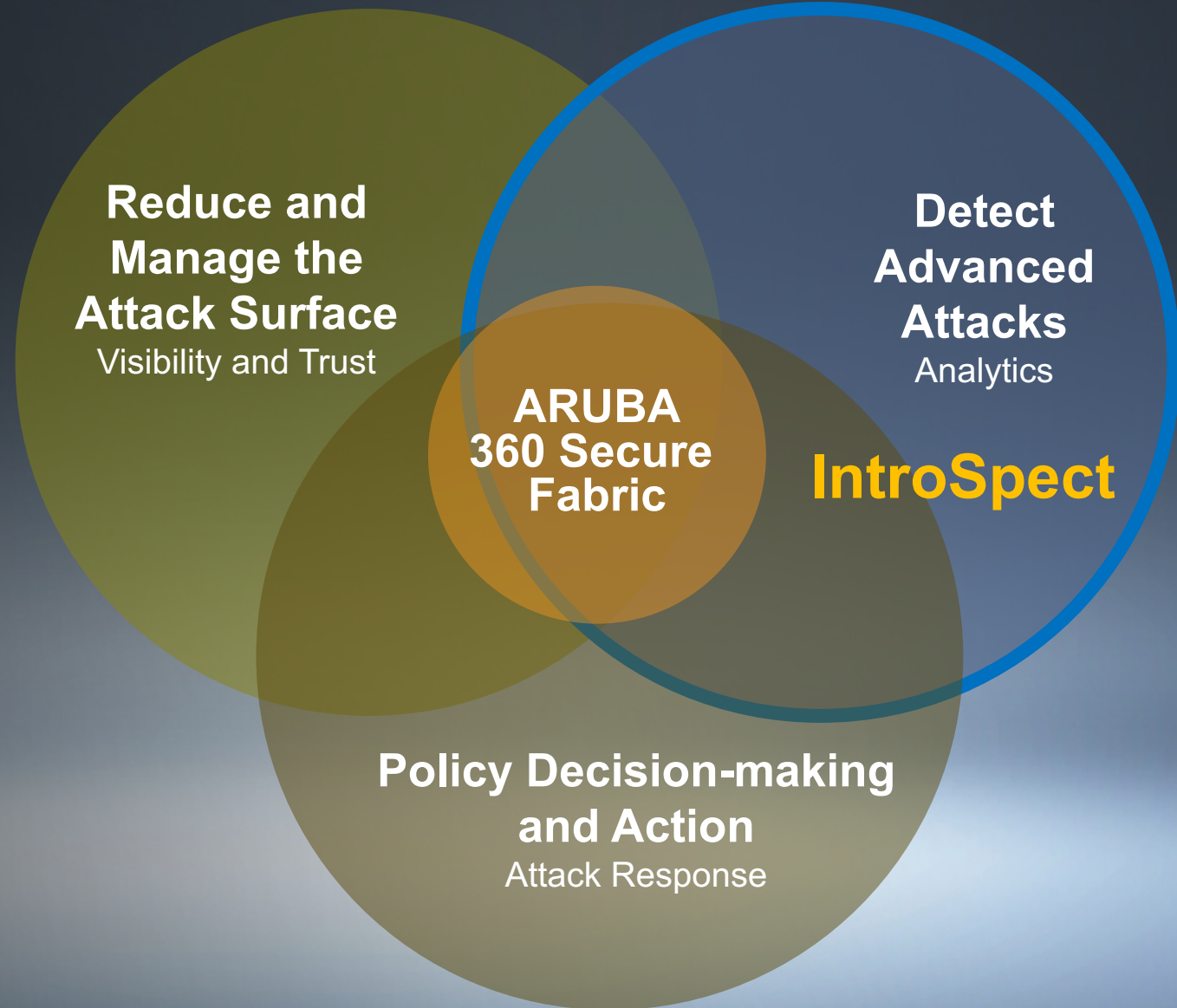
SECURITY SPEND



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.

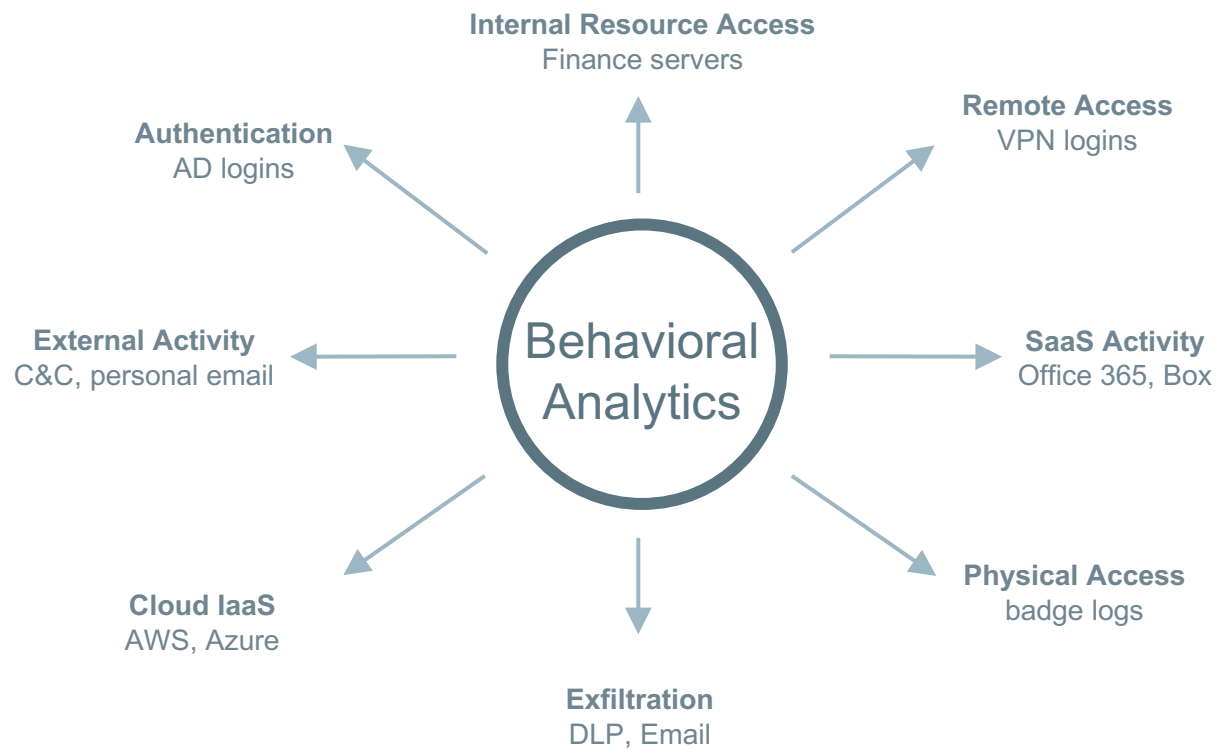


EFFICIENCY AND EFFECTIVENESS

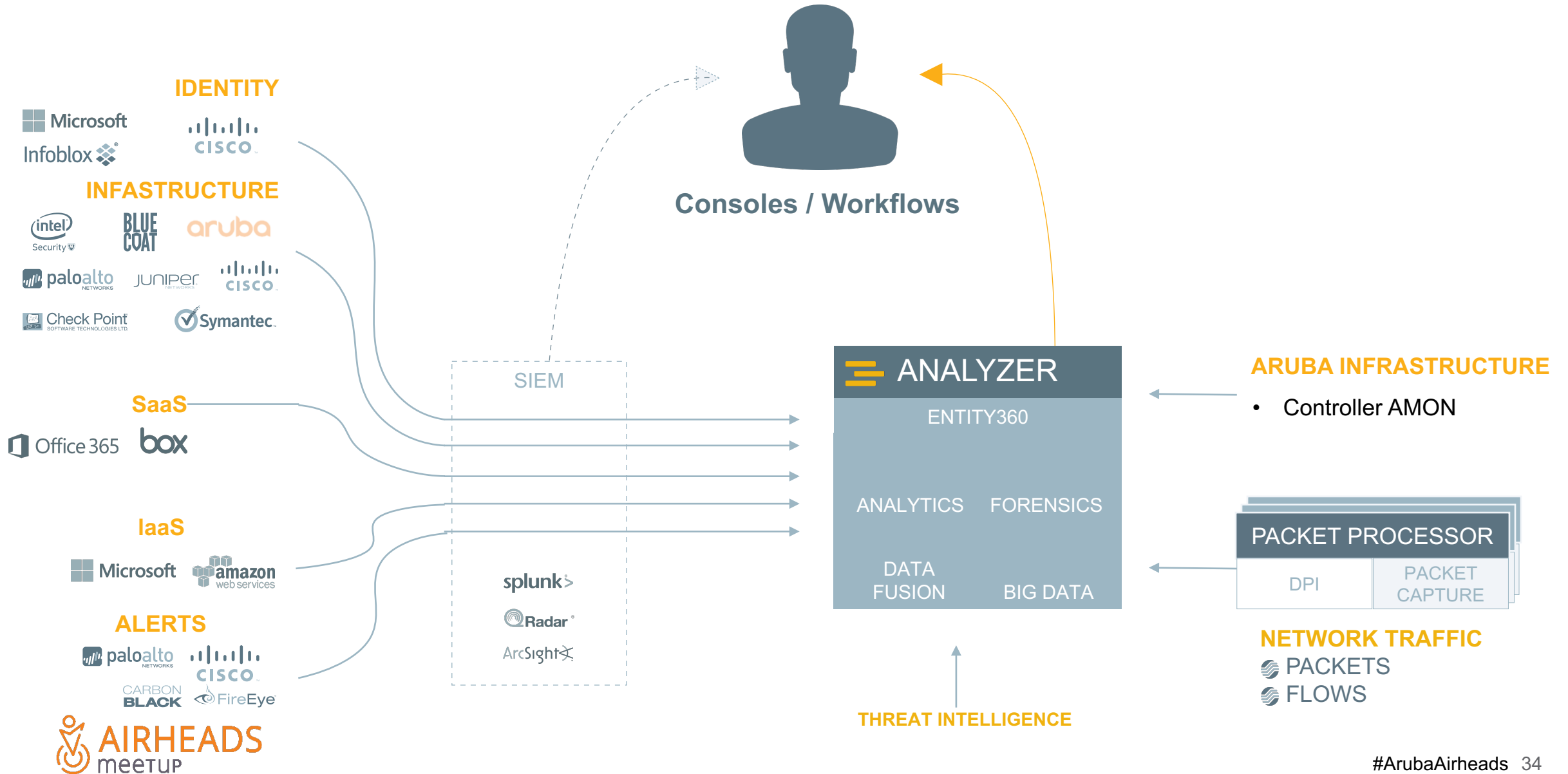
of the security team

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

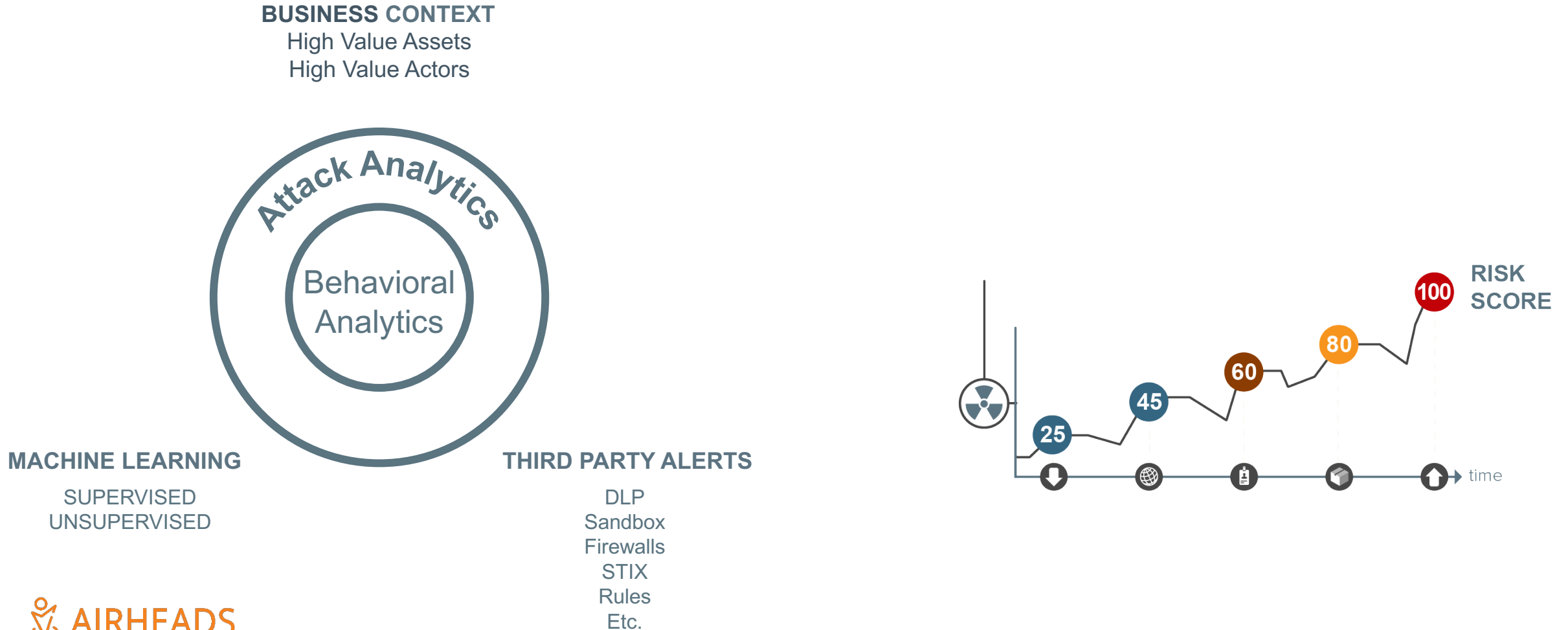
Behavior – Many Different Dimensions



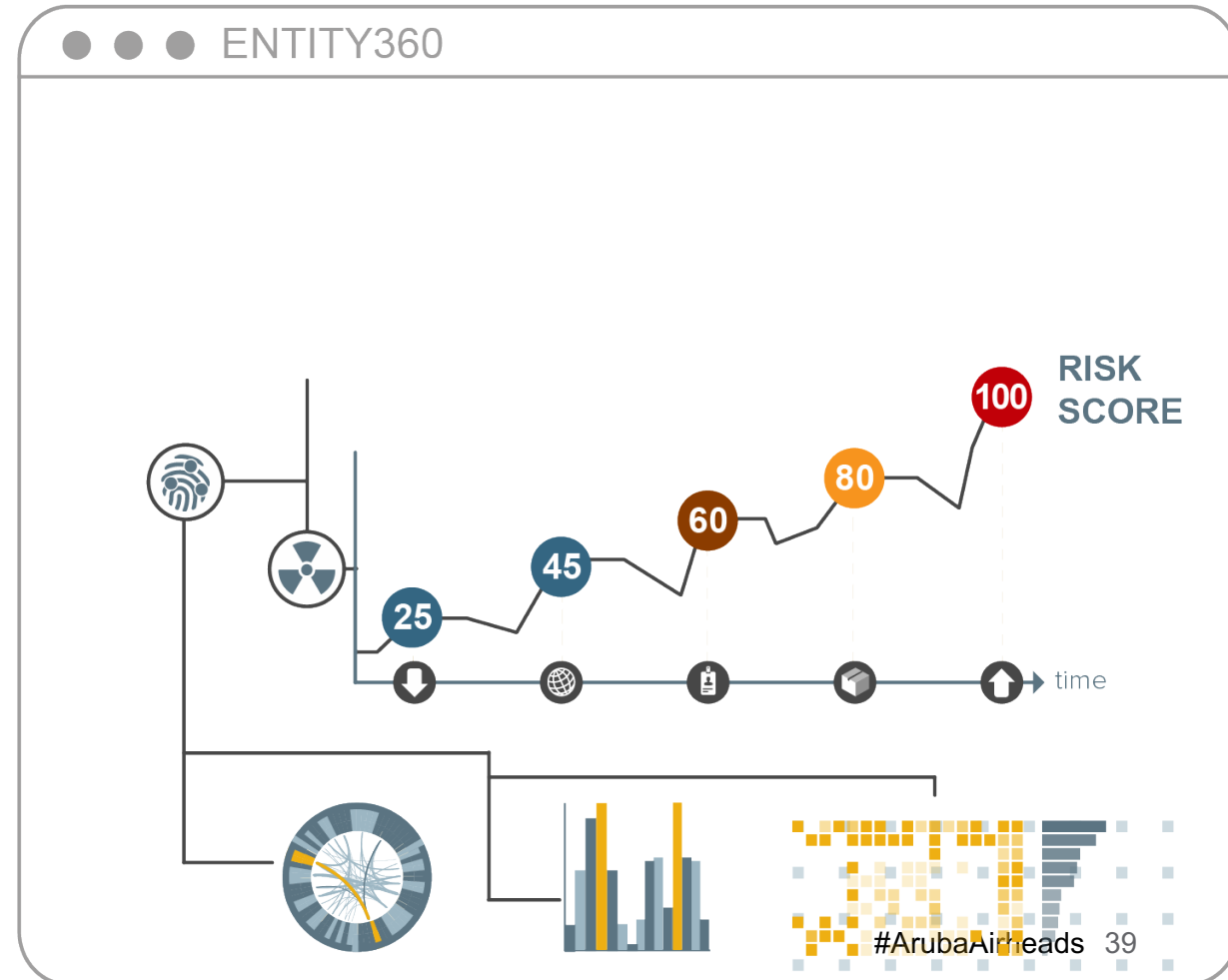
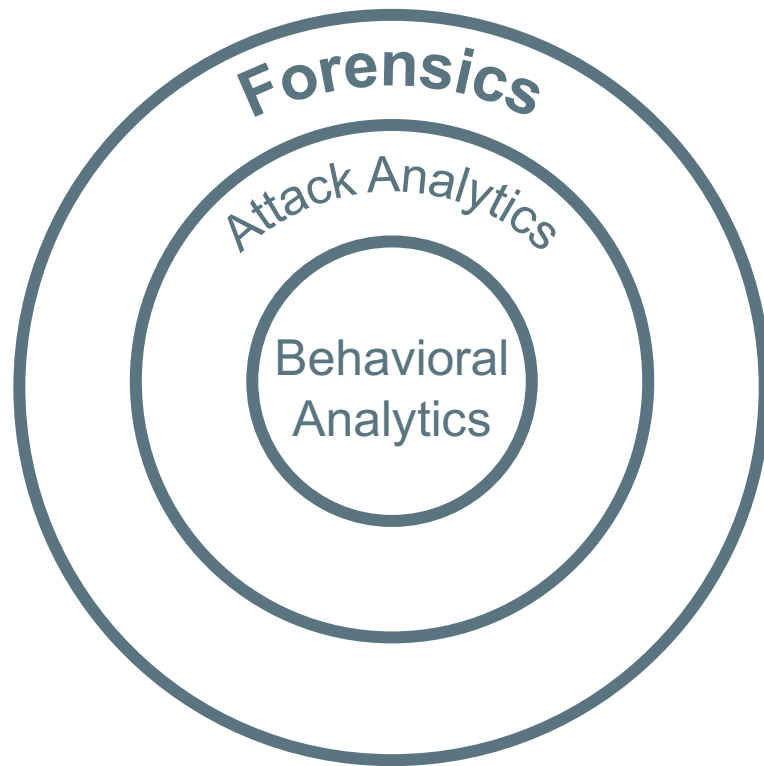
SOLUTION – INTEGRATED WITH SECURITY ECOSYSTEM



Finding the Malicious in the Anomalous



Accelerated Investigation and Response



IntroSpect Summary

Diverse Data Sources

FOR

Analytics + Forensics

SUPPORTING

Attack Detection + Incident Investigation

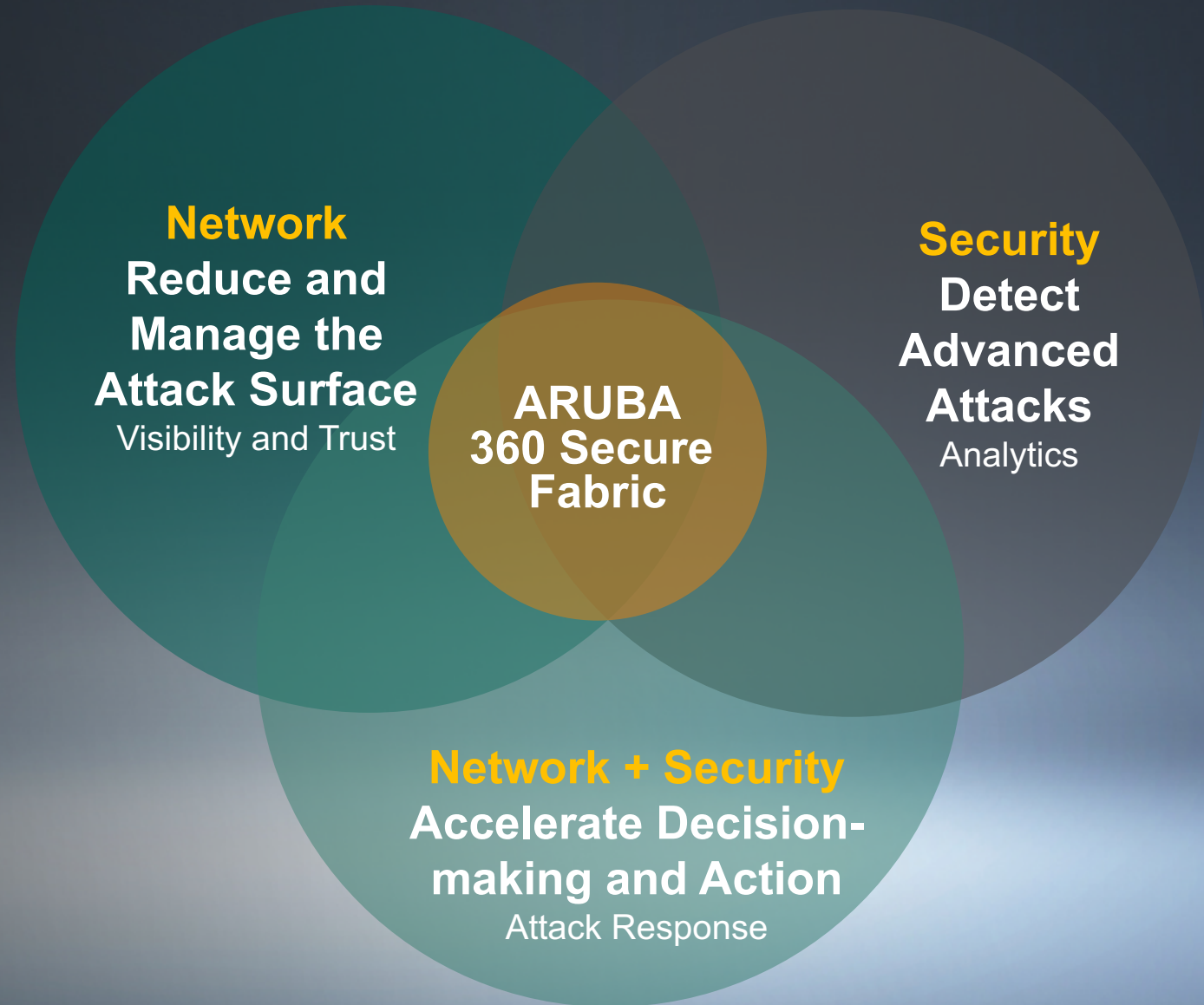
ALL IN A

Self-Contained Solution + Open Platform

AVAILABLE

Streamlined for Aruba Networks + Scaled for Enterprise UEBA

THE NEW SECURITY IMPERATIVE



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

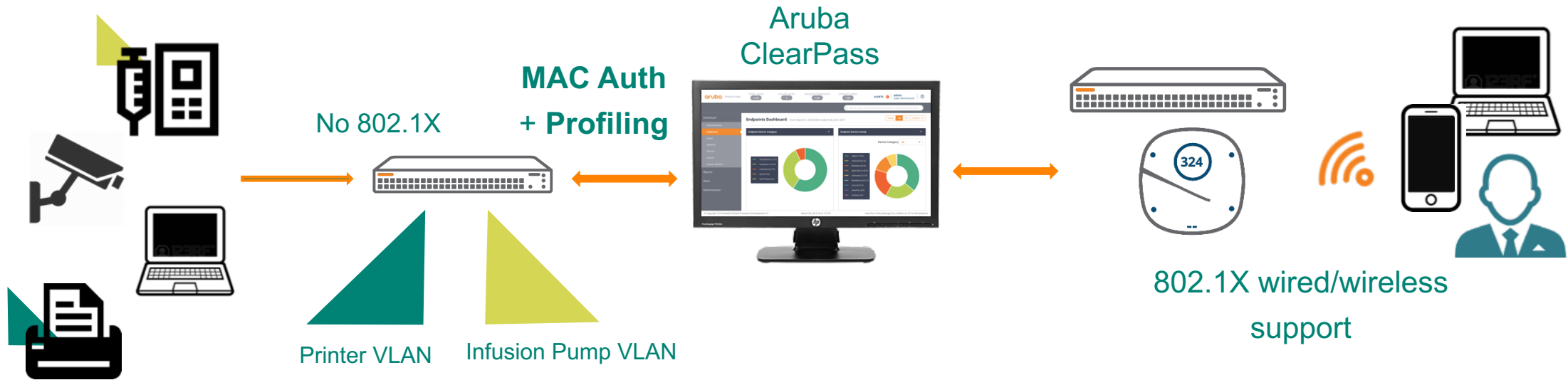


50% of IoT may be
wired



- 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.

Colorless ports benefits

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

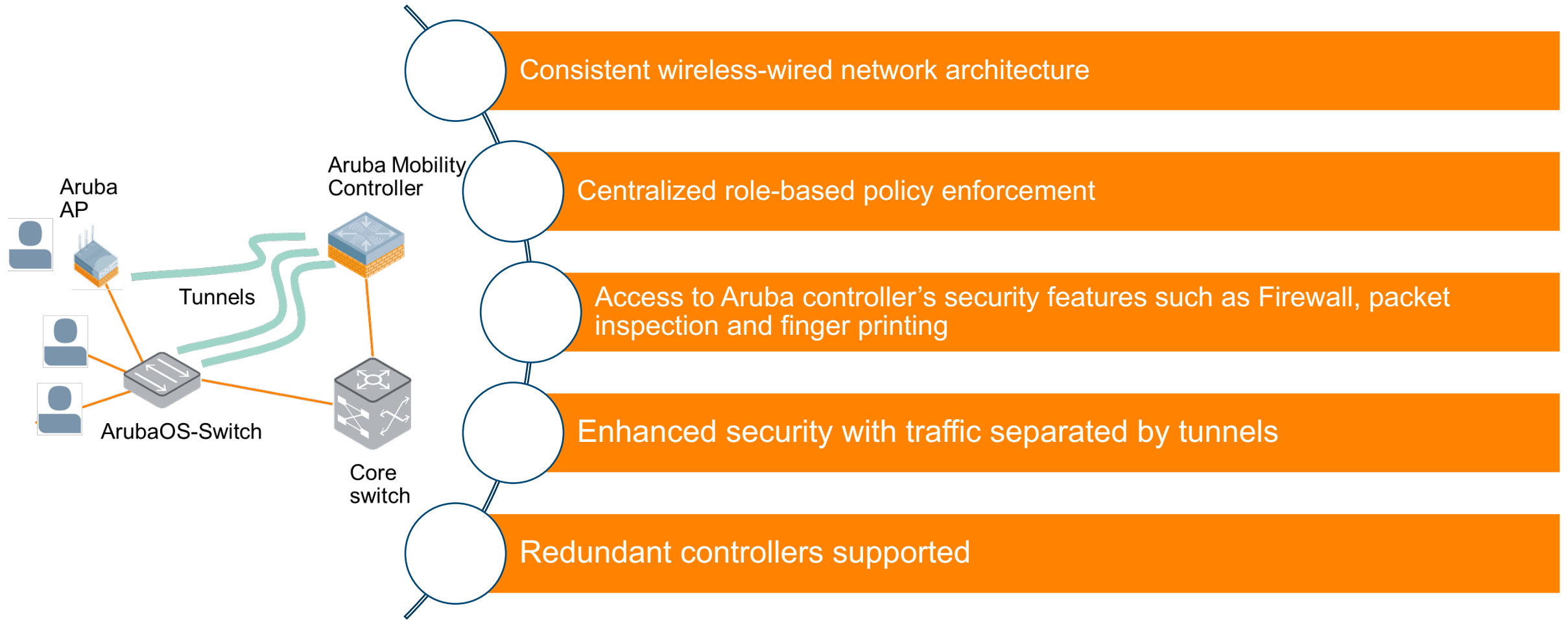
Simplified switch configuration

- all access ports are configured the same

Tunneled Node

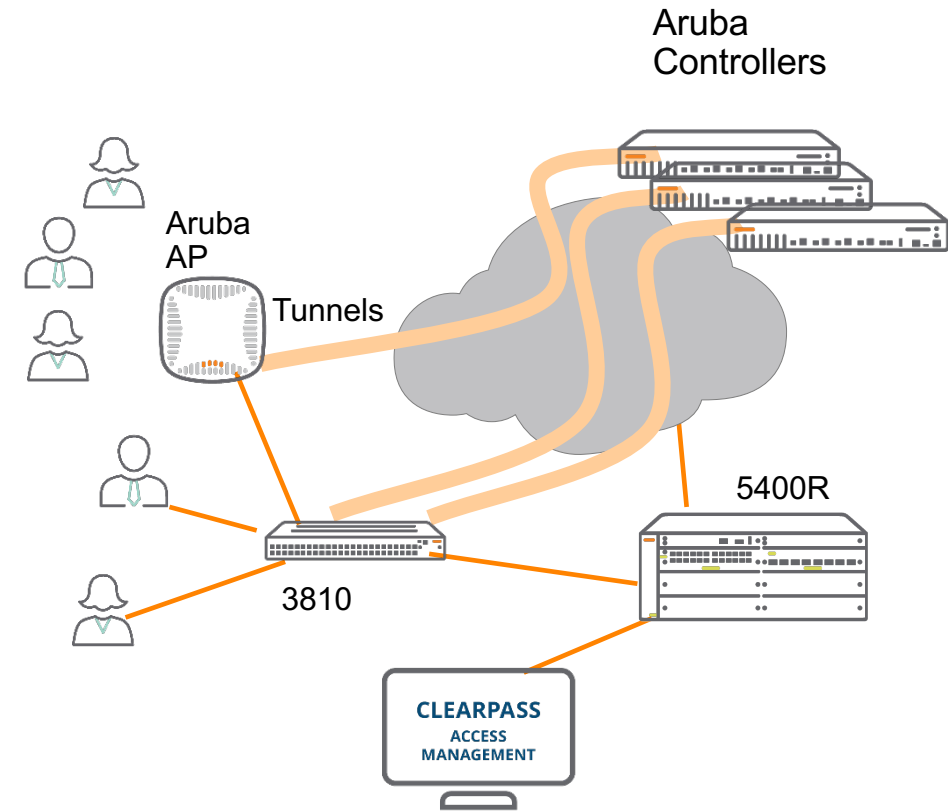
Suppose your switch is a wired access point

Tunneled Node: 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
 - Requires AOS 8.1 or later in the controllers



Policy source and enforcement for different scenarios

Scenario	Datapath & Policy Enforcement	Switch mode	Policy decision	Policy/role Content
Colorless ports with dACL	Local switch	Standard	ClearPass	ClearPass
Colorless ports with Role based access	Local switch	Role based access	ClearPass (fallback local)	Local switch
Per port tunneled node	Mobility controller	Either mode	ClearPass (L2 fallback controller)	Mobility controller
Per user tunneled node	Switch (local) / Controller (tunneled)	Role based access	ClearPass (fallback local)	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)
Less moving parts
- You have both options available in your toolkit.

Policy/role
Content

ClearPass

Local switch

Mobility controller

Switch (local) /
Controller
(tunneled)

Tunneled node benefits

Benefits of tunneled node

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

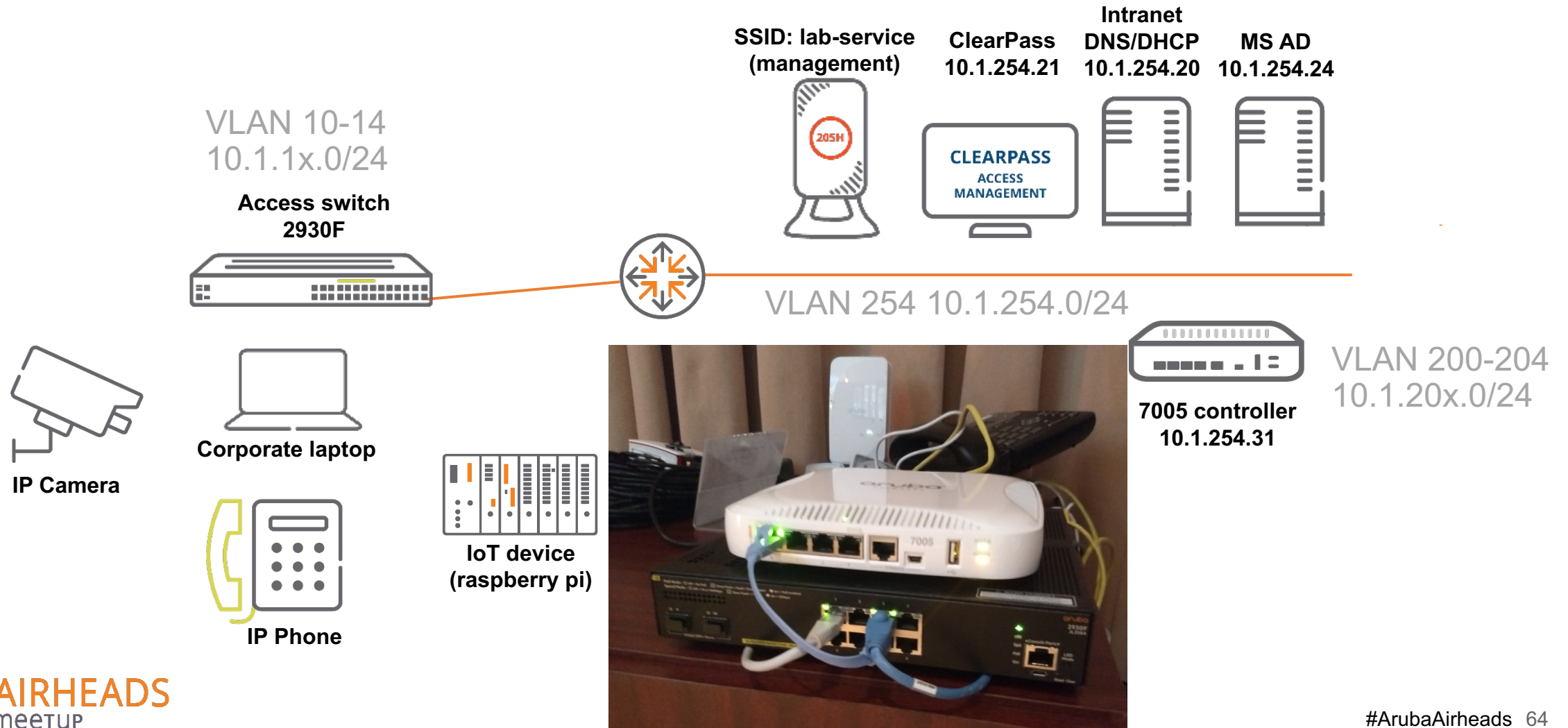
Flexible where needed with per user tunneled node

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

Tunneled Node Demo

When the rubber meets the road!

Demo setup colorless ports and tunneled node



Configuration (switch local role)

```
aaa authorization user-role enable
```

```
class ipv4 "class-ipcam"
```

```
    10 match ip 0.0.0.0 255.255.255.255 10.1.254.24 0.0.0.0
```

```
    20 match ip 0.0.0.0 255.255.255.255 10.1.254.20 0.0.0.0
```

```
    exit
```

```
class ipv4 "class-dhcp-dns"
```

```
    10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
```

```
    20 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
```

```
    exit
```

```
class ipv4 "class-internal"
```

```
    10 match ip 0.0.0.0 255.255.255.255 10.1.254.0 0.0.0.255
```

```
    exit
```

```
policy user "pol-ipcam"
```

```
    10 class ipv4 "class-dhcp-dns" action permit
```

```
    20 class ipv4 "class-ipcam" action permit
```

```
    30 class ipv4 "class-internal" action deny
```

```
    exit
```

```
aaa authorization user-role name "camera"
```

```
    policy "pol-ipcam"
```

```
    vlan-id 14
```

```
    exit
```

Configuration (tunneled controller side)

```
ip access-list session logon-minimal
  user any udp 68 deny
  any any svc-dns permit
  any any svc-dhcp permit
  any host 10.1.254.20 svc-ntp permit
  any network 169.254.0.0 255.255.0.0 any deny
  any network 240.0.0.0 240.0.0.0 any deny
```

```
ip access-list session allow-monitoring
  any host 10.1.254.20 any permit
```

```
ip access-list session deny-internal
  any network 10.0.0.0 255.0.0.0 any deny
  any network 172.16.0.0 255.240.0.0 any deny
  any network 192.168.0.0 255.255.0.0 any deny
```

```
ip access-list session deny-any
  any any any deny log
```

user-role "iot-internet-only"

```
access-list session logon-minimal
access-list session allow-monitoring
access-list session deny-internal
access-list session allowall
```

Configuration (switch tunneled role)

```
aaa authorization user-role enable
```

```
vlan 204
```

```
    name "untrust-tun-204"
```

```
    no ip address
```

```
    exit
```

Note: Not assigned to any interface!

```
tunneled-node-server
```

```
    controller-ip 10.1.254.31
```

```
    mode role-based
```

```
    exit
```

```
aaa authorization user-role name "iot-tun"
```

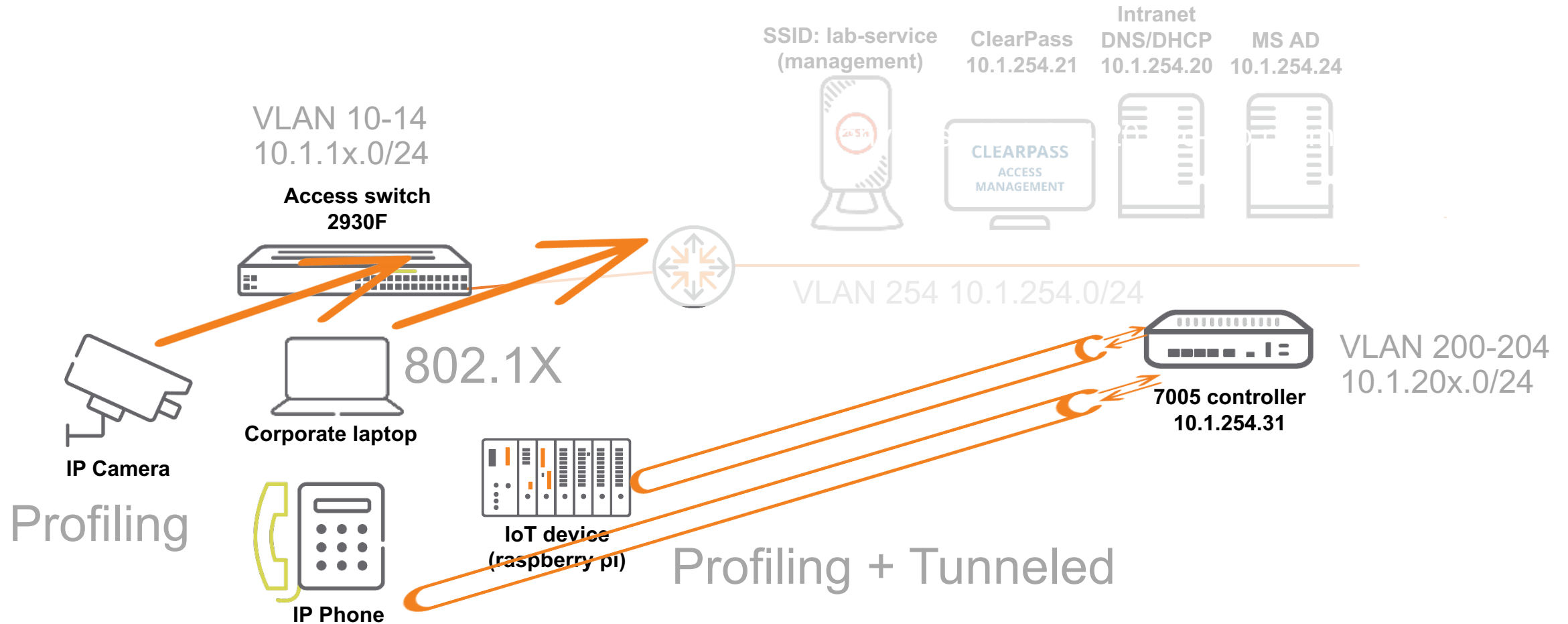
```
    policy "pol-allowall"
```

```
    vlan-id 204
```

```
    tunneled-node-server-redirect secondary-role "iot-internet-only"
```

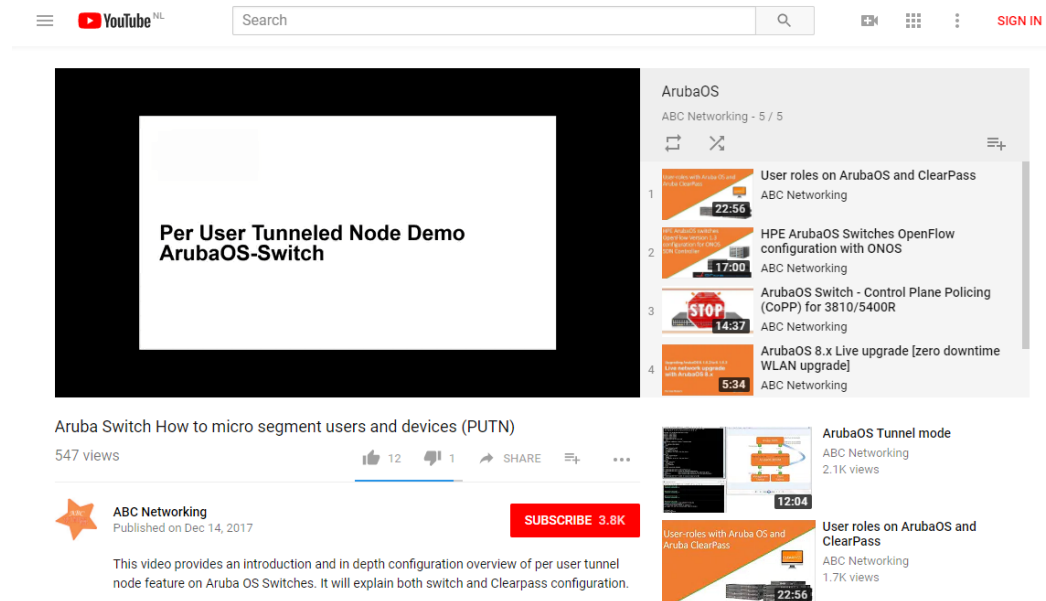
```
    exit
```


Demo setup colorless ports and tunneled node



Where to get more information?

- Wired Policy Enforcement Solution Guide by Tim Cappalli
[support.arubanetworks.com / Airheads](https://support.arubanetworks.com/Airheads)
- ABC Networking YouTube channel
- Arubapedia Mobile-first reference architecture
https://afp.arubanetworks.com/afp/index.php/Mobile-first_reference_architecture

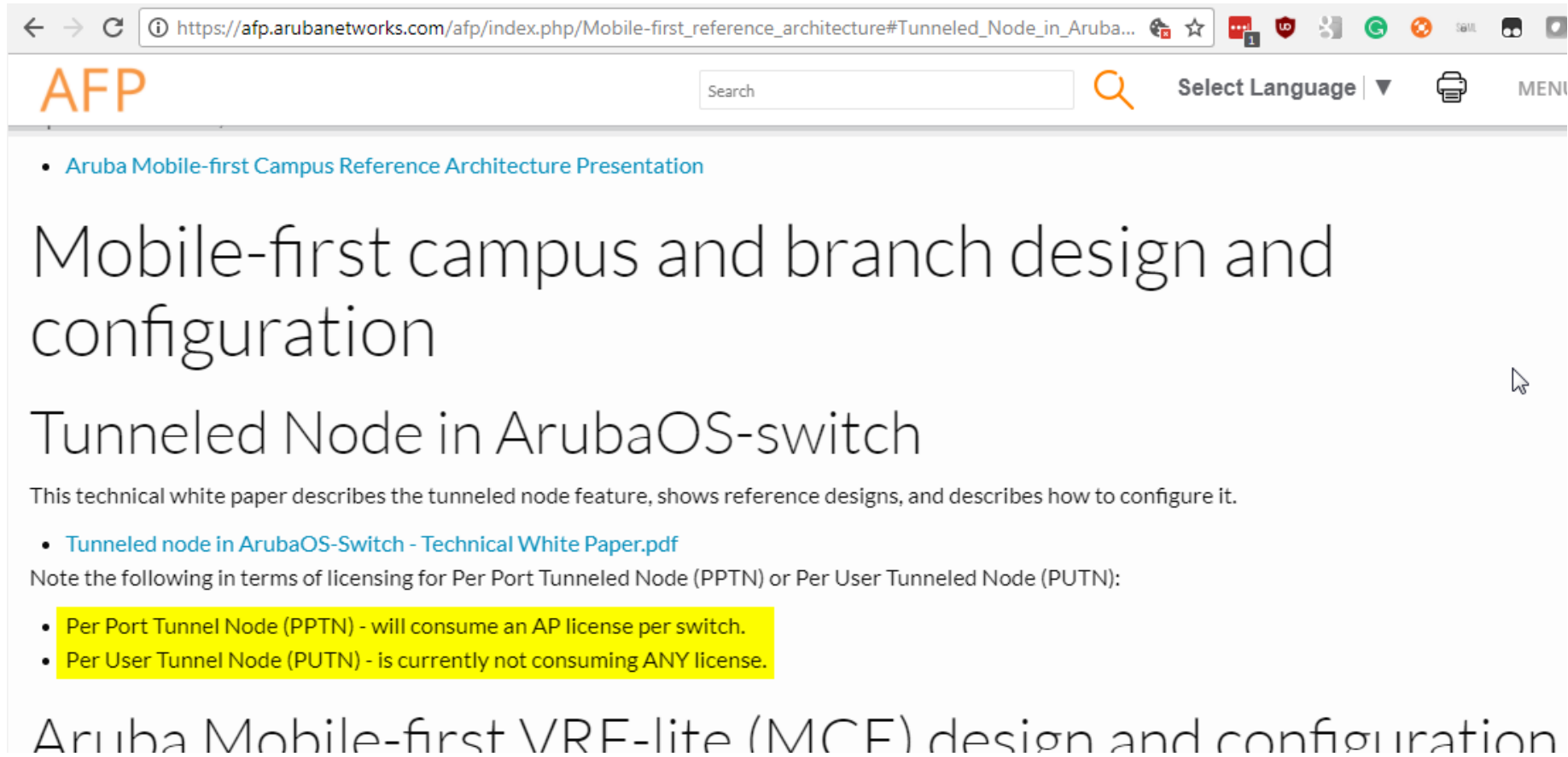


Wired Policy
Enforcement

aruba
a Hewlett Packard
Enterprise company
ClearPass

Solution Guide

Licensing



The screenshot shows a web browser window with the URL https://afp.arubanetworks.com/afp/index.php/Mobile-first_reference_architecture#Tunneled_Node_in_Aruba.... The page header includes the AFP logo, a search bar, a language selection dropdown, and a menu icon. The main content area features a blue link for the presentation, followed by the title "Mobile-first campus and branch design and configuration" and the subtitle "Tunneled Node in ArubaOS-switch". A paragraph describes the technical white paper. Below this, a link to the PDF is provided, followed by a note on licensing for PPTN and PUTN. Two bullet points are highlighted in yellow, stating that PPTN consumes an AP license per switch, while PUTN currently consumes no license. The section concludes with the title "Aruba Mobile-first VRF-lite (MCF) design and configuration".

AFP

Search

Select Language ▼

MENI

- [Aruba Mobile-first Campus Reference Architecture Presentation](#)

Mobile-first campus and branch design and configuration

Tunneled Node in ArubaOS-switch

This technical white paper describes the tunneled node feature, shows reference designs, and describes how to configure it.

- [Tunneled node in ArubaOS-Switch - Technical White Paper.pdf](#)

Note the following in terms of licensing for Per Port Tunneled Node (PPTN) or Per User Tunneled Node (PUTN):

- Per Port Tunnel Node (PPTN) - will consume an AP license per switch.
- Per User Tunnel Node (PUTN) - is currently not consuming ANY license.

Aruba Mobile-first VRF-lite (MCF) design and configuration

Note the word currently, which means this is subject to change.

Idea is to look at switches as if they are wired access points from a licensing point.

Prepare for AP+PEFNG+RFP (if applicable) to purchase at some point in time.

Questions

aruba
a Hewlett Packard
Enterprise company



AIRHEADS
meetup