Aruba EPS Zero Trust Security

aruba
a Hewlett Packard Enterprise company

Sriharsha Narasimhan
CTO, HPE Aruba India

sriharsha.narasimhan@hpe.com

@sriharshaz

https://www.linkedin.com/in/sriharsha-narasimhan/

Sriharsha Narasimhan

CTO, HPE Aruba India

Sriharsha Narasimhan is Chief Technology Officer for Aruba, Hewlett Packard Enterprise. His core responsibilities include driving technology and strategic initiatives around Digital Experiences, Network Analytics, Network Security, Location Based Services, IT-OT and IoT across industry verticals. He is with Hewlett Packard for over 19 years and held multiple roles across strategy, management, engineering, and solution architecture.

Sriharsha has over 32 years experience as an IT professional with expertise in architecture, design, and development of embedded & enterprise solutions across market verticals. Prior to joining Hewlett Packard in 2001, he has worked for multiple organizations in India and USA, where he successfully lead teams in product development & engineering, sales and management areas.

CHALLENGES AT THE EDGE

TECHNOLOGY SILOS HINDER AGILITY

Fragmented management of switching, wireless, security, and WAN edge platforms cause significant challenges in provisioning, monitoring, and troubleshooting

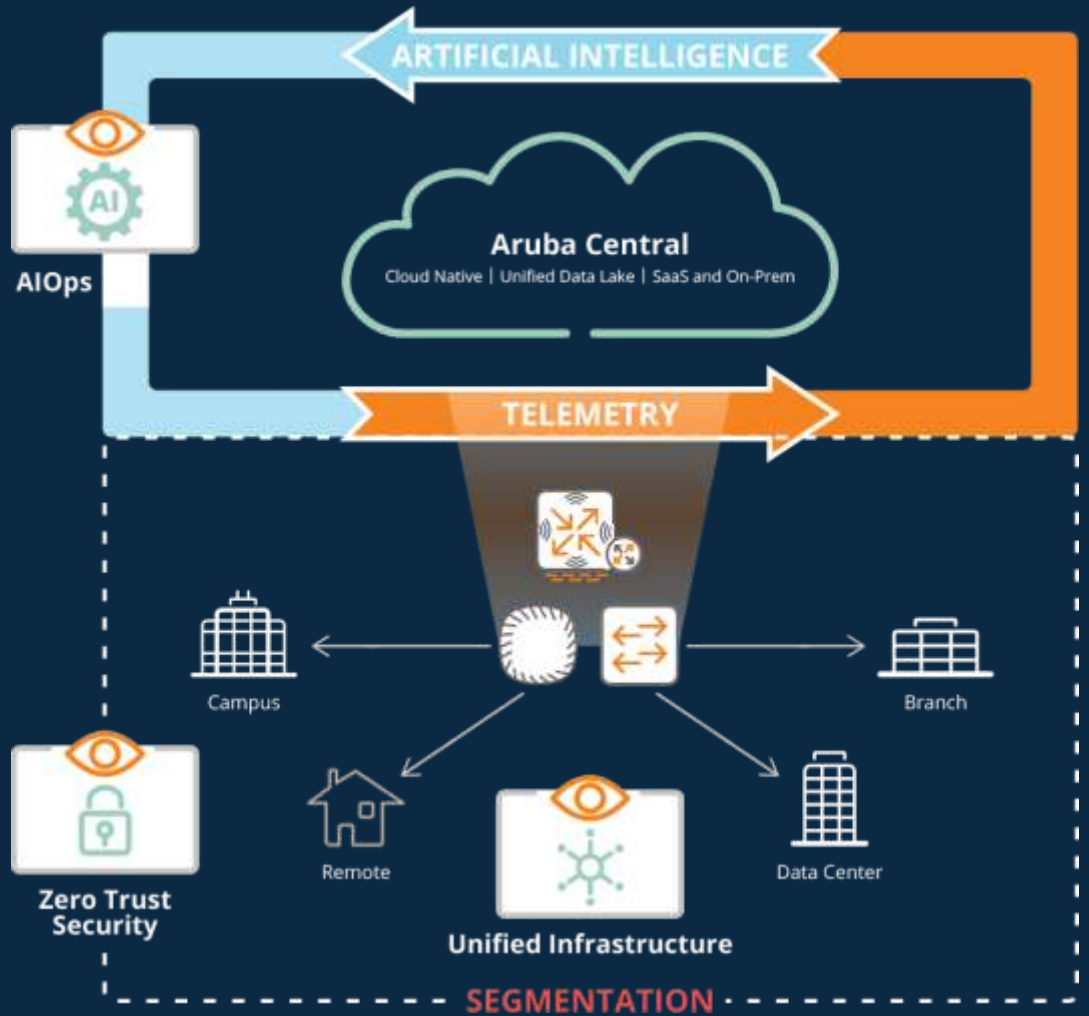
SECURITY THREATS INCREASE NETWORK COMPLEXITY

The security landscape is rapidly changing due to personal devices and IOT becoming commonplace attack vectors

MANUAL OPERATION AND POOR VISIBILITY CREATE FRAGILE NETWORKS

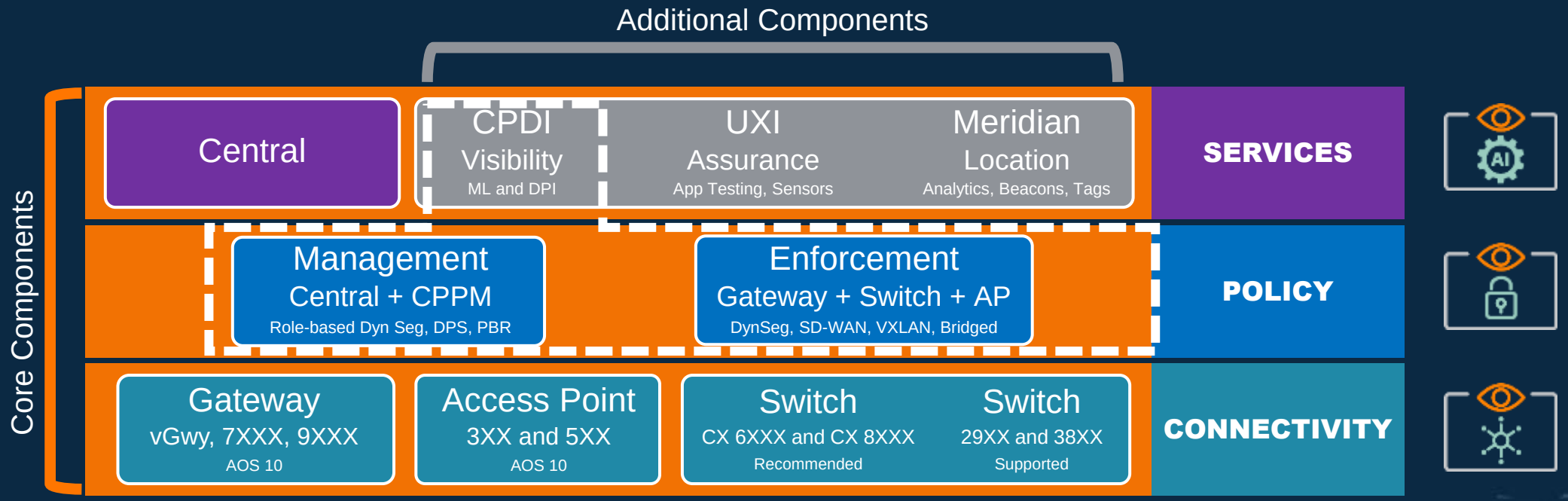
Manual actions are slow and will likely lead to human error. Lack of data makes troubleshooting and issue resolution painful

INTRODUCING THE
ARUBA ESP ARCHITECTURE

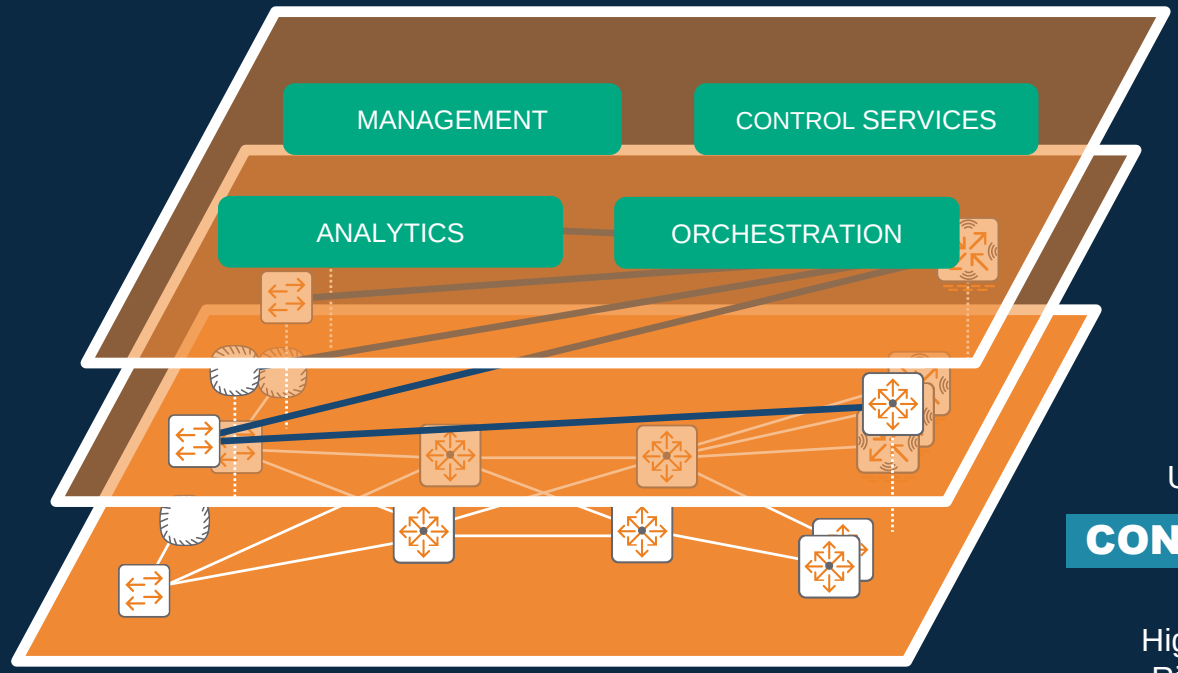


LAYERS OF
ARUBA ESP ARCHITECTURE

COMPONENTS OF ARUBA ESP ARCHITECTURE



ARUBA ESP ARCHITECTURE
BUILT ON BEST PRACTICES



ZERO TRUST SECURITY

OVERLAY

POLICY

Segmentation
Transport Independence
Service Insertion

CLOUD NATIVE

SERVICES

Flexible Deployment
Elasticity
Extensibility

AI OPERATIONS

UNDERLAY

CONNECTIVITY

Flexibility
High Availability
Rich Telemetry

UNIFIED INFRASTRUCTURE

Aruba Zero Trust Security

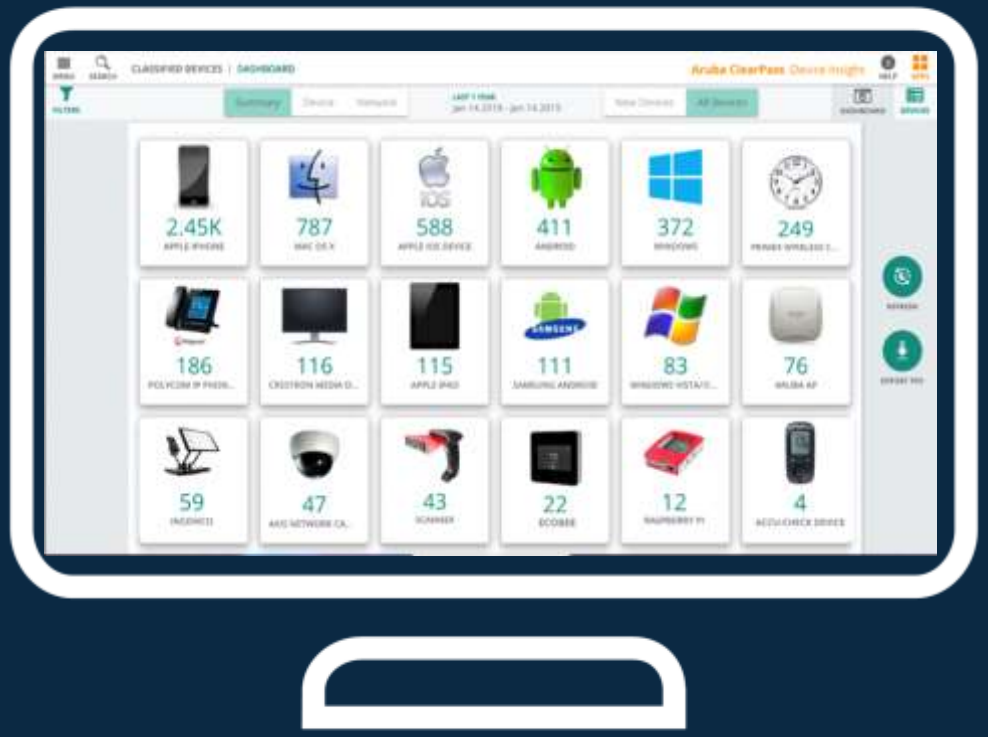
VISIBILITY: Understand what is connected to the network

Focus areas

- ❑ No “invisible” connections

ZERO TRUST FRAMEWORK
DEVICE VISIBILITY

VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting



CLEARPASS
DEVICE INSIGHT 2.0

AI-Powered

Cloud-Enabled

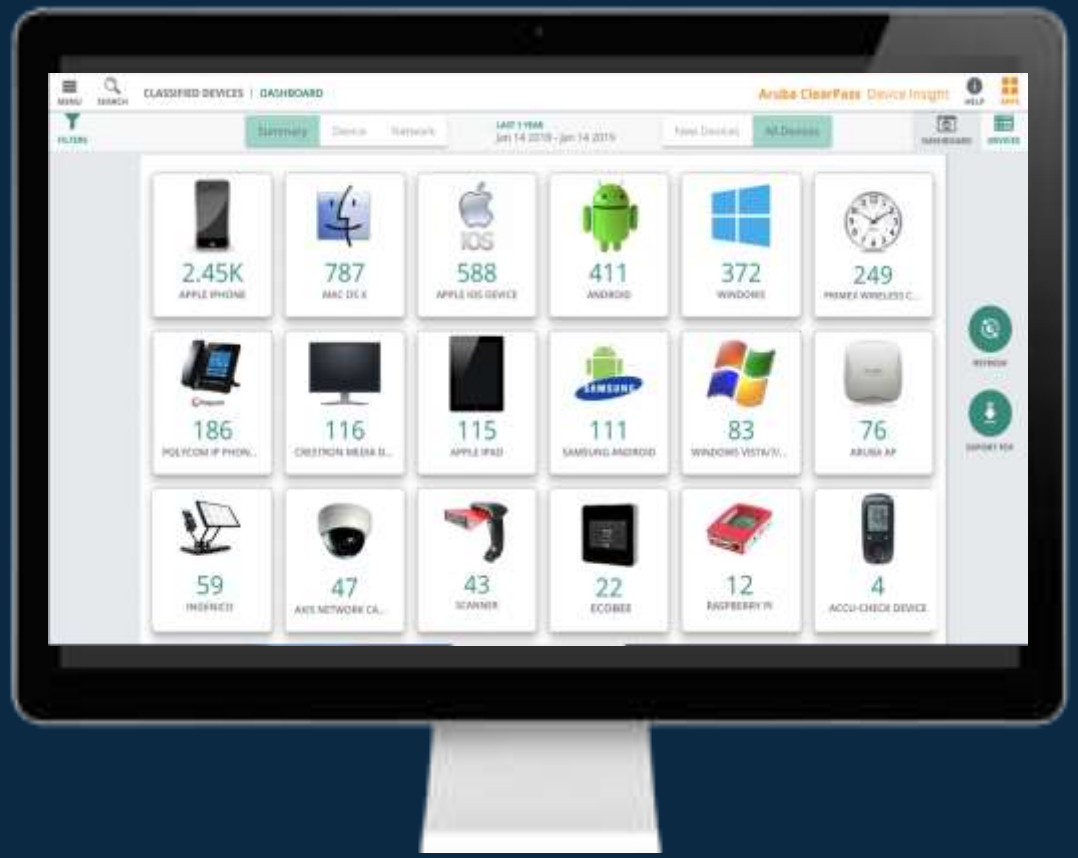
Enhanced by Crowdsourcing

Integration with Policy Manager

Device Visibility is key to proper segmentation

VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting

CLEARPASS DEVICE INSIGHT
OVERVIEW



Reduces Risk by Eliminating Blind Spots
through DPI-based discovery and profiling of devices

Automatically Clusters Unknown Devices and recommends classification
using advanced machine learning and crowdsourcing intelligence

Enriches Visibility
with vulnerabilities / posture assessment and risk score

Ensures Secure Access
via seamless integration with ClearPass Policy Manager

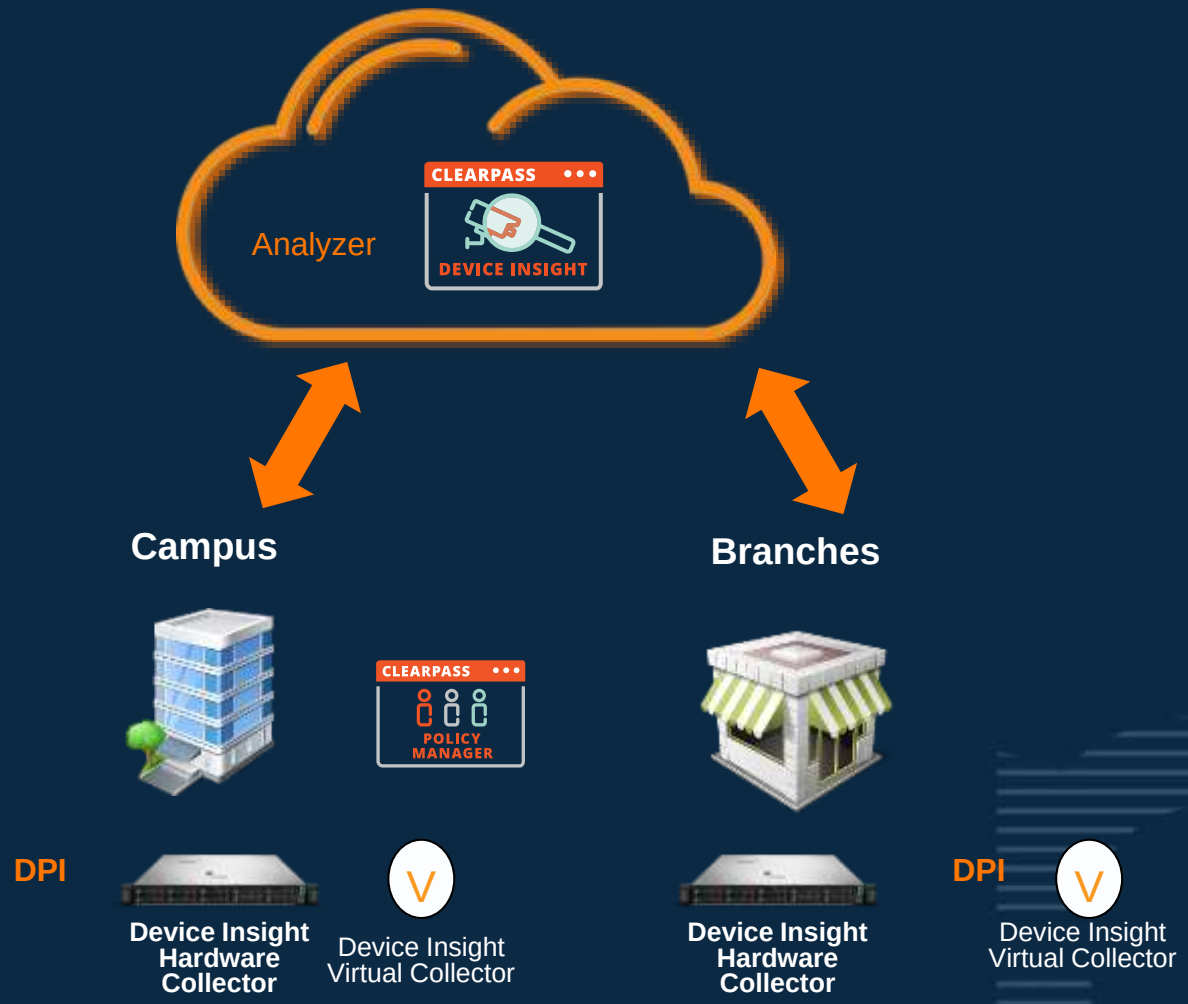
CLEARPASS DEVICE INSIGHT
SOLUTION OVERVIEW

VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting

On-premises Data Collector – Physical appliance or virtual machine with passive collection and active scanning

Cloud-based Analyzer – Responsible for fingerprinting, ML based classification, reporting, and integration with ClearPass Policy Manager

Deep Packet Inspection – Device attributes are extracted, and encrypted metadata is sent to the cloud for analysis



VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting

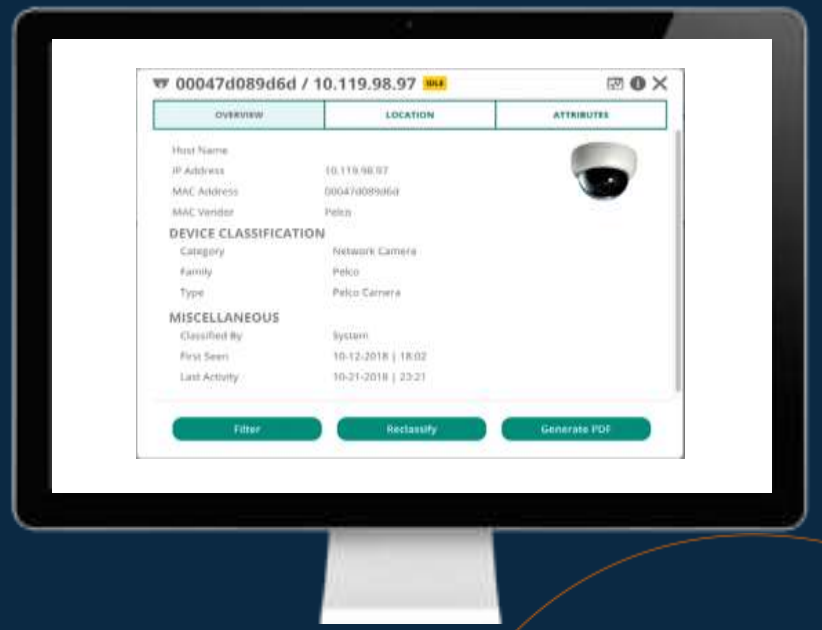
LEVERAGING RICH DEVICE CONTEXT

Deep Packet Inspection (DPI)

- Device Attributes
- IP/MAC Address
- Application Access
- Communication Protocols
- Communication Frequency

MACHINE LEARNING

CROWDSOURCING



TRADITONAL PROFILING TECHNIQUES
LACK DEVICE CONTEXT

VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting

STATIC ATTRIBUTES
DHCP | MAC OUI

GENERIC “APPLE”, “WINDOWS” or “Linux” DEVICE

NMAP = Network Mapper
SNMP = Simple Network Management Protocol
WMI = Windows Management Instrumentation

CLEARPASS DEVICE INSIGHT

FROM GENERIC TO GRANULAR DEVICE VIEW

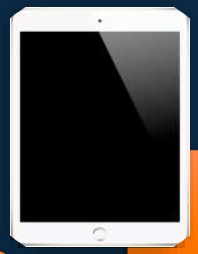
VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting

Actionable

Conference Room iPad on the 3rd Floor running the scheduling app

Behavior Based
- SPAN
- HTTP User Agent
- Netflow/sFlow/IPFIX
- Applications, metadata
- Domain Names
- Communication Patterns

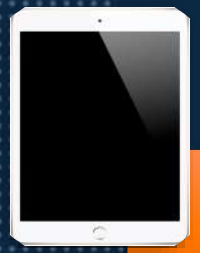
Basic



Apple iPad Connected to 3rd Floor AP

Scan Based
- IP/MAC
- Wired or Wireless Location (SNMP)
- Device Vendor
- IP Address
- Operating System (WMI, SSH)
- Applications
- Open Ports

Unhelpful



Apple iPad

MAC, DHCP Based
- DHCP Options
- DHCP Fingerprint
- MAC OUI

ZERO TRUST FRAMEWORK
POLICY MANAGER

VISIBILITY
Device Discovery and Profiling
Custom Fingerprinting

Role-based Policy

paloalto NETWORKS servicenow
Carbon Black. Check Point SOFTWARE TECHNOLOGIES LTD.
CYLANCE okta

150+ Partners

Bi-Directional Data Exchange w/ Tags

WLANs

ClearPass Device Insight
ENHANCED DISCOVERY / PROFILING

ClearPass Policy Manager
AUTOMATED SEGMENTATION AND ENFORCEMENT

Switching

Internet of Things (IoT)

BYOD and Corporate Owned

Context from Multiple Sources

Aruba Zero Trust Security

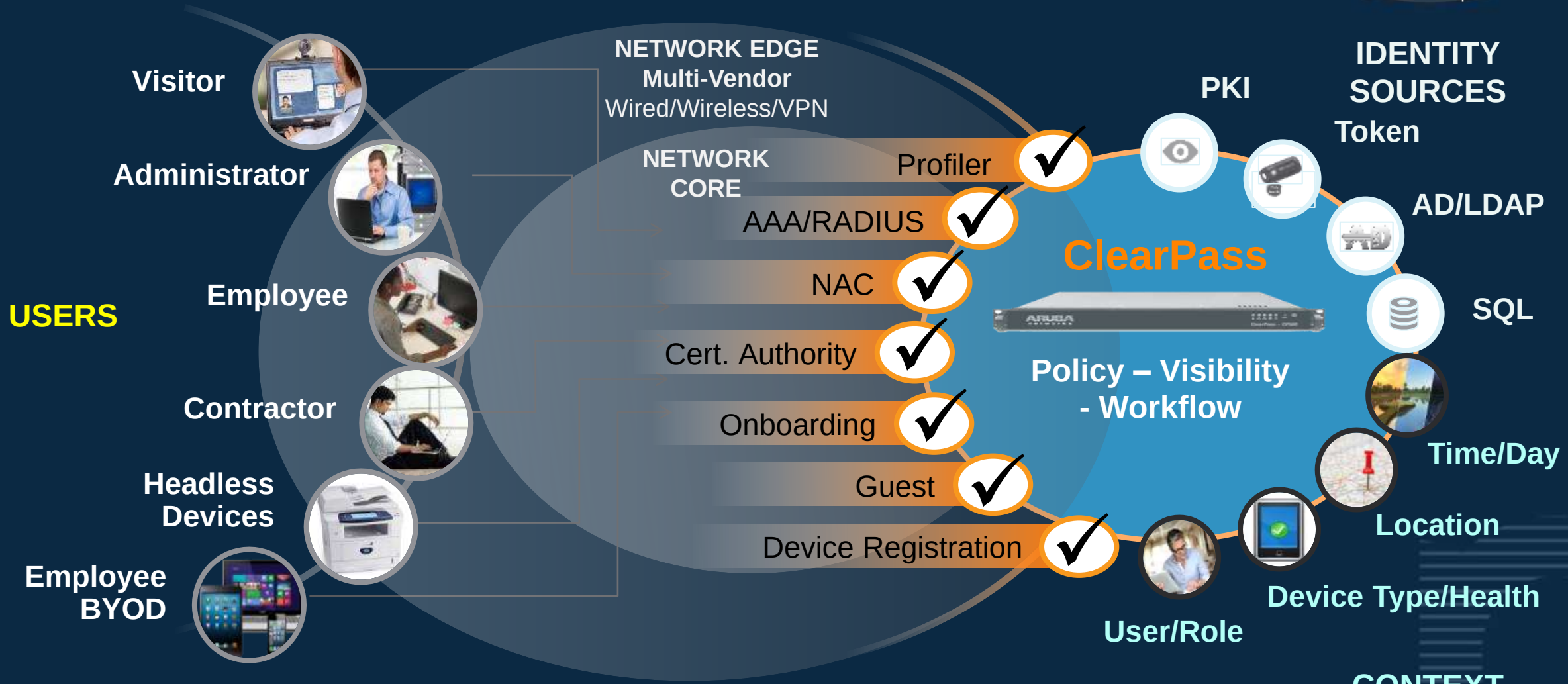
AUTHENTICATION: Authenticate all users and devices

Focus areas

- ❑ Not all devices have the same security stack (Corp laptop vs BYOD vs IoT)
- ❑ Untrusted devices should have “least access”

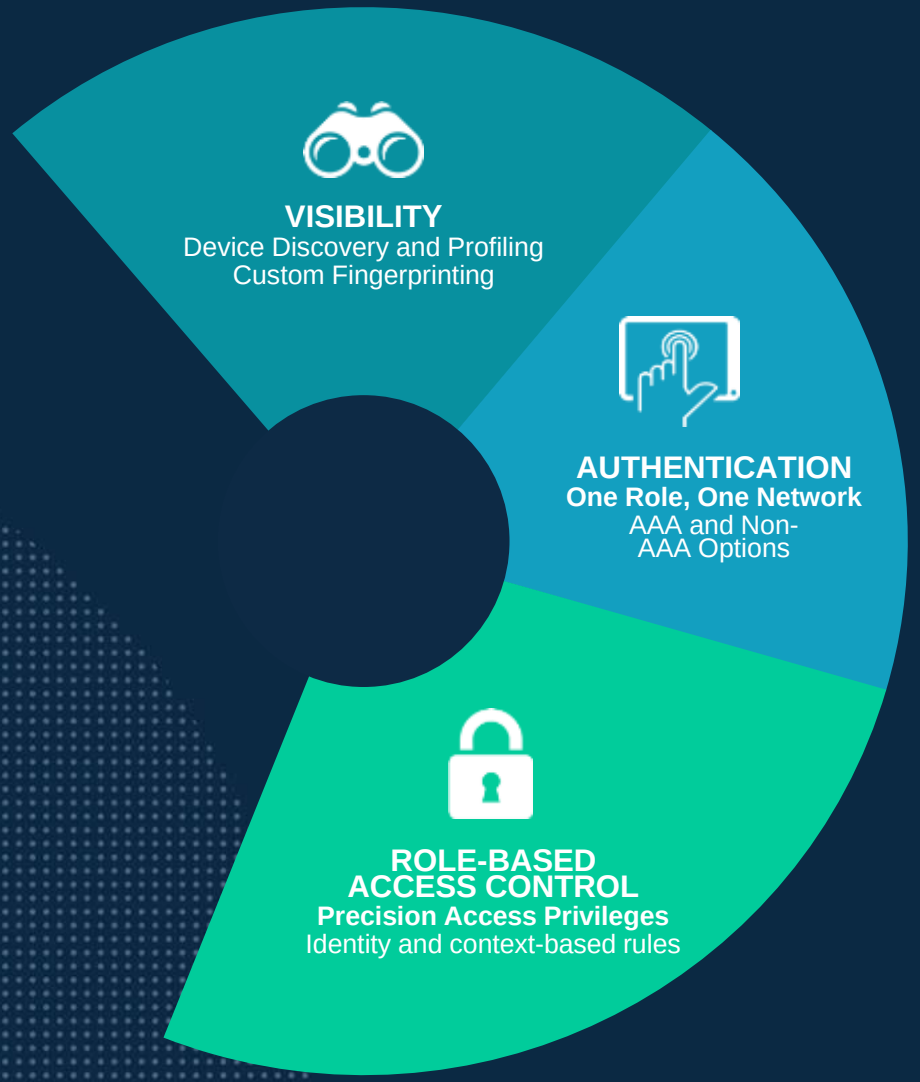
ClearPass Core Functionality

AUTHENTICATION
One Role, One Network
AAA and Non-AAA Options



Aruba Zero Trust Security

ROLE BASED ACCESS: Devices and users should be segmented



Focus areas

- ❑ Context needs to be considered (location, time, device type)
- ❑ Untrusted devices should have “least access”

ROLE-BASED ACCESS CONTROL
Precision Access Privileges
Identity and context-based rules

Think of VLANs as the yellow line on the road. Traffic is not supposed to cross that yellow line, but nothing prevents a vehicle from doing so.

VLANs define a network traffic isolation policy, but they are not technologically capable of preventing a malicious actor from moving between VLANs and gaining access to privileged information.

Therefore, new ways of segmenting networks must be created because all future networks need to be segmented by default.

Developing a Framework to Improve Critical Infrastructure Cybersecurity
Prepared by Forrester, for NIST, Aug 2013

Traditional network segmentation

Tedious and Error Prone

EMPLOYEES
BYOD
IOT

```
access-list 11 permit udp any any eq domain
access-list 11 permit udp any eq domain any
access-list 11 permit tcp any any eq domain
access-list 11 permit tcp any eq domain any
access-list 11 permit tcp any 10.11.12.0/24 eq ftp
access-list 11 permit tcp any 10.11.12.0/24 eq ftp-data established
Access-list 11 deny any any
vlan 100
 name user-vlan
interface vlan 100
 ip address 10.11.55.0 255.255.255.0
 ip access-group 11 in

ip vrf byod
vlan 101
 name byod-vlan
access-list 12 permit
interface vlan 101
 ip address 192.168.100.0 255.255.255.0


vlan 102
 name IOT-Camera
vlan 103
 name IOT-Lights
vlan 104
 name IOT-HVAC
vlan 105
 name IOT-Locks
vlan 106
 name IOT-WaterSensor
vlan 107
 name IOT-SmokeAlarm
vlan 108
 name IOT-Audio
```

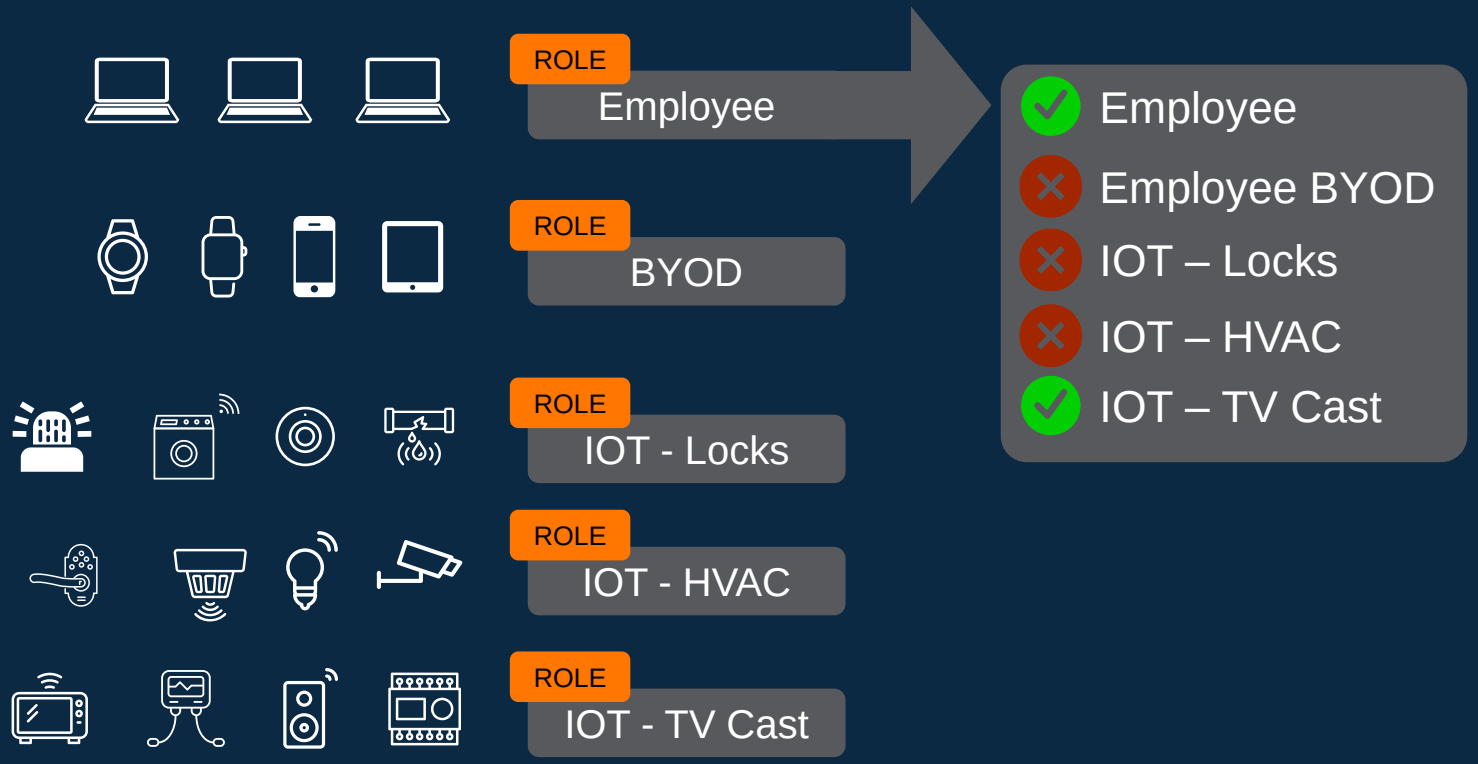
ROLE-BASED ACCESS CONTROL
Precision Access Privileges
Identity and context-based rules

Complex hop-by-hop IP-based segmentation slows the deployment of new devices on the network

ACLs either become unmanageable or are nonexistent ultimately leading back to security struggles

ROLE-BASED ACCESS CONTROL
Precision Access Privileges
Identity and context-based rules

ZERO TRUST FRAMEWORK
PROTECTS AND SIMPLIFIES



DYNAMIC SEGMENTATION

Software defined approach eliminates VLAN sprawl and complex enforcement rules

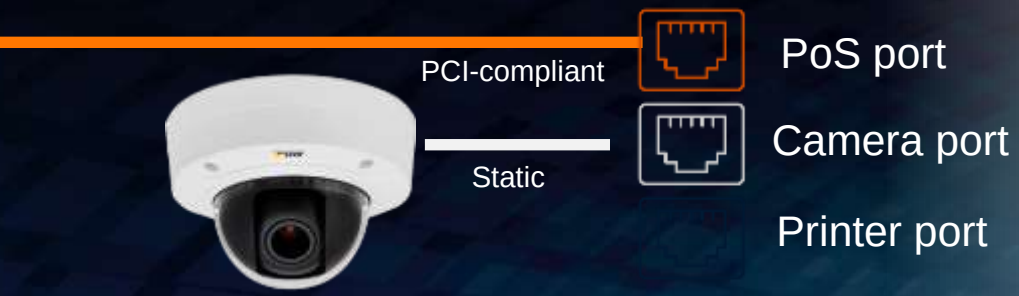
Delivers wired and wireless micro-segmentation at a Campus or Branch to secure endpoints based on Role

Helps implement a Zero Trust Network

ENFORCED BY DYNAMIC SEGMENTATION

ROLE-BASED ACCESS CONTROL
Precision Access Privileges
Identity and context-based rules

PORT-BASED
Manual configuration of ACLs, VLANs, QoS



Hard to scale for device type and quantity across multiple sites

DYNAMIC ROLE-BASED
Automate configurations with context

Flatten configurations at high scale based on user, device, app

Colorless Switch Ports

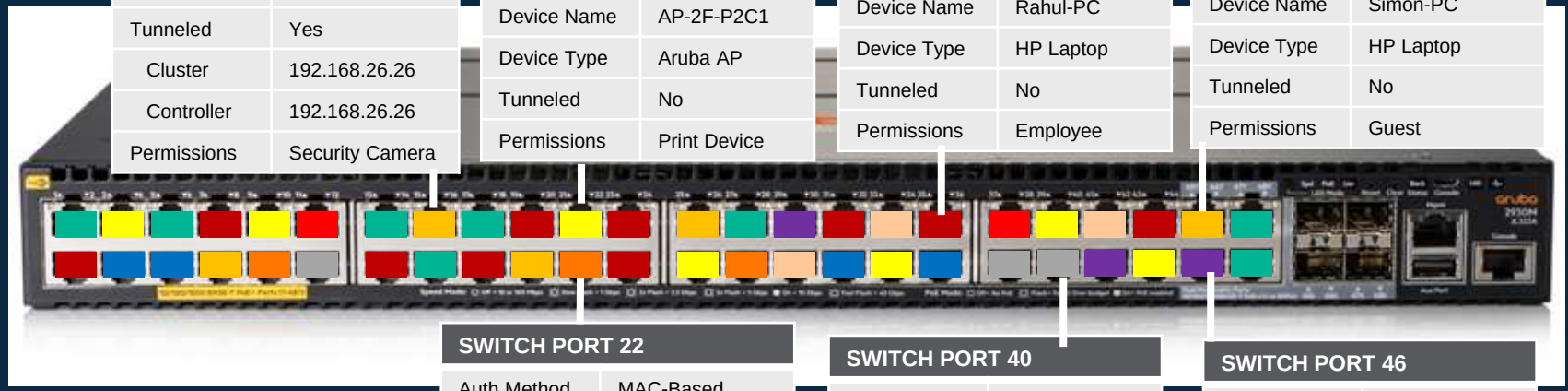
ROLE-BASED ACCESS CONTROL
Precision Access Privileges
Identity and context-based rules

SWITCH PORT 15	
Auth Method	MAC-Based
Role	Camera
Device Name	2F-P2-CAM
Device Type	Camera
Tunneled	Yes
Cluster	192.168.26.26
Controller	192.168.26.26
Permissions	Security Camera

SWITCH PORT 21	
Auth Method	MAC-Based
Role	Access Point
Device Name	AP-2F-P2C1
Device Type	Aruba AP
Tunneled	No
Permissions	Print Device

SWITCH PORT 35	
Auth Method	802.1X
Role	Engineer
Device Name	Rahul-PC
Device Type	HP Laptop
Tunneled	No
Permissions	Employee

SWITCH PORT 41	
Auth Method	MAC-Based
Role	Guest
Device Name	Simon-PC
Device Type	HP Laptop
Tunneled	No
Permissions	Guest



SWITCH PORT 22	
Auth Method	MAC-Based
Role	IP-Phone
Device Name	2FP2C1-PH
Device Type	VOIP Phone
Tunneled	No
Permissions	Voice over phone

SWITCH PORT 40	
Auth Method	MAC-Based
Role	Sensor
Device Name	Fi Sensor
Device Type	IOT
Tunneled	No
Permissions	IOT Device

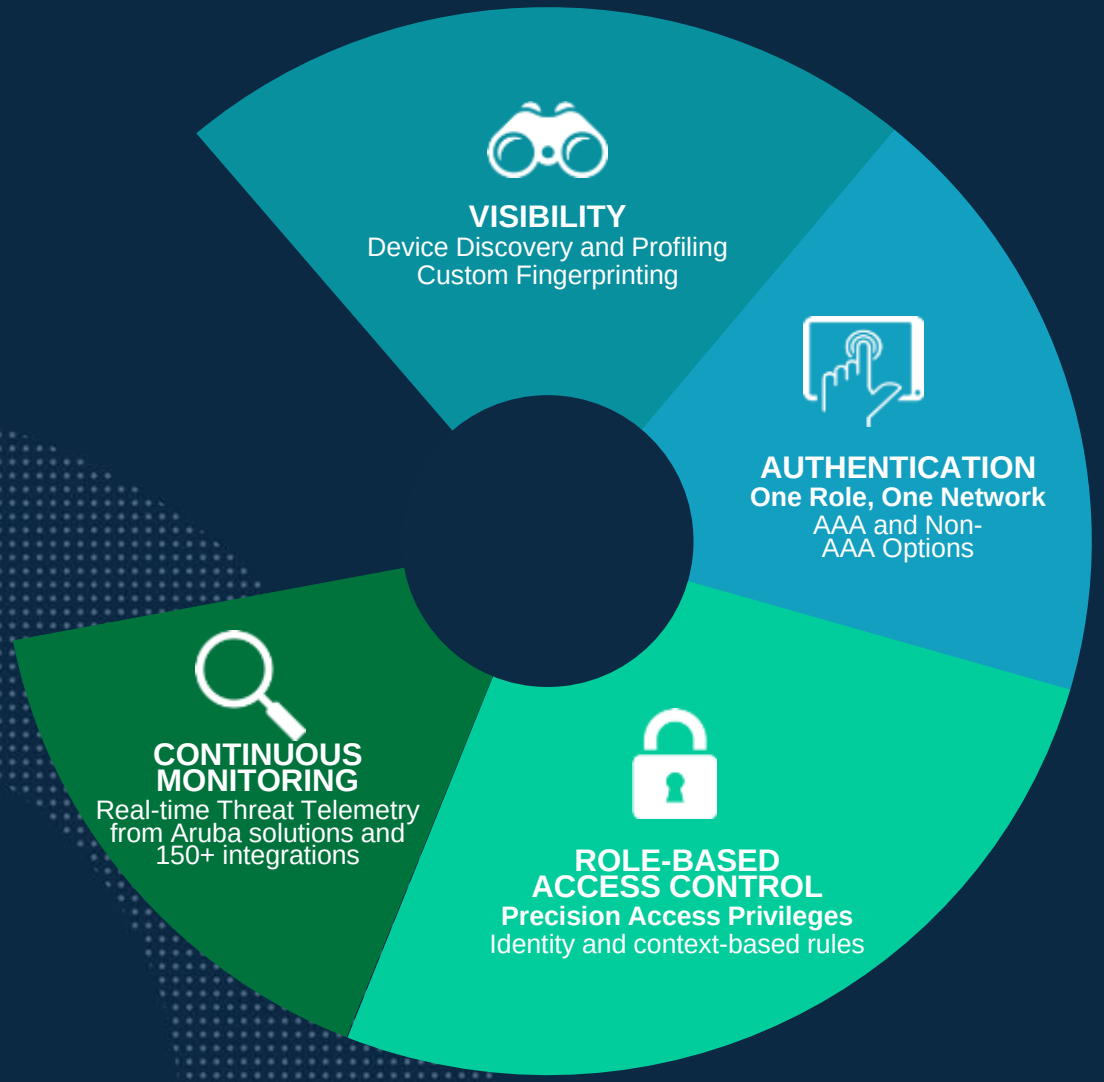
SWITCH PORT 46	
Auth Method	MAC-Based
Role	Printer
Device Name	HP-2F-P3-PRN
Device Type	HP Printer
Tunneled	No
Permissions	Print Device

Infrastructure	Access Point
Camera	VOIP Phone
Engineer	Printer
Temp Sensor	Guest
Headless	Apple TV

Switch access ports carry the same config ***(colorless)*** and based on the device type connected (PC, AP, IP Phone, Printer, Camera or IOT), user/device role is downloaded dynamically!

Aruba Zero Trust Security

MONITOR CONTINUOUSLY: Security checks need to be ongoing, not one time



Focus areas

- ❑ Continuously monitor user and device for changes in posture and behavior
- ❑ Access decisions are based on continuous monitoring (reduce access or deny)

Security Enterprise in ever challenging environment

Gartner CARTA Strategy

Continuous Adaptive Risk and Trust Assessment

CONTINUOUS MONITORING

Real-time Threat Telemetry from Aruba solutions and 150+ integrations

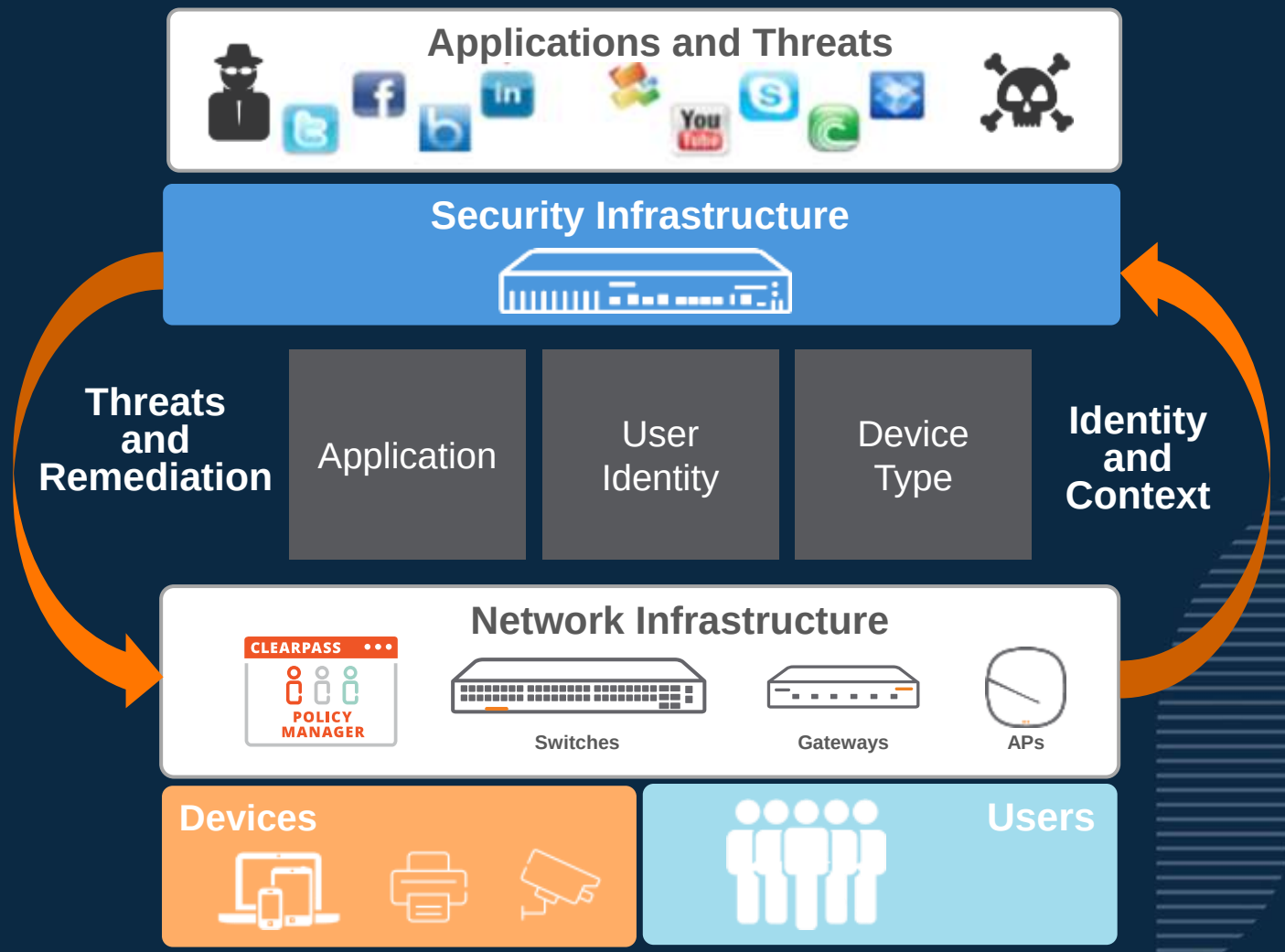
- Perfect attack prevention, perfect authentication and invulnerable applications are never possible
- Digital risk and trust are fluid, not binary and fixed, and need to be discovered and continuously assessed
- Security infrastructure and decisions must be context-aware and adaptable to different levels of risk, opportunities and trust levels

Source: Gartner CARTA Strategy 2018

Continuous Monitoring with Real-Time adaption

CONTINUOUS MONITORING
Real-time Threat Telemetry from Aruba solutions and 150+ integrations

- Decisions are based on continuous monitoring
- Access can be reduced or denied based on risk-level changes

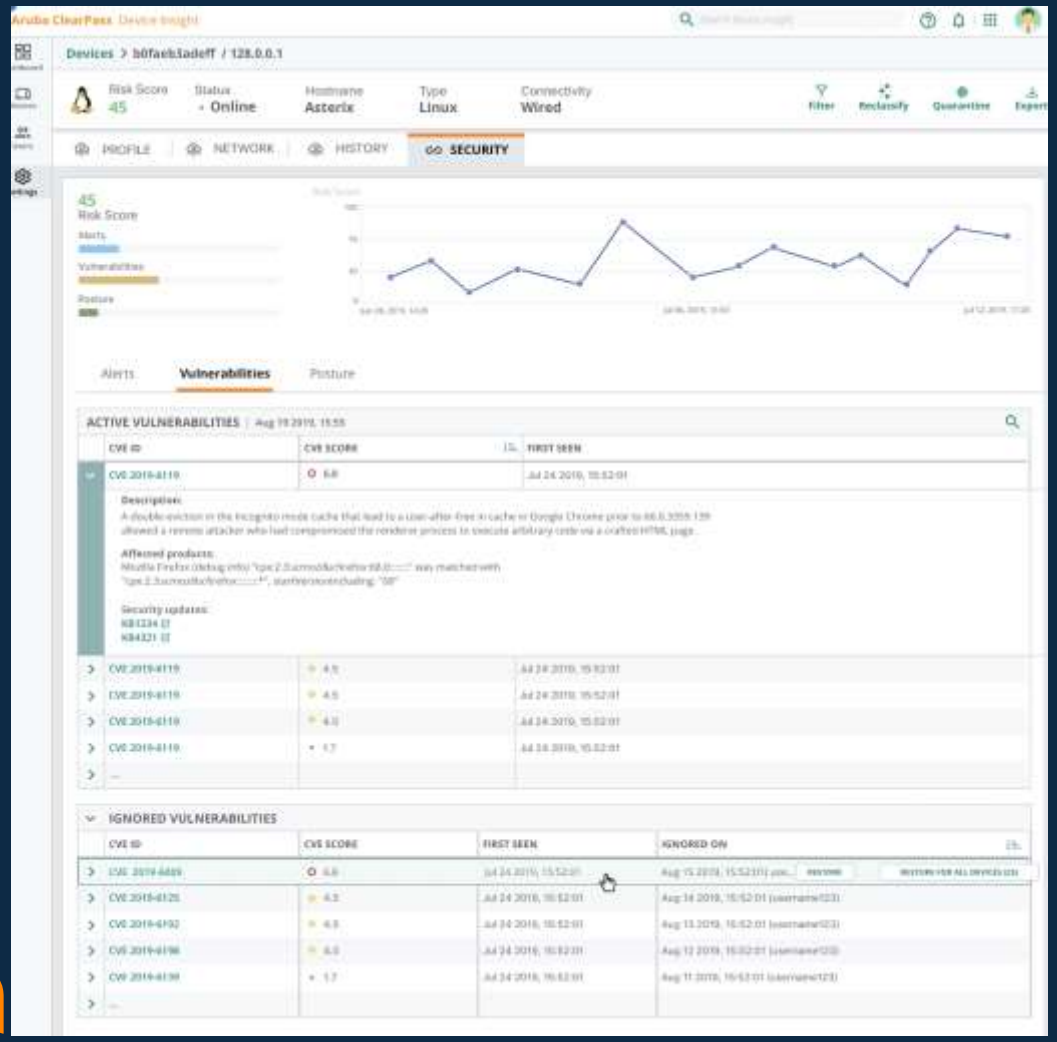


Visibility into Vulnerabilities

ClearPass Device Insight – Device Security Status

NEW

CONTINUOUS MONITORING
Real-time Threat Telemetry from Aruba solutions and 150+ integrations



- Most sought after feature for multiple customers including LAUSD
- Complete visibility into vulnerabilities based on passive and active data collection
- Automated learning based on customer feedback

Agentless Posture Assessment

ClearPass Device Insight – Device Security Status

NEW

CONTINUOUS MONITORING
Real-time Threat Telemetry from Aruba solutions and 150+ integrations

- Assign a posture to the device based on pre-defined rules
- Supported for Windows OS and will be extended to other operating systems

SD-Branch: UNIFIED BRANCH SECURITY

CONTINUOUS MONITORING
Real-time Threat Telemetry from Aruba solutions and 150+ integrations

- App-User Aware Firewall
- Deep Packet Inspection
- Web content & URL filtering
- App & URL reputation
- Cloud Security integrations
- **Intrusion Detection & Prevention System** NEW

Threat Visibility
- Sliceable threat trending overtime
- Overlay with app/user launch and network direction
- Threat source and impact

Policy driven enforcement
- Out of box IDS / IPS policies
- User defined whitelisting
- False Positive Management flow

Correlate to Manage Incident
- Externalizable events streamed to SOC
- Alert and notifications based on business impact
- Stream events to REST endpoints

SD-Branch: Security Dashboard

CONTINUOUS MONITORING
Real-time Threat Telemetry from Aruba solutions and 150+ integrations

- Threats Over Time
  - User/App Launch & Network Traffic vs Threat
  - Threat Trend
- Threat Metrics
  - By category, type and severity
  - Threat prevalence
  - Impacted users / devices
  - Source and level of impact
- Drilldowns
- SIEM integration (splunk is the 1st to come)

CONTEXT FROM 150+ TOOLS YOU MAY ALREADY USE

SECURITY

CROWDSTRIKE
CARBON BLACK
Attivo NETWORKS
Check Point
CYLANCE
FireEye
FORTINET
Juniper
tenable
McAfee
paloalto
Symantec.
BIGFIX
Microsoft

AUTH

Auth0
Azure Active Directory
DUO
Envoy
Cloud Identity
IMAGEWARE SYSTEMS
okta
PingIdentity
sine
tesm

OT/ICS

CLARITY
Indegy
CyberX
NOZOMI NETWORKS

LOGGING

ArcSight
splunk>
QRadar
solarwinds
HOTSPOT
Authorize.Net
PayPal
worldpay

MESSAGING

Microsoft Teams
pagerduty
TWILIO SendGrid
servicenow
slack
twilio

PROPERTY

Agilysys
ORACLE | micros Opera
protel
Silverbyte

EMM

BlackBerry
CITRIX
G Suite
IBM MaaS360
Microsoft
jamf
MobileIron
SAP
SOTI
Workspace ONE
MOSYLE

SOCIAL

amazon.com
facebook.
GitHub
Google
Instagram
LinkedIn
salesforce
twitter

CONTINUOUS MONITORING
Real-time Threat Telemetry from Aruba solutions and 150+ integrations

Aruba Zero Trust Security

ENFORCEMENT: Rapid response to ongoing threat

Focus areas

- ❑ Proactively analyze all threat insights
- ❑ Respond to threat and trigger multiple actions, including alerting

CLEARPASS POLICY MANAGER
DATA EXCHANGE

ENFORCEMENT AND RESPONSE
Attack Response
Event-triggered actions

ClearPass Device Insight
ENHANCED DISCOVERY / PROFILING

Internet of Things (IoT)

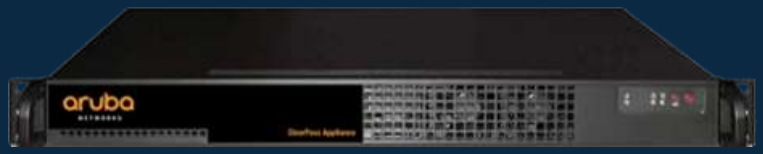
BYOD and Corporate Owned

Device Classification

Additional Context for endpoints

Endpoint Authentication Context

Additional Context for endpoints



ClearPass Policy Manager
AUTOMATED SEGMENTATION AND ENFORCEMENT

ClearPass Adaptive Response

End to end defence: Identify and React to Threat

ENFORCEMENT AND RESPONSE
Attack Response
Event-triggered actions

1. Discover and Authorize

User/Device Context

ClearPass Secure Access Control

2. Monitor and Alert

McAfee
FORTINET
RAPID7
FireEye

360 Security Exchange Partners

Actionable Alerts

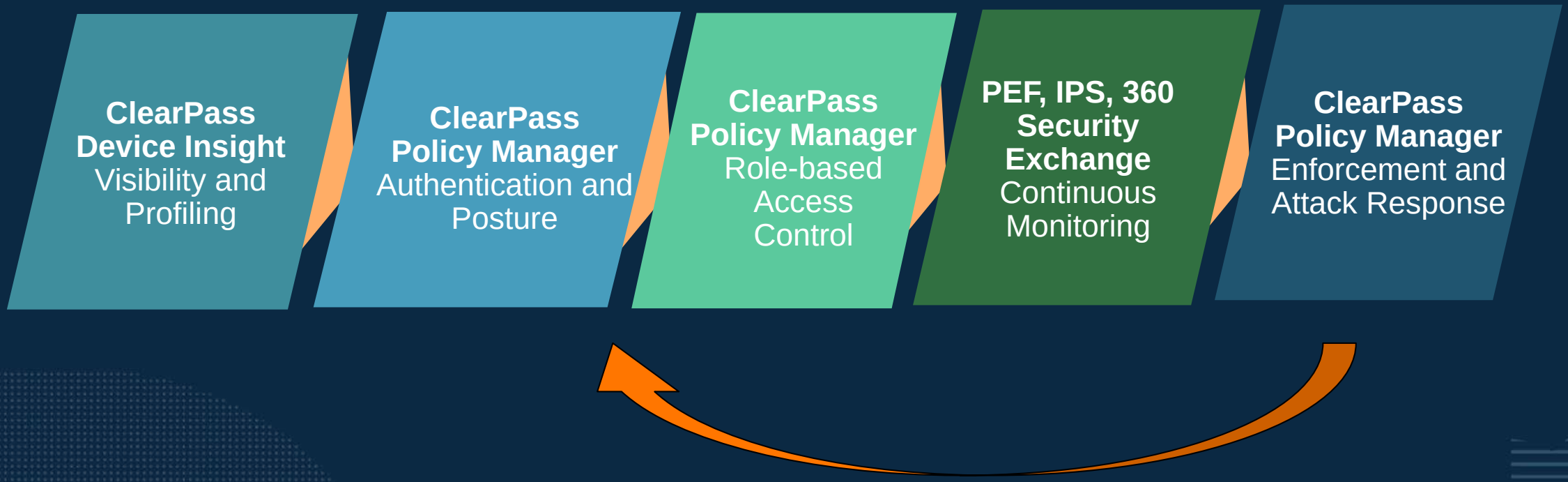
3. Decide and Act

- Real-time Quarantine
- Re-authentication
- Bandwidth Control
- Blacklist
- Role-change

ClearPass Adaptive Response

SECURE CONNECTIVITY
AUTOMATED, CLOSED-LOOP

ENFORCEMENT AND RESPONSE
Attack Response
Event-triggered actions



“Replace one-time security gates with context-aware, adaptive and programmable security platforms”
Gartner – Seven Imperatives to adopt a CARTA strategic approach

aruba
a Hewlett Packard Enterprise company

Thank You


sriharsha.narasimhan@hpe.com


@sriharshaz


https://www.linkedin.com/in/sriharsha-narasimhan/