HPE Aruba Networking and NIS2 compliancy

Ken Van Campenhout
HPE Aruba Networking

Hewlett Packard Enterprise

HPE Aruba Networking and NIS2 compliancy

Ken Van Campenhout
Aruba BeLux Technical Enablement

December 5th, 2023

Article 21 paragraph 2

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

HPE Aruba Networking Solutions for EU NIS 2 Directive

Article 21 Solutions Overview

(b) Incident Handling	Automatic response with ClearPass, Integration with SIEM, Fwd Syslog
(c) Business Continuity	HPE Aruba Hitless failover, ISSU, Live Upgrade, HA design, etc
(d) Supply chain Security	HPE Trusted supply chain security from component, to Manufacturing and Distribution
(e) Security in NIS acquisition, dev, vulnerability	HPE Software Development Life Cycle Aruba Threat Labs
(h) Cryptography procedure, Encryption	AOS8 Centralized Crypto management in Gateways, Military Grade Encryption Support for IPSEC, RADSEC and MACSEC
(j) Use of Multiple Factor Authentication	ClearPass and Aruba 360 Secure Exchange partners such as PingID, Duo, etc.. . HPE Aruba Networking SSE ZTNA continuous Monitoring (AXIS).
(j) Use of Secure Voice, Video and text Com	HPE Aruba Air Slice for Application-aware Quality of Service (QoS)

Supply Chain Security – HPE Aruba Trusted Infrastructure

Components

Secure Development Life Cycle (SDLC)

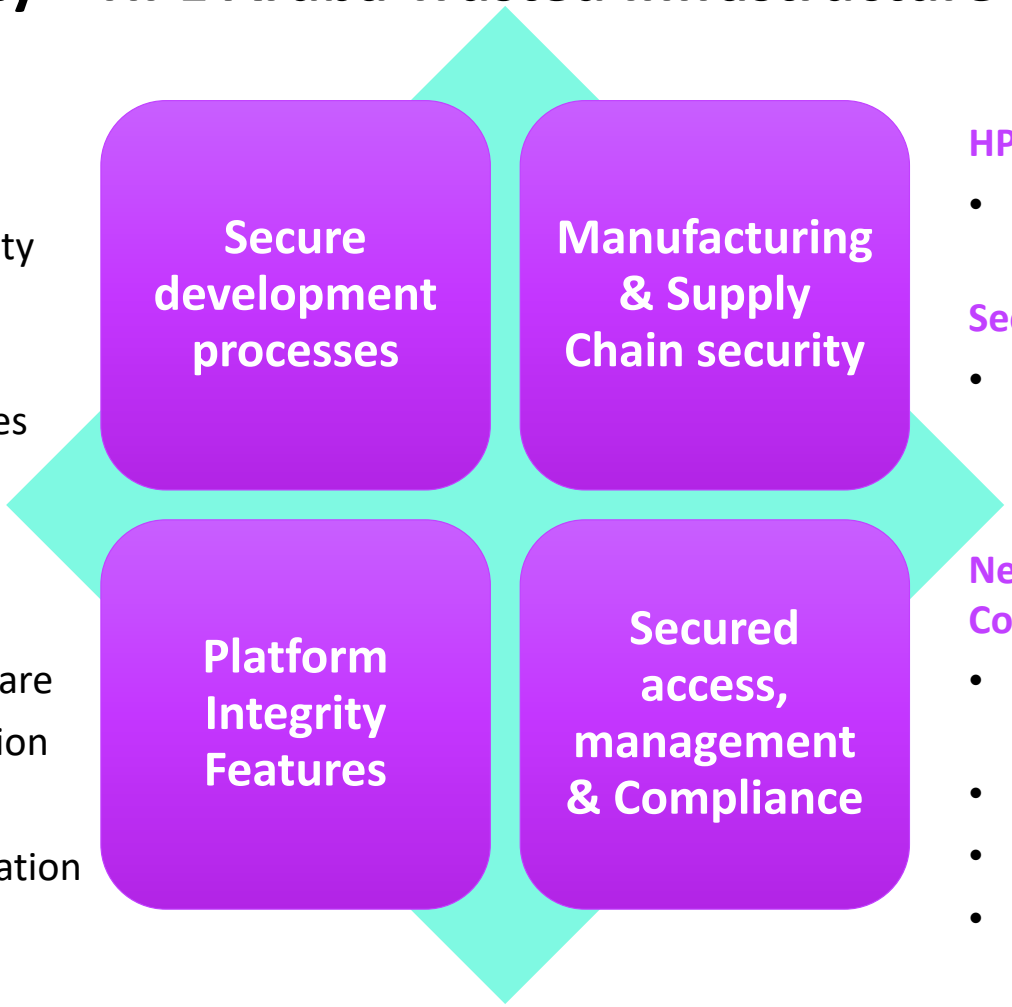
- Developer training and security awareness
- Product security assessments
- Secure development processes
- Static analysis / Code review
- Vulnerability / Bug Bounty

Hardware

- Root of Trust – protect firmware
- TPM – reporting, key protection

Firmware

- Secure boot / signature validation
- Authenticated updates



HPE Trusted supply chain security

- From component, to Manufacturing and Distribution

Secure Recycling

- Zeroization

Network Operation and Compliance

- Secure management (SSH, TLS, PKI, etc)
- TACACS+
- Confidential Support
- Compliance and Certifications: First to NIST, FIPS, Common Criteria EL4 GDPR and more

Trusted Infrastructure
Root of Trust (ROT)

- A Root of Trust is Hardware or Software (or both together) that are *unconditionally* trusted.
- A Root of Trust (RoT) must always behave in the expected manner because RoT misbehavior will not be detected.
- Secure RoT's are critical for detection and preventing persistence of Malware.
- The Core Root of Trust is the first piece of code that executes on a platform at boot time
- This code is signed, and its signature is stored on a secure component : The TPM chip

HPE Supply Chain Security

Zero Trust starts in the Supply Chain

Design | **Sourcing** | **Build** | **Fulfillment** | **Distribution** | **Sustainment & Operations** | **Disposal**

Prevent, monitor, detect, analyze & report incidents of confirmed counterfeit & malicious taint

Secure design and compliance

Origin and traceability

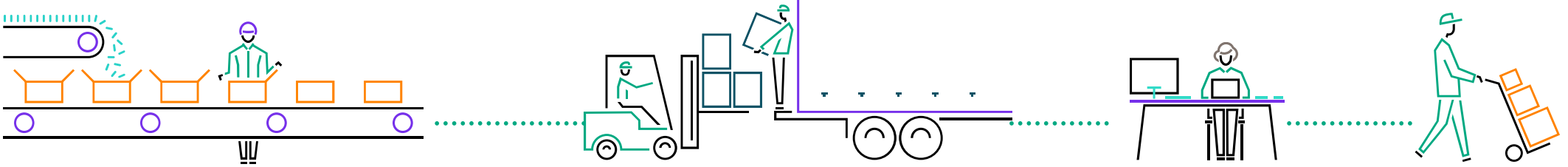
Factory security controls

Product testing and authentication

Secure delivery

Security labeling and anti-counterfeit

Secure erase



Basic cyber hygiene practice

(89) Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

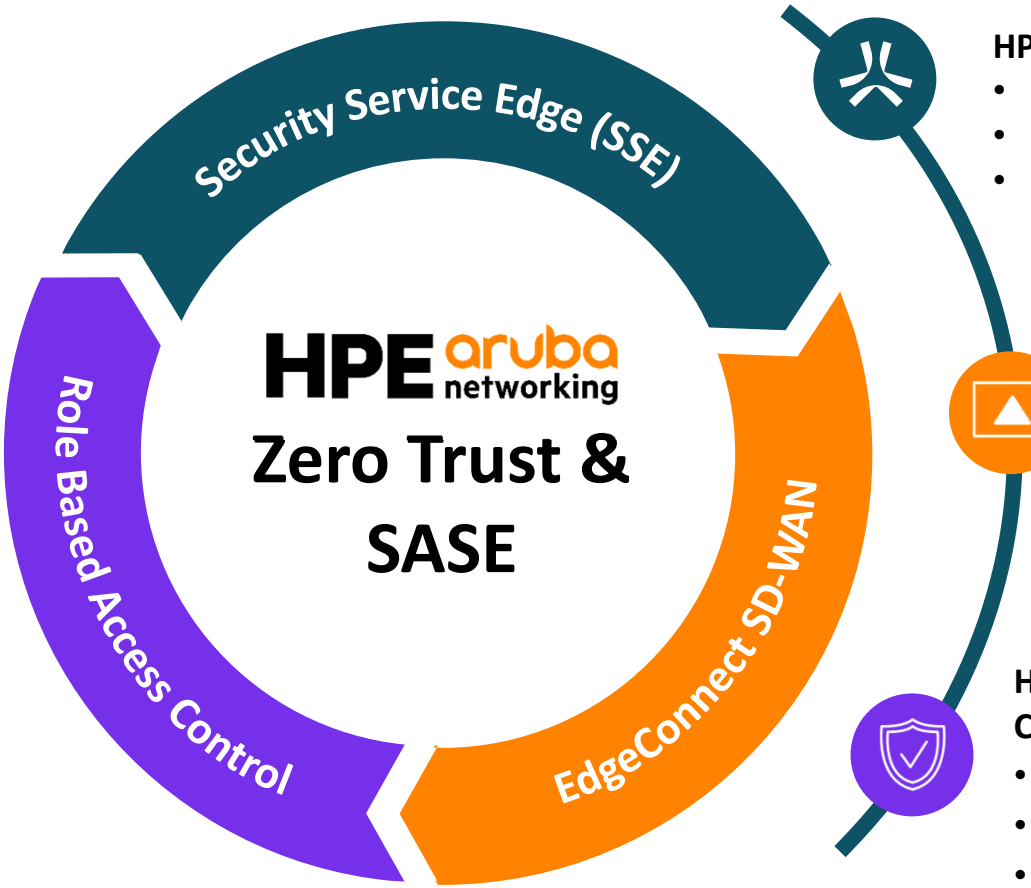
HPE Aruba Networking Solutions for EU NIS 2 Directive

Basic Cyber Hygiene practice (89) Solutions overview

Zero Trust Principles	HPE Aruba Zero Trust Solutions
Software Update	Aruba Central Live Firmware Upgrade, Wi-Fi Firmware Recommender, Hot-Patching Services
Device Configuration	Aruba Central , Aruba Fabric Composer
Network Segmentation	Choice of Centralized and Distributed Dynamic Segmentation, CX10k
Identity and Access Management	ClearPass Policy Manager, Central Cloud Auth, SSE (AXIS ZTNA)
User Awareness	Aruba Central Client and Application visibility (wired and wireless)
Use of Machine Learning	Aruba Central Cloud AIOps including Client Insights

Delivering the experience users want, with the security the business needs

Zero trust controls to protect users and applications, no matter where they connect



HPE Aruba Networking SSE

- Unified ZTNA, SWG, CASB and DEM
- Multi-cloud backbone across 500 edges
- Zero trust access for all ports and protocols

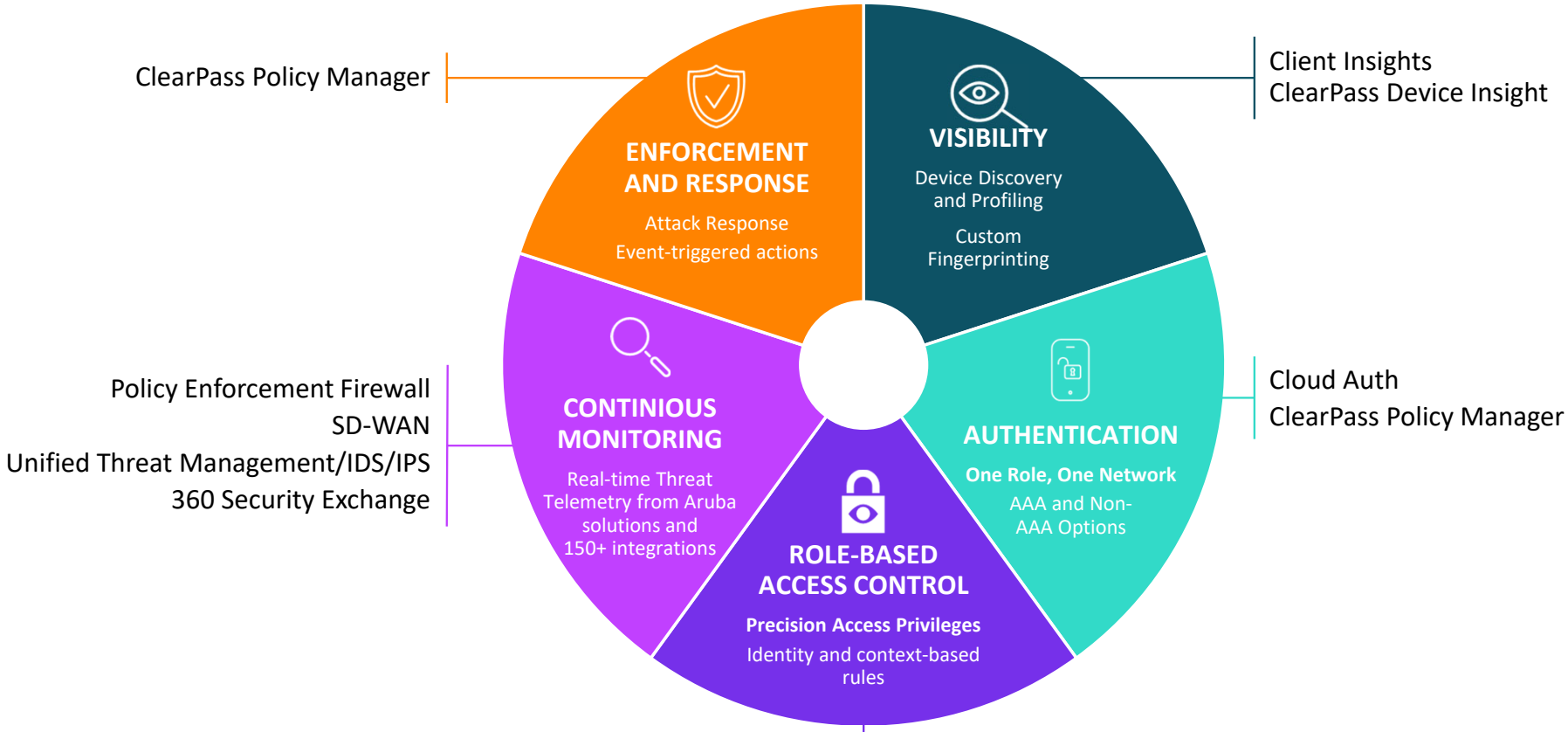
EdgeConnect Secure WAN Edge

- Secure SD-WAN
- Multi-cloud
- Improved QoE

HPE Aruba Networking Central NetConductor & ClearPass Network Access Control

- AI-powered client visibility & profiling
- Dynamic Segmentation
- Continuous Monitoring

HPE Aruba Networking Zero Trust security foundation



Aruba's User Roles

What Are User-Roles

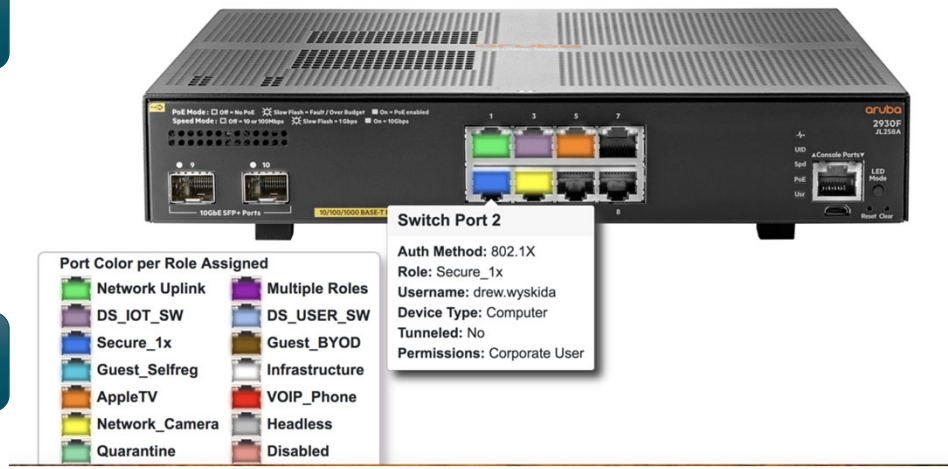
- A simple container for policy and security
  - VLAN, overlay/underlay path, QoS, Rate Limiters, MTU, POE priority, STP port settings
- ***Have existed for ~20 years in Aruba products.***
  If you're on an Aruba AP, you're using user roles!

How to Apply User-Roles

- User-Roles are applied dynamically once a device authenticates with any AAA method.
- Can be applied with a device profile.
- Can be dynamically or statically applied

Benefits

- Apply policy based on role configuration
- No need to preconfigure access ports - ACLs, rate limiters, QoS, etc.
- Associated to the client not the physical port.

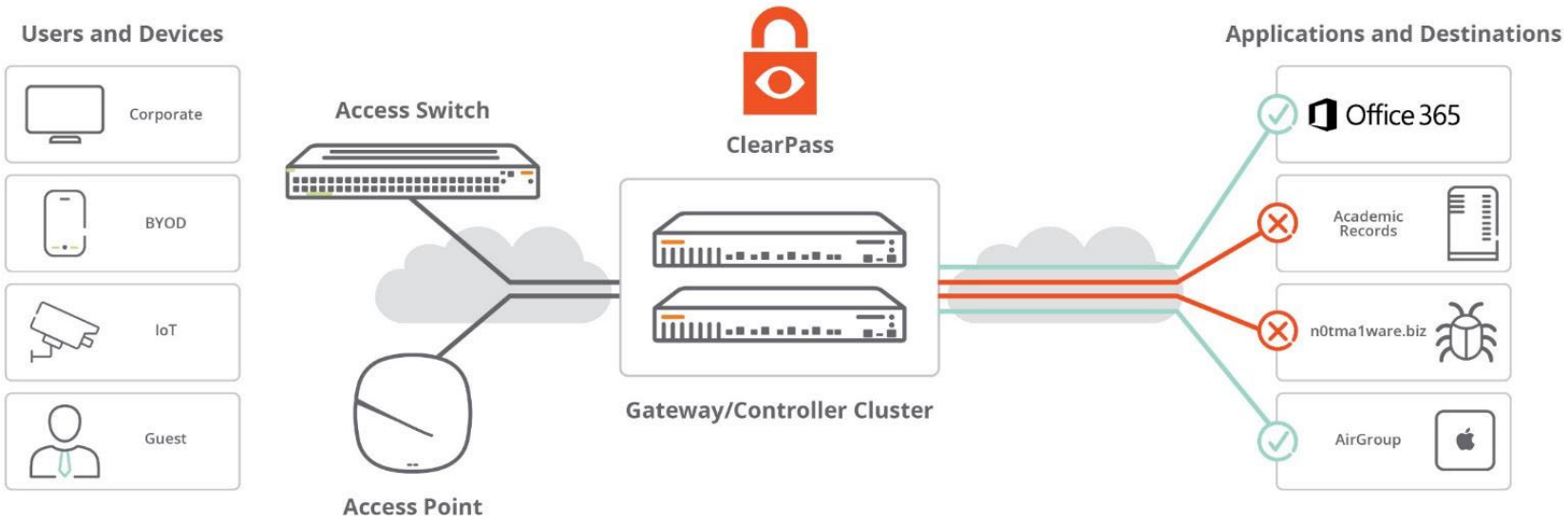



```
aaa authentication port-access dot1x authenticator
    radius server-group ClearPass
    enable

aaa authentication port-access mac-auth
    radius server-group ClearPass
    enable

interface 1/1/1-1/1/48
    aaa authentication port-access dot1x authenticator
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable
```

Unified and secure Dynamic Network Segmentation

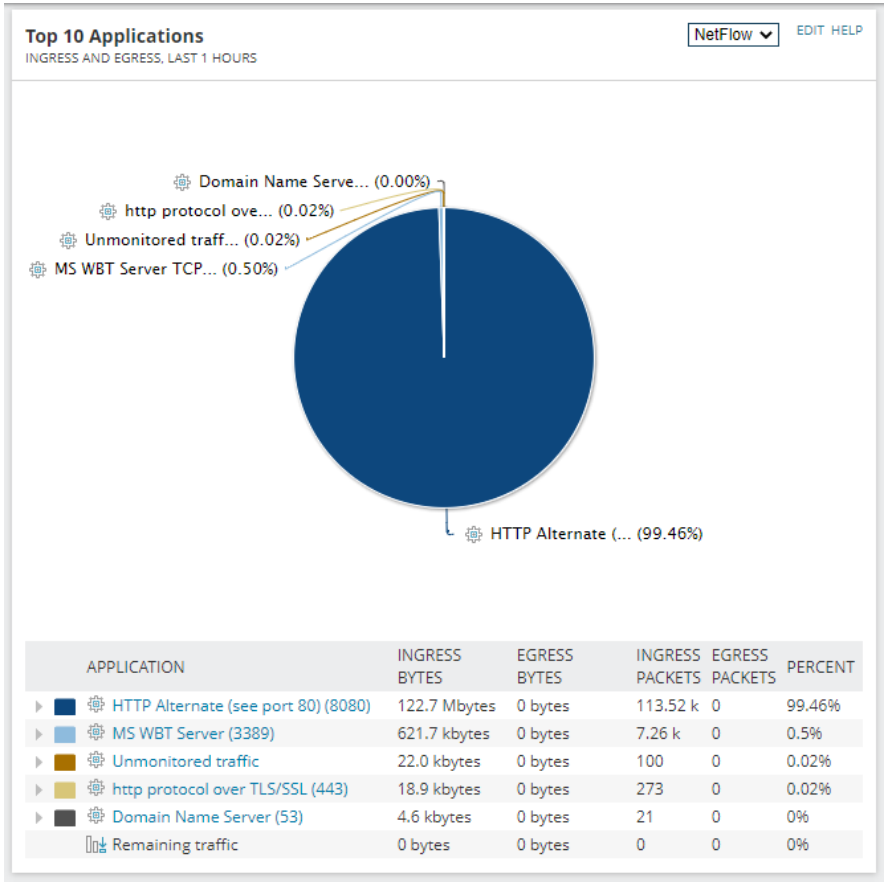


AUTOMATED
Save time and reduce misconfigurations

SEGMENTED
Improve traffic separation and security posture

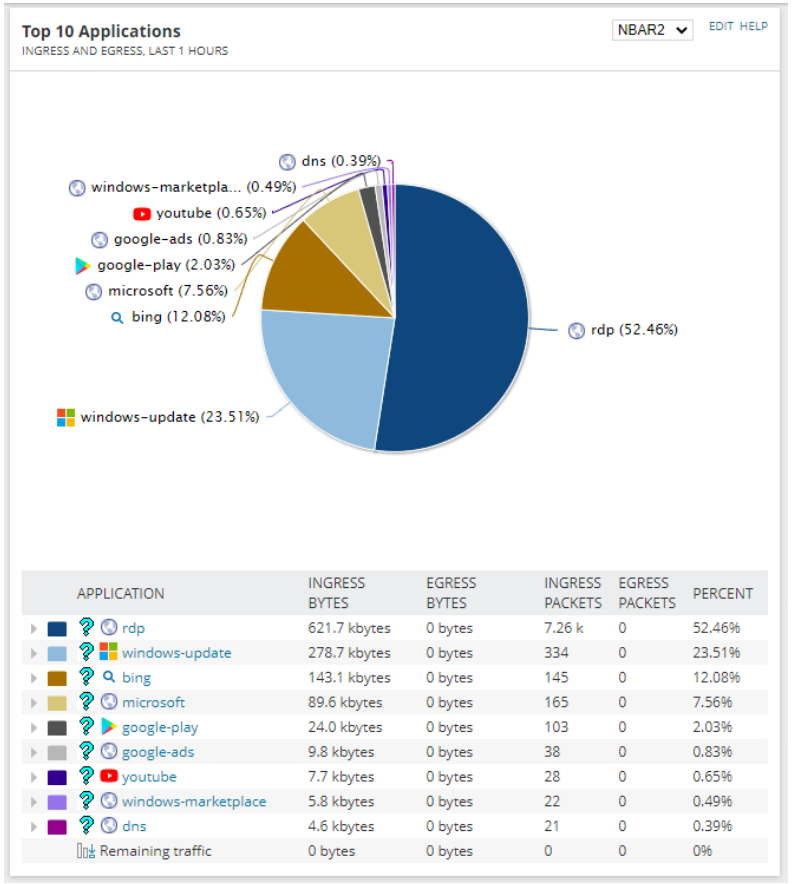
CENTRALIZED
Enhance visibility and management

Application Visibility for Micro Segmentation in Campus



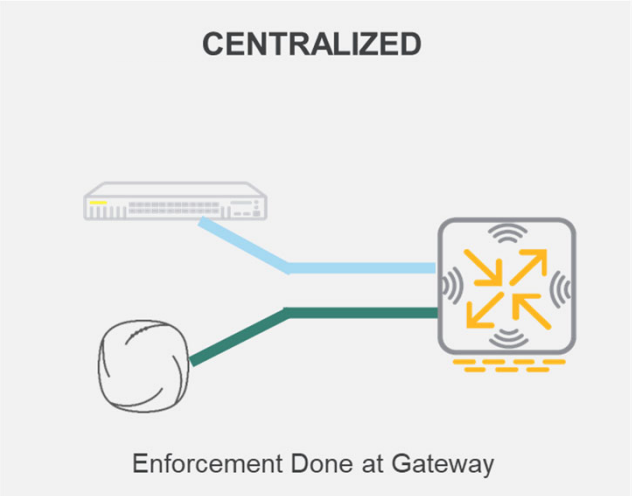
APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
HTTP Alternate (see port 80) (8080)	122.7 Mbytes	0 bytes	113.52 k	0	99.46%
MS WBT Server (3389)	621.7 kbytes	0 bytes	7.26 k	0	0.5%
Unmonitored traffic	22.0 kbytes	0 bytes	100	0	0.02%
http protocol over TLS/SSL (443)	18.9 kbytes	0 bytes	273	0	0.02%
Domain Name Server (53)	4.6 kbytes	0 bytes	21	0	0%
Remaining traffic	0 bytes	0 bytes	0	0	0%

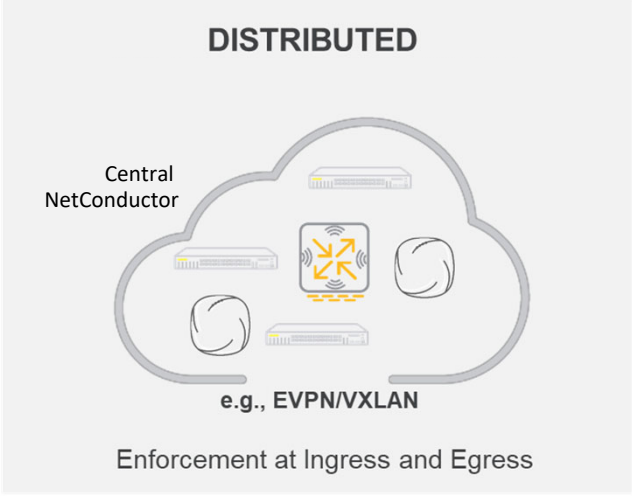
enable application recognition



APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
rdp	621.7 kbytes	0 bytes	7.26 k	0	52.46%
windows-update	278.7 kbytes	0 bytes	334	0	23.51%
bing	143.1 kbytes	0 bytes	145	0	12.08%
microsoft	89.6 kbytes	0 bytes	165	0	7.56%
google-play	24.0 kbytes	0 bytes	103	0	2.03%
google-ads	9.8 kbytes	0 bytes	38	0	0.83%
youtube	7.7 kbytes	0 bytes	28	0	0.65%
windows-marketplace	5.8 kbytes	0 bytes	22	0	0.49%
dns	4.6 kbytes	0 bytes	21	0	0.39%
Remaining traffic	0 bytes	0 bytes	0	0	0%

HPE Aruba Dynamic Segmentation with choice of overlays





- ***ClearPass Policy Manager***
- ***Policy Enforcement Firewall***

✓ Simple and easy to deploy

✓ Consistent experience across wired & wireless

✓ Enhanced security features

- **Central NetConductor**
- **Flexible NAC (ClearPass Policy Manager, Cloud Auth, other)**
- **Inline enforcement via switches & gateways**

✓ Open & multi-vendor ready

✓ Higher scale and performance

✓ Consistent operations across campus & data center

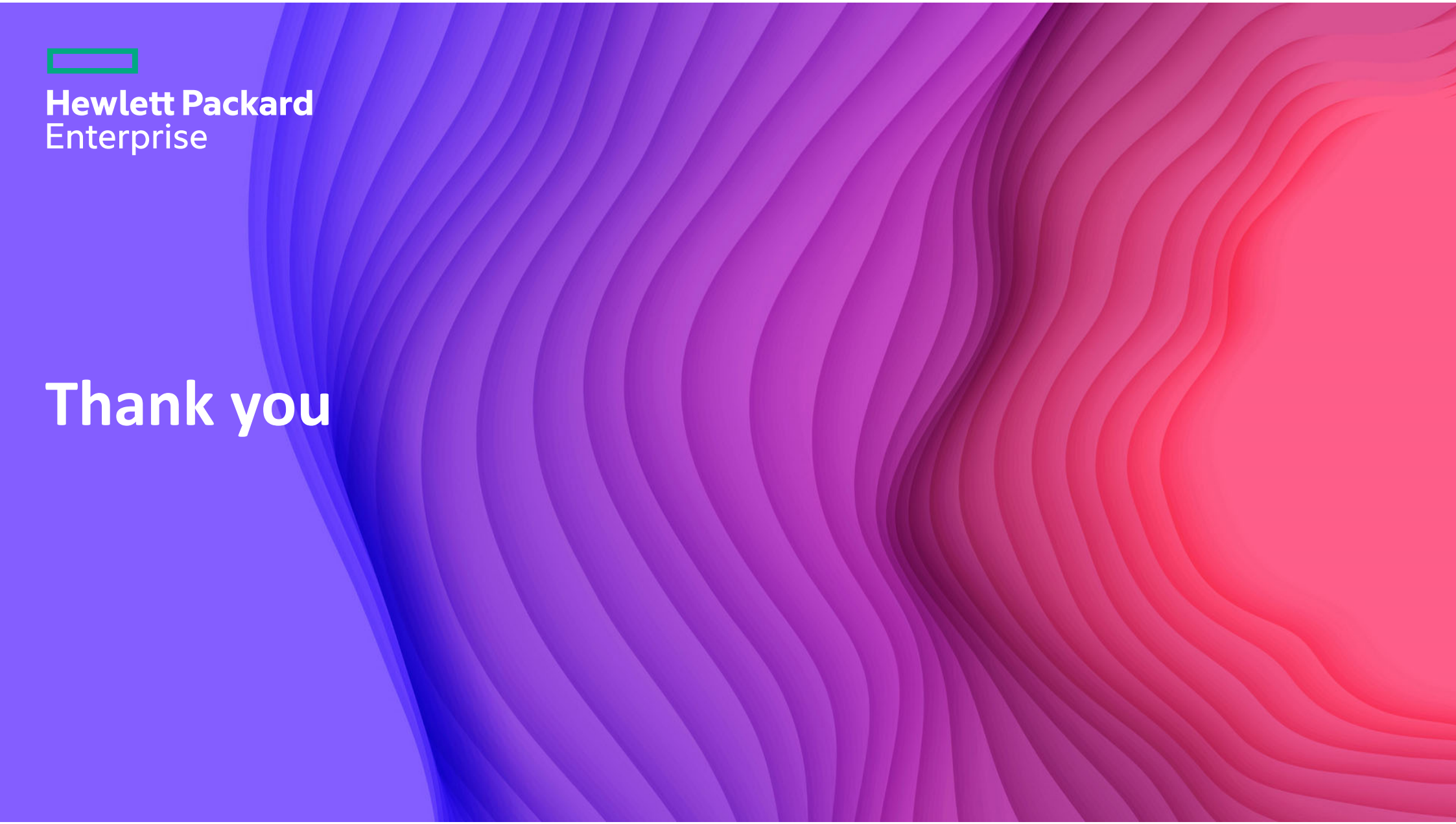
Conclusion

Conclusion

- **HPE Aruba Networking covers MANY** the Networking aspects of the Directive including **Zero trust Principles, Dynamic Network segmentation, Intelligent Firmware and configuration Management, Industry leading Identity and access management** with ClearPass and ATMOS ZTNA, and **leading machine learning** Central AIOPs.

- HPE Aruba Networking offers 40+ WLAN, LAN, DCN and SD-WAN secure connectivity technologies covering the cybersecurity, **many are unique in the market.**

- HPE Aruba Networking has a very strong trusted Infrastructure covering the entire supply chain :
  - **Secure development processes,**
  - **Trust supply chain for Trusted Delivery and Operational Integrity,**
  - **Hardware root of trust for Firmware protection and secure boot**
  - and **Secure management**


Hewlett Packard
Enterprise
Thank you