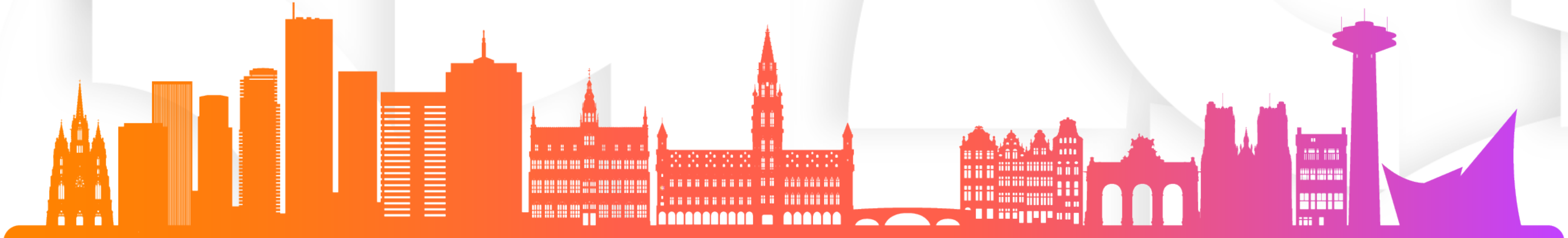
atmosphere'23
BELGIUM

How HPE Aruba Networking can help you to reach EU Cyber security NIS 2 directive compliance

Bruno Hareng, HPE Aruba Networking EMEA Cybersecurity Lead

October 19th, 2023



HPE aruba networking

DISCUSSION / TOPIC THREAD

Wired Intelligent Edge

Bring performance and reliability to your network with the Aruba Core, Aggregation, and Access layer switches. Discuss the latest features and functionality of the ArubaOS-Switch and ArubaOS-CX devices, and find ways to improve security across your network to bring together a mobile first solution.

LAG between two 8320 clusters for multiple VLANs

This thread has been viewed 37 times

1. LAG between two 8320 clusters for multiple VLANs

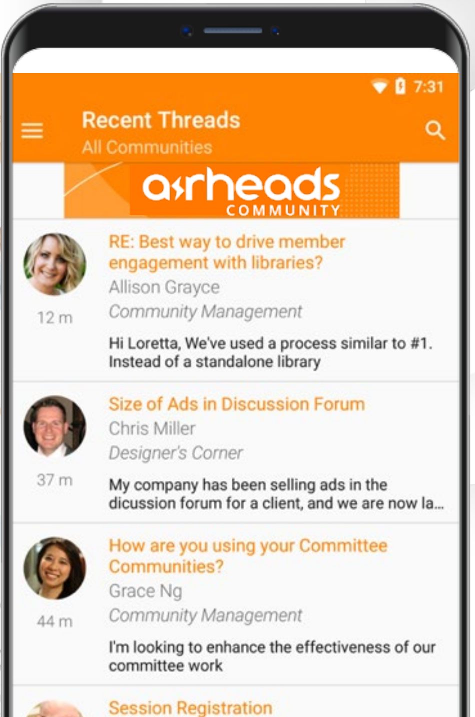
sfpit1202

Posted Nov 18, 2022 06:53 PM

I have 2 VSX Clusters. One has 2 Fiber 8320s and the other is 2 Ethernet 8320s. I currently have tv between the two clusters using the DAC ports. The LAGs are only one VLAN each.

I was trying to setup another LAG between the clusters that would carry multiple other VLANs. I v it set up just like the other LAGs that are working except instead of vlan access # I am using vlan t

I set up 1 ethernet port on the two ethernet switches and added them to the LAG just to test and wondering, is there any reason why 1/1/51 would not work as a LAG with multiple VLANs? I read



RE: Best way to drive member engagement with libraries?
Allison Grayce
Community Management
12 m
Hi Loretta, We've used a process similar to #1. Instead of a standalone library

Size of Ads in Discussion Forum
Chris Miller
Designer's Corner
37 m
My company has been selling ads in the discussion forum for a client, and we are now la...

How are you using your Committee Communities?
Grace Ng
Community Management
44 m
I'm looking to enhance the effectiveness of our committee work

Session Registration

airheads COMMUNITY

Join Today!

www.community.arubanetworks.com

Agenda

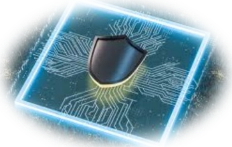
Introduction to the NIS2 Cyber Security European Directive

HPE Aruba Networking NIS 2 Directives Solutions overview (Article 21)

HPE Aruba Networking basic Cyber Hygiene solutions (Preamble 89)

Conclusion

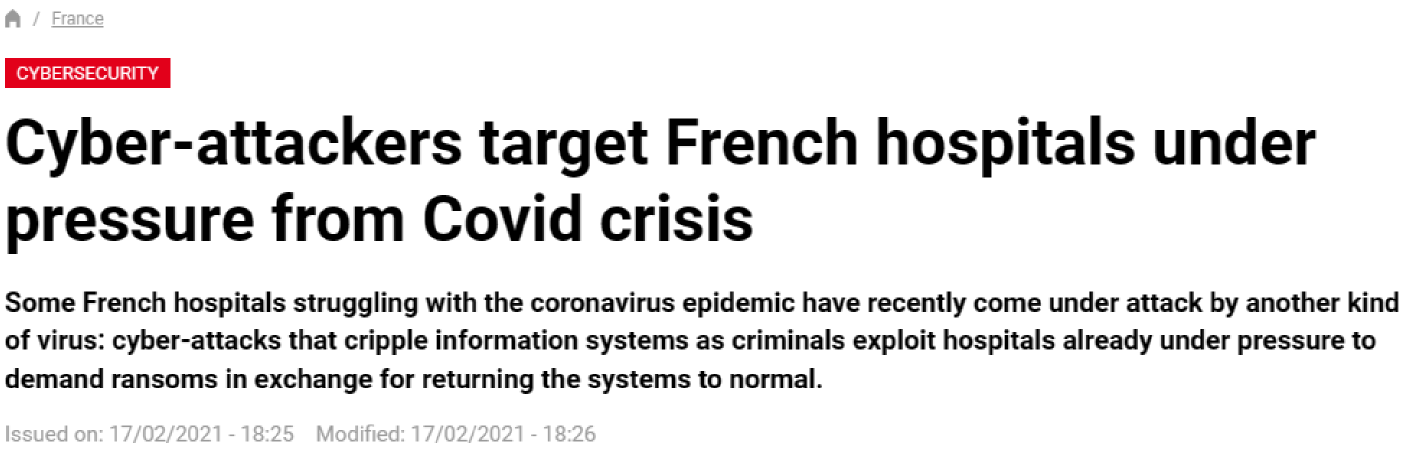
HPE Aruba Networking is leading in Highly Secure Networks

High-Security Customers	THE WHITE HOUSE WASHINGTON THE PENTAGON WASHINGTON D.C. DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE UNITED STATES OF AMERICA JOINT SPECIAL OPERATIONS COMMAND Microsoft
Security Certifications	FIPS VALIDATED 140-2 ™ DISA APPROVED Approved Products List for DoD Networks NATIONAL SECURITY AGENCY CYBERSECURITY Common Criteria PCI DSS COMPLIANT ICSA labs CERTIFIED SECURE SD-WAN FR FedRAMP ™ GDPR
Awards	Cyber Catalyst by Marsh SC awards 2019 Winner INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2019
Trusted Infrastructure	Code Signing  Hardware Root-of-Trust Encrypted Control Channels TPM Device Identity
Vulnerability Research	aruba a Hewlett Packard Enterprise company // THREAT LABS bugcrowd #1 Crowdsourced Security Company

Introduction to the NIS2 Cyber Security European Directive

NIS = Network and Information System

Why EU NIS 2 cybersecurity directive ? Rise of attacks during COVID pandemic



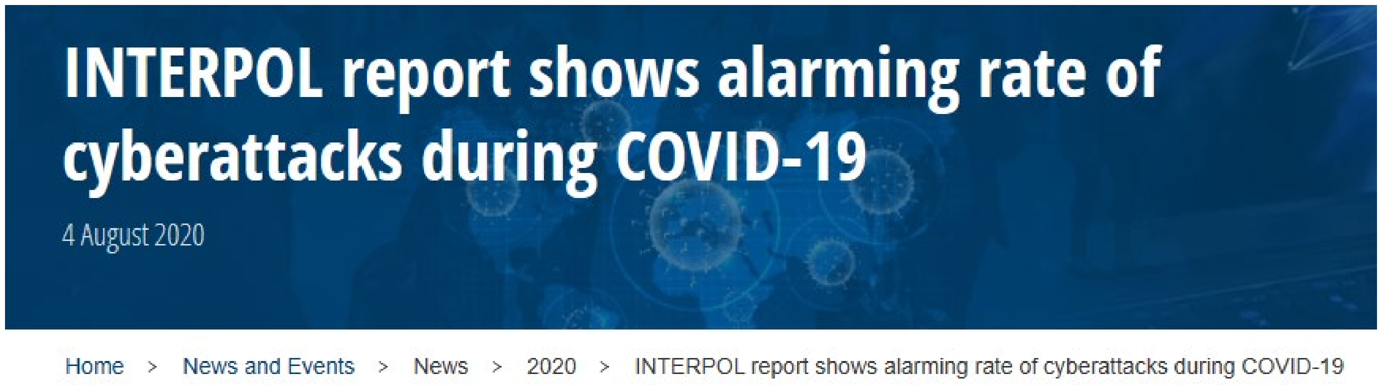
/ France

CYBERSECURITY

Cyber-attackers target French hospitals under pressure from Covid crisis

Some French hospitals struggling with the coronavirus epidemic have recently come under attack by another kind of virus: cyber-attacks that cripple information systems as criminals exploit hospitals already under pressure to demand ransoms in exchange for returning the systems to normal.

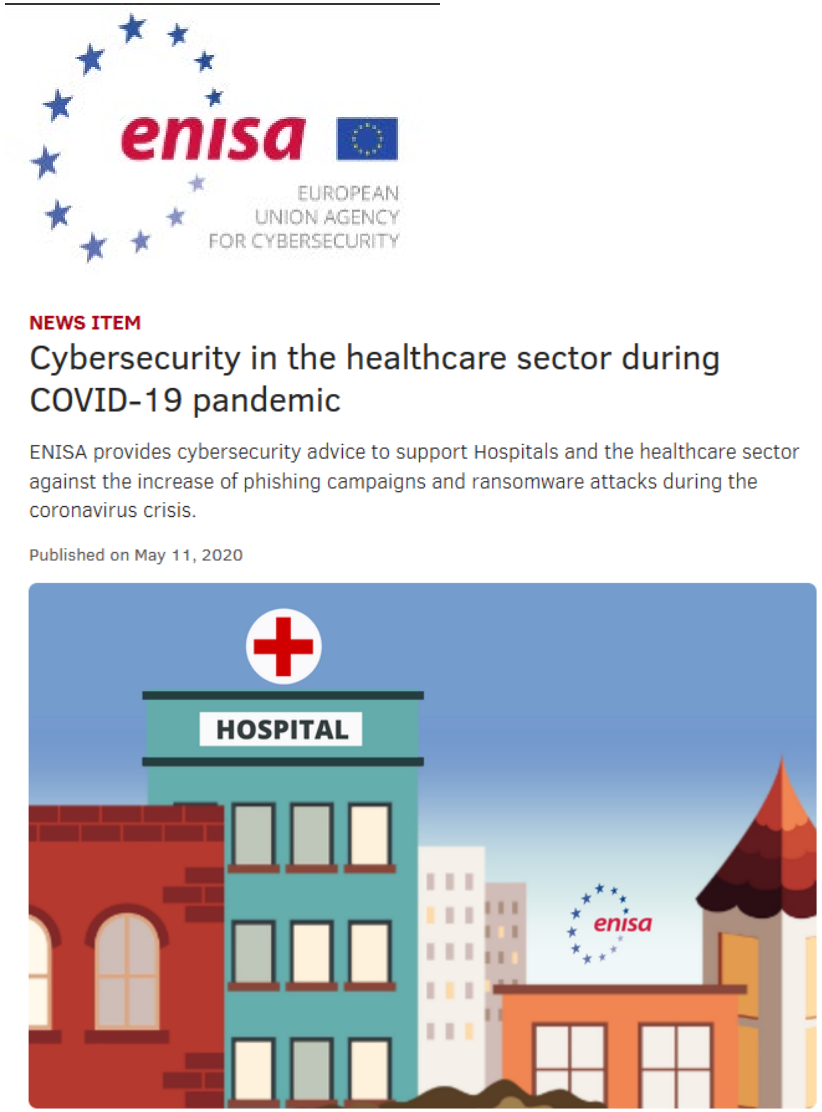
Issued on: 17/02/2021 - 18:25   Modified: 17/02/2021 - 18:26



INTERPOL report shows alarming rate of cyberattacks during COVID-19

4 August 2020

Home > News and Events > News > 2020 > INTERPOL report shows alarming rate of cyberattacks during COVID-19



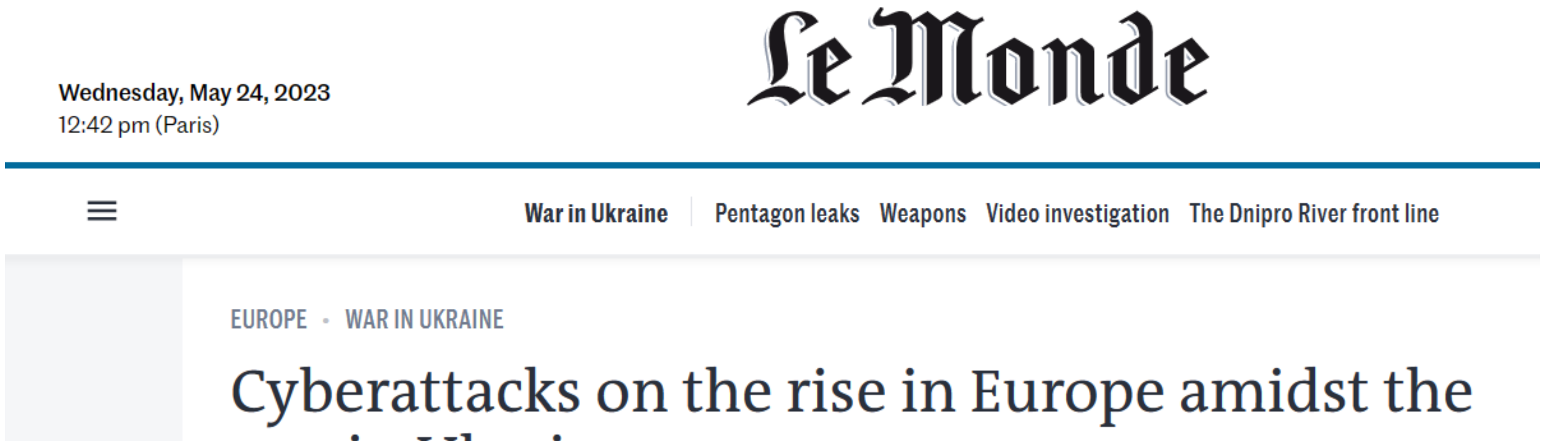
NEWS ITEM

Cybersecurity in the healthcare sector during COVID-19 pandemic

ENISA provides cybersecurity advice to support Hospitals and the healthcare sector against the increase of phishing campaigns and ransomware attacks during the coronavirus crisis.

Published on May 11, 2020

Why EU NIS 2 cybersecurity directive ? Ukraine (Cyber) War



Wednesday, May 24, 2023
12:42 pm (Paris)

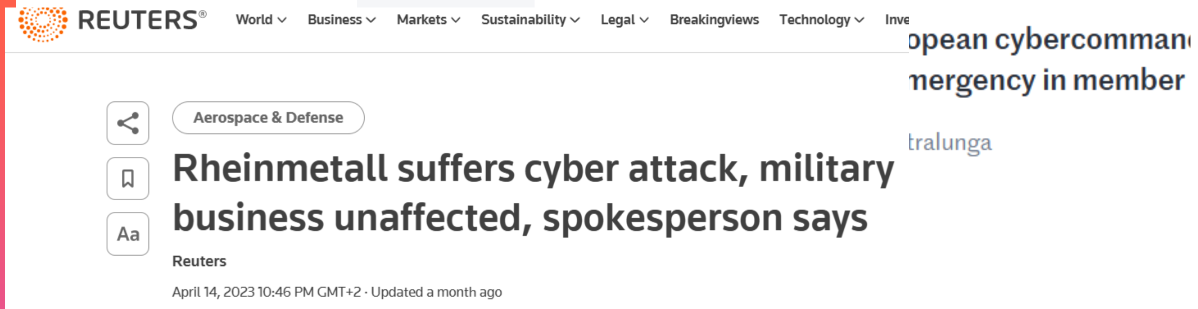
Le Monde

EUROPE · WAR IN UKRAINE

Cyberattacks on the rise in Europe amidst the war in Ukraine

opean cybercomman
mergency in member

tralunga

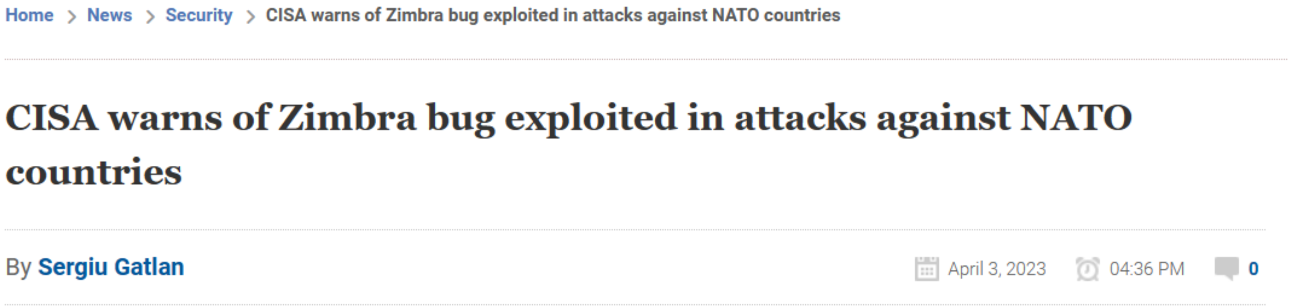


Aerospace & Defense

Rheinmetall suffers cyber attack, military business unaffected, spokesperson says

Reuters

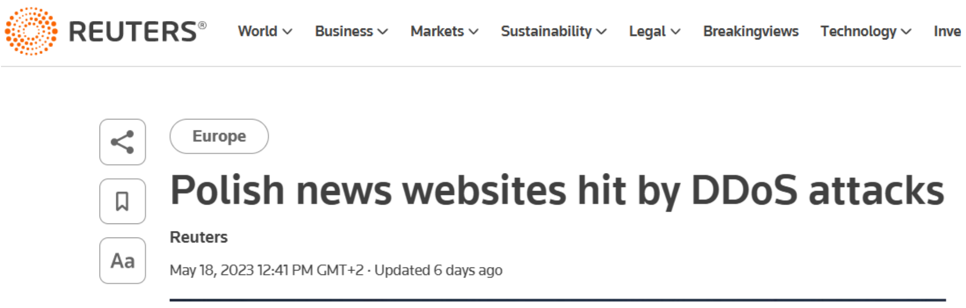
April 14, 2023 10:46 PM GMT+2 · Updated a month ago



Home > News > Security > CISA warns of Zimbra bug exploited in attacks against NATO countries

CISA warns of Zimbra bug exploited in attacks against NATO countries

By Sergiu Gatlan April 3, 2023 04:36 PM 0

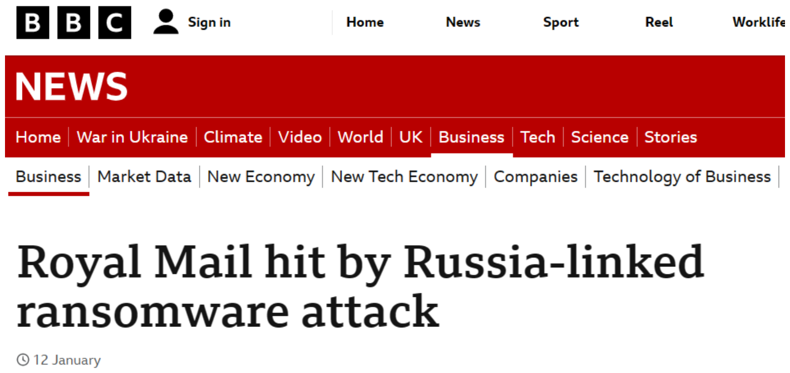


Europe

Polish news websites hit by DDoS attacks

Reuters

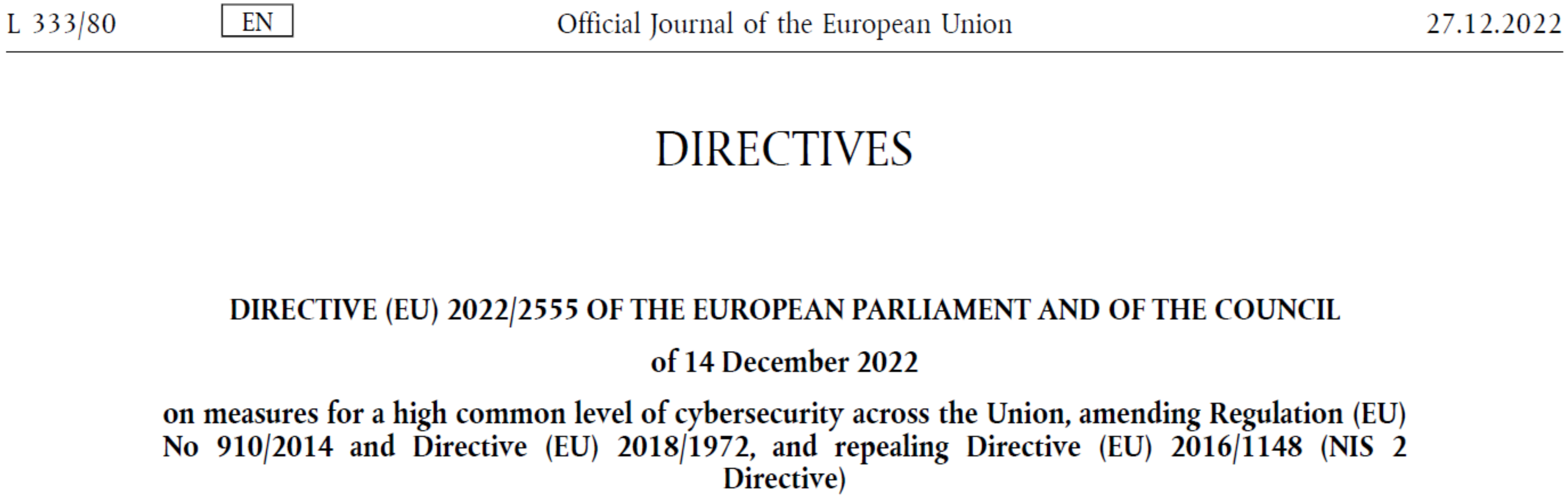
May 18, 2023 12:41 PM GMT+2 · Updated 6 days ago



Royal Mail hit by Russia-linked ransomware attack

12 January

EU NIS 2 Directive Context and Objectives



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

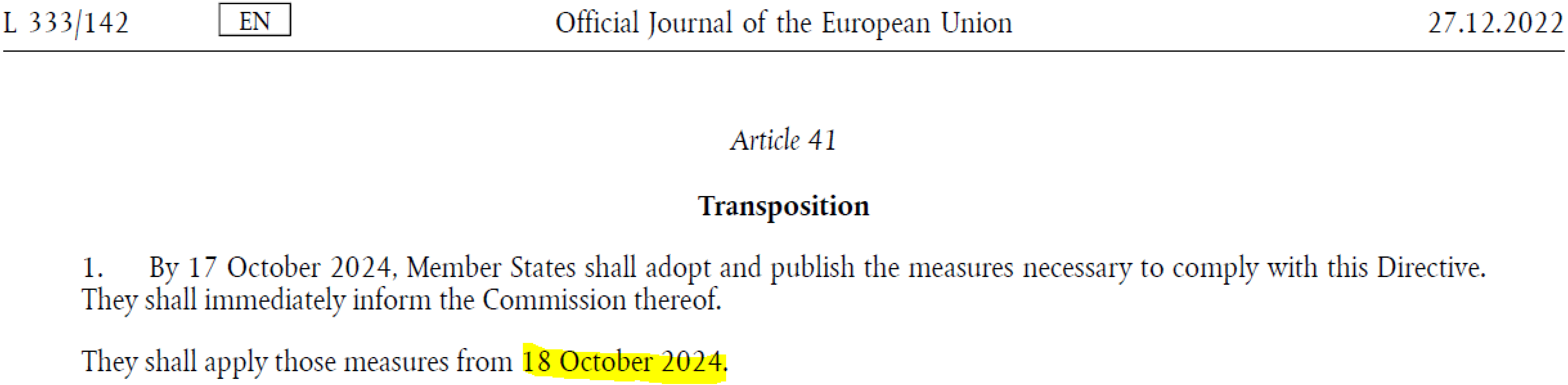
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Objectives:

1. **Increase the level of cyber-resilience of all public and private entities which fulfil important functions for the economy and society in the European Union**
2. **Reduce inconsistencies in resilience in the sectors already covered by the NIS 1 directive (2016)**
3. **Improve the level of joint situational awareness and the collective capability to prepare and respond to attacks**

EU NIS 2 Directive Timelines

- **Initial work started in 2020 after various EU parliament resolutions and EU Council conclusions**
- **November 10, 2022 - the European Parliament adopts the NIS 2 Directive.**
- **November 28, 2022 - The EU Council adopts the NIS 2 Directive.**
- **December 27, 2022 – The NIS 2 directive is published in the Official Journal of the EU**
- **Next step:** Member states must incorporate the provisions of the NIS 2 Directive into national law in **21 months**



L 333/142 EN Official Journal of the European Union 27.12.2022

Article 41

Transposition

1. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 18 October 2024.

EU NIS 2 Scope- Essential and Important Entities – 50+ employees / 10M€+

1 Million + enterprises and administrations are directly or indirectly are impacted

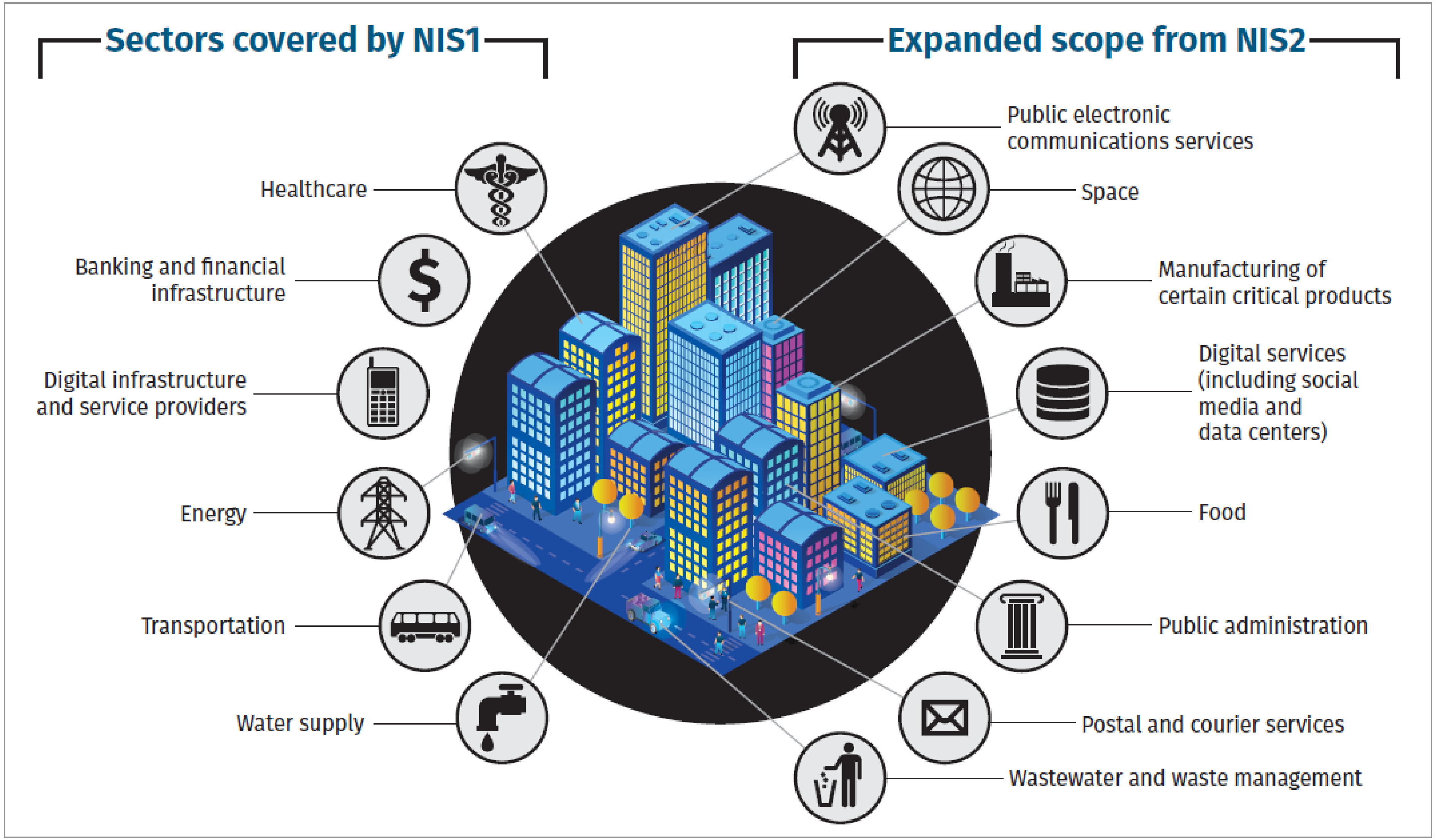

Sectors covered by NIS1
Healthcare
Banking and financial infrastructure
Digital infrastructure and service providers
Energy
Transportation
Water supply
Expanded scope from NIS2
Public electronic communications services
Space
Manufacturing of certain critical products
Digital services (including social media and data centers)
Food
Public administration
Postal and courier services
Wastewater and waste management

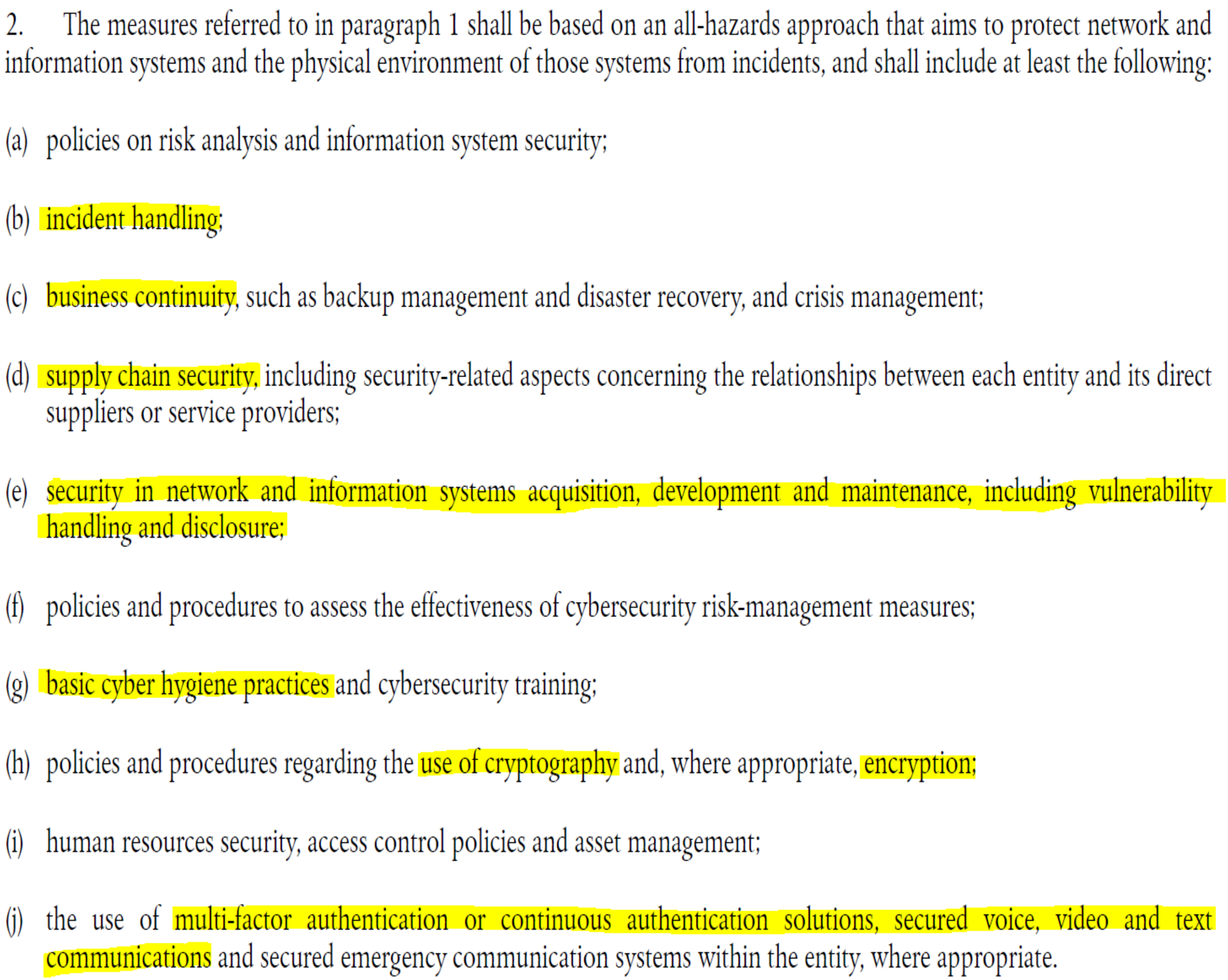
Figure 4. NIS2 In-Scope Sectors

Source: SANS Institute

HPE Networking NIS 2 Directives Solutions Overview

Article 21

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)

21-2-c Business Continuity

HPE Aruba Networking Availability Technologies

- Air Slice
- Client Match
- AP / Gateways Hitless failover
- AP Seamless Upgrade
- AirMatch
- AOS 10 Live Upgrade
- WLAN Application Assurance

WIFI

- CX VSX Active Gateway/ Forwarding
- CX ISSU
- CX VSX And VSX live upgrade (ESU)
- CX Always PoE On

Campus

- SDWAN DDoS Protection
- SDWAN Cloud Traffic Steering

SD-WAN

- CX10k DDoS Protection

DCN

- Central FedRAMP
- Configuration Backup & Recovery in Central
- Central HA Design
- CPPM Cluster HA

NETWORK MANAGEMENT

21-2-d/e Supply Chain Security – HPE Aruba Trusted Infrastructure

Secure Development Life Cycle (SDLC)

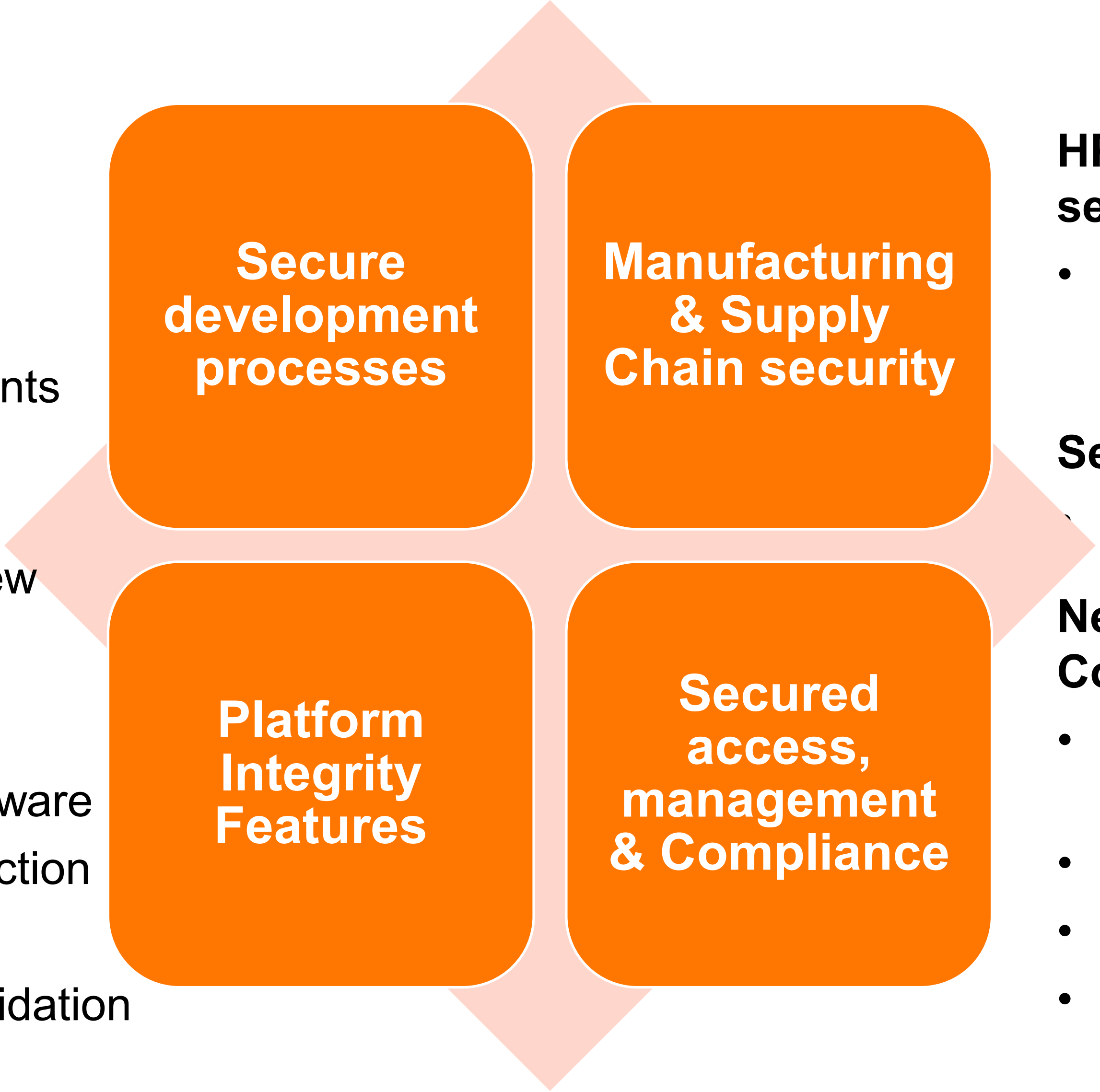
- Developer training and security awareness
- Product security assessments
- Secure development processes
- Static analysis / Code review
- Vulnerability / Bug Bounty

Hardware

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

Firmware

- Secure boot / signature validation
- Authenticated updates


Secure development processes
Manufacturing & Supply Chain security
Platform Integrity Features
Secured access, management & Compliance

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

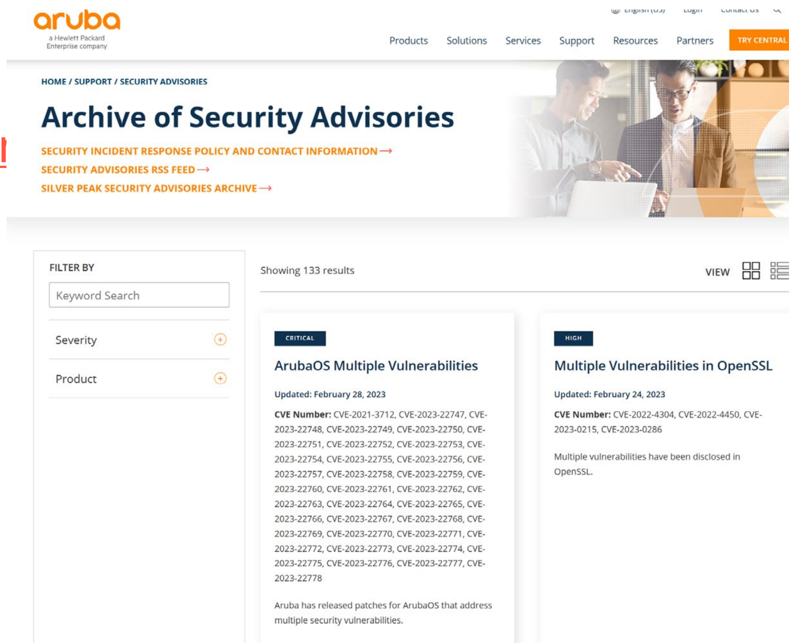
21-2-e Vulnerability Handling – HPE Aruba Threat Labs

– Aruba Threat Labs is the internal threat research organization tasked with keeping Aruba products secure.

– Its role is to stay on top of threats, find vulnerabilities through original research, manage Aruba’s bug bounty program, and act as the face of the PSIRT (Product Security Incident Response Team)

– Security Advisories | Aruba (arubanetworks.com)

– Product Security Incident Response Policy | Aruba (arubanetworks.coı



HOME / SUPPORT / SECURITY ADVISORIES

Archive of Security Advisories

SECURITY INCIDENT RESPONSE POLICY AND CONTACT INFORMATION ⟶

SECURITY ADVISORIES RSS FEED ⟶

SILVER PEAK SECURITY ADVISORIES ARCHIVE ⟶

Showing 133 results

ArubaOS Multiple Vulnerabilities

Updated: February 28, 2023

CVE Number: CVE-2021-3712, CVE-2023-22747, CVE-2023-22748, CVE-2023-22749, CVE-2023-22750, CVE-2023-22751, CVE-2023-22752, CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756, CVE-2023-22757, CVE-2023-22758, CVE-2023-22759, CVE-2023-22760, CVE-2023-22761, CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769, CVE-2023-22770, CVE-2023-22771, CVE-2023-22772, CVE-2023-22773, CVE-2023-22774, CVE-2023-22775, CVE-2023-22776, CVE-2023-22777, CVE-2023-22778

Aruba has released patches for ArubaOS that address multiple security vulnerabilities.

Multiple Vulnerabilities in OpenSSL

Updated: February 24, 2023

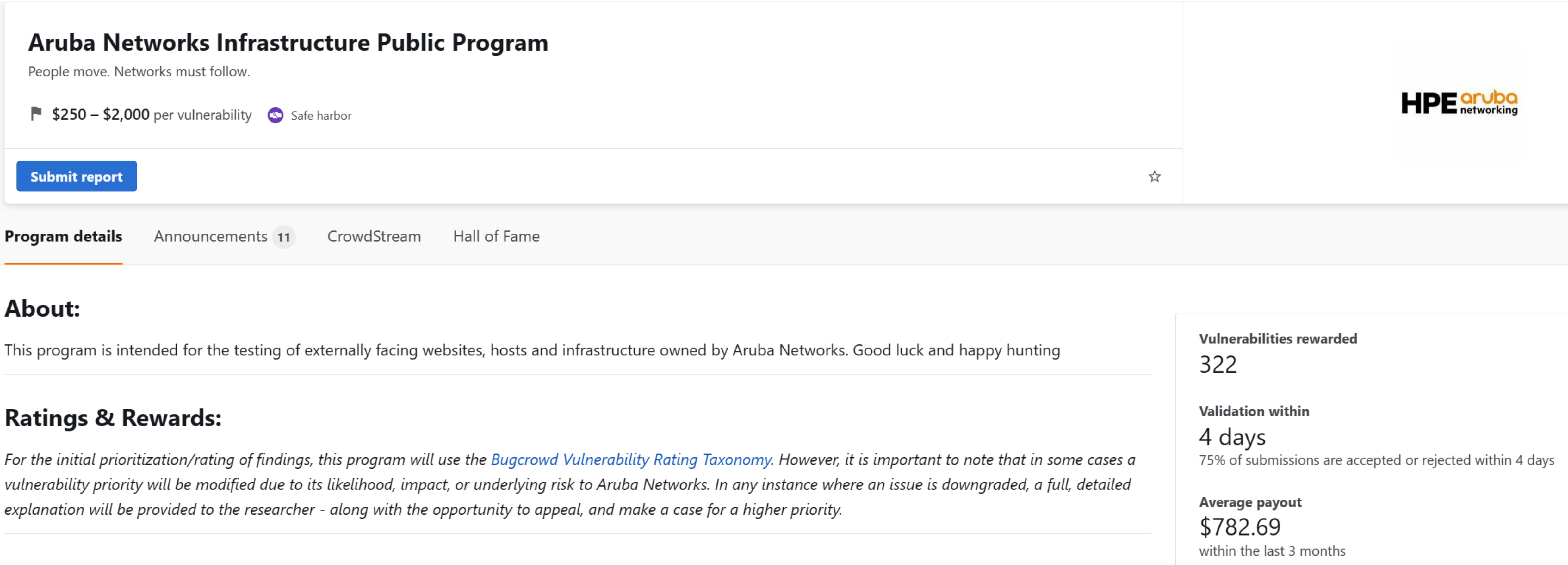
CVE Number: CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286

Multiple vulnerabilities have been disclosed in OpenSSL.

Aruba Networks’s bug bounty program - Bugcrowd

bugcrowd
#1 Crowdsourced Security Company

https://bugcrowd.com/aruba-public



Aruba Networks Infrastructure Public Program

People move. Networks must follow.

$250 – $2,000 per vulnerability   Safe harbor

About:

This program is intended for the testing of externally facing websites, hosts and infrastructure owned by Aruba Networks. Good luck and happy hunting

Ratings & Rewards:

For the initial prioritization/rating of findings, this program will use the Bugcrowd Vulnerability Rating Taxonomy. However, it is important to note that in some cases a vulnerability priority will be modified due to its likelihood, impact, or underlying risk to Aruba Networks. In any instance where an issue is downgraded, a full, detailed explanation will be provided to the researcher - along with the opportunity to appeal, and make a case for a higher priority.

Vulnerabilities rewarded
322

Validation within
4 days
75% of submissions are accepted or rejected within 4 days

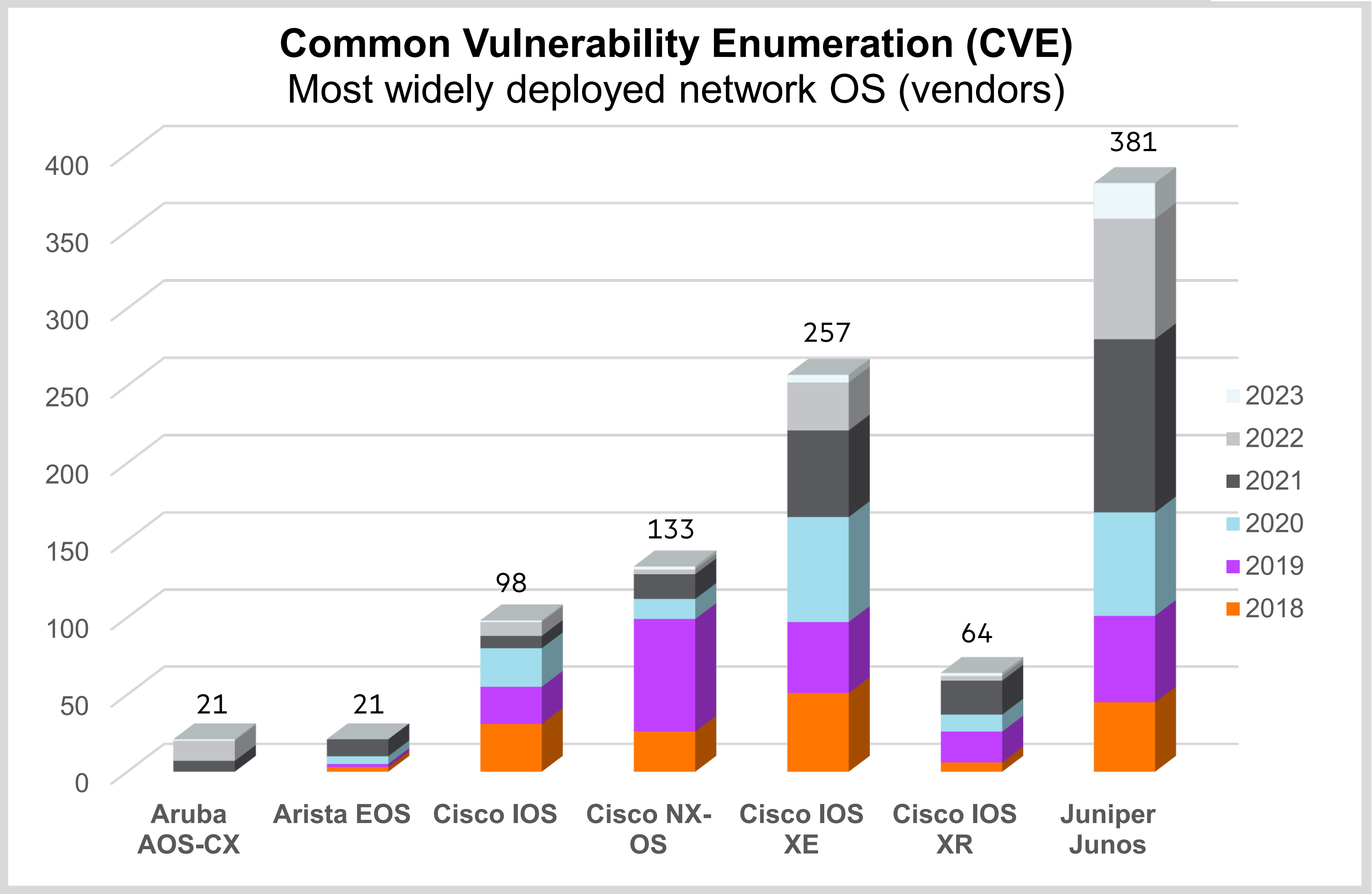
Average payout
$782.69
within the last 3 months

AOS-CX – Leader in low level of CVE – Common Vulnerability Enumeration

HPE Aruba Networking commitment to quality with Customer First, Customer Last global NTL team

- “Shift left” test philosophy
- Exhaustive scale testing
- ~50,000 test cases per day
- ~85% test case automation
- 10,000+ automated test cases for over 40 protocols

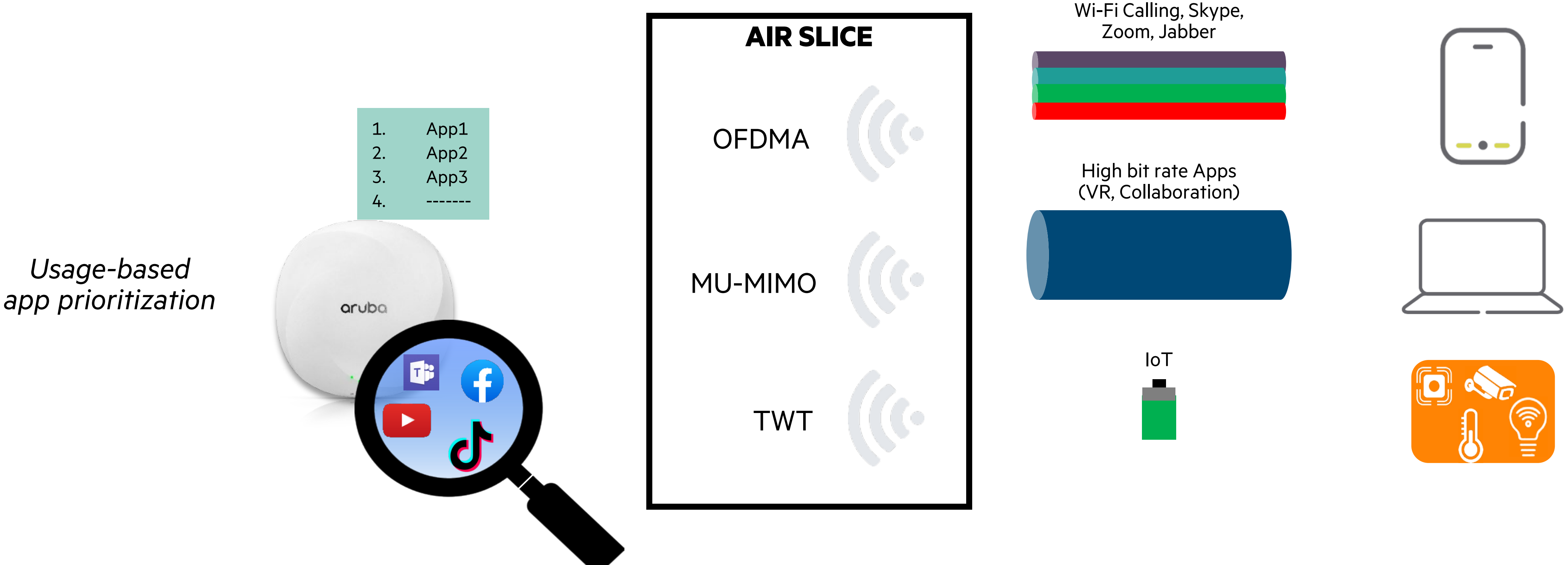
Quality focused development and test lowers CVEs, reduces network disruptions



https://cve.mitre.org

21-2-j Secure video, voice and text communication – HPE Aruba Air Slice

Application-aware Quality of Service (QoS)



Usage-based app prioritization
1. App1
2. App2
3. App3
4. -------
aruba
AIR SLICE
OFDMA
MU-MIMO
TWT
Wi-Fi Calling, Skype, Zoom, Jabber
High bit rate Apps (VR, Collaboration)
IoT

Application identification via Aruba's Layer 7 DPI engine

Scheduling intelligence provides fine-grained QoS assurance for individual applications

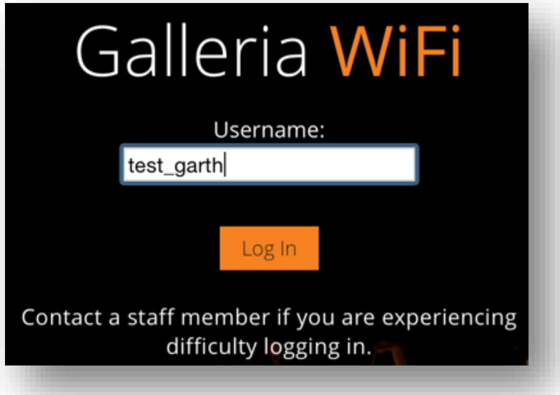
RF SLAs: Guaranteed bit rate, improved battery life, bounded latency/jitter/packet loss

Leverages Wi-Fi 6 constructs: MU-MIMO, OFDMA, TWT (Target Wake Time)

Benefits Wi-Fi 6 and earlier generations, based on use of internal queuing

21-2-j Multi-Factor Authentication with ClearPass: Example DUO Workflow

Step 1 – Who are you?

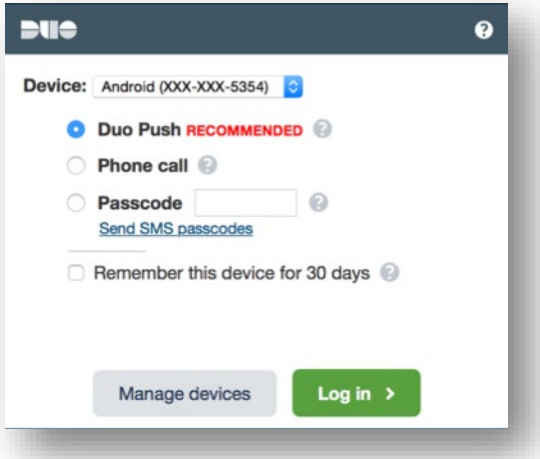


Galleria WiFi

Username: test_garth

Contact a staff member if you are experiencing difficulty logging in.

Step 2 – 1st Factor Something You Have



Device: Android (XXX-XXX-5354)

● Duo Push RECOMMENDED

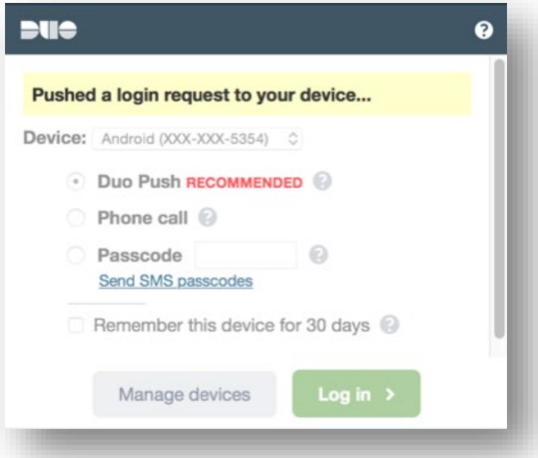
○ Phone call

○ Passcode

Send SMS passcodes

□ Remember this device for 30 days

Step 3 – Request Approval from Known Device



Pushed a login request to your device...

Device: Android (XXX-XXX-5354)

● Duo Push RECOMMENDED

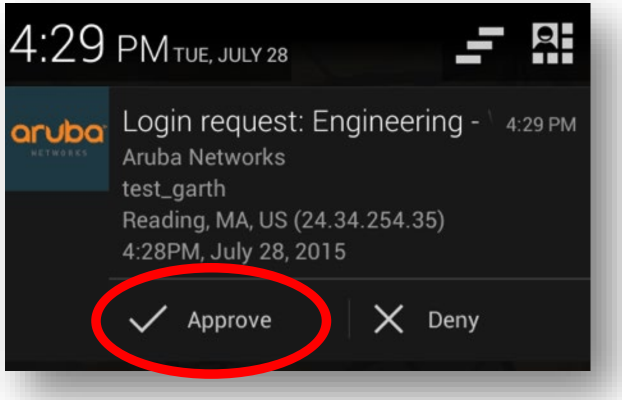
○ Phone call

○ Passcode

Send SMS passcodes

□ Remember this device for 30 days

Step 4 – Approve from Known Device



4:29 PM TUE, JULY 28

Login request: Engineering - 4:29 PM

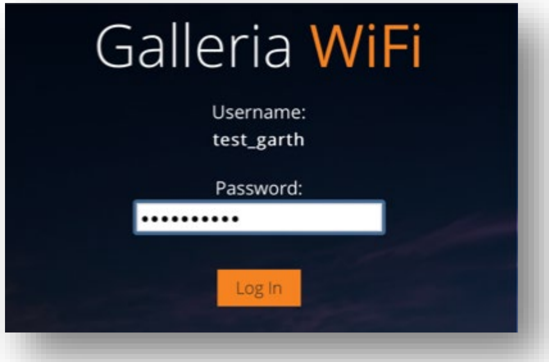
Aruba Networks

test_garth

Reading, MA, US (24.34.254.35)

4:28PM, July 28, 2015

Step 5 – 2nd Factor Something You Know

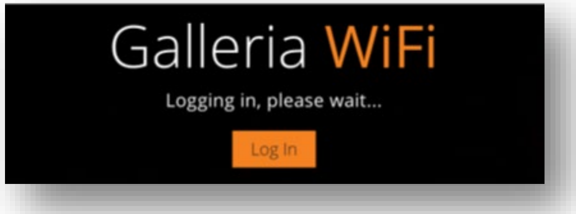


Galleria WiFi

Username: test_garth

Password: ••••••••••••

Step 6 – Logging in!

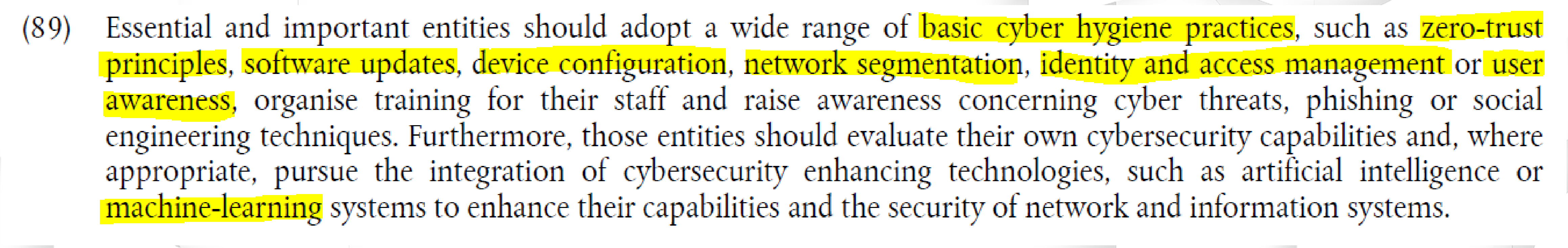


Galleria WiFi

Logging in, please wait...

HPE Networking Solutions overview for Basic Cyber Hygiene practice

Preamble 89



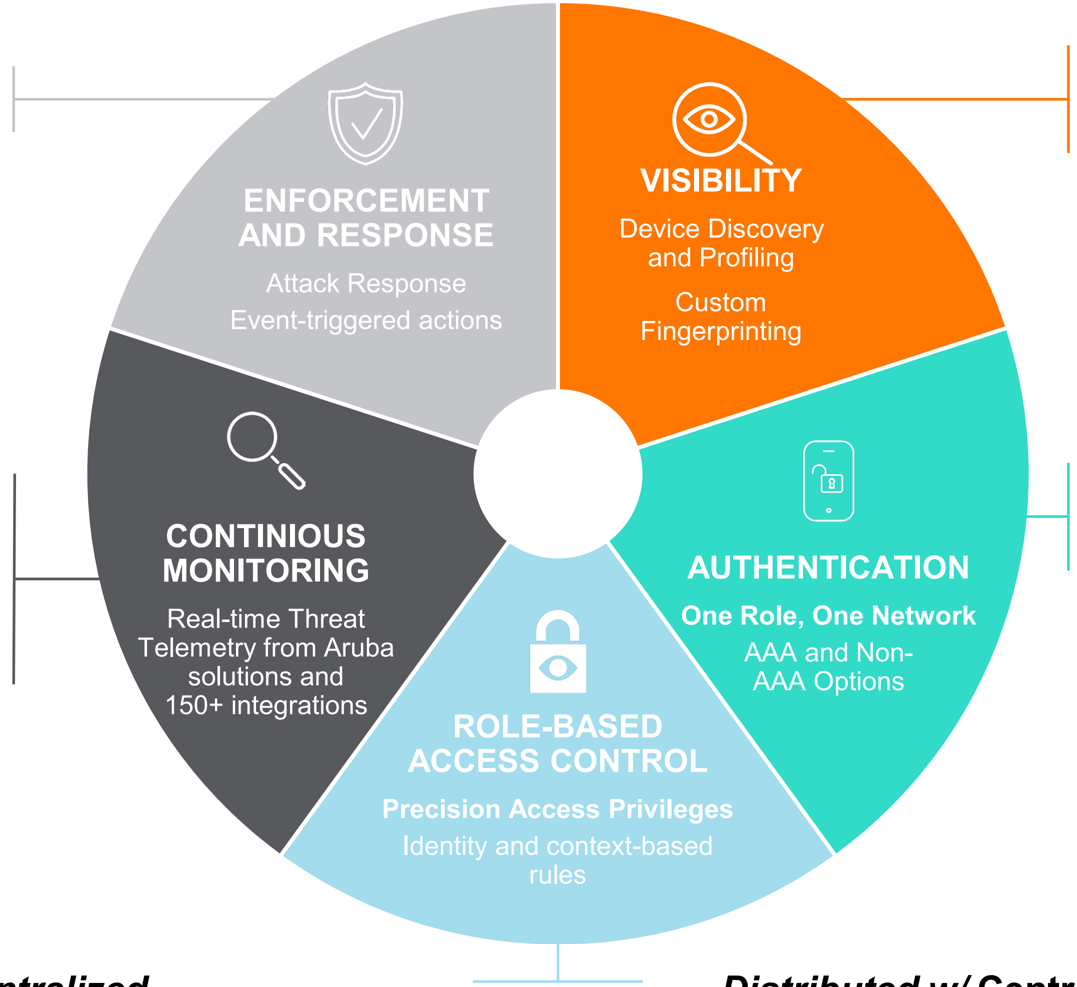
(89) Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning 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, HPE Aruba 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

21-2-g - HPE Aruba Networking Zero Trust security foundation



ClearPass Policy Manager

Client Insights
ClearPass Device Insight

ENFORCEMENT AND RESPONSE

Attack Response
Event-triggered actions

VISIBILITY

Device Discovery and Profiling

Custom Fingerprinting

CONTINIOUS MONITORING

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

AUTHENTICATION

One Role, One Network

AAA and Non-AAA Options

ROLE-BASED ACCESS CONTROL

Precision Access Privileges

Identity and context-based rules

Policy Enforcement Firewall
SD-WAN
Unified Threat Management/IDS/IPS
360 Security Exchange

Cloud Auth
ClearPass Policy Manager

Centralized

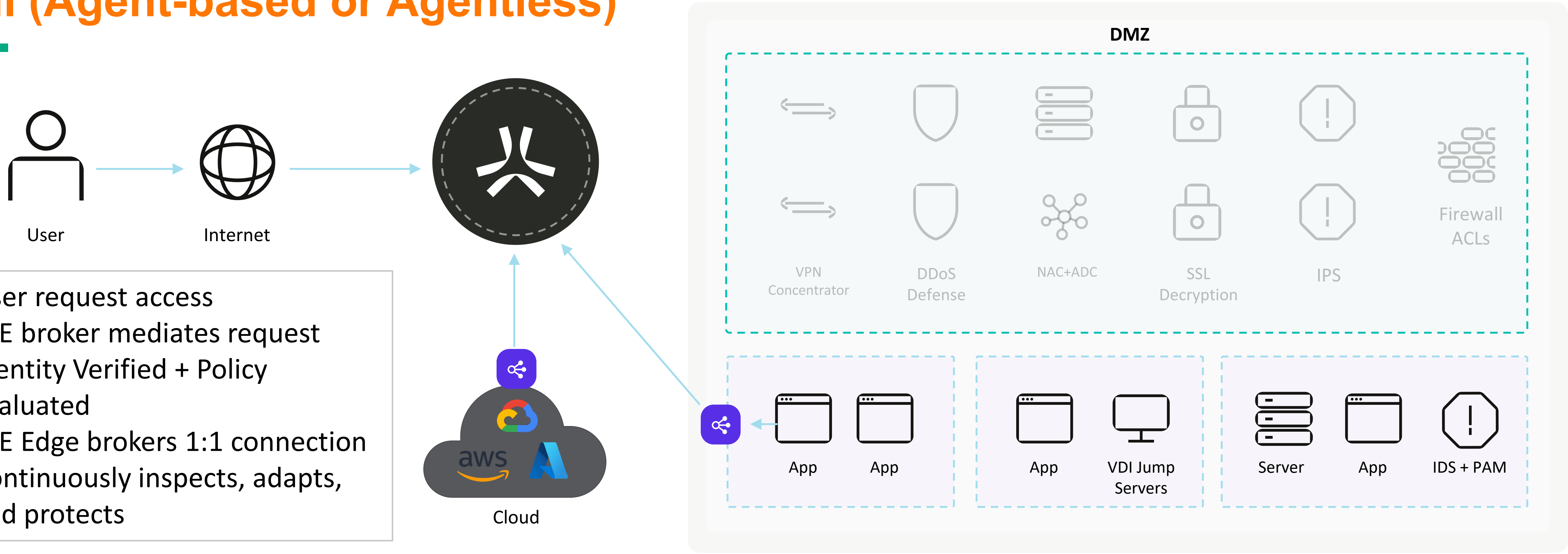
- ClearPass Policy Manaţ
- Policy Enforcement Fire

Dynamic Segmentation

***Distributed w/* Central NetConductor**

- Policy Manager, Flexible NAC
- Inline Enforcement via Switches & Gateways

21-2-g-zero trust principles - HPE Aruba Axis ZTNA delivers zero trust access for all (Agent-based or Agentless)



1. User request access
2. SSE broker mediates request
3. Identity Verified + Policy Evaluated
4. SSE Edge brokers 1:1 connection
5. Continuously inspects, adapts, and protects

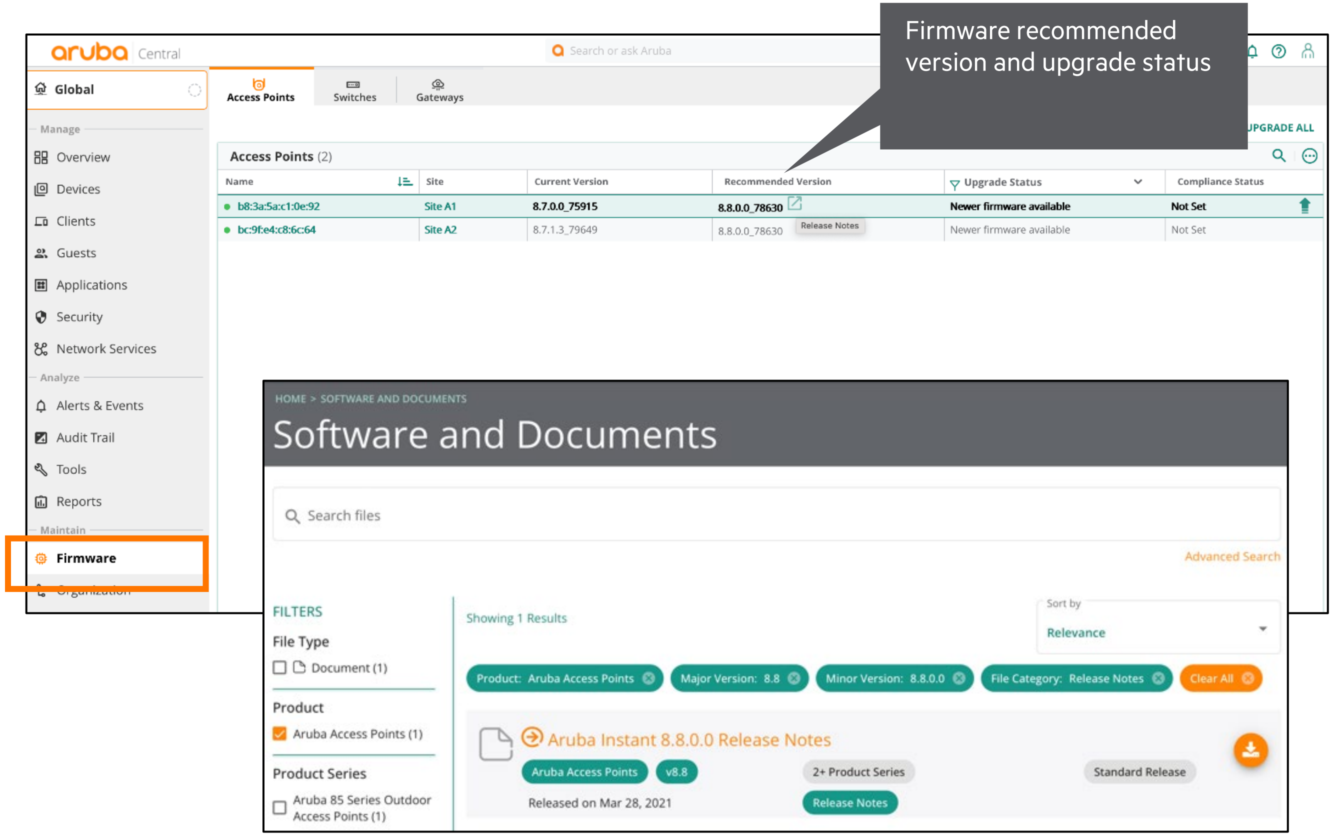
The invisible network.
Inside-out connections make apps completely invisible and never exposed to the internet.

Application access,
never network access.
Remote users only receive access to authorized applications without placing user or device on the corporate network.

Granular least privilege access.
App-to-user connections provide built-in app segmentation without complex network segmentation. One-to-one connections make lateral movement impossible for unauthorized users.

21-2-g– software updates - Wi-Fi Firmware Recommender

Proactive ML-based firmware recommendations to eliminate manual overhead



Firmware recommended version and upgrade status

Access Points (2)

Name	Site	Current Version	Recommended Version	Upgrade Status	Compliance Status
b8:3a:5a:c1:0e:92	Site A1	8.7.0.0_75915	8.8.0.0_78630	Newer firmware available	Not Set
bc:9f:e4:c8:6c:64	Site A2	8.7.1.3_79649	8.8.0.0_78630	Newer firmware available	Not Set

Reduced risk of non-compliance with proactive AI-powered firmware recommendations for APs

70% of enterprises without a firmware upgrade plan will be breached due to a firmware vulnerability

Source : Gartner, 2022

Key Capabilities

AIOps Powered: ML- based firmware upgrade recommendation for Instant 6.x/8.x and AOS 10 APs

Reduced Manual Overhead: eliminates dependency on human recommendations and static data files

Enhanced Accuracy : Monitors software per AP model, TAC cases opened per version, firmware popularity, age and other related parameters, eliminating guesswork

21-2-g– software updates - Hot-Patching Services with CX switches

Hyper-targeted, custom fixes for defects and vulnerabilities

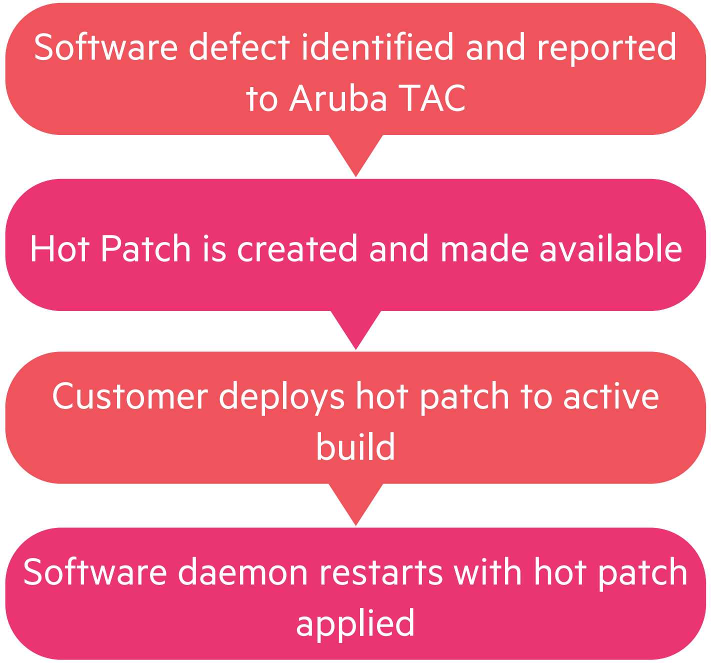
What is a Hot Patch?

- Precise fixes for critical defects and security vulnerabilities
- No physical reboot required; automatically re-applied on future reboots
- Custom branch fixes are aggregated and rolled into future releases

Benefits

- Unique to implemented software release, no need to re-qualify a new image
- Quick turn & implementation–weeks, not months–from initial customer request to install
- No impact to active network or traffic when applied
- Hot patch included in next minor release

Total Downtime: 0%

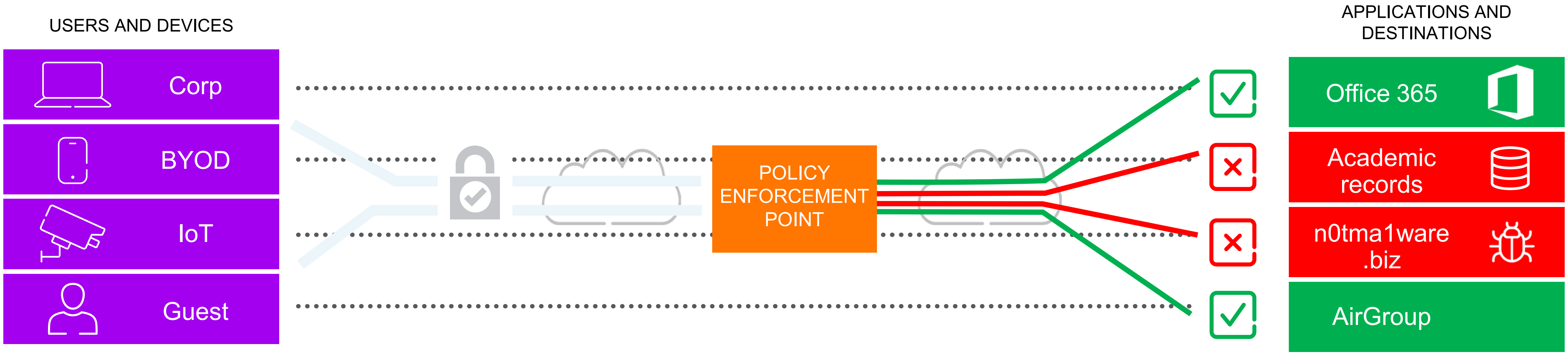

Software defect identified and reported to Aruba TAC
Hot Patch is created and made available
Customer deploys hot patch to active build
Software daemon restarts with hot patch applied

Configurations Supported

Chassis Stack Standalone

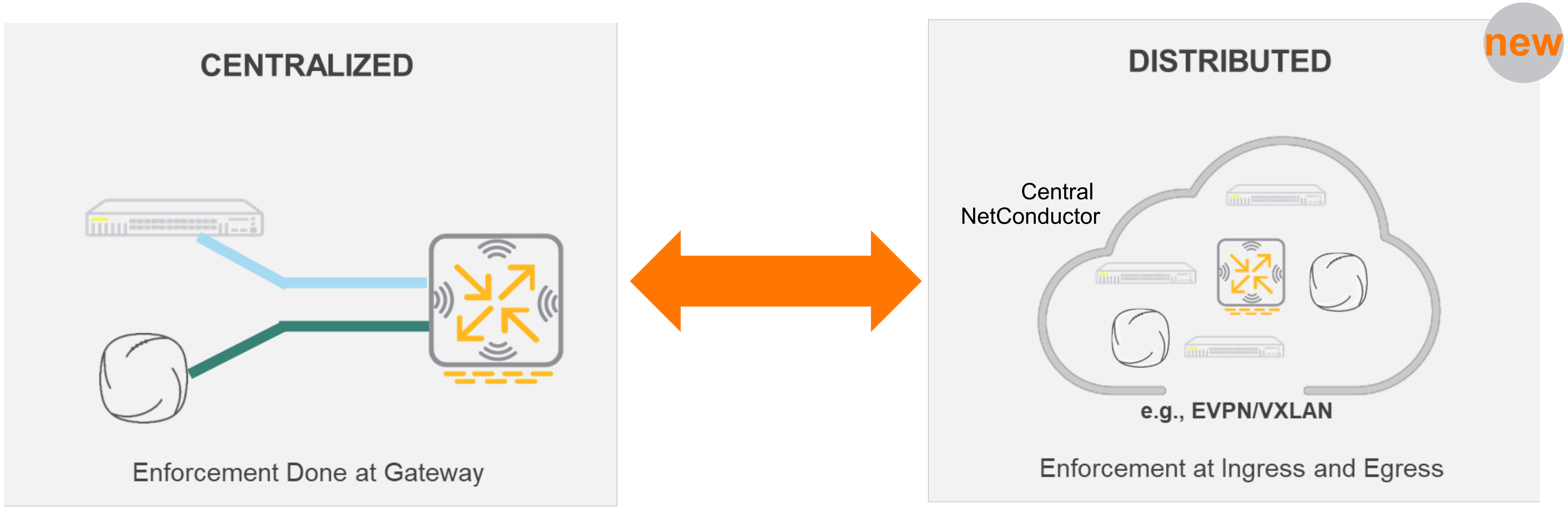
21-2-g– HPE Aruba Unified Dynamic Segmentation Solutions

Automatically enforce least-privilege access to resources based on identity



Choice & flexibility in enforcement model

21-2-g– HPE Aruba Dynamic Segmentation with choice of overlays



CENTRALIZED

Enforcement Done at Gateway

DISTRIBUTED

new

Central NetConductor

e.g., EVPN/VXLAN

Enforcement at Ingress and Egress

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

✓ Simple and easy to deploy

✓ Consistent experience across wired & wireless

✓ Enhanced security features

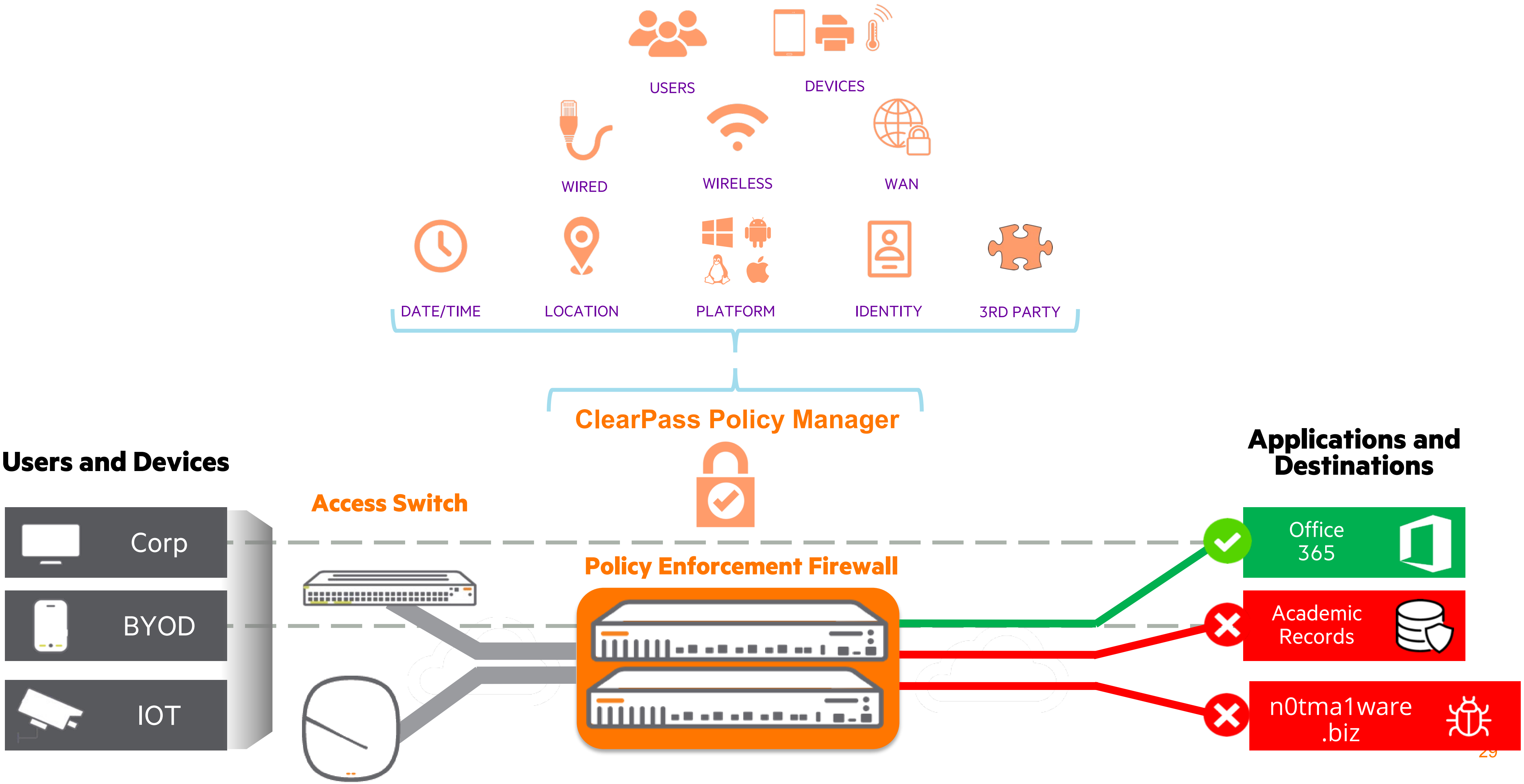
- **Central NetConductor**
- **Flexible NAC (ClearPass Policy Manager, Cloud Auth, ot**
- **Inline enforcement via switches & gateways**

✓ Open & multi-vendor ready

✓ Higher scale and performance

✓ Consistent operations across campus & data center

Context Enabled Dynamic Segmentation with Clearpass



USERS

DEVICES

WIRED

WIRELESS

WAN

DATE/TIME

LOCATION

PLATFORM

IDENTITY

3RD PARTY

ClearPass Policy Manager

Users and Devices

Access Switch

Policy Enforcement Firewall

Applications and Destinations

Corp

BYOD

IOT

Office 365

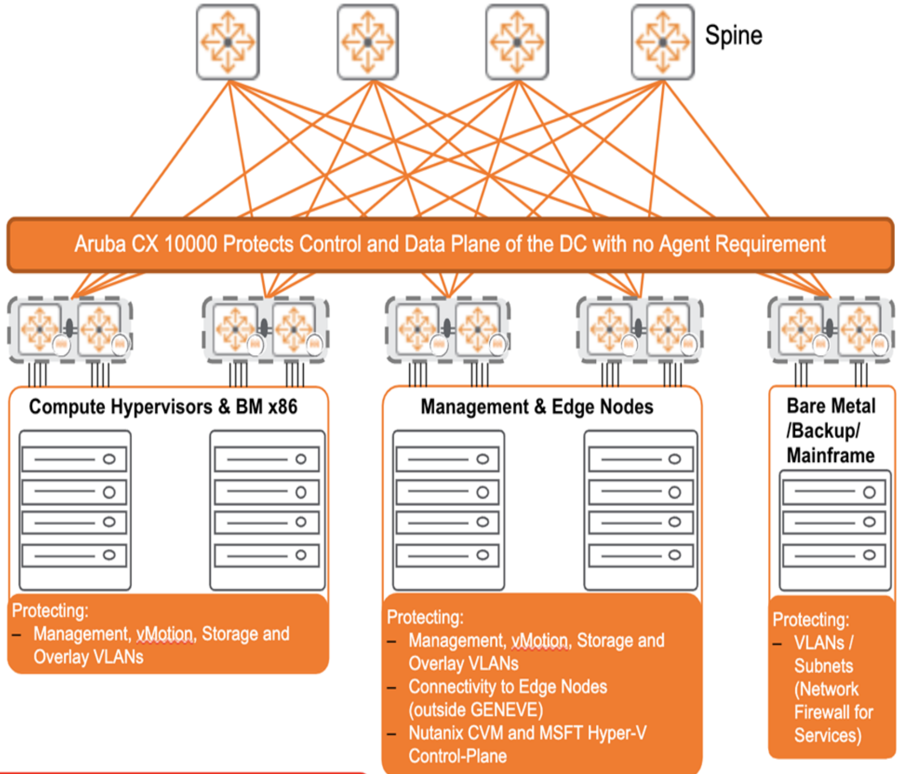
Academic Records

n0tma1ware .biz

21-2-g– Aruba CX10000 - Secure DC East-West Stateful Segmentation

Protect the Unprotected

- **Protection for all systems -** Legacy, proprietary & non-x86 operating systems
- **Protection for critical Data Center control plane infrastructure**
  - iLO, iDRAC, IPMI, VMWARE vmkernels, Nutanix CVM, Microsoft Hyper-V)
  - Storage or Backups
  - VSAN/Nutanix CVM Control Plane of appliances
- **Preserve server CPU usage from agents** running on hosts
- **Secure Airgap** – Server root access can't disable security agent
- **Active/Active Firewall includes** Connection Tracking, DDoS, ALG & logging
- **Simplified Micro & Macro Segmentation** with orchestration integration
- **Radical TCO benefits!**


Spine
Aruba CX 10000 Protects Control and Data Plane of the DC with no Agent Requirement
Compute Hypervisors & BM x86
Protecting:
– Management, vMotion, Storage and Overlay VLANs
Management & Edge Nodes
Protecting:
– Management, vMotion, Storage and Overlay VLANs
– Connectivity to Edge Nodes (outside GENEVE)
– Nutanix CVM and MSFT Hyper-V Control-Plane
Bare Metal /Backup/ Mainframe
Protecting:
– VLANs / Subnets (Network Firewall for Services)

- Software agents protects the data plane of workloads only
- *Software agents provide host process visibility

Network Segmentation and Zero trust Networking in the DC

CX10K with 800G Stateful L4 Firewall Build In

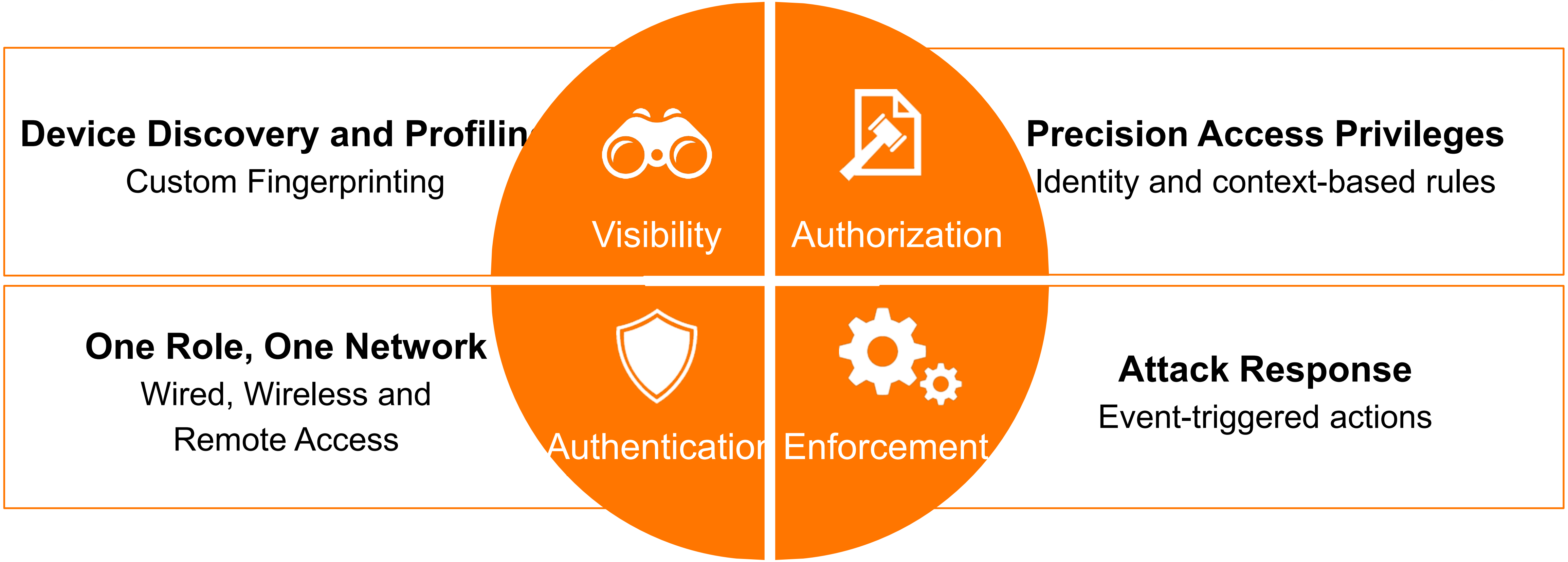
Protect the Unprotected with **70+% lower TCO**

21-2-g Identity and access management -ClearPass Policy Manager

End-to-end user & device visibility, control, and automation

CLEARPASS

ClearPass
Access Management



Device Discovery and Profilin
Custom Fingerprinting

Precision Access Privileges
Identity and context-based rules

One Role, One Network
Wired, Wireless and
Remote Access

Attack Response
Event-triggered actions

Vendor-neutral—**no lock-in**

A Sample of Clearpass 3rd Party Partners and Integrations

SECURITY

- Carbon Black.
- Check Point SOFTWARE TECHNOLOGIES LTD.
- FORTINET
- JUNIPER NETWORKS
- FireEye
- RAPID7
- McAfee
- paloalto NETWORKS
- Symantec.
- tenable
- TREND MICRO
- Windows Defender
- Infoblox NEXT LEVEL NETWORKING

AUTH

- okta
- Envoy
- sine
- zoom
- teem
- Microsoft

LOGGING

- ArcSight
- splunk>
- IBM QRadar

IOT/ OT

- CLAROTY Clarity for OT Networks
- CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY
- Bastille
- Indegy
- NOZOMI NETWORKS
- ordr
- PHILIPS

MESSAGING

- Microsoft Teams
- pagerduty
- SendGrid
- servicenow
- slack
- twilio

HOTSPOT

- Authorize.Net
- PayPal
- worldpay

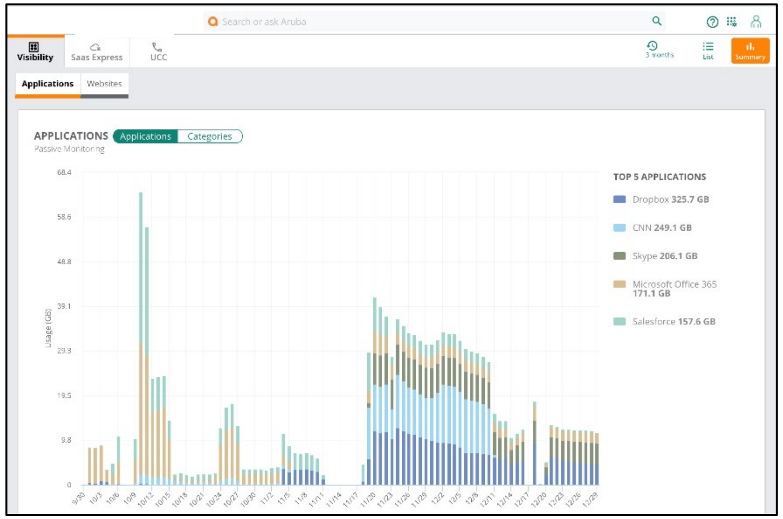
UEM

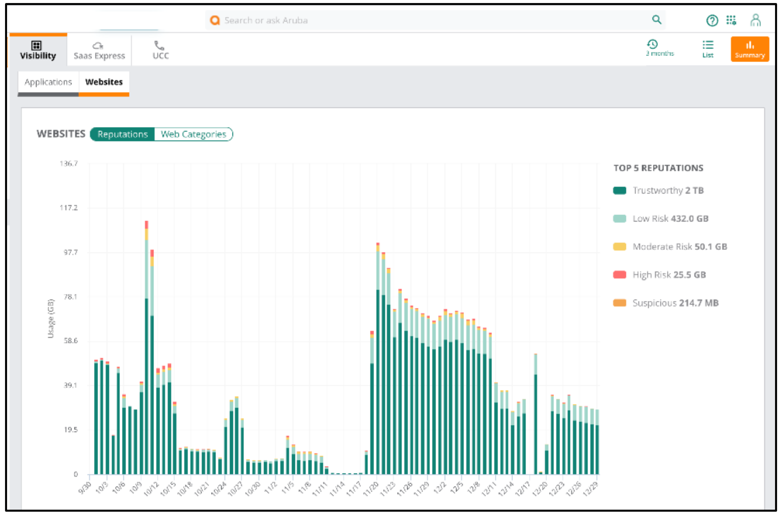
- airwatch by vmware
- casper SUITE
- CiTRIX
- G Suite
- IBM MaaS360
- Intune
- MobileIron
- SAP
- SOTI
- BlackBerry UEM
- JAMF software
- VMware Workspace ONE
- CROWDSTRIKE

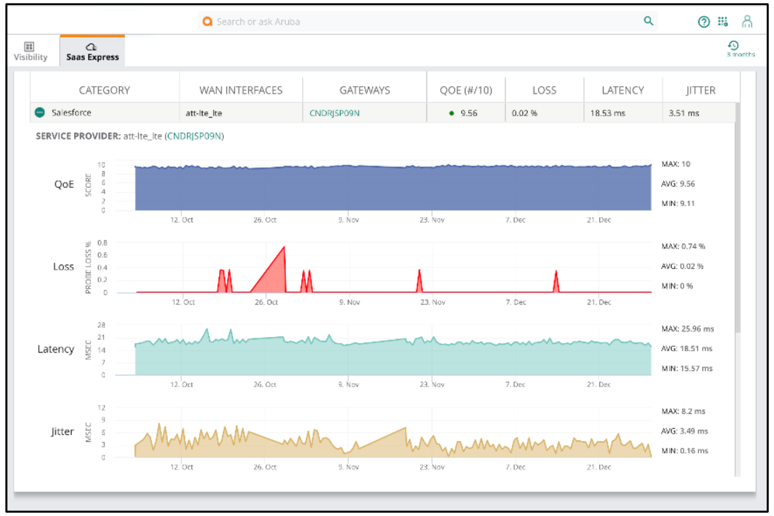
SOCIAL

- amazon
- facebook
- GitHub
- Google
- Instagram
- LinkedIn
- salesforce
- twitter

21-2-g– User awareness - Application and Web Visibility







CATEGORY	WAN INTERFACES	GATEWAYS	QOE (#/10)	LOSS	LATENCY	JITTER
Salesforce	att-lte_lte	CNDRJSP09N	● 9.56	0.02 %	18.53 ms	3.51 ms

SERVICE PROVIDER: att-lte_lte (CNDRJSP09N)

Monitor app and web usage to optimize and secure the network

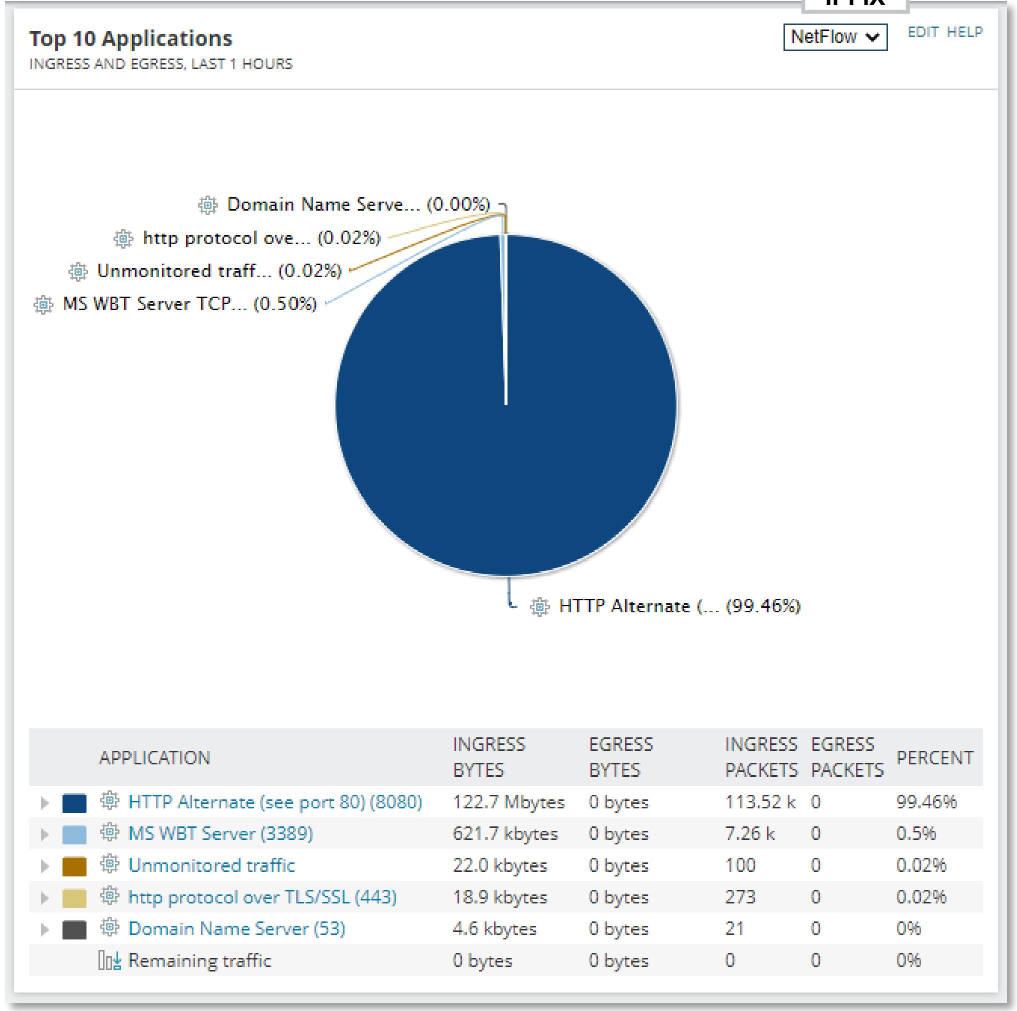
Prioritize business critical apps and block inappropriate content

Enforce policies on a per user, device or location basis

Get QoE ratings and understand delays due to jitter, latency, etc.

Outcome for Network Admin: 6300 CX Switching Application Visibility

IPFIX



Domain Name Serve... (0.00%)
http protocol ove... (0.02%)
Unmonitored traff... (0.02%)
MS WBT Server TCP... (0.50%)
HTTP Alternate (... (99.46%)

Top 10 Applications
INGRESS AND EGRESS, LAST 1 HOURS

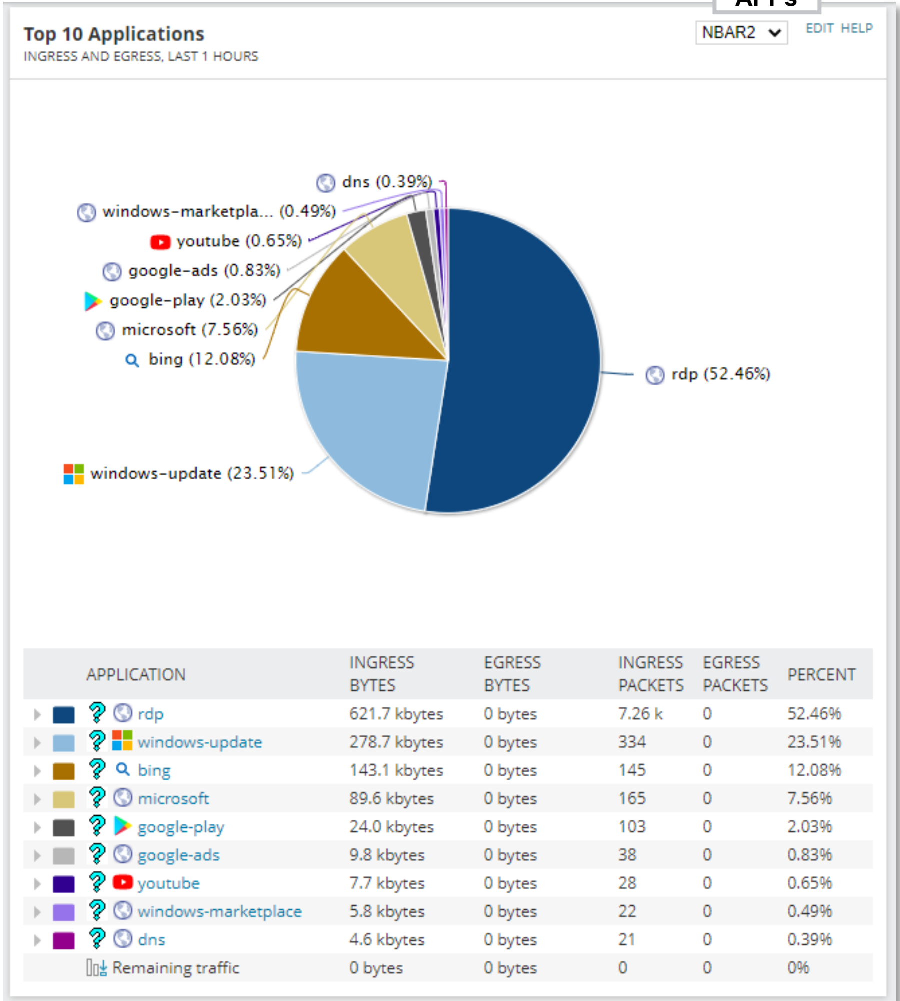
NetFlow EDIT HELP

	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%

Traffic report with **IPFIX only**

enable application recognition

APPs



Top 10 Applications
INGRESS AND EGRESS, LAST 1 HOURS

NBAR2 EDIT HELP

	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%

IPFIX + **APP-RECOGNITION**

21-2-g– Using machine learning - Aruba Central Cloud AIOps Portfolio

Full-service AI-powered IT Insights

AI Insights

Proactive network anomaly detection and optimization

Find …

AI Search

Natural language queries for fast troubleshooting

AI Assist

Automated Aruba TAC trouble ticket generation

ClientMatch

Real-time network roaming optimization

AirMatch

Proactive adjustments to RF values in real-time

Network Insights- Planning, Setup, Troubleshooting & Optimization

Client Insights

Accurate IoT profiling to drive capacity planning & security policies

Client Insights: Behavior / Security

Incident Detection

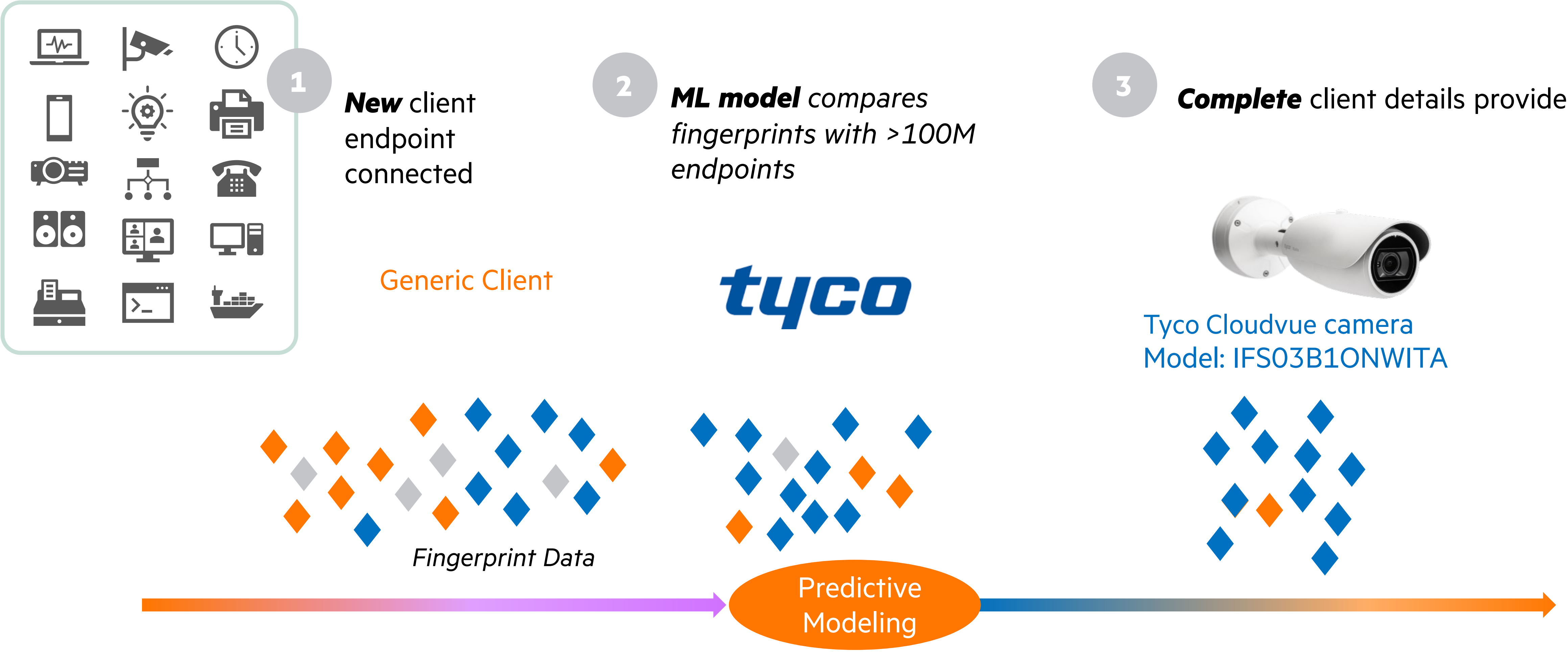
UXI

Automated application performance monitoring

User Insights: Application Experience

21-2-g– Using machine learning - AI/ML Models - An Inside Look

Multiphase Predictive Accuracy



1 ***New*** client endpoint connected

Generic Client

2 ***ML model*** *compares fingerprints with >100M endpoints*

tyco

3 ***Complete*** client details provided

Tyco Cloudvue camera
Model: IFS03B1ONWITA

Fingerprint Data

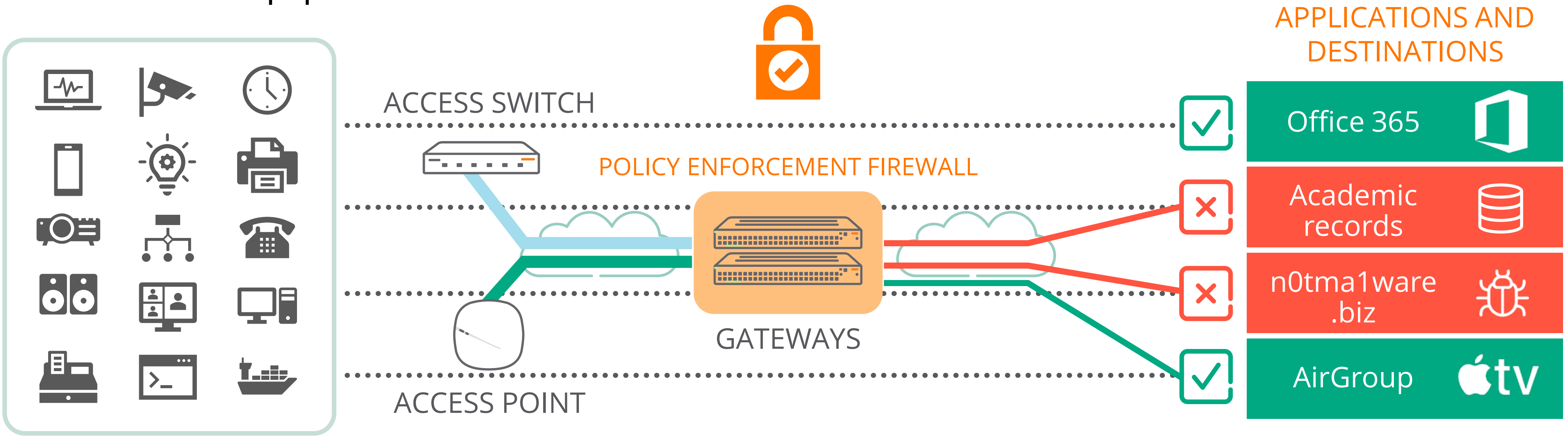
Predictive Modeling

AI Enables IOT Dynamic Segmentation for Secure Network Access

Now Aided by IoT Detection and Behavior Monitoring

3 **Automated** change of authorization (CoA) can take client offline

1 **Always-on** visibility with no dedicated equipment

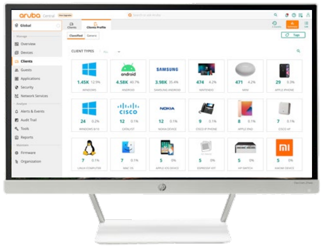


2 **Change** in traffic behavior identified

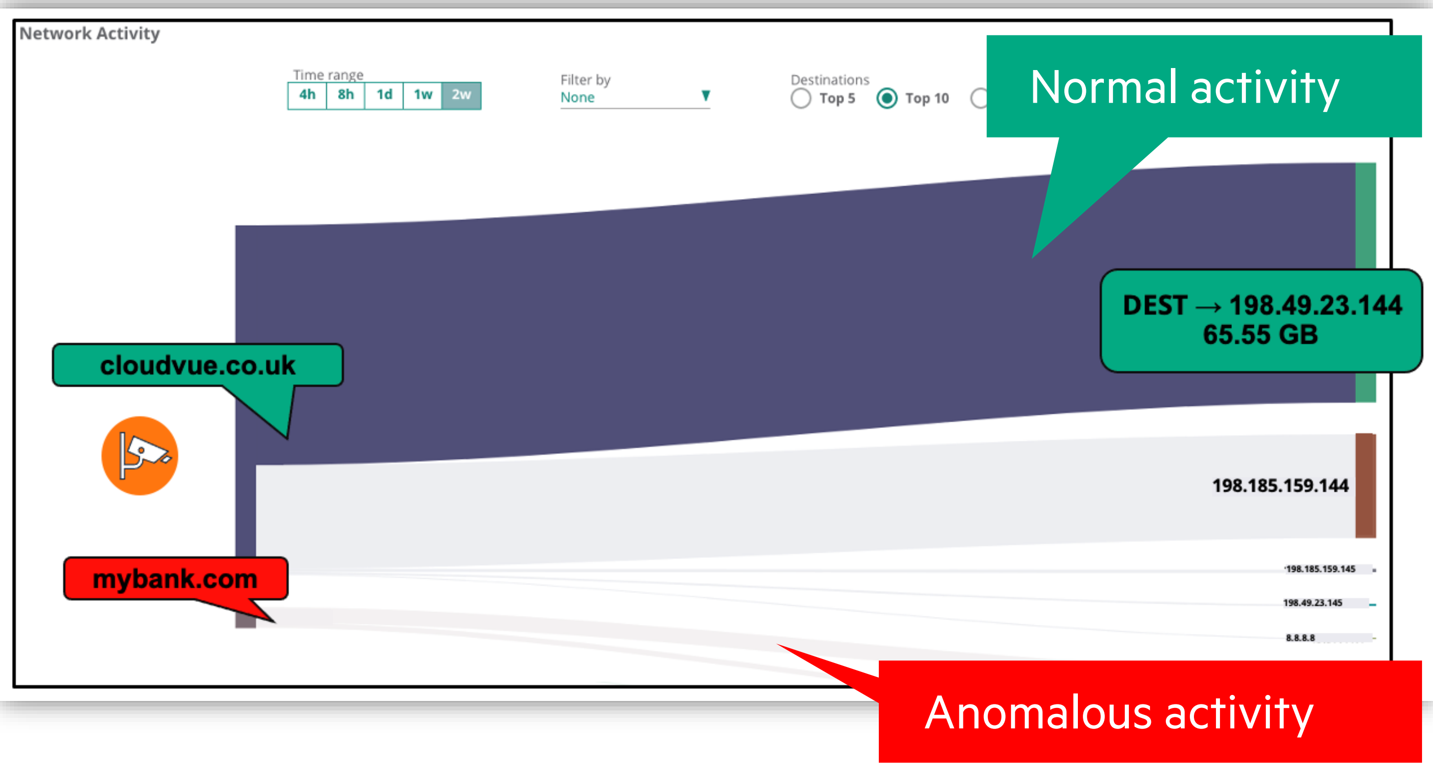
21-2-g– Using machine learning - Easy-To-See Client Activity

Single Solution for Network and Zero Trust Security

- **Tracks over 4500 applications**
- **Highlights activity by destination and bandwidth used**
- **Faster problem resolution**



Aruba Central cloud



Normal activity

DEST → 198.49.23.144
65.55 GB

cloudvue.co.uk

mybank.com

Anomalous activity

Conclusion

HPE Aruba Networking has a comprehensive and integrated solution to help you to increase your cyber resilience

- **HPE Aruba Networking covers** ALL the Networking aspect of the NIS 2 EU Directive including
- **Zero trust Principles, Dynamic Network segmentation, Intelligent Firmware and configuration Management, Industry leading Identity and access management** with ClearPass and SSE ZTNA, and **machine learning** with Central AIOPs

- HPE Aruba Networking is **leading in Defense class LAN and WLAN** secure networks

- 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**

HPE Aruba Networking Comprehensive Solution for NIS 2 Compliance

Aruba Central

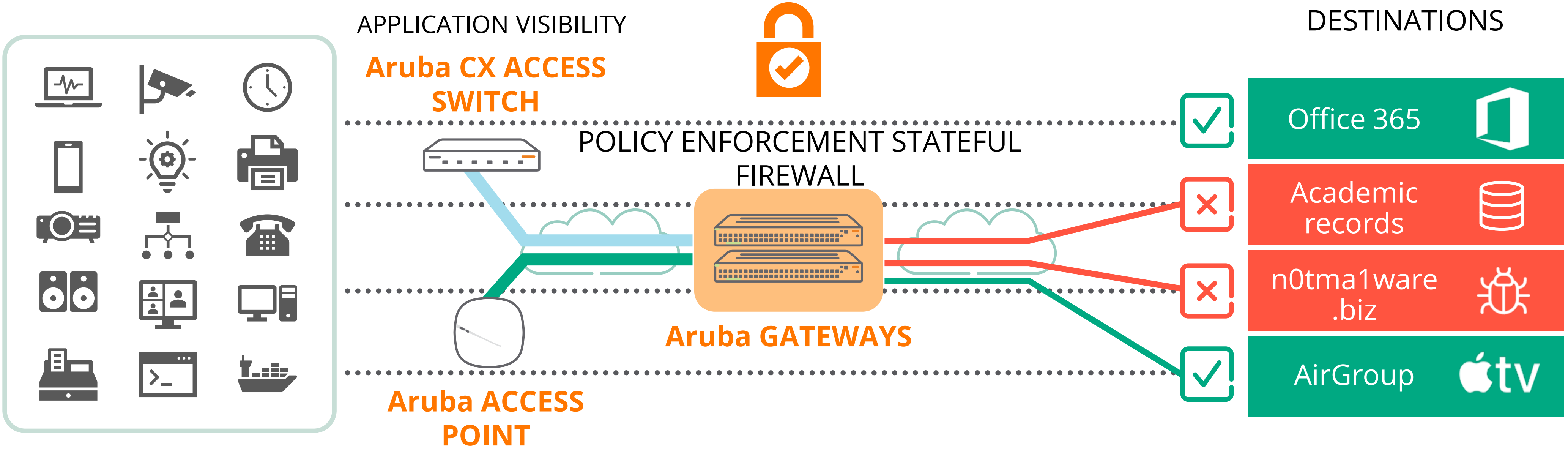
Configuration / Firmware / User awareness

ClearPass Policy Manager

DYNAMIC MICRO SEGMENTATION

PEOPLE AND THINGS

APPLICATIONS AND DESTINATIONS



APPLICATION VISIBILITY

Aruba CX ACCESS SWITCH

POLICY ENFORCEMENT STATEFUL FIREWALL

Aruba GATEWAYS

Aruba ACCESS POINT

✓ Office 365

✗ Academic records

✗ n0tma1ware .biz

✓ AirGroup tv

TRUSTED INFRASTRUCTURE: SDLC , SUPPLY CHAIN, VULNERABILITY MGT, CERTIFIED

Call to Action
(no time like the present)

- Start to audit your Network versus NIS 2
- Engage with HPE Aruba Networking

To get a simple and cost-contained solution to NIS 2 compliance