Klaar om uw traditionele VPN te vervangen door ZTNA?

NIS2-opvolgwebinars

Wiki Webinar

by inetum. realdolmen

Praktische afspraken

- Vragen via chat
- Iedereen op mute
- Q&A na de presentatie
- Evaluatie met link naar de slides worden na de webinar doorgestuurd

inetum
realdolmen
Positive digital flow

HPE aruba networking

Hewlett Packard Enterprise

HPE aruba networking

Security-First, AI-Powered Networking
Secure access modernization with SSE

Farouk – SASE Channel North Europe

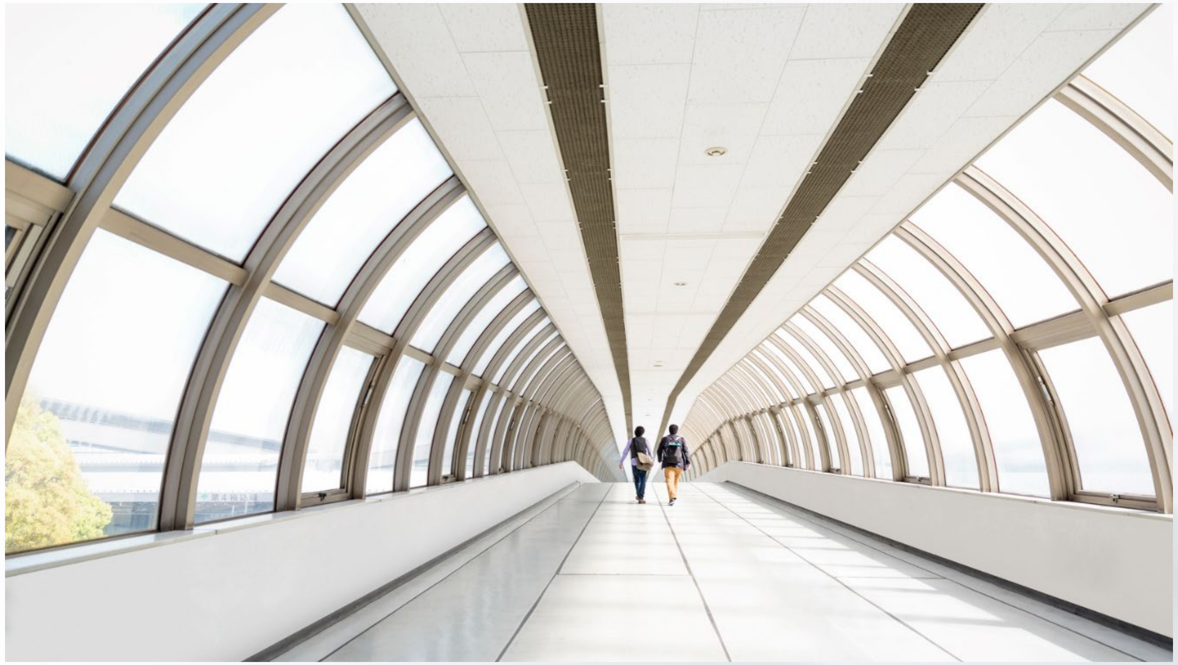
May 14th, 2024

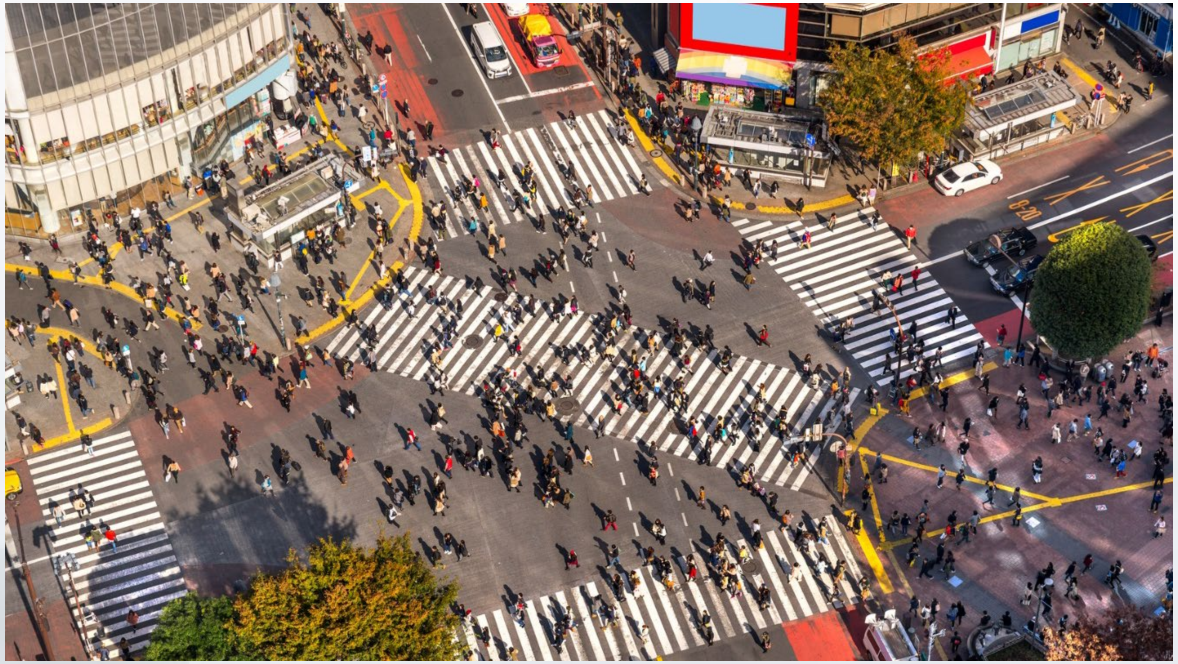
Fortress Mentality and myths

Inside the walls everything is trusted

All critical assets live inside the walls

Paradigms are shifting





Ubiquitous secure access

Apps	Anything
People	Anytime
Things	Anywhere

Increasing complexity

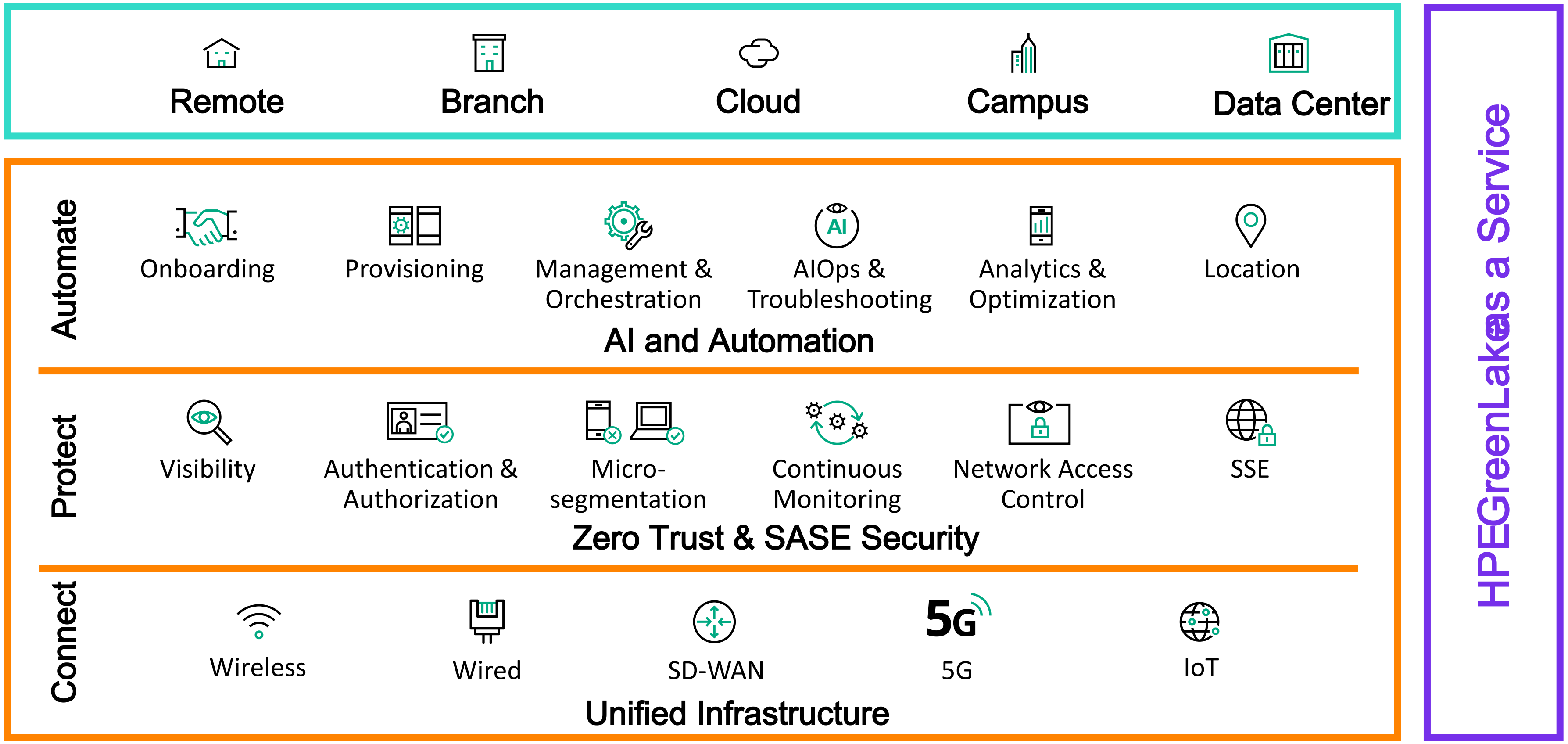
Evolving threats	Security
Generative AI	Governance
Talent gaps	Privacy

The modern workplace is **MOBILE**

And **95%** of businesses still rely on VPN

Orchestrating network services from edge-to-cloud

Powered by HPE Aruba Networking Central



Remote Branch Cloud Campus Data Center

Automate

Onboarding

Provisioning

Management & Orchestration

AIOps & Troubleshooting

Analytics & Optimization

Location

AI and Automation

Protect

Visibility

Authentication & Authorization

Micro-segmentation

Continuous Monitoring

Network Access Control

SSE

Zero Trust & SASE Security

Connect

Wireless

Wired

SD-WAN

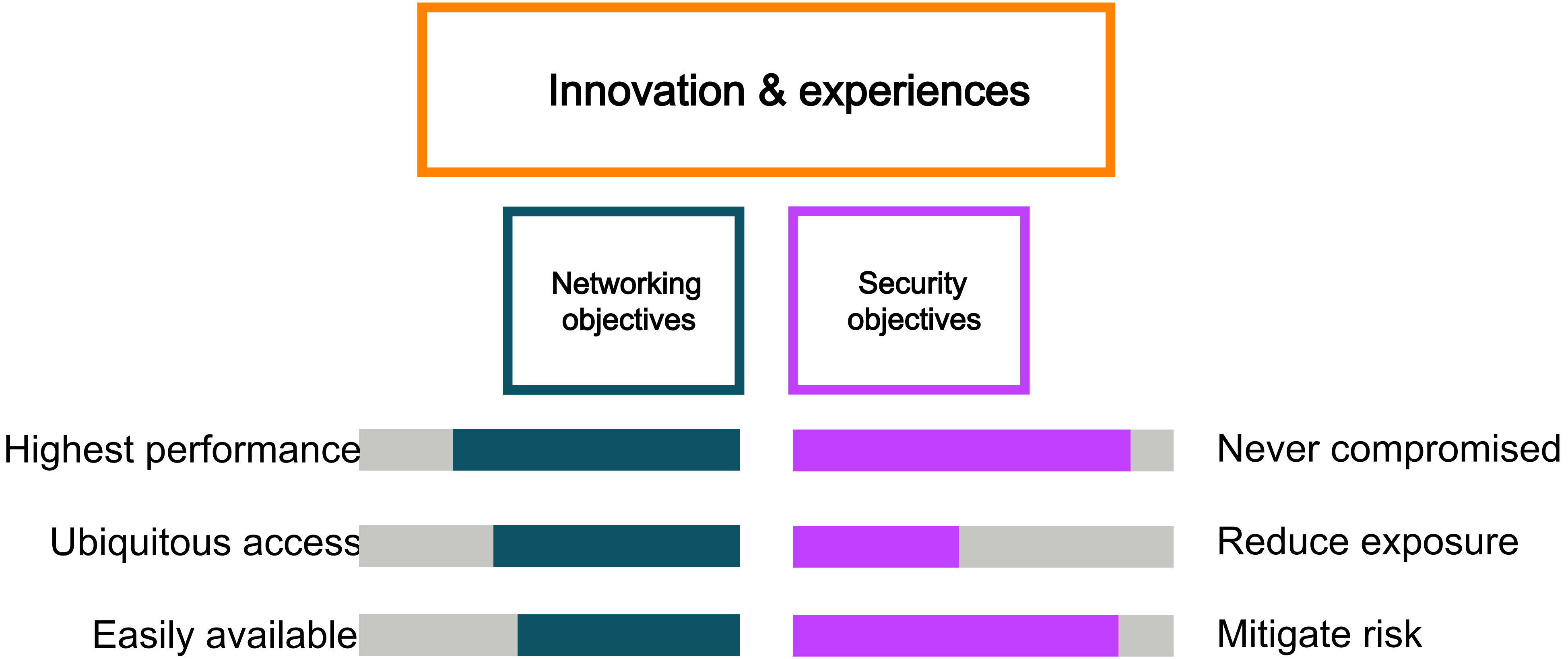
5G

IoT

Unified Infrastructure

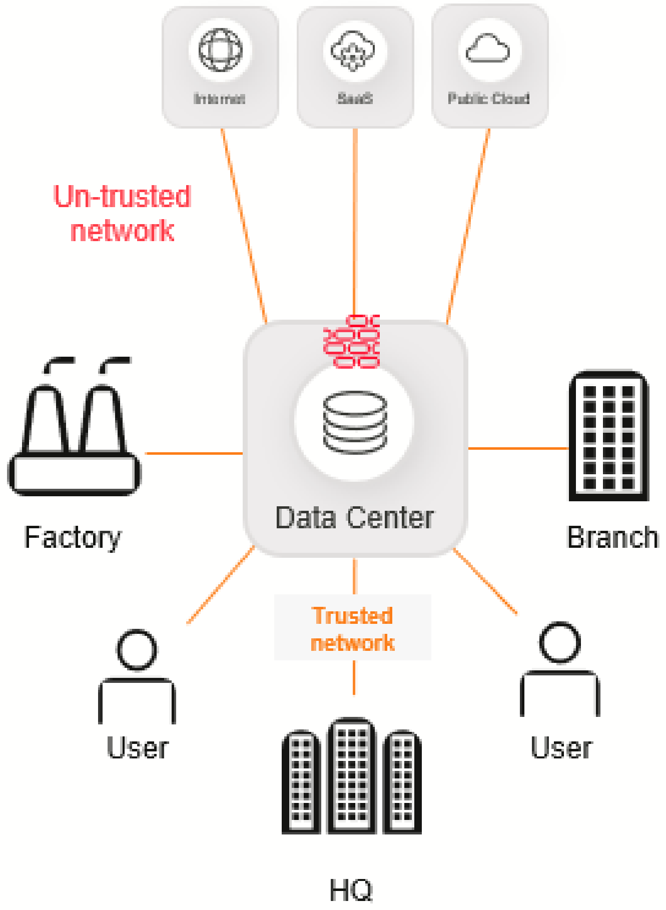
HPE GreenLake as a Service

How do you balance multiple objectives?

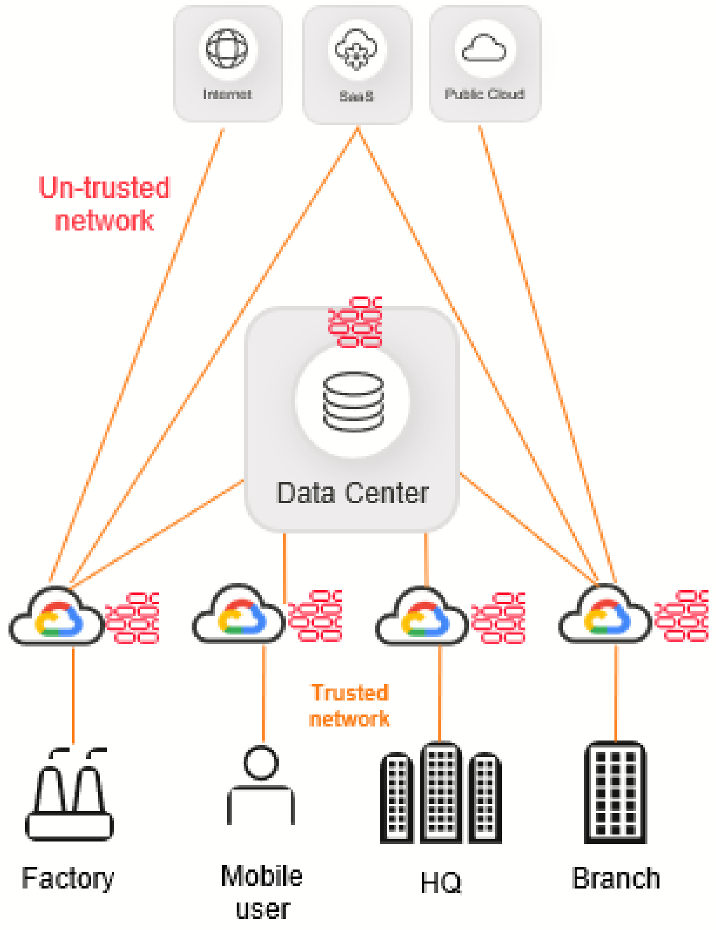


Three approaches to secure access

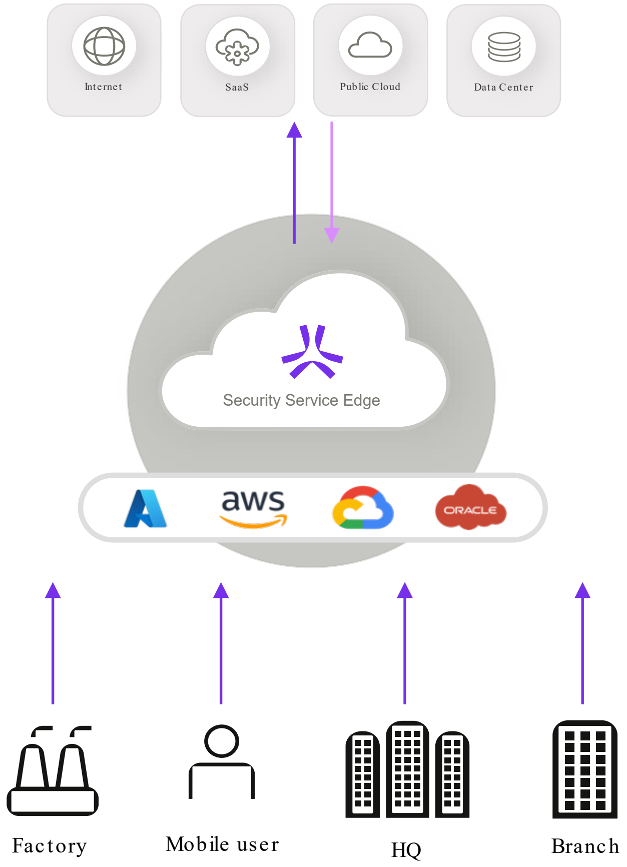
1.Hub and spoke



2. Virtualized cloud firewalls



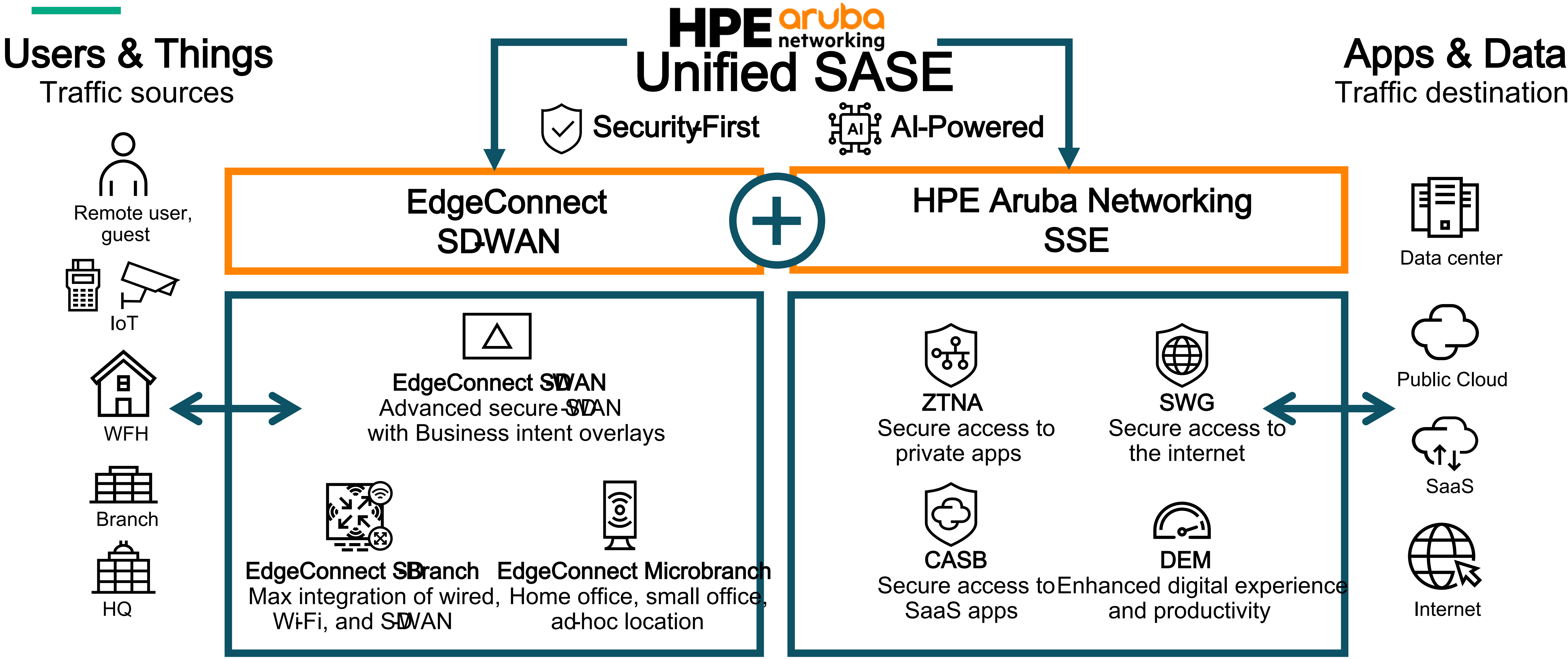
3. Security Service Edge



SASE brings network and security together

HPE Aruba Networking Unified SASE

Deploy industry-leading EdgeConnect SD-WAN with the cloud-native HPE Aruba Networking SSE platform



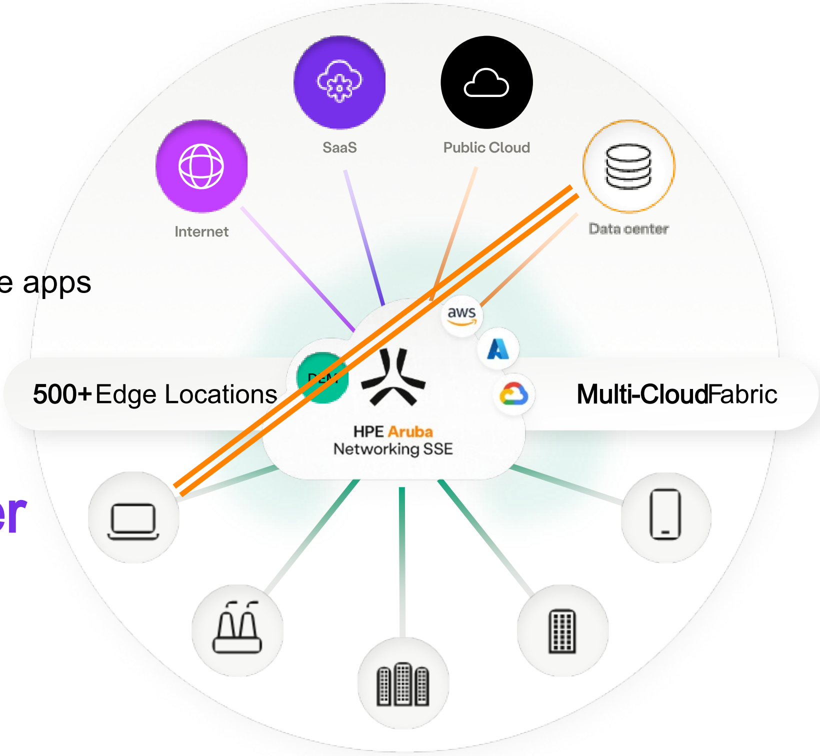
HPE Aruba Networking Security Service Edge (SSE) platform

The 4 pillars of SSE

Zero Trust Network Access

Secure access to private applications in the data center or cloud.

i.e Minimize app exposure to Internet, remove network access, replace VPN, Inspect traffic, support all private apps



Secure Web Gateway

Secure access to the Internet and protect against malicious online threats.

i.e Filtering, SSL inspection, malware scanning, reputation-based blocking, AI-based Sandboxing

Cloud Access Security Broker

Secure access to SaaS applications and protect against data loss.

i.e Control block upload/download from Box, Sharepoint, Facebook, Salesforce

Digital Experience Monitoring

Monitor user performance and to troubleshoot user access issues for all traffic.

i.e Monitor performance of each session, minimize mean time to remediation of user issues

ZTNA is the most popular start point for SSE

Out of the 3 core SSE technologies, which do you plan to begin with?

47%

Zero Trust Network Access (ZTNA)

33%

Cloud Access Security Broker (CASB)

20%

Secure Web Gateway (SWG)

2023 SSE Adoption Report by Cybersecurity Insiders – click here to download

VPN Pains

VPNs ARE A SECURITY RISK

97% of businesses know their VPNs are being targeted

VPN is a weak point

Virtual or Vulnerable

92% are concerned that VPN will jeopardize their environment

VPNs DELIVER A POOR EXPERIENCE

VPN traffic must be backhauled to the nearest DC location – often 100s of miles away – creating a latent user experience

81% are dissatisfied with their VPN experience

VPNs ARE COMPLE TO MANAGE

Each appliance in the inboun stack is managed and update separately

Scaling VPN gateways is a logistical nightmare

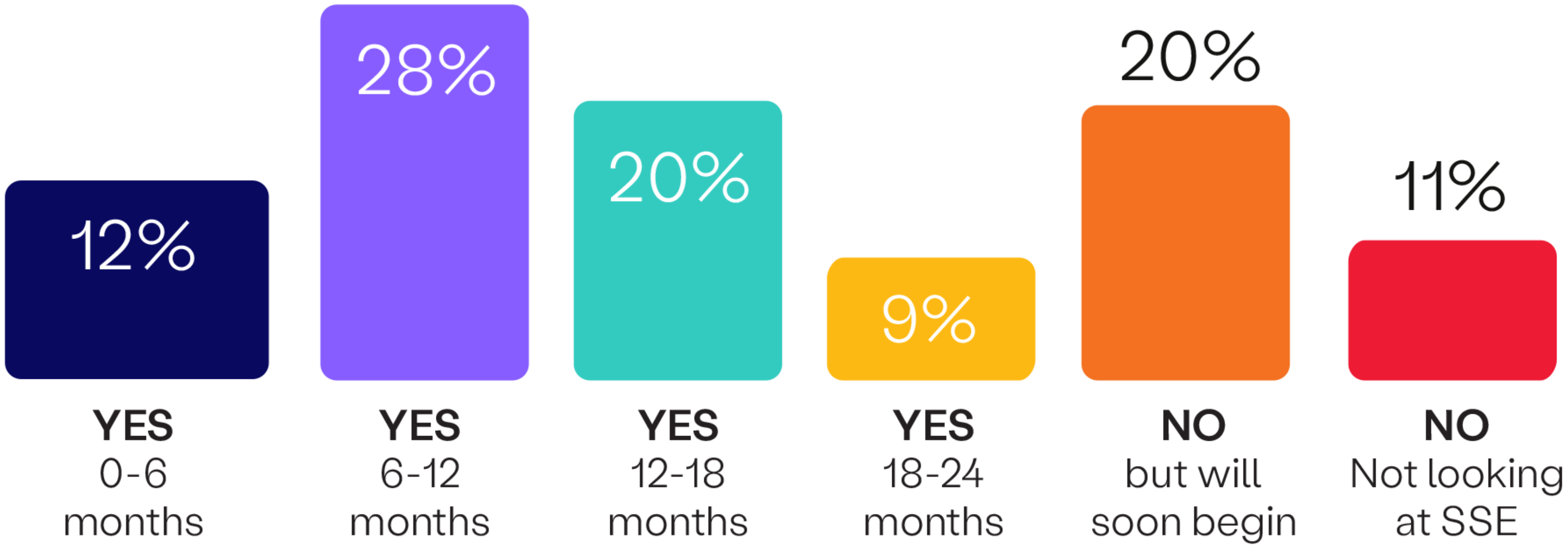
65% of organizations have 3+ VPN gateways to manage

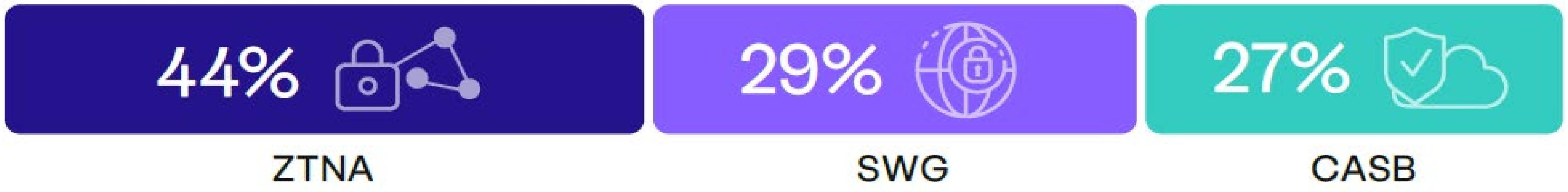
2024 VPN risk report

SSE Adoption

Starting with ZTNA

69% of organizations plan to adopt SSE within the next 2 years





Foundation

Foundation Plus

Advanced

HPE Aruba Networking SSE SKU details

Manage all SSE capabilities from a single platform and a single policy engine

Foundation

Elevate secure remote access and simplify management with a modern-day ZTNA

- Zero trust Network Access

Foundation Plus

Unify access security and user productivity with secure access across all private apps with ZTNA and internet access with SWG

- Zero trust Network Access
- Secure Web Gateway

Advanced

Enhance data loss security with CASB and optimize user and network performance with DEM while building on the foundations of ZTNA and SWG

- Zero trust Network Access
- Secure Web Gateway
- CASB/DLP
- Digital Experience Monitoring

Advanced Plus

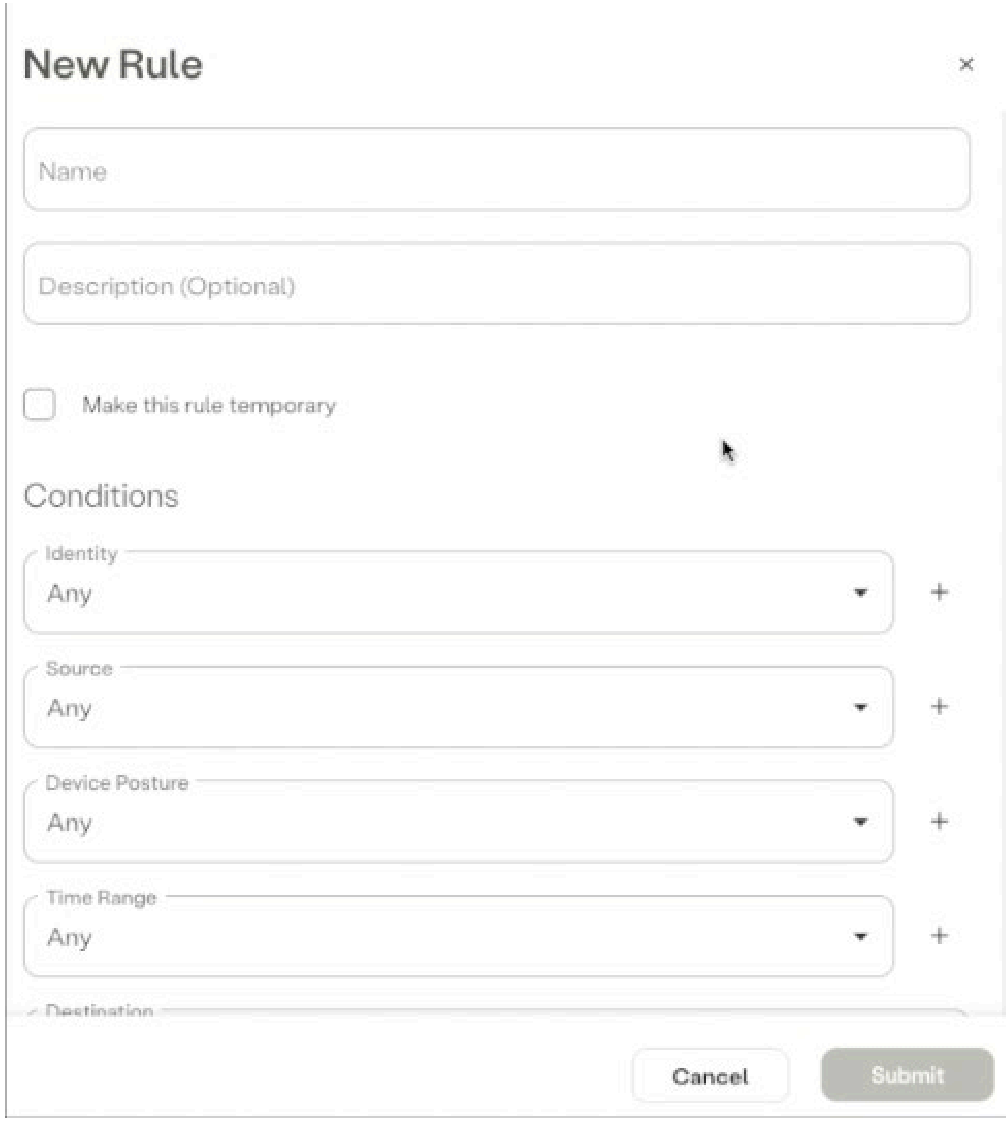
Unlock full SSE value for your business. Unmatched security with advanced ZTNA, DLP and malware scanning. Maximized connectivity with Local Edge deployments and zero trust server-to-server support.

- Zero trust Network Access
- Secure Web Gateway
- CASB/DLP
- Digital Experience Monitoring
- Advanced DLP*

Simple secure remote access ZTNA

Michael
CSO

1. Configuration



New Rule

Name

Description (Optional)

□ Make this rule temporary

Conditions

Identity: Any

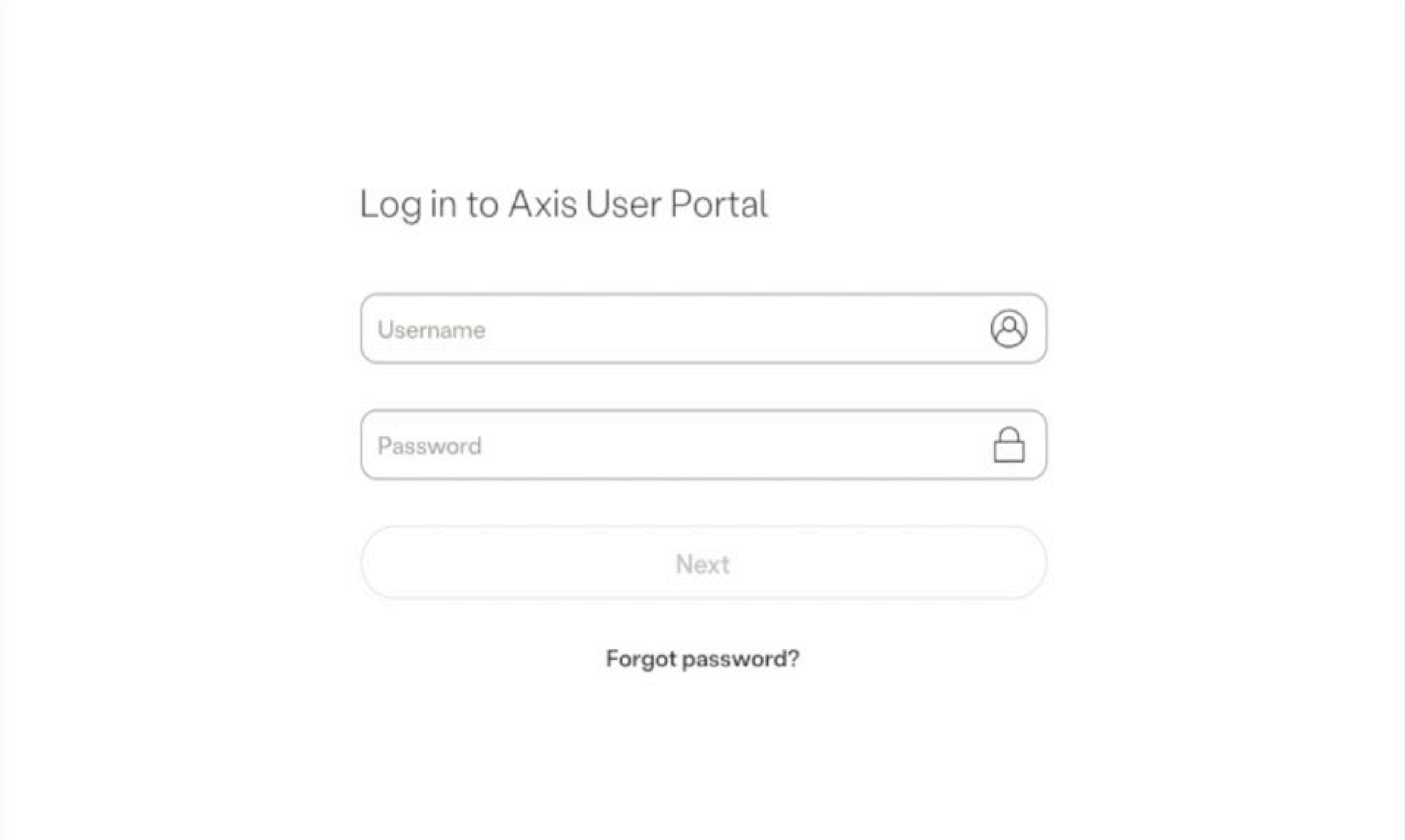
Source: Any

Device Posture: Any

Time Range: Any

Destination

Simple secure remote access ZTNA



Log in to Axis User Portal

Username

Password

Next

Forgot password?

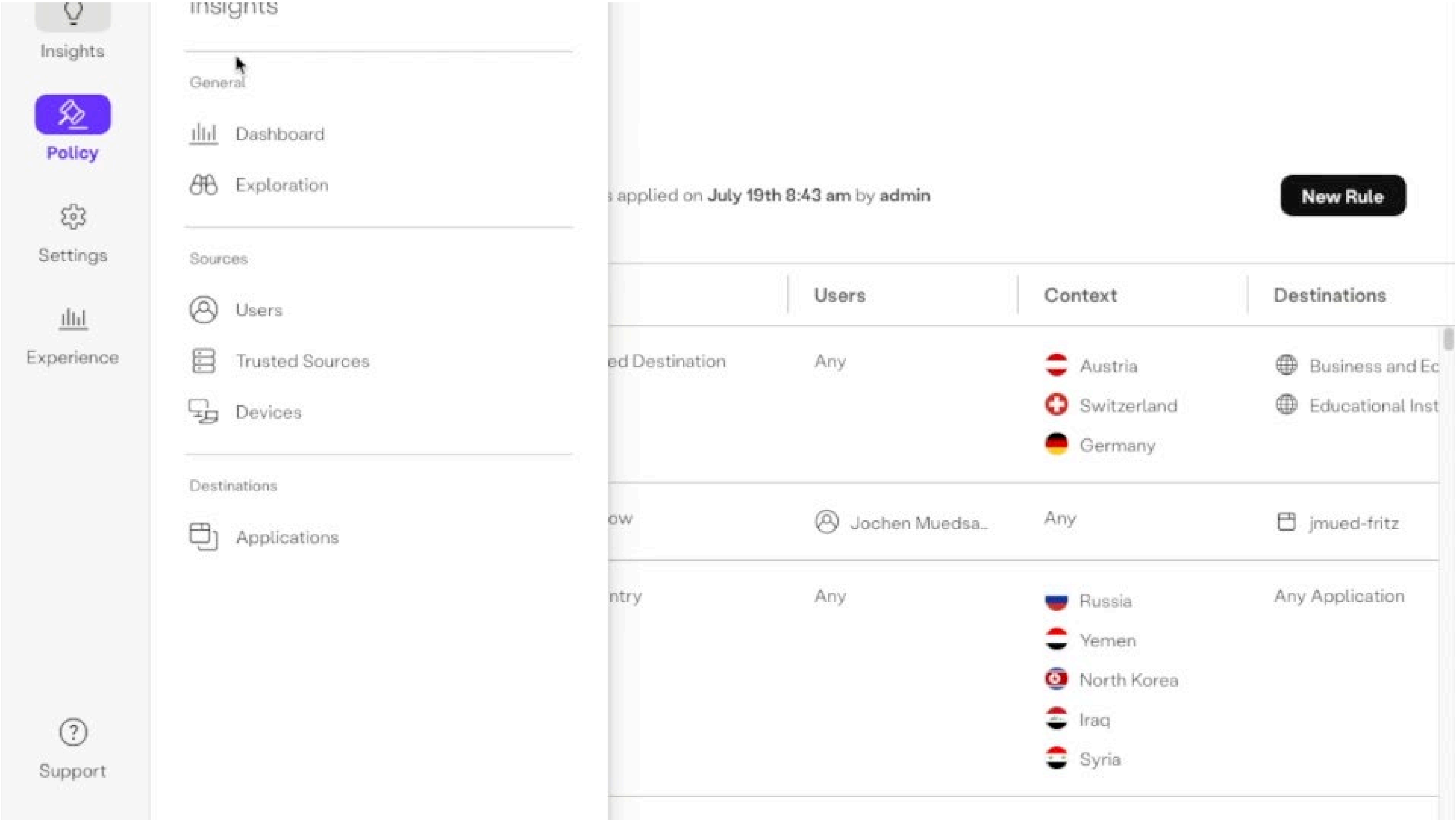
Pradeep
Remote worker

2. Connect to Portal

Simple secure remote accessZTNA

Michael
CSO

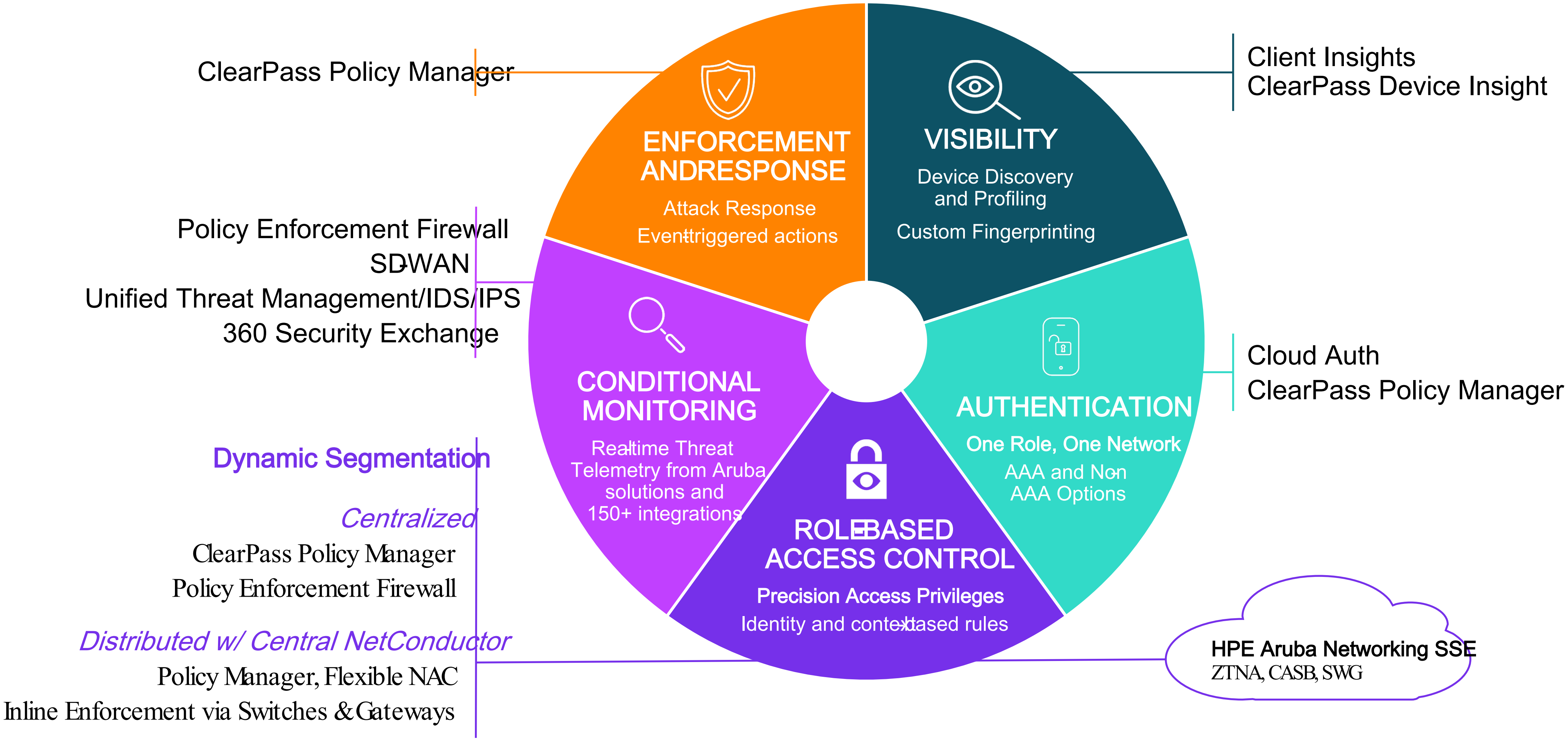
1. Configuration
3. Verification



applied on **July 19th 8:43 am** by **admin**

	Users	Context	Destinations
ed Destination	Any	Austria Switzerland Germany	Business and Ec Educational Inst
ow	Jochen Muedsa_	Any	jmued-fritz
ntry	Any	Russia Yemen North Korea Iraq Syria	Any Application

HPE Aruba Networking Zero Trust Security foundation



ClearPass Policy Manager

ENFORCEMENT ANDRESPONSE

Attack Response

Event-triggered actions

VISIBILITY

Device Discovery and Profiling

Custom Fingerprinting

Client Insights

ClearPass Device Insight

Policy Enforcement Firewall

SD-WAN

Unified Threat Management/IDS/IPS

360 Security Exchange

CONDITIONAL MONITORING

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

AUTHENTICATION

One Role, One Network

AAA and Non-AAA Options

Cloud Auth

ClearPass Policy Manager

ROLE-BASED ACCESS CONTROL

Precision Access Privileges

Identity and context-based rules

Dynamic Segmentation

Centralized

ClearPass Policy Manager

Policy Enforcement Firewall

Distributed w/ Central NetConductor

Policy Manager, Flexible NAC

Inline Enforcement via Switches & Gateways

HPE Aruba Networking SSE

ZTNA, CASB, SWG

EU NIS 2 Scope -Essential and Important Entities -250+ employees / 50M€+

1 Million + enterprises and administrations WW are directly or indirectly(*) are impacted

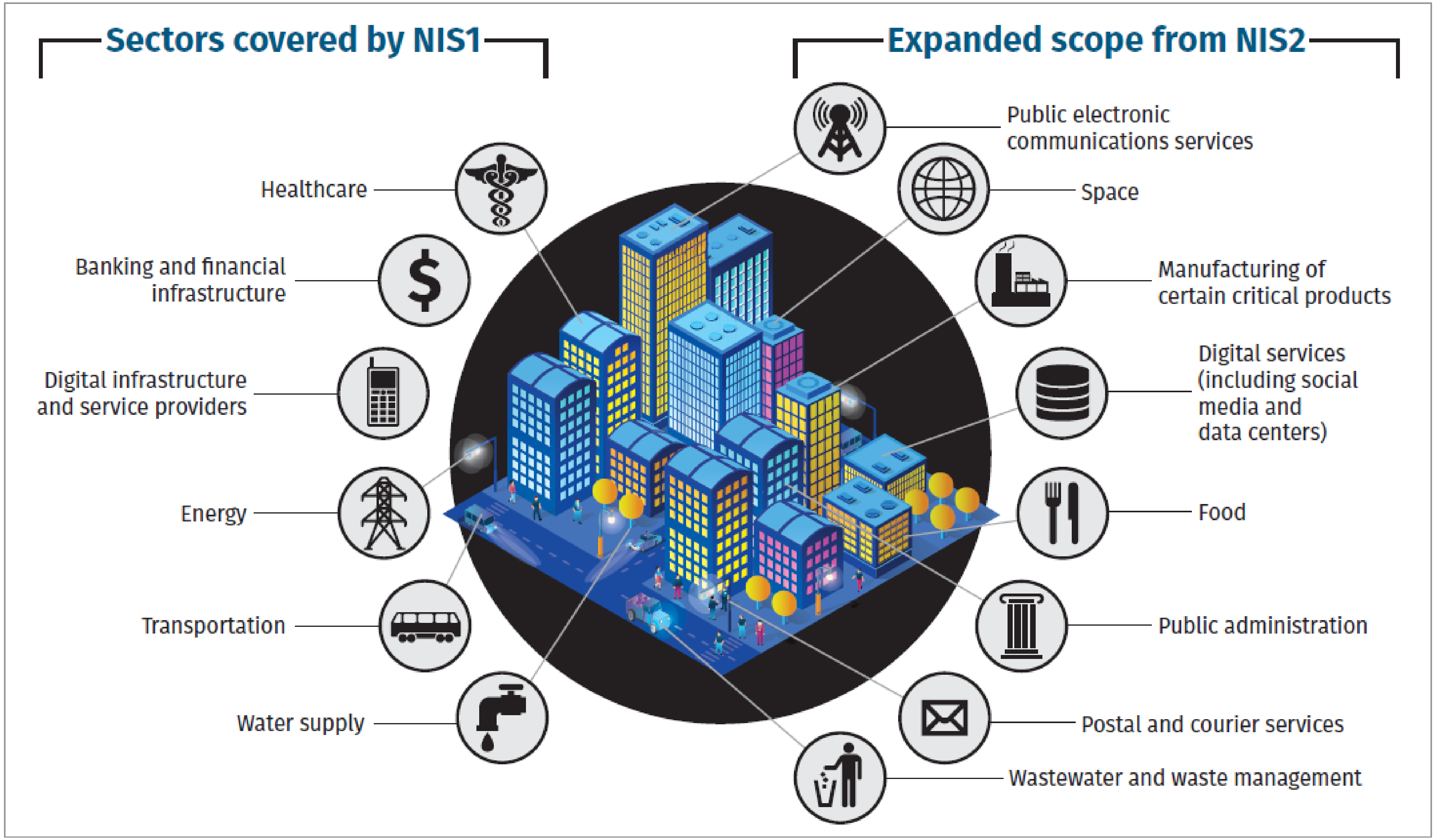
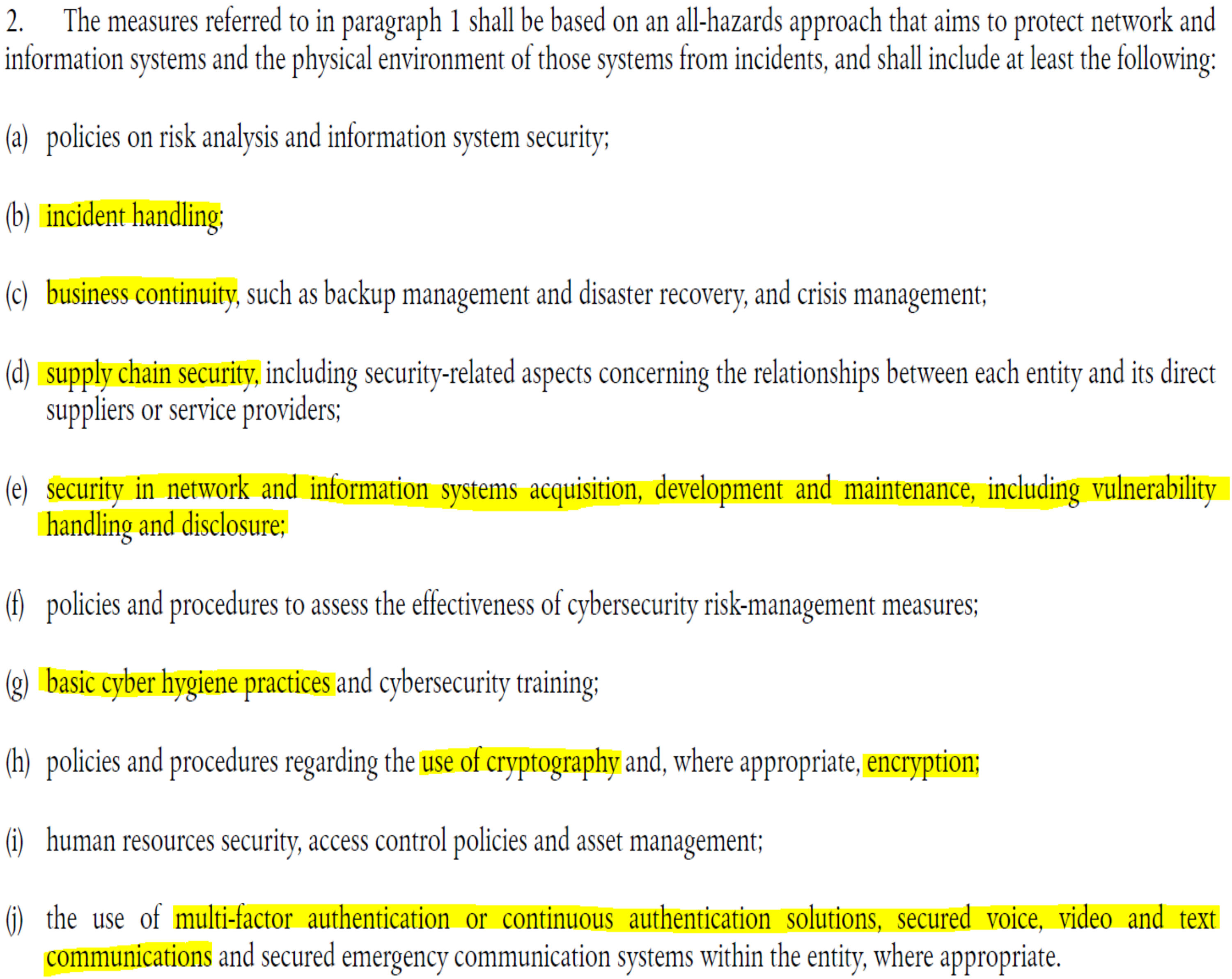

Sectors covered by NIS1
Healthcare
Banking and financial infrastructure
Digital infrastructure and service providers
Energy
Transportation
Water supply
Expanded scope from NIS2
Public electronic communications services
Space
Manufacturing of certain critical products
Digital services (including social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

Figure 4. NIS2 In-Scope Sectors

Source: SANS Institute

Fines of a maximum of at least 10 M€ or 2 % of the total worldwide annual turnover = GDPR

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;

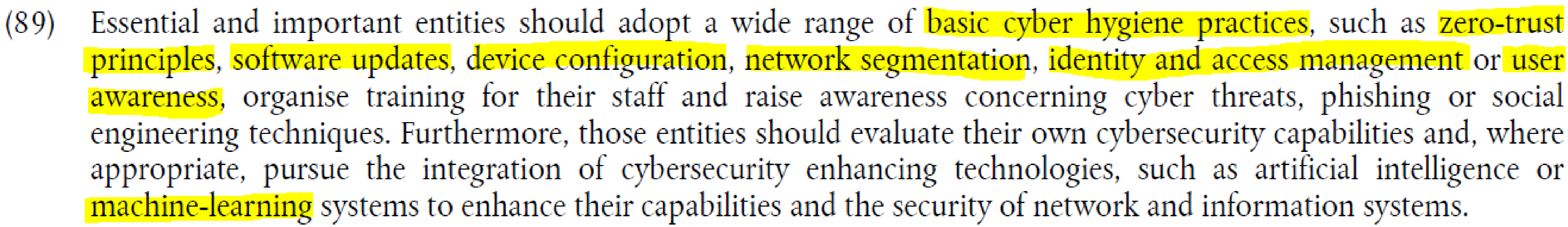
(g) basic cyber hygiene practices and cybersecurity training;

(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 Networking Solutions overview for Basic Cyber Hygiene practice (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

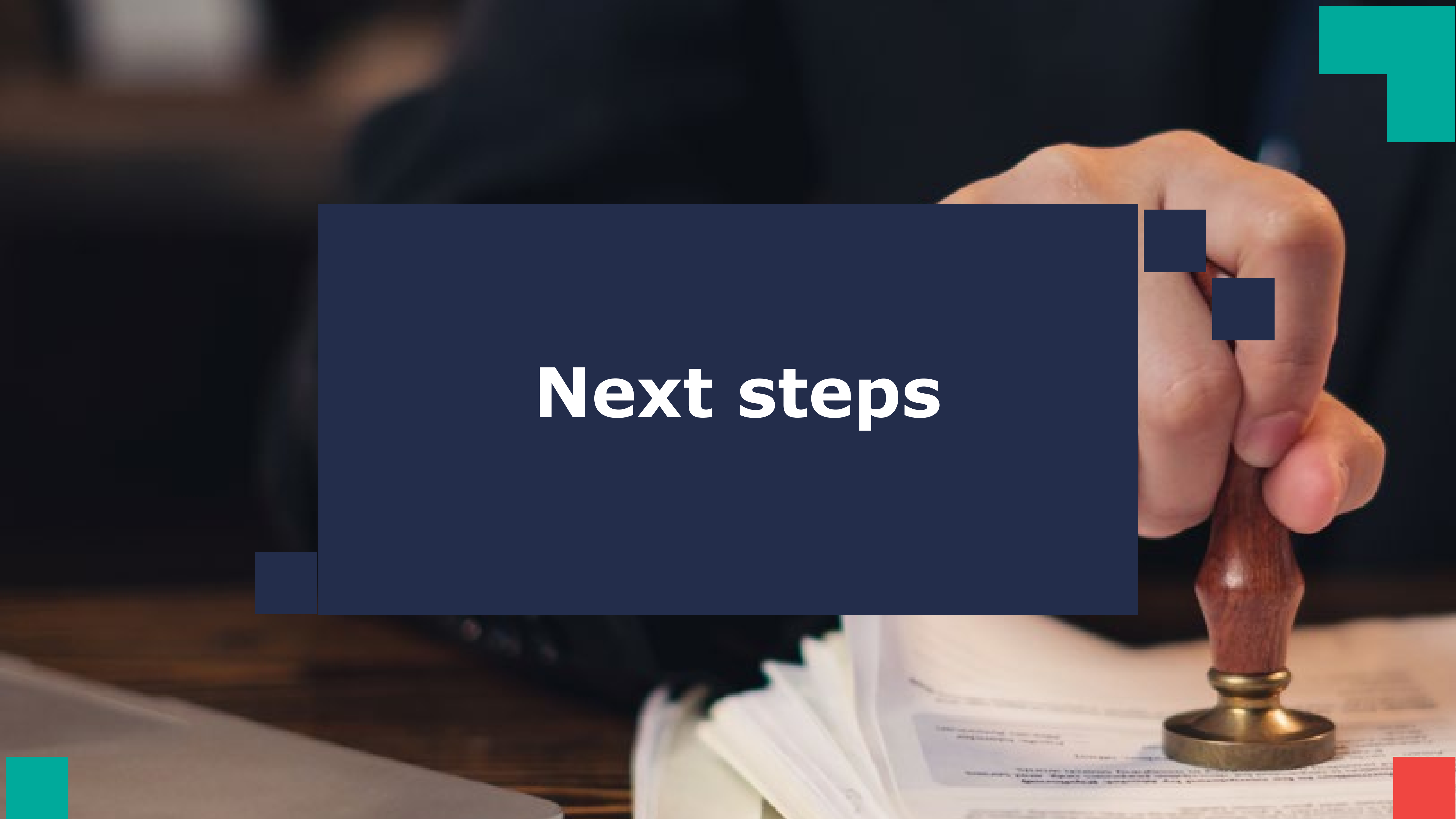
Basic Cyber Hygiene practice (89) Solutions overview

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, EdgeConnect SSE (AXIS ZTNA)
User Awareness	Aruba Central Client and Application visibility
Use of Machine Learning	Aruba Central Cloud AIOps including Client Insights

The way forward

HPE aruba networking

Security-first, AI-powered networking



Next steps

How Inetum-Realdolmen can help

At Inetum-Realdolmen, we understand the importance of cybersecurity and the need to comply with regulatory frameworks such as NIS2

We provide tools and guidance to help you meet the minimum measures required by NIS2, such as risk assessments, security procedures, and incident response plans

Our team of cybersecurity experts can work with you to assess your current security posture and develop a customized security plan that meets your specific needs

You can have peace of mind knowing that your systems and data are protected by industry-leading security solutions.

CYBERSECURITY ACCELERATOR PROGRAM

Identify & Inspire

Audit & Assessment
Ethical hacking
Roadmap
Proof of Concept

Protect & Integrate

Zero Trust implementation

- Identities
- Devices
- Data
- Applications
- Networks & Infrastructure

Detect & Operate

Managed Security Services
Vulnerability Management
MDR Services

Respond & Optimize

Incident Response
Governance
CISO as a Service
User Awareness

Opvolgevents NIS2

26/3

Hoe stealth een stap vooruit blijven met CrowdStrike?

23/4

NIS2 is IT en OT
(Fortinet)

25/4

How positively change the security behavior of your employees with Hoxhunt?

14/5

Ready to replace your legacy VPN with ZTNA?
(Aruba)

23/5

The Belgian NIS2 law
(Beltug)

29&30/5

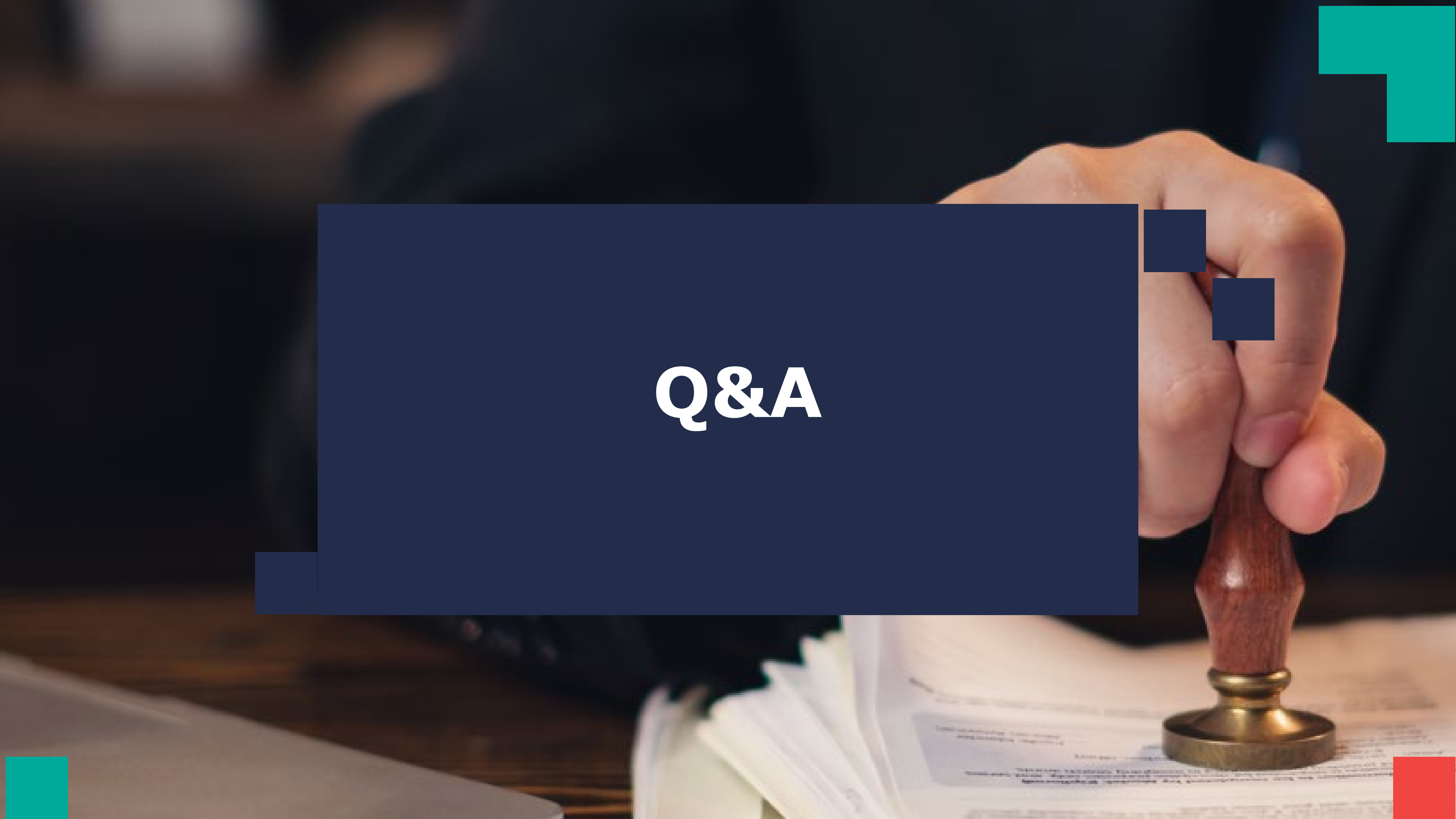
Meet us at Cybersec Europe 2024

11/6

Hoe Threat Intelligence u helpt bij het nemen van betere beveiligingsbeslissingen
(Secutec)

Contacteer ons via:

- info@inetum-realdolmen.world
- Uw vertrouwde contactpersoon bij Inetum-Realdolmen



Q&A

Bedankt