Ciberseguridad **SASE** para alineamiento con la Directiva NIS2

Alberto Pérez | SASE Business Development
South Europe | alberto.perez@hpe.com

February 2025

Today's Common Challenge
Business Happening, Everywhere

People & Things

- Home
- Restaurant
- Cameras
- Machines
- Office
- Sensors
- POS
- BYOD

Applications

- SaaS
- IaaS/PaaS
- Hybrid: staying on-prem in the DC

Connectivity

- Broadband
- FTTH
- Satellite
- Cellular
- MPLS

Users think security hinders performance, innovation and productivity

3/4
Business is Throttled

Business leaders feel their security exposure is increasing

68%
Business is at Greater Risk

Employee Challenges – Modern Workplace

Internet Access and SaaS Applications

- **Internet access without security or control**
- **Over 90% of Internet traffic is SSL-encrypted** including malware
- **Difficult to handle authentication** with new generation SaaS applications
- Impossible to control the **information stored in SaaS**
- Migration to SaaS apps is complex

Internal Applications Access

- **Attack Surface**
- **Least Privilege Access**
- Attaching Employees into the network
- **VPN issues**
- Traffic backhauling sub-optimal
- **Distribution / Provisioning of applications is laborious** and difficult to maintain

Employee Security without a Perimeter

- Users surfing the Internet or accessing applications **outside our perimeter are highly exposed**
- **Difference in security policy** in DC/HQ vs. Rest
- Difficult-to-manage personal information policies and **complex regulatory compliance**
- Need for **different layers of security** that are not necessarily integrated

User Experience

- **Segmented visibility** across multiple platforms and possible blind spots
- **Complex Troubleshooting**
- Differentiated performance Inside vs. Outside HQ/DC
- Difficulty integrating with support tools, experience measurement and next-generation APIs
- **Multiple user experiences depending on the Device**

Multiple devices, IoT, OT...

Enterprise Challenges

Data Security

- Inability to adequately manage all sources containing company data
- Legal issues with respect to security or compliance mandates

Application Provision and Cloud Migration

- Point to multi-point connections required
- Difficulty orchestrating multi-vendor, multi-region or hybrid applications

Contractor / 3rd Party Access

- Access to corporate applications from non-platform devices
- Difficulty or impossibility to deploy agents.
- Extranet or point-to-point VPN required

Secure IoT devices

- Highly inefficient network segmentation unable to provide security in connected IoT/OT environments
- Inability to manage differentiated roles for users and IoT/OT

Cost and Architecture

- Complex and inefficient architectures
- The network do not scale adequately, are unable to adapt and rely on protocols not ready for today's env.
- Perimeter and hardware-based security

Business Agility and Merge & Acquisition

- Need for integration of complex systems
- Working access with overlapping IP space
- Access to infrastructure needed for new employees with non-platformed PCs

Productivity

- Very low capacity to adapt to the business or service.
- Inefficient architectures highly linked to hardware renewal.
- Limited operational efficiency due to difficulties in provision, mgmt. and troubleshooting.

Visibility

- No visibility into network, apps. and user performance
- Lack of vision regarding the use of the applications
- Impossible to understand employee usage patterns to propose improvements

The regulatory landscape has made it harder to protect my business

NIST

SOC2
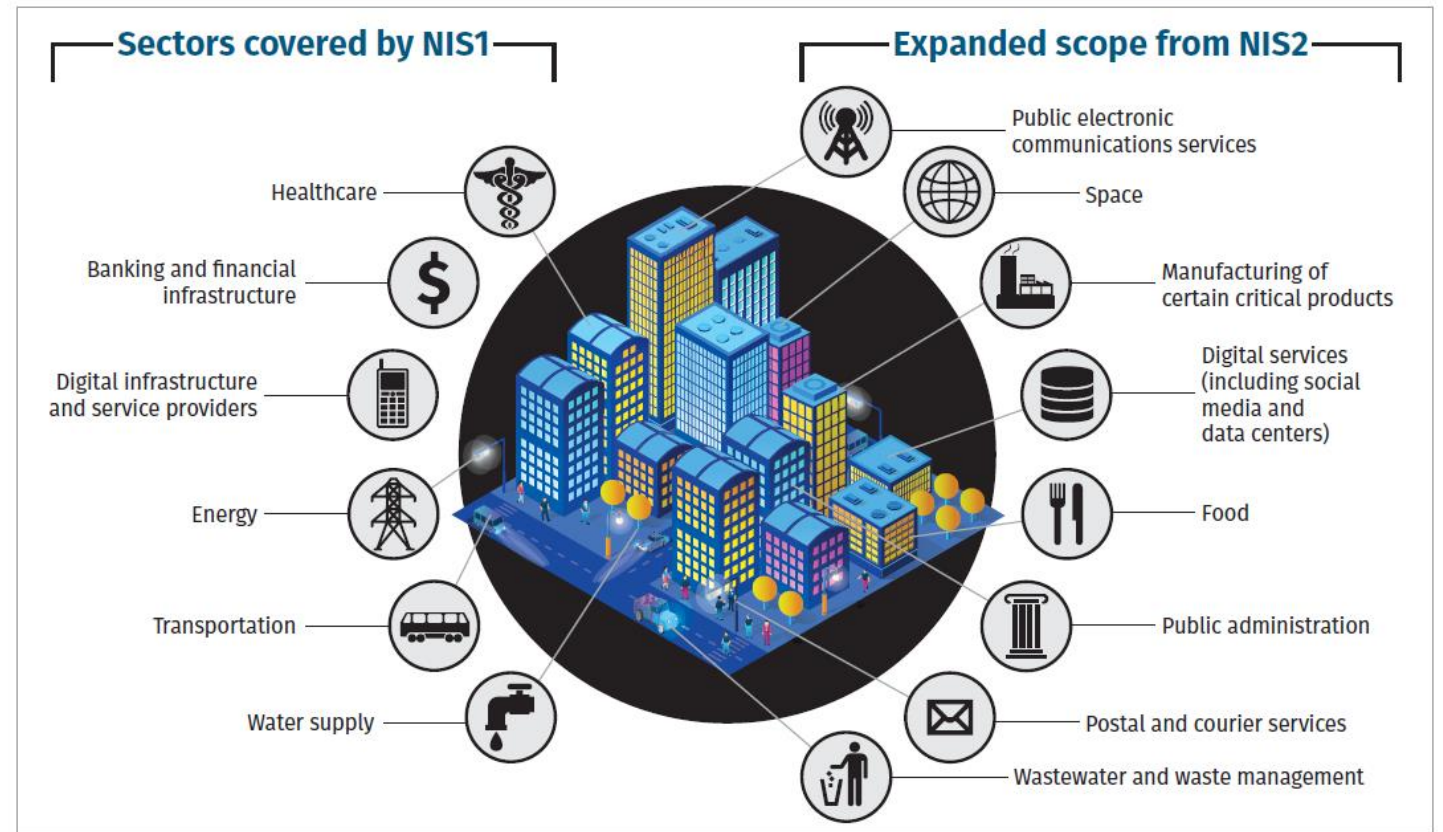
ISO 27001 / 27002

NIS2

Common Criteria

ENS

DORA

NERC-CIP

GDPR

HIPAA

FISMA

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

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

Source: SANS Institute

Figure 4. NIS2 In-Scope Sectors

** Fines of a maximum of at least 10 M€ or 2 %
of the total worldwide annual turnover = GDPR*
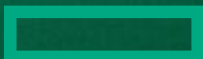
Activating Zero Trust principles intrinsically across all networking

Zero-trust security is a framework built around the concept of least-privileged access, in which no user or application should be inherently trusted.

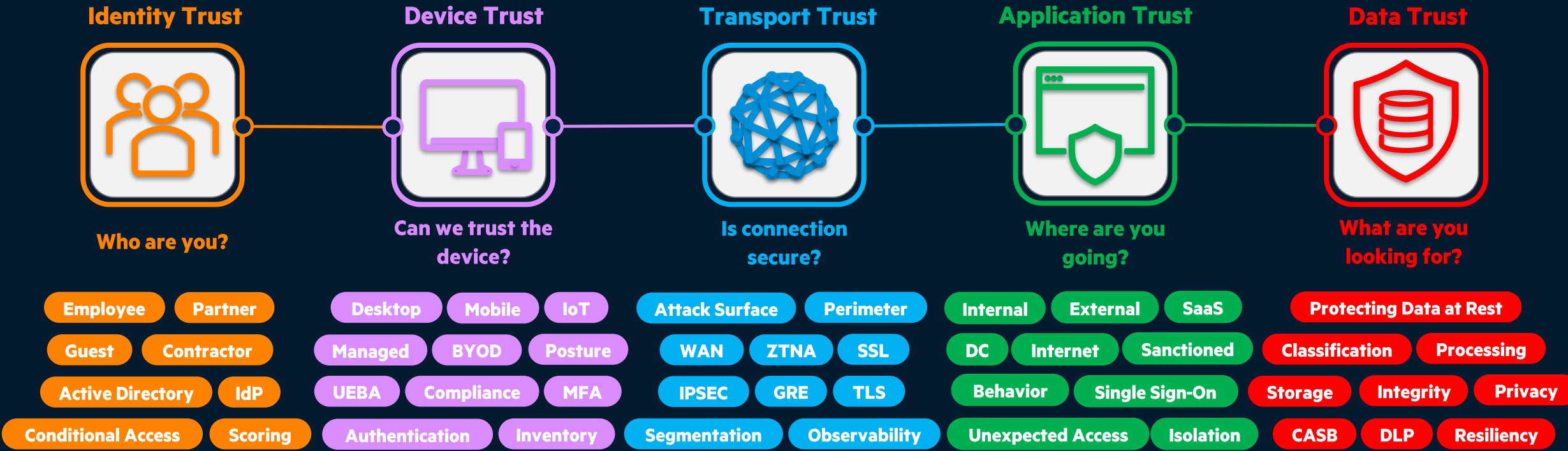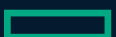## Identity Trust
Who are you?

- Employee
- Partner
- Guest
- Contractor
- Active Directory
- IdP
- Conditional Access
- Scoring

Device Trust
Can we trust the device?

- Desktop
- Mobile
- IoT
- Managed
- BYOD
- Posture
- UEBA
- Compliance
- MFA
- Authentication
- Inventory

Transport Trust
Is connection secure?

- Attack Surface
- Perimeter
- WAN
- ZTNA
- SSL
- IPSEC
- GRE
- TLS
- Segmentation
- Observability

Application Trust
Where are you going?

- Internal
- External
- SaaS
- DC
- Internet
- Sanctioned
- Behavior
- Single Sign-On
- Unexpected Access
- Isolation

Data Trust
What are you looking for?

- Protecting Data at Rest
- Classification
- Processing
- Storage
- Integrity
- Privacy
- CASB
- DLP
- Resiliency

Zero Trust Security

Zero Trust principles cannot be applied to islands of innovation. A holistic approach is mandatory

Zero Trust Security
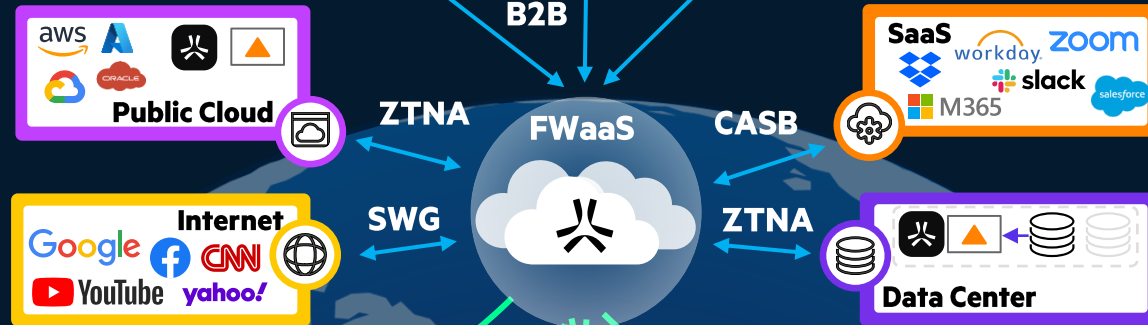
Identity-based
Least-Privilege Access

Micro-Segmentation &
Consistent Enforcement

Continuous Monitoring

Unified SASE

**Multi-Cloud Native
SaaS Platform**

IDP — PingIdentity, okta, onelogin, Azure Active Directory

EDR — Microsoft Intune, SentinelOne, CROWDSTRIKE, VMware Workspace ONE

SIEM — LogRhythm, syslog-ng, splunk>, Azure Sentinel

B2B

Remote Worker

Agent / Agentless

All OS Supported

Unlimited Traffic

Unlimited Devices

SDWAN Embedded

All PoPs Included

Public Cloud — aws, Azure, ORACLE

ZTNA   FWaaS   CASB

SaaS — workday, zoom, slack, salesforce, Dropbox, M365

Internet — Google, CNN, YouTube, yahoo!

SWG   ZTNA

Data Center

Legacy Branch

Legacy Router / FW
Onramp

IPsec Integration

ZTNA / SWG / CASB
Services

SDWAN

Business Intent Overlays

SD-WAN Fabric Orch.

Path Conditioning and QoS

App visibility and control

Zero Trust segmentation

Advanced crypto

Zero Touch Configuration

Services

Devices

Legacy Branches

HQ

Agentless User

Factory

Remote Worker
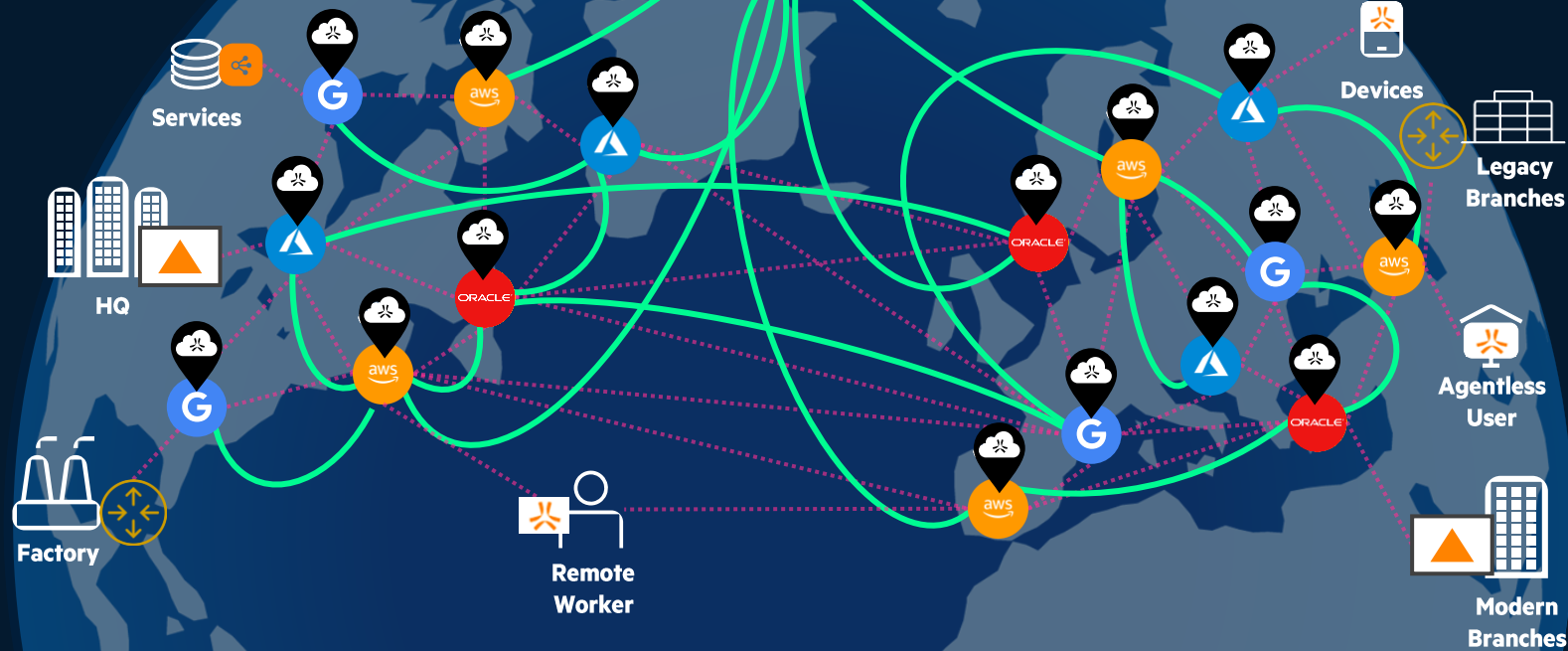
Modern Branches

Transformation Journey with HPE aruba networking

Stream 1:

Smart Digital Workplace

Stream 2:

Zero Trust Remote Access

Stream 3:

Twist Security to Employee Focus

Stream 4:

Network Modernization Multi-Cloud, Branch & Edge

Stream 5:

Reimagine Desktops & Apps with RBI

Stream 6:

Expanding Security Capabilities

Stream 7:
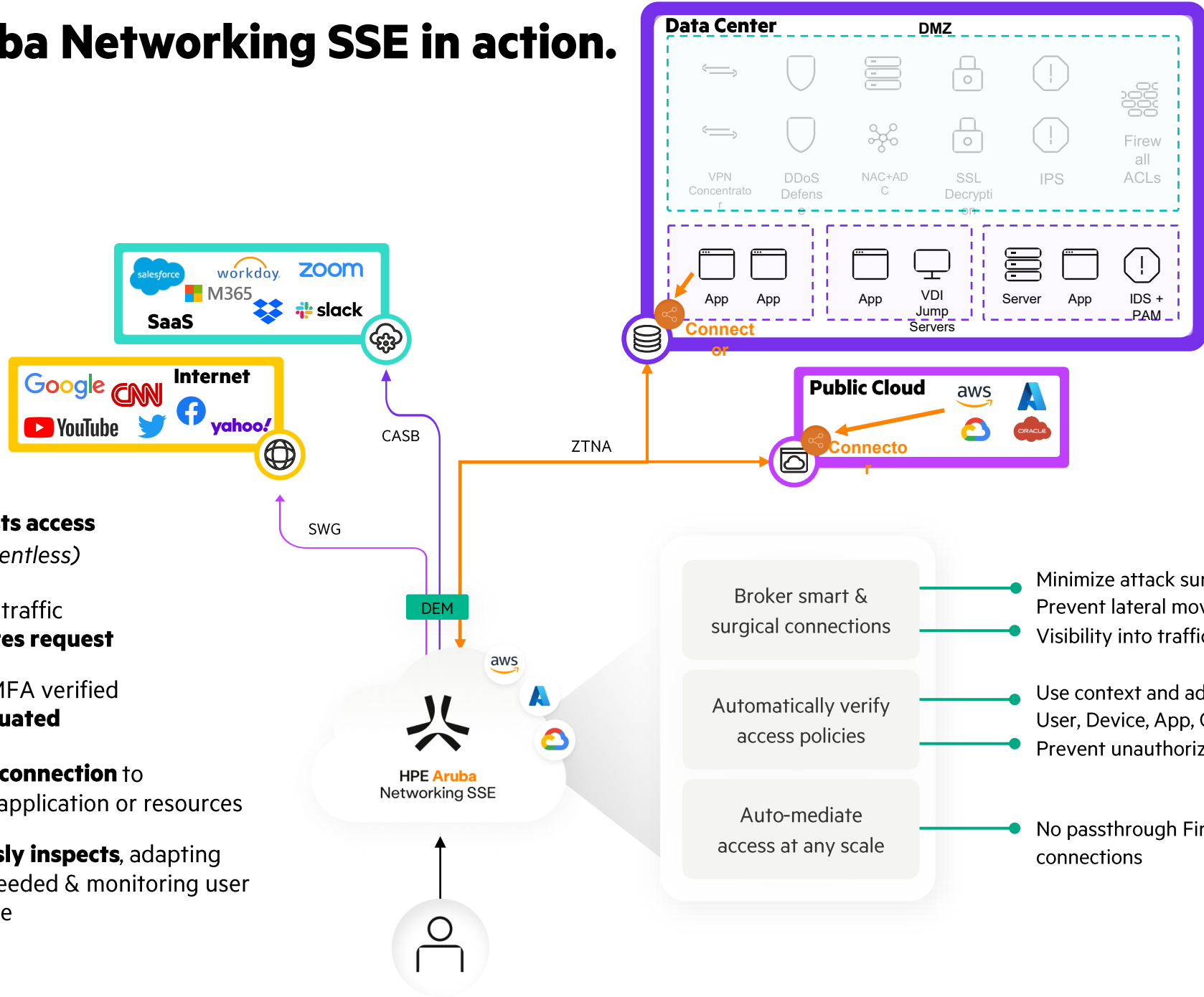
CI/CD, AIOps, Automations and Integrations

Stream 8:

Improving the User Experience in 360°

Select where your journey begins

	VPNs	ZTNA 1.0	Aruba ZTNA
Keep Users Off The Network	⊖	⊕	⊕
Reduce attack surface of infrastructure	⊖	⊕	⊕
DDoS proof Private Apps	⊖	⊕	⊕
Application Discovery	⊖	⊕	⊕
Agentless Web, SSH, RDP, Git, DB, VNC Access	⊖	⊖	⊕
Full SSE Inspection/ Continuous Authorization / Visibility	⊖	⊖	⊕
Per app segments, User group pairing	⊖	⊖	⊕
Any Port / Protocol (P2P / VOIP, AS400, etc.)	⊖	⊖	⊕
Server Initiated Flows / Push Patching	⊖	⊖	⊕
Multi-cloud PoP resilience	⊖	⊖	⊕
Smart Routing for ZTNA Connectors	⊖	⊖	⊕
IPsec Tunnels for ZTNA	⊖	⊖	⊕
Local Edge Private POP	⊖	⊖	⊕

HPE Aruba Networking SSE in action.

Data Center DMZ

VPN Concentrator | DDoS Defense | NAC+ADC | SSL Decryption | IPS | Firewall ACLs

App | App | App | VDI Jump Servers | Server | App | IDS + PAM

Connector

The invisible network

Application access, never network access

Granular least privilege access.

SaaS
salesforce · workday · zoom · M365 · Dropbox · slack

Internet
Google · CNN · YouTube · Twitter · Facebook · yahoo!

Public Cloud
aws · Azure · Google Cloud · Oracle

Connector

CASB

ZTNA

SWG

DEM

1. **User requests access**
   (agent or agentless)

2. Auto-route traffic and **mediates request**

3. Identity + MFA verified **Policy evaluated**

4. **Broker 1:1 connection** to authorized application or resources

5. **Continuously inspects**, adapting access as needed & monitoring user performance

aws · Azure · Google Cloud

HPE Aruba Networking SSE

Broker smart & surgical connections	Minimize attack surface: Prevent lateral movement Visibility into traffic
Automatically verify access policies	Use context and adaptive access: User, Device, App, Content Prevent unauthorized Access
Auto-mediate access at any scale	No passthrough Firewall / VPN connections
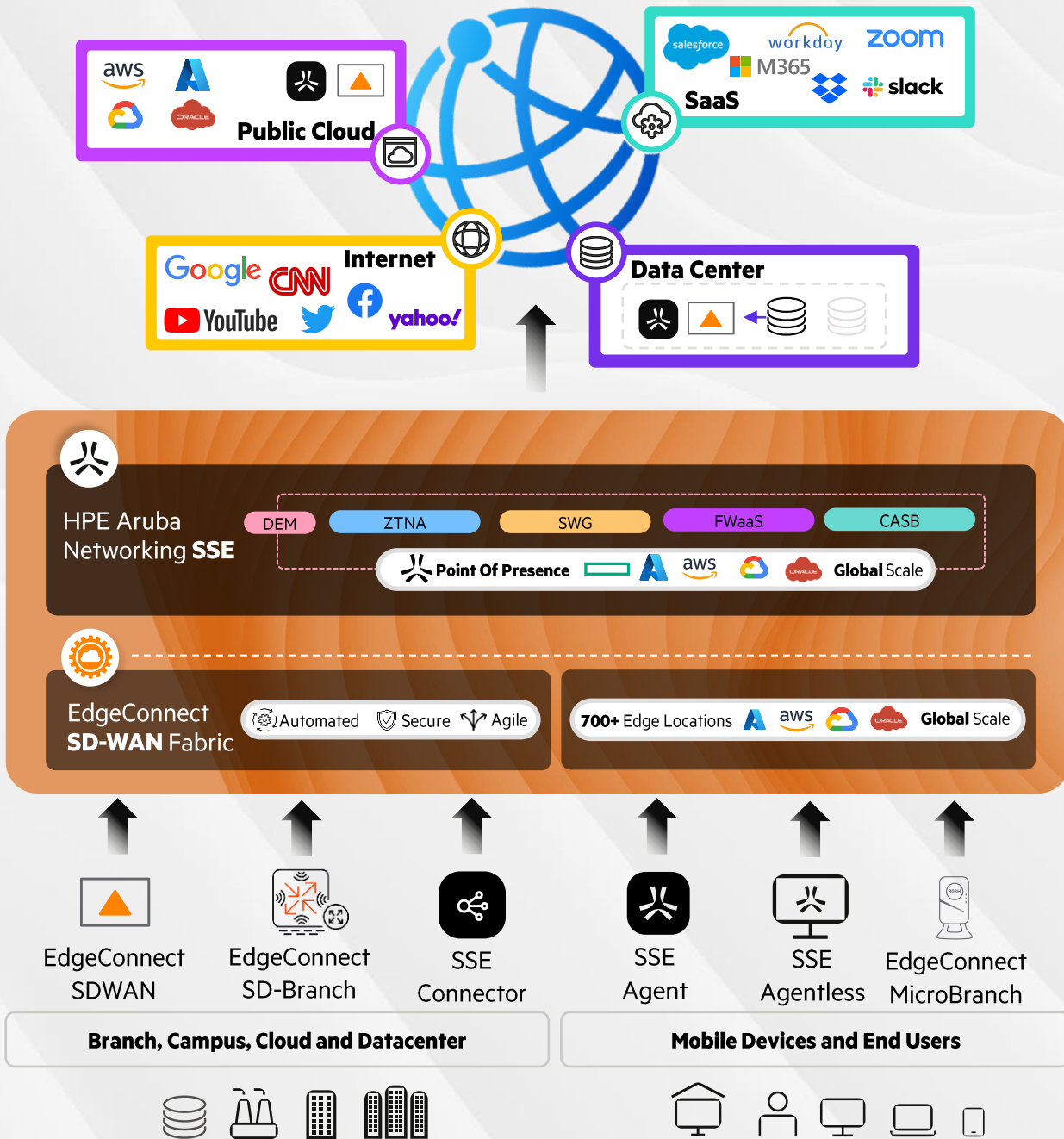
HPE aruba networking **Unified SASE**

Multi-Cloud Native SaaS Platform

+Secure

360° Security

+Simple

Easier to Deploy & Operate

+Productivity

Frictionless User Experience in any Use Case

SDWAN
- ✓ Virtual Overlay Architecture (BIOs) ≪ NIS2
- ✓ Per Packet Traffic Management
- ✓ Path Conditioning
- ✓ High Scalability & Resiliency ≪ NIS2
- ✓ Cloud Native Integration (IaaS/PaaS)
- ✓ SaaS Performance Enhancement
- ✓ Real Time Visibility
- ✓ Advanced Routing (BGP, OSPF)
- ✓ ZTP

Security
- ✓ Certified Stateful Firewall (L3-L7) ≪ NIS2
- ✓ DDoS defense
- ✓ Zero Trust Segmentation
- ✓ VRF Segmentation ≪ NIS2
- ✓ Automated SSE Orchestration

Add-On
- ✓ WAN Optimization
- ✓ Dynamic Threat Defense ≪ NIS2
- ✓ Multitenant Orchestrator
- ✓ On-prem Airgap Solution

Public Cloud

SaaS

Internet

Data Center

HPE aruba networking

Unified SASE Platform

HPE **SSE**

| DEM | ZTNA | SWG | FWaaS | CASB |

Points Of Presence — Global Scale

HPE **SDWAN** Fabric

Automated · Secure · Agile

700+ Edge Locations — Global Scale

HPE SDWAN

HPE SSE Agent

HPE SSE Agentless

Branch, Campus, Cloud and Datacenter | **Mobile Devices and End Users**
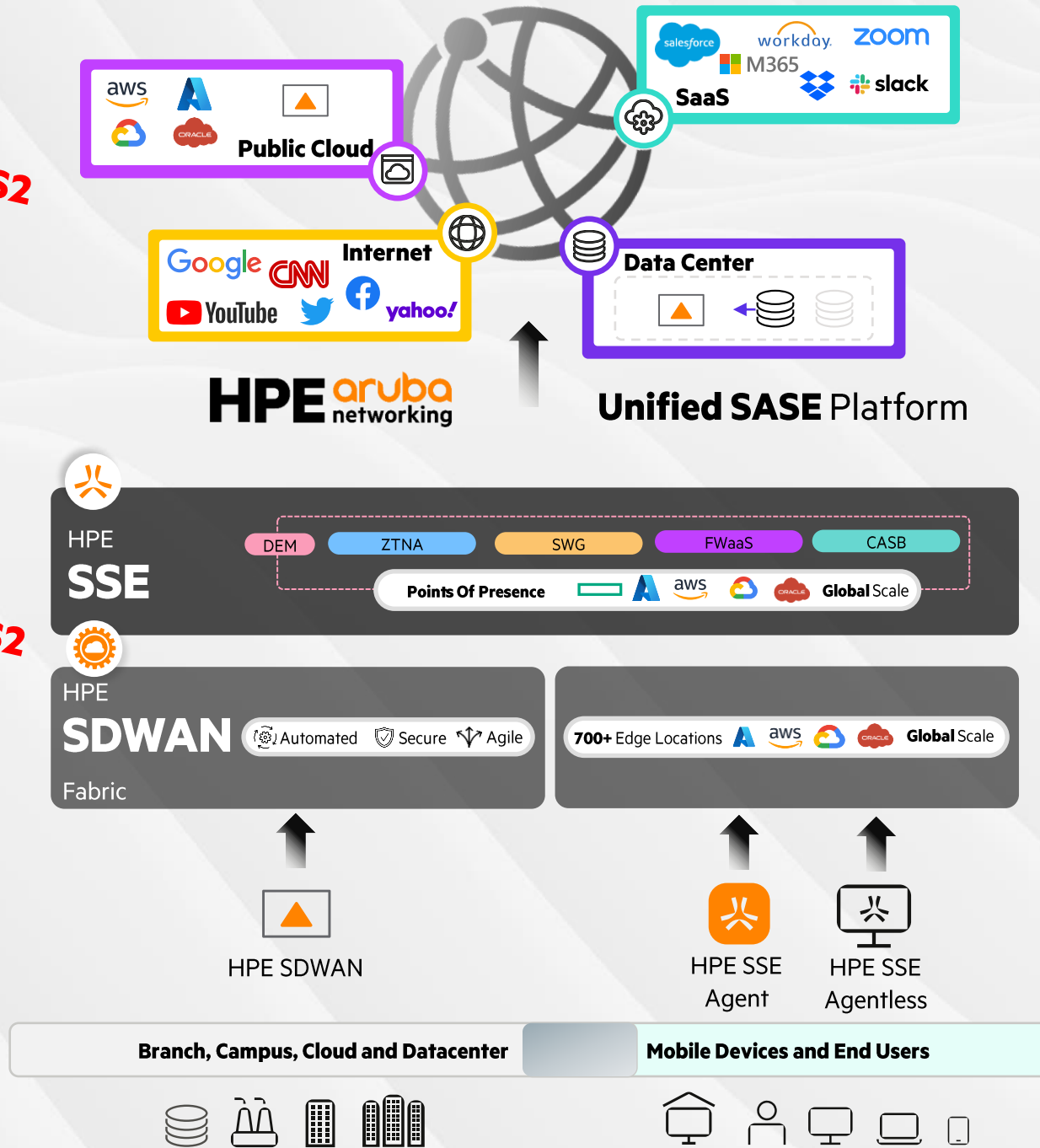
Private Data
- ✓ Zero Trust Network Access
- ✓ Agentless ≪ NIS2
- ✓ Discovery

External Data
- ✓ FWaaS ≪ NIS2
- ✓ Secure Web Gateway ≪ NIS2
- ✓ CASB ≪ NIS2
- ✓ Advanced DLP
- ✓ Malware Scan ≪ NIS2

Operations
- ✓ Dashboard
- ✓ Agent
- ✓ IDP
- ✓ MCN
- ✓ Digital Experience Monitoring
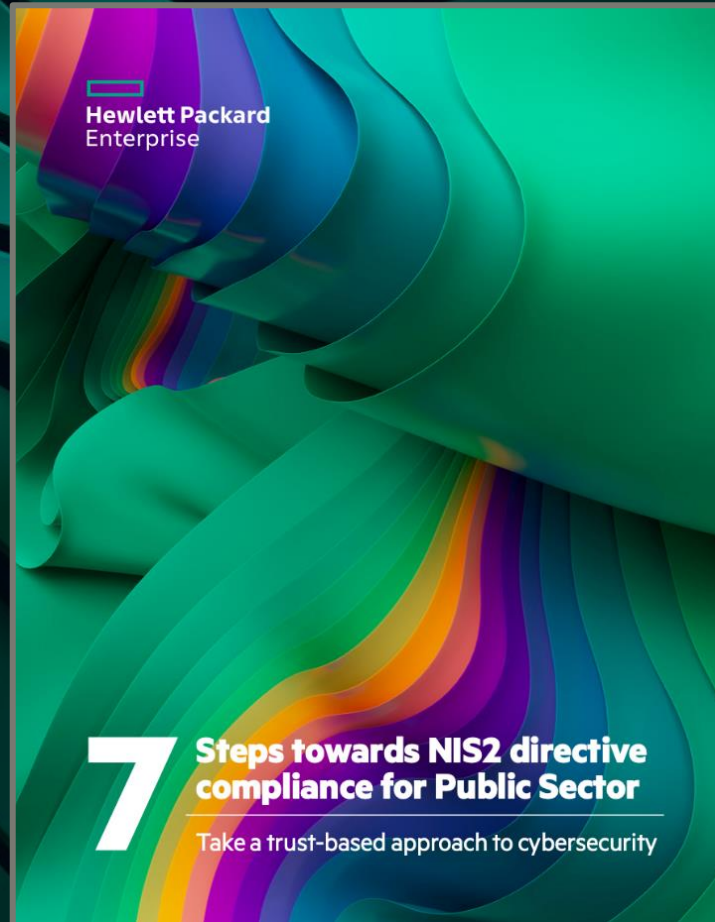- ✓ Local Edge ≪ NIS2
- ✓ Server to Server

Add-On
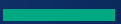- ✓ Sandbox Security Package ≪ NIS2

13

Helpful documents

https://www.hpe.com/psnow/ebook/306180
d2-4609-4110-b476-b7beb01f3677