

Hewlett Packard
Enterprise

Delivering Edge-to-Cloud Security with HPE Aruba Networking

Tiago Rés

Systems Engineer
January 30th, 2025

An Interconnected World in the Digital Era

New opportunities...new challenges... innovation



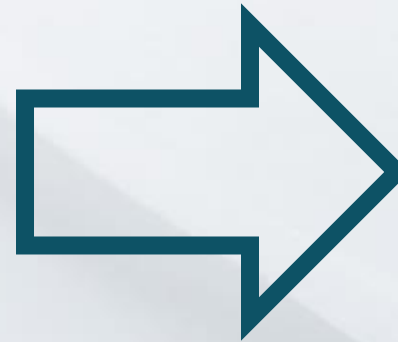
Digital transformation



Cloud-first IT architecture



The mobile worker/WFA



WAN transformation



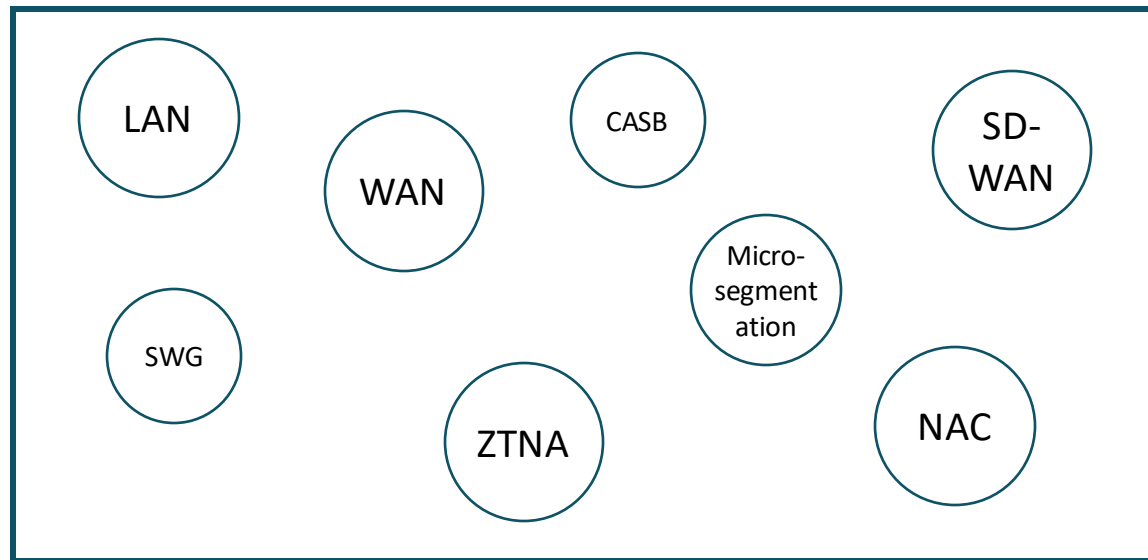
Security transformation



Security-first: The network as a Zero Trust Security solution

Provides a common Zero Trust foundation for networking and security teams

Before: A patchwork approach

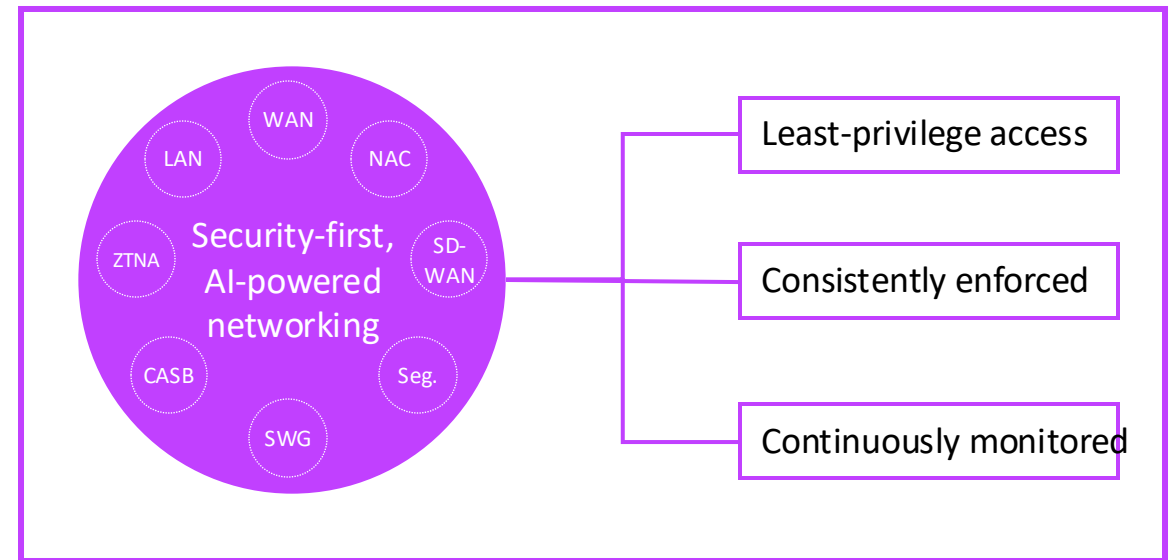


Siloed operations

Complexity & inconsistency

Blind spots & gaps

After: Activating Zero Trust intrinsically

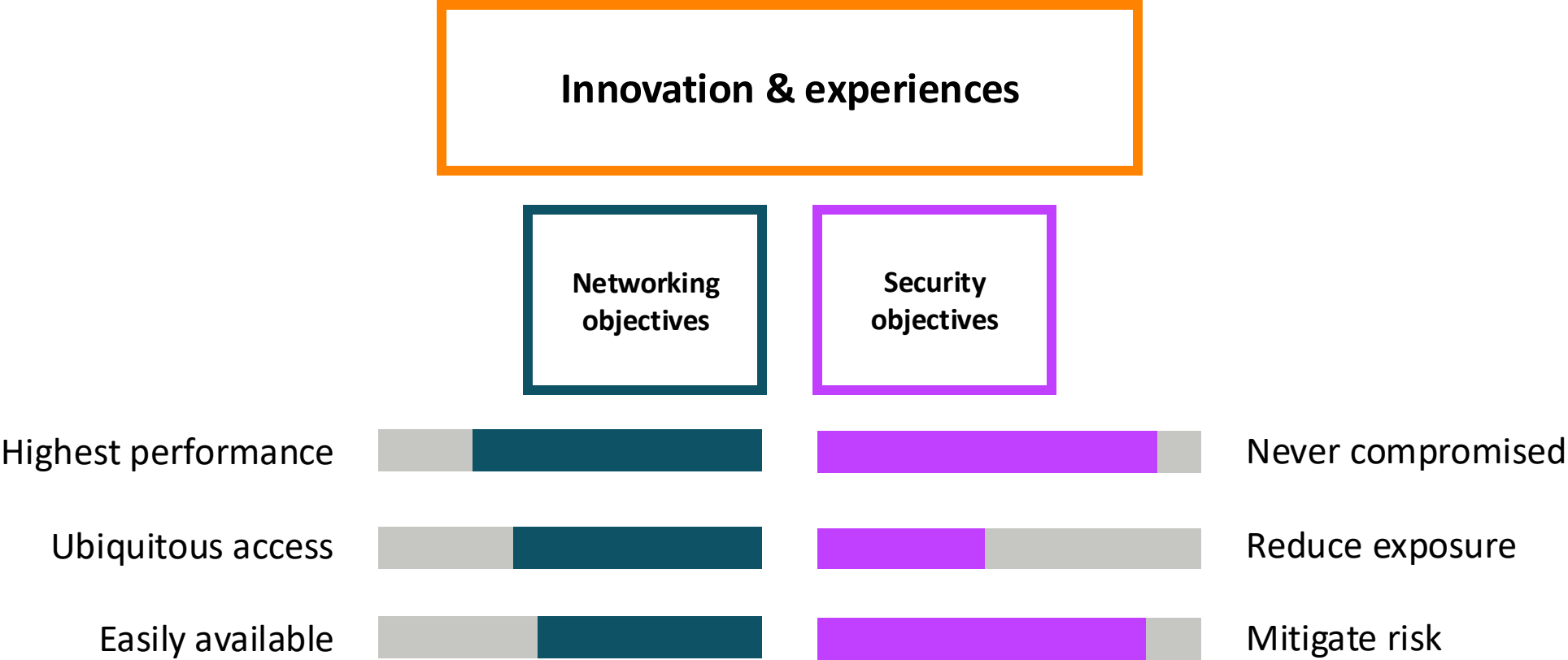


Built-in everywhere

Protects everything

Works with the anything

How do you balance multiple objectives?

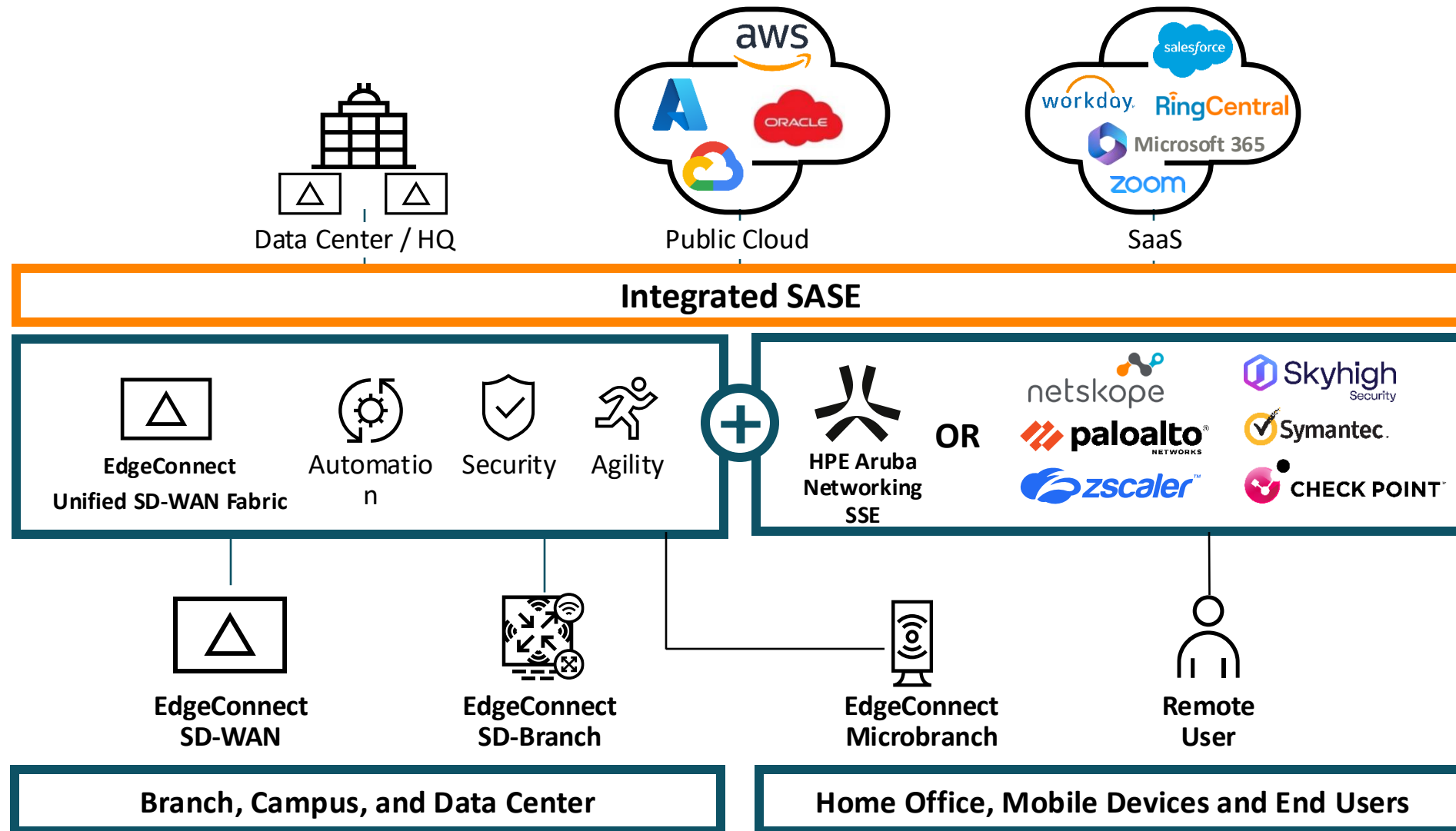




What is SASE?

**SASE brings
network and
security
together**

Shift toward single-vendor or multi-vendor SASE



EdgeConnect SD-WAN

Why SD-WAN?

EdgeConnect SD-WAN Key Use Cases

Improve business-critical applications



- Provide private line-like performance over the internet with path conditioning, SaaS and WAN optimization capabilities
- Run high quality voice and video over broadband internet
- Prioritize mission-critical applications with business intent overlays
- Get the highest quality of experience

Support cloud-first organizations



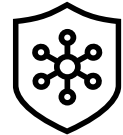
- Intelligently steer traffic to the cloud and eliminate the need for backhauling traffic
- Build a unified SASE platform or seamlessly connect to multiple third-party SSE solutions
- Deploy EdgeConnect SD-WAN to any cloud providers (Azure, AWS...)

Replace branch firewalls & routers



- Consolidate branch network and security functions
- Built-in next-generation firewall with IDS/IPS, DDoS protection
- Protect data in transit with IPsec tunnels
- Full support for OSPF and BGP
- Easily deploy security policies with zero-touch provisioning

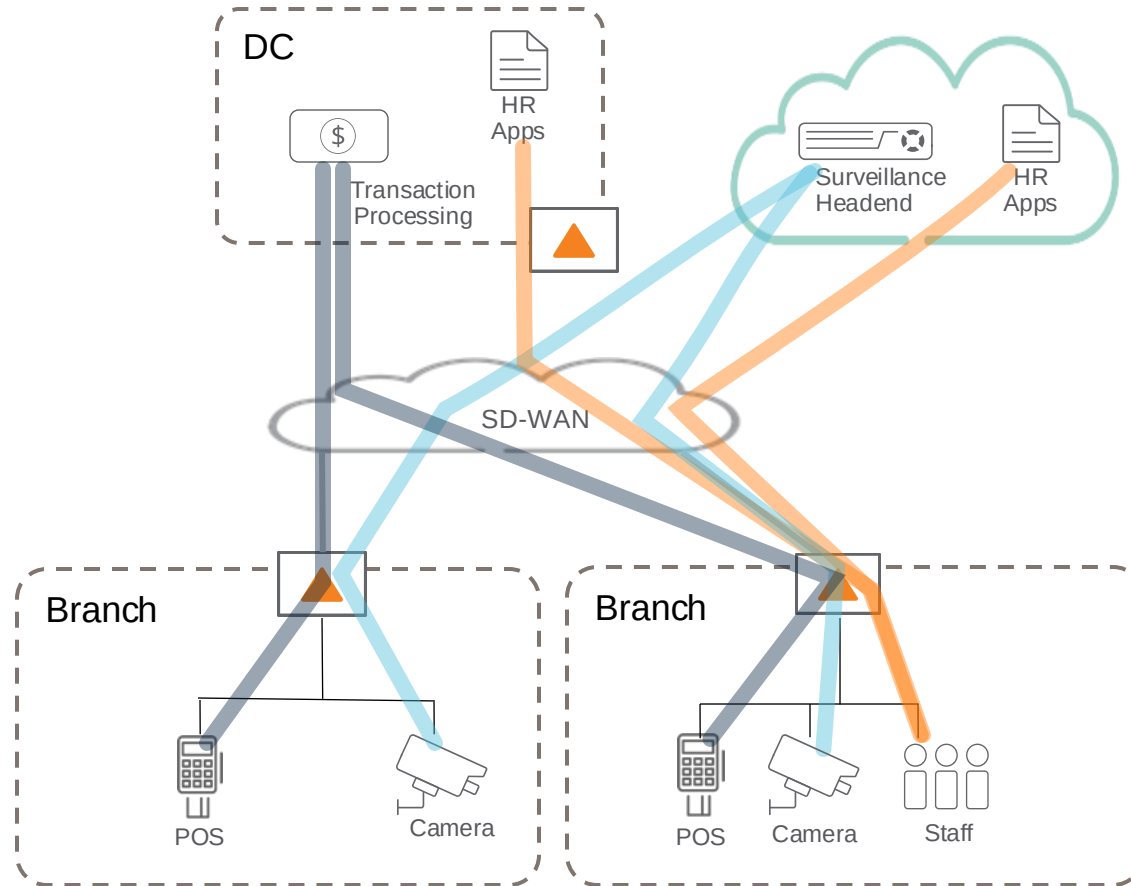
Secure IoT devices



- Implement zero-trust network segmentation to complement SASE
- Ensure that users and IoT devices can only reach network destinations consistent with their policy
- Go beyond what is defined by SASE

Zero Trust Dynamic Segmentation Extended to the WAN

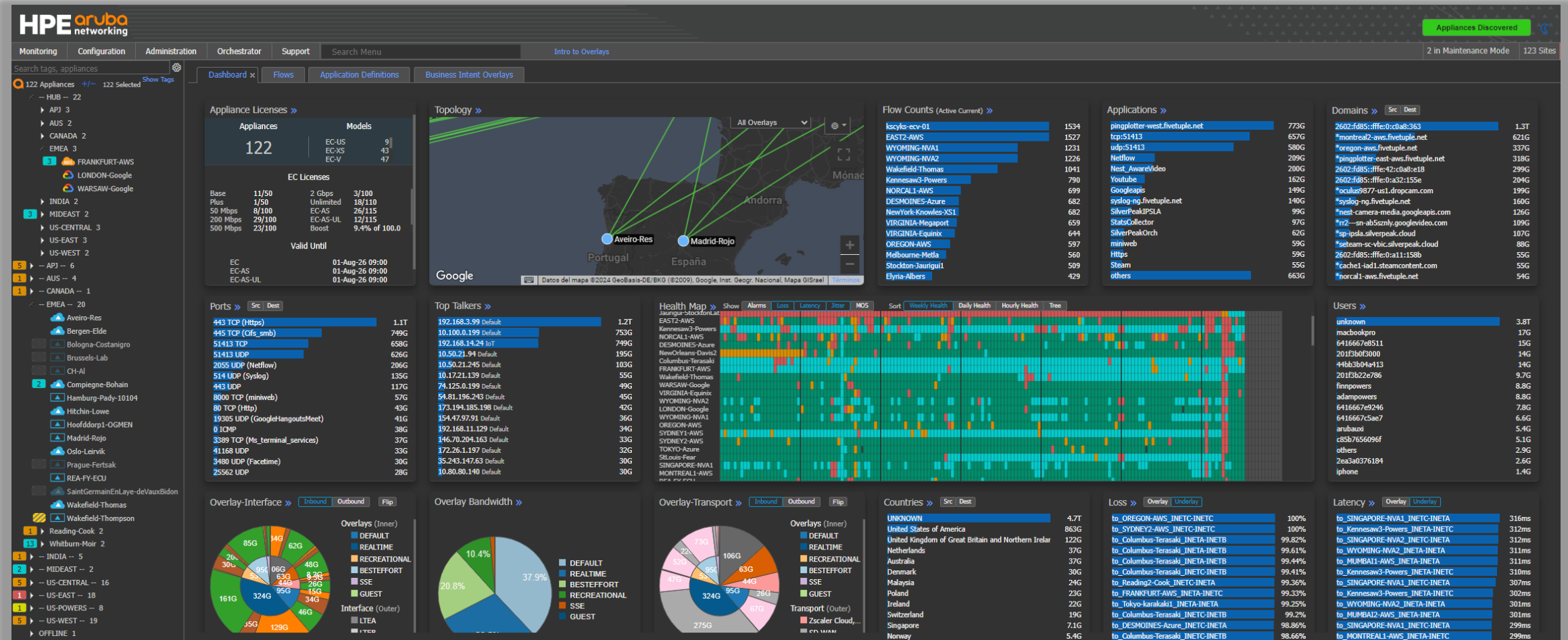
Users/devices can only communicate with destinations consistent with their role



- Identify users and devices by **identity, role and security posture**
- Dynamically **segment and isolate** application traffic based on context
- **Business-driven** policy example

	Camera	Surveillance Headend	POS Terminal	Transaction Processing	Contract Recruiter	HR Apps
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
POS Terminal	✗	✗	✗	✓	✗	✗
Transaction Processing	✗	✗	✓	✓	✗	✗
Contract Recruiter	✗	✗	✗	✗	✗	✓
HR Apps	✗	✗	✗	✗	✓	✓

Application and Network Visibility



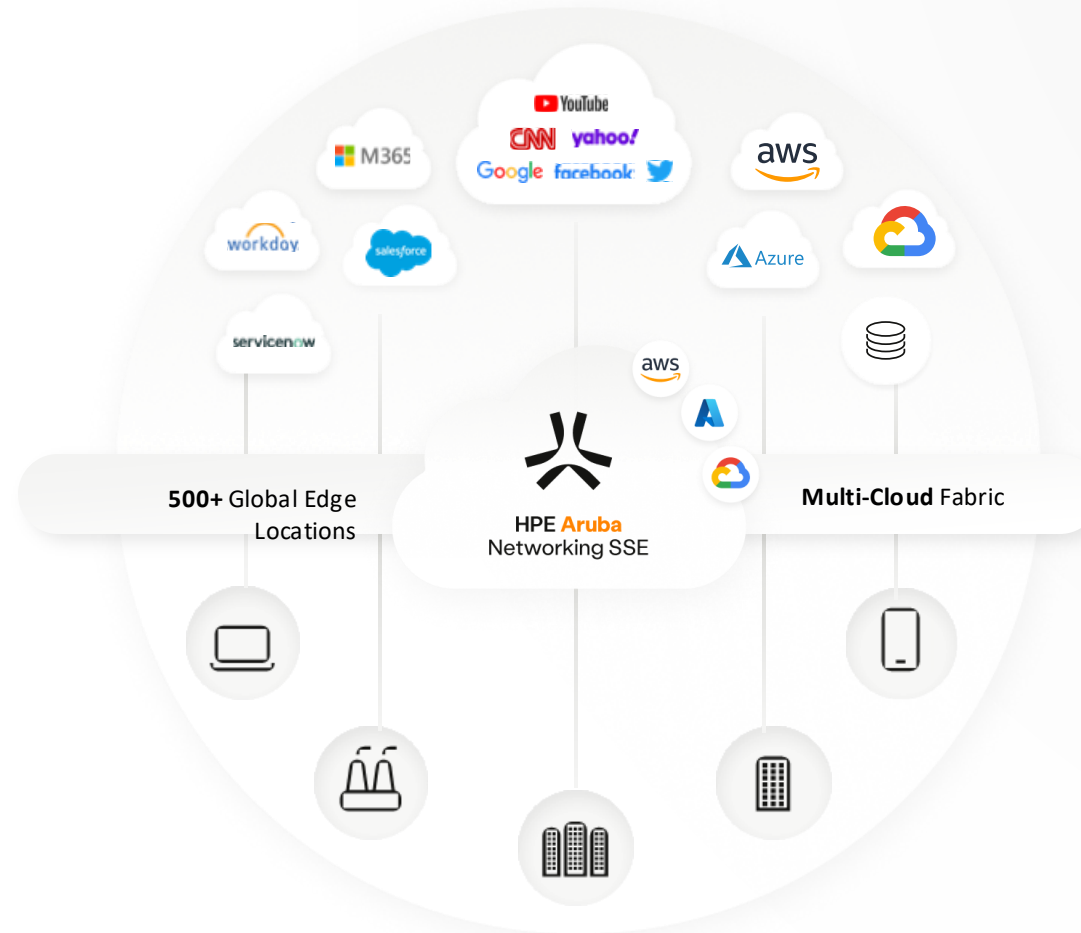
EdgeConnect SSE

A modern approach to secure connectivity with Next-Gen SSE

Security Service Edge

- ✓ **Unified service – power of one**
Unified ZTNA, SWG, CASB and DEM service with one cloud, one UI, and one policy

- ✓ **Secure access for all resources**
Secure access across any private app, Internet site, or SaaS app - using modern zero trust capabilities



- ✓ **Intelligent cloud Global scale**
Smart-routing across 500+ edges across 5 continents running an AWS, Azure, and Google backbone.

- ✓ **Prioritized user experience**
SSO/MFA integrations, digital experience monitoring, and an intuitive User Portal

Secure access to applications for remote or third-party users, replace VPN

HPE Aruba Networking ZTNA (Zero Trust Network Access)

VPN replacement

- Replace traditional VPN solutions by providing secure access for any user, any device, and any private application.

Single pane of glass

- Configure granular policies for all private applications in a centralized policy engine.

Agent and agentless

- Private apps can be accessed with, or without, an agent. Integrations with any SSO solution creates a frictionless user experience

Least privilege access

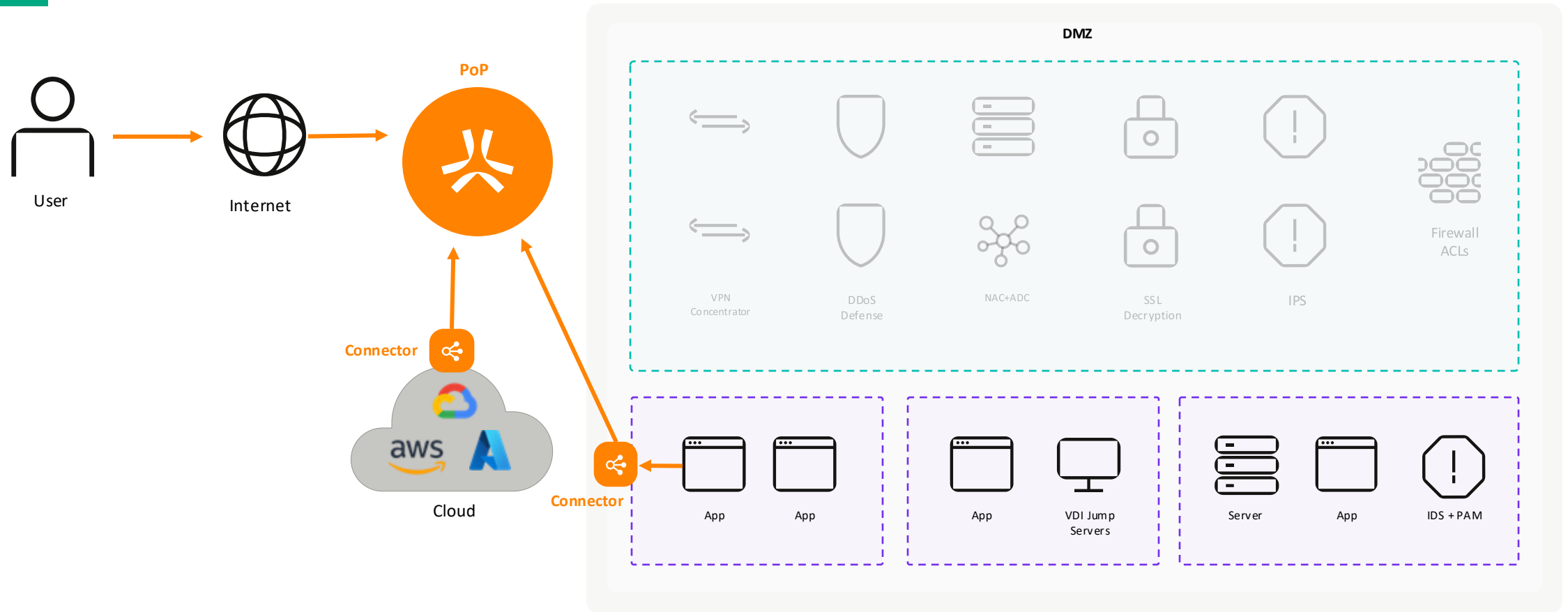
- Identity and policy-based access without placing users onto the network, exposing apps, or any firewalls or ACLs

The screenshot displays the 'Policy' configuration page in the HPE Aruba ZTNA console. The page features a table of policies with columns for Priority, Enabled status, Name, Users, Context, Destinations, Action, and Profiles. Annotations highlight specific features:

- Block access from risky destinations:** Points to the 'Destinations' column for Policy 2, which lists 'Iraq', 'Russia', and 'North Korea'.
- Define access to internal and external apps in a single policy:** Points to the 'Destinations' column for Policy 3, which lists various applications like 'DropBox - Managed', 'Box Managed', 'Pornography and Adult', 'Malware Sites', and 'Gambling'.
- Leverage rich device posture for context:** Points to the 'Context' column for Policy 7, which lists 'Windows 10 + patches' and 'CrowdStrike Enabled'.

Priority	Enabled	Name	Users	Context	Destinations	Action	Profiles
1	On	SSH internal	Daniel Reisel	Any	Any Application	Allow	Default Profiles
2	On	High Risk Nations	Any		Any Application	Block	Default Profiles
3	On	Block Malware, Gambling, Dropbox Uploads	All Full Time Employees...	Windows Baseline Mac Baseline	DropBox - Managed Box Managed Pornography and Adult Malware Sites Gambling	Block	Client SSL Inspection And 5 Default Profiles
4	On	All Employees - Managed Devices	All Full Time Employees...	Windows Baseline Mac Baseline iOS Device Posture	Salesforce All Employee Apps VOIP SSL Exclusion Category	Allow	Default Profiles
5	On	All Employees - BYOD	All Full Time Employees...	Any	All Employee Apps SSL Exclusion Category	Allow	BYOD Policy And 5 Default Profiles
6	On	Accounting Team - Accounting Apps	Accounting	Any	Accounting Apps	Allow	Default Profiles
7	On	HR Team - HR Apps	Human Resources	Windows 10 + patches CrowdStrike Enabled	HR Apps	Allow	Default Profiles
8	On	Contractors - Contractor Apps	Contractors	Any	Contractor Apps	Allow	Contractors RDP Profile

HPE Aruba SSE delivers zero trust access for all



The invisible network

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

Application access, never network access

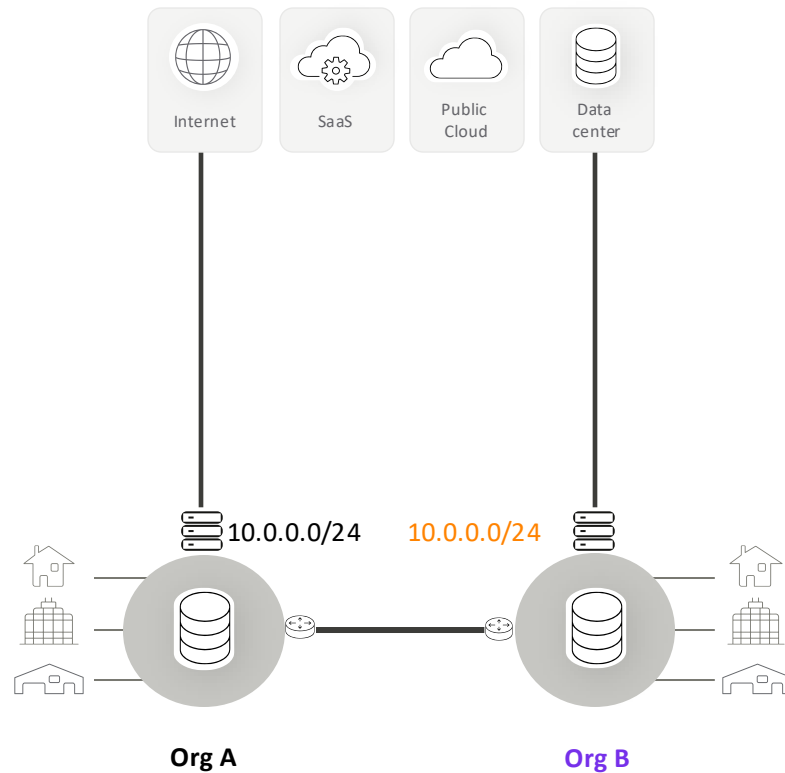
Remote users only receive access to authorized applications without placing user or device on the corporate network.

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.

Streamline M&A IT Integration Projects with ZTNA

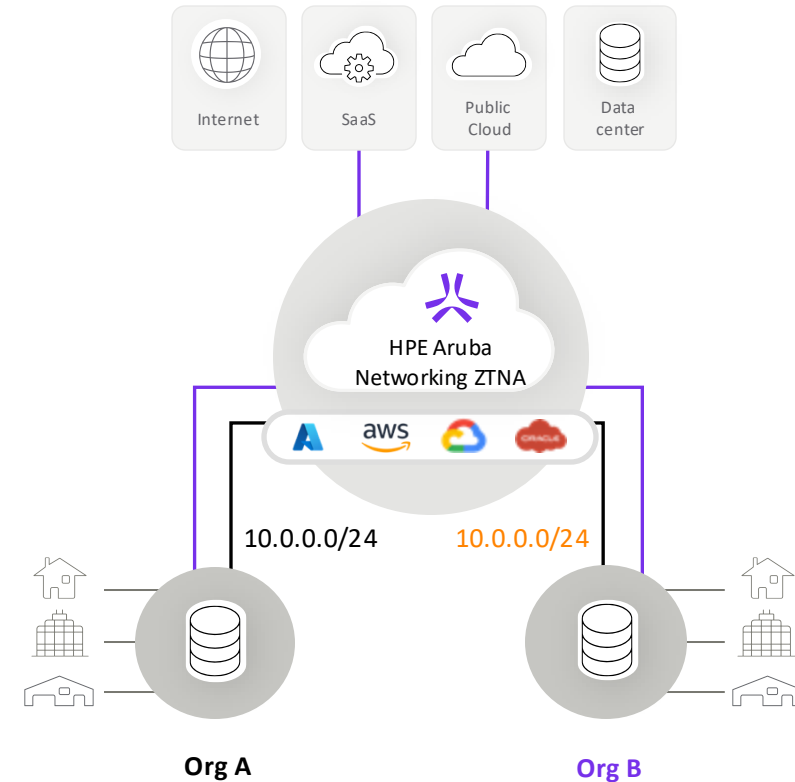
M&A with traditional networking



- Network convergence and NATing for IP overlaps
- Security standards often not on par
- Requires ACLs via firewalls for network access

HPE aruba
networking

M&A with ZTNA



- Networks left as is, no need to consolidate
- Standardized security across both companies
- Users have direct-to-app access w/o network access

Protect against malicious web traffic and eliminate cybersecurity risks

HPE Aruba Networking SWG (Secure Web Gateway)

Inspection of all traffic

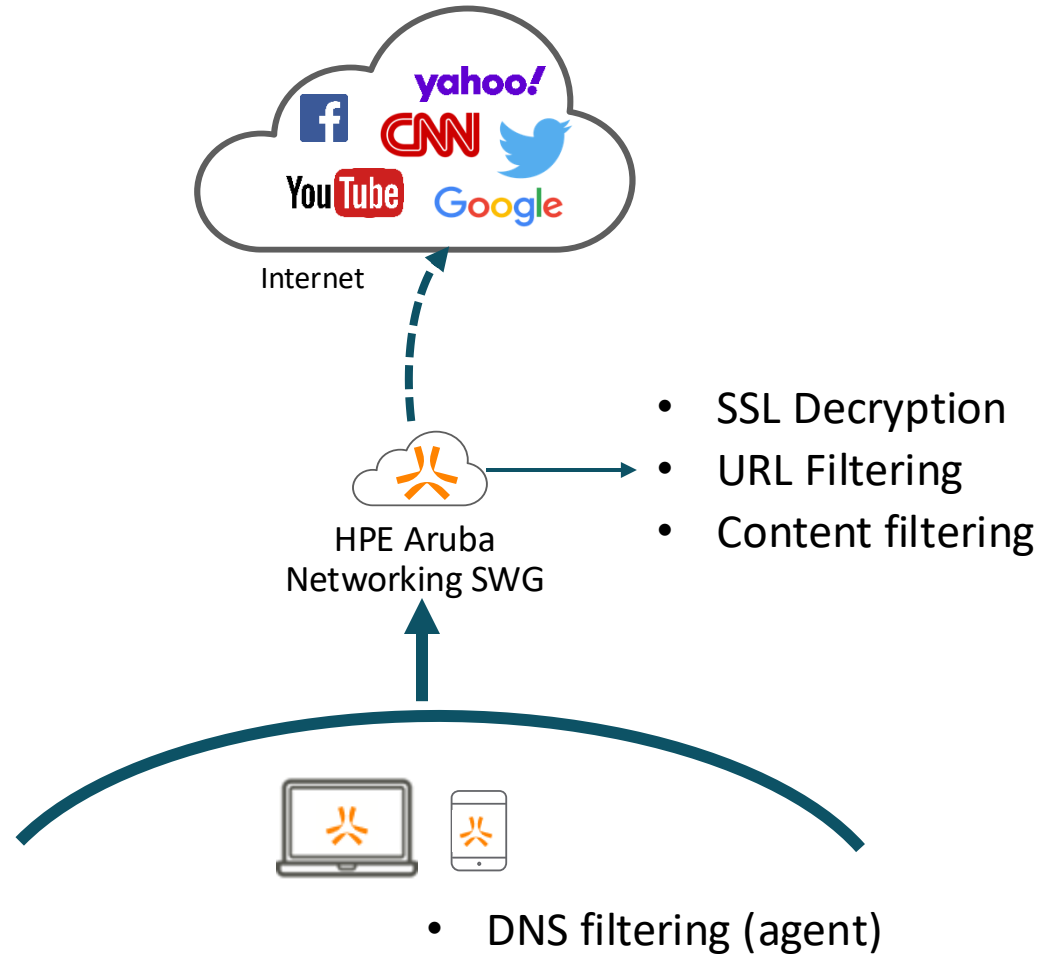
- Secure and protect against malicious threats and perform several security inspections including URL filtering, malicious code detection and web access control.

Three-layer protection

- DNS filter blocks domains and IPs. Destinations, that needs further inspection are sent to the closest PoP to be SSL decrypted and then go through URL filtering and content filtering.

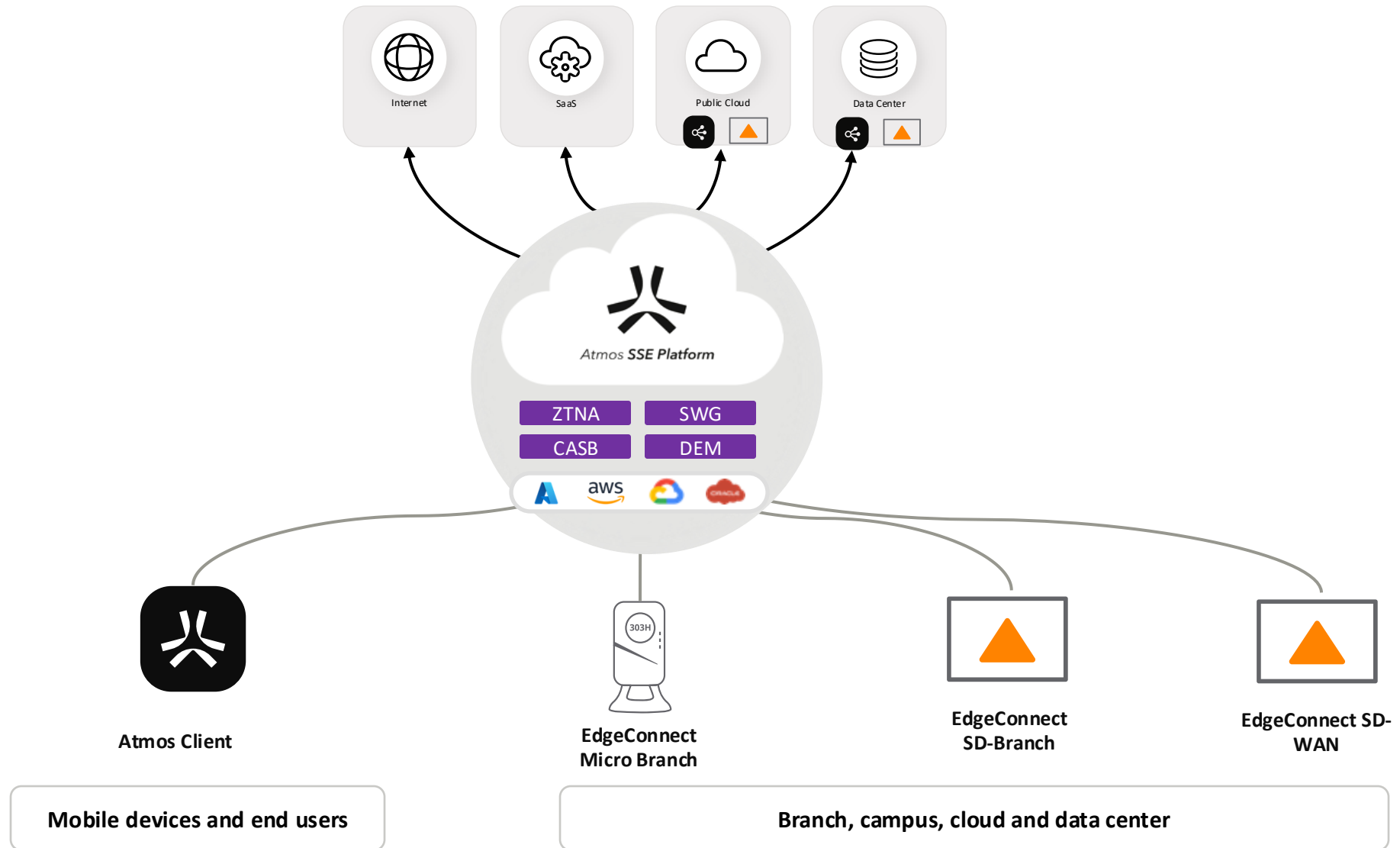
Data Leak Prevention (cross platform)

- Protect sensitive data from leaking out to the Internet.



Unified SASE

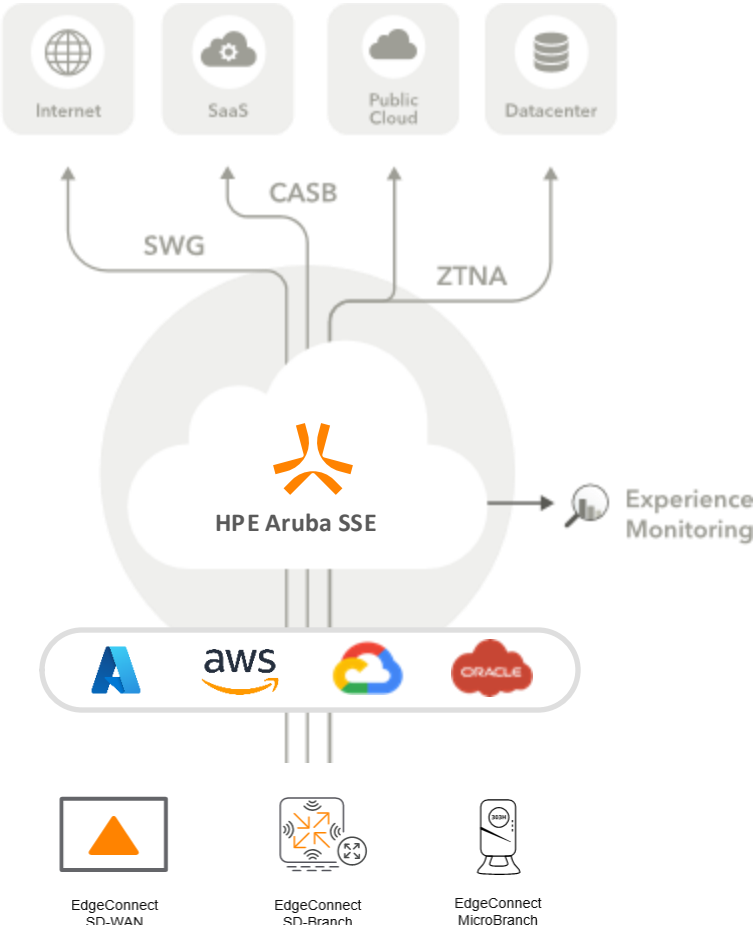
Work from anywhere with unified SASE



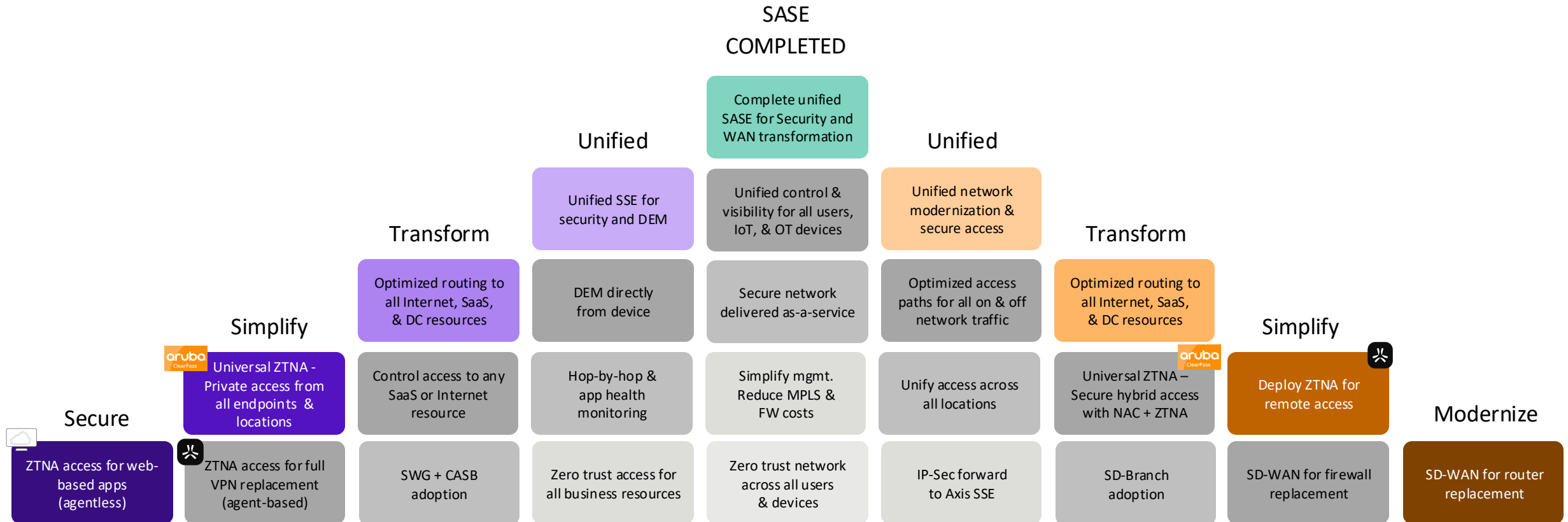
Complete SASE Picture

SD-WAN Traffic to Internal Subnets							Breakout Traffic to Internet & Cloud Services			
Priority	Overlay	Region	Topology	Hubs +	Primary Interfaces	Backup Interfaces	QoS & Security +	Policy Order	Primary Interfaces	Backup Interfaces
1	Management	Global	Regional Mesh		INTERNET1 INTERNET2 MPLS1	LTE If Pri & Sec Down		Branch	HUB-London HUB-NewYork HUB-Barcelona	
=	Match Traffic	Regions						1	Break out	INTERNET2 INTERNET1
×	Overlay ACL				High Quality Waterfall: Overall Quality			2	Backhaul	Waterfall: Fixed Order
2	RealTime	Global	Mesh		INTERNET1 INTERNET2 MPLS1	LTE If Pri & Sec Below Service Level		Branch	HUB-London HUB-NewYork HUB-Barcelona	
=	Match Traffic	Regions						1	Break out	INTERNET2 INTERNET1
×	Overlay ACL				Custom Waterfall: Overall Quality			2	Backhaul	Waterfall: Auto
3	CriticalApps	Global	Regional Hub & Spoke		INTERNET1 INTERNET2 MPLS1	LTE If Pri & Sec Down		Branch	HUB-London HUB-NewYork HUB-Barcelona	
=	Match Traffic	Regions						1	HPE SSE	INTERNET1 INTERNET2
×	Overlay ACL				High Quality Waterfall: Overall Quality			2	Break out	Waterfall: Auto
4	BulkApps	Global	Mesh		INTERNET1 INTERNET2 MPLS1			Branch	HUB-London HUB-NewYork HUB-Barcelona	
=	Match Traffic	Regions						1	Backhaul	Balanced
×	Overlay ACL				High Throughput Balanced: Link Capacity ...					
5	WebBrowsing	Global	Regional Hub & Spoke		INTERNET1 INTERNET2 MPLS1			Branch	HUB-London HUB-NewYork HUB-Barcelona	
=	Match Traffic	Regions						1	HPE SSE	INTERNET1 INTERNET2
×	Overlay ACL				High Throughput Balanced: Link Capacity ...			2	Break out	Balanced
								3	Backhaul	
6	DefaultOverlay	Global	Regional Hub & Spoke		INTERNET1 INTERNET2 MPLS1			Branch	HUB-London HUB-NewYork HUB-Barcelona	
=	Match Traffic	Regions						1	Break out	INTERNET1 INTERNET2
×	Overlay ACL				High Throughput Balanced					

Context	Destinations	Action	Profiles
Barcelona-Miguel	Nudity	Block	SSL Inspection
Zaragoza-Iker	Gambling		And 6 Default Profiles
Lisboa-TiagoRes	Pornography and Adult		
Madrid-Miguel - Rest	Games		
Madrid-Miguel-IoT			
Barcelona-Miguel	Google Docs	Allow	SSL Inspection
Zaragoza-Iker	Google Drive		mrojo-File Security Profile (Exter...
Lisboa-TiagoRes	Dropbox (Restrict upload)		And 5 Default Profiles
Madrid-Miguel - Rest			
Madrid-Miguel-IoT			



SSE – Phase 1 in the journey to unified SASE



70% Start with SSE → ← 30% Start with SD-WAN



Thank you

