softsource VBRIDGE

Hewlett Packard Enterprise

Behind the Breach

HPE aruba networking

softsource VBRIDGE

Hewlett Packard Enterprise

Steve Isles

SASE LEAD, ANZ HPE ARUBA NETWORKING

HPE aruba networking

HPE's Believe it or Not

Mind-blowing facts from Aotearoa and beyond!

A Cyberattack Every 39 Seconds

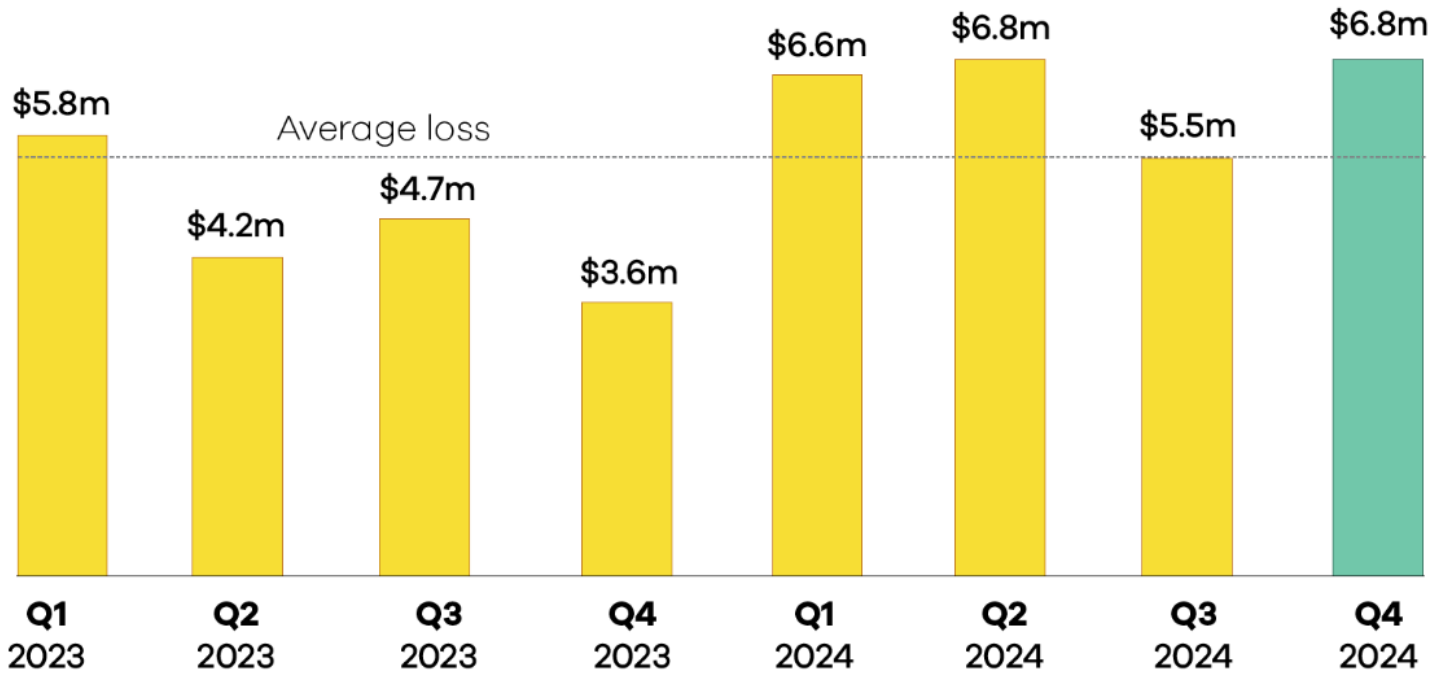
Globally, a cyberattack occurs every 39 seconds.

400% **more IoT malware attacks year over year.**

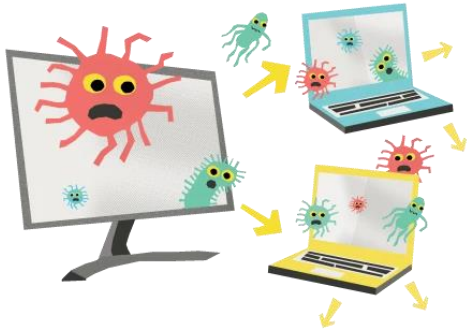
69% **of attacks targeted Mexico and the US**

Source: Check Point Research, Q2 2024 Threatlabz

New Zealand: Not Immune



- CERT NZ responded to 1,358 incidents in Q4 2024 alone
- Scams and fraud were the most reported categories



Source: CERT NZ Q4 2024

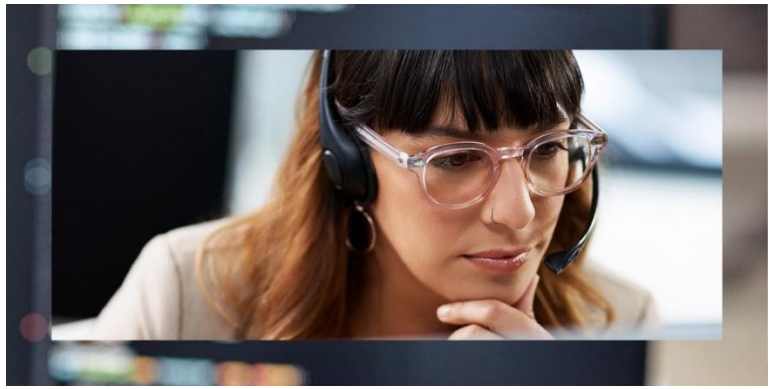
Human error remains the single largest cause of data breaches. Up to 95% in 2024.

Source: Infosecurity Magazine, 2024

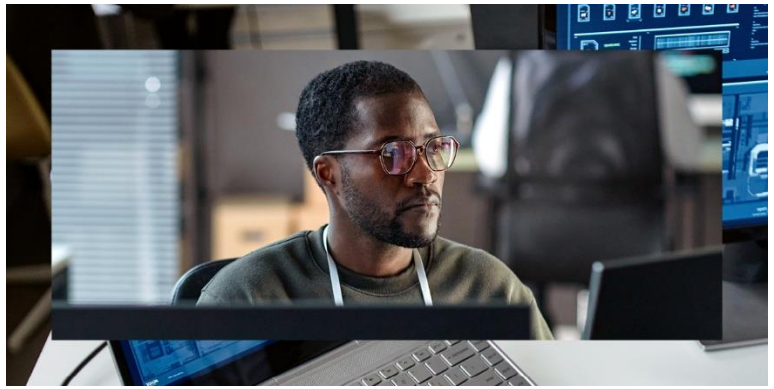
AI: Predictive Defender or Unseen Threat?

30% of security pros use it daily

42% are exploring its use



63% say they're not ready for AI-based threats



Source: 2024 ISC2 Cybersecurity Workforce Study

Home is Where the Hack Is

- Since 2023, there's been an 82% increase in home network attacks.
- Unsecured IoT & smart home devices and remote work are the new attack surface.
- Devices face an average of 10 attacks per day.

Source: NETGEAR/Bitdefender, Zayo Group 2024

Cyber Villains aren’t just teenagers in hoodies

Organised Cybercrime

Badbox

What: Malware preloaded on cheap Android devices
How: Sold via online marketplaces, often used in schools/businesses.
Risk: Remote access, data theft, ad fraud. Survives factory reset.
Takeaway: If it’s cheap and unknown, it’s probably compromised.

Hacktivists

Anonymous Sudan

What: Hacktivist group with alleged Russian-links posing as Sudanese.
How: DDoS attacks targeting Western banks, airlines, and gov.
Risk: Site takedowns, ransom demands, public disruption.
Takeaway: Ideology meets extortion. Public-facing = vulnerable.

Alleged Nation-State Actors

Salt Typhoon

What: Chinese state-backed cyber crew targeting critical infrastructure.
How: Uses admin tools to stay invisible. Breaches via unpatched edge devices.
Risk: Espionage, long-term access, possible war-time disruption.
Takeaway: They're quiet, but lethal. You won’t see them coming.

What can we do about it?

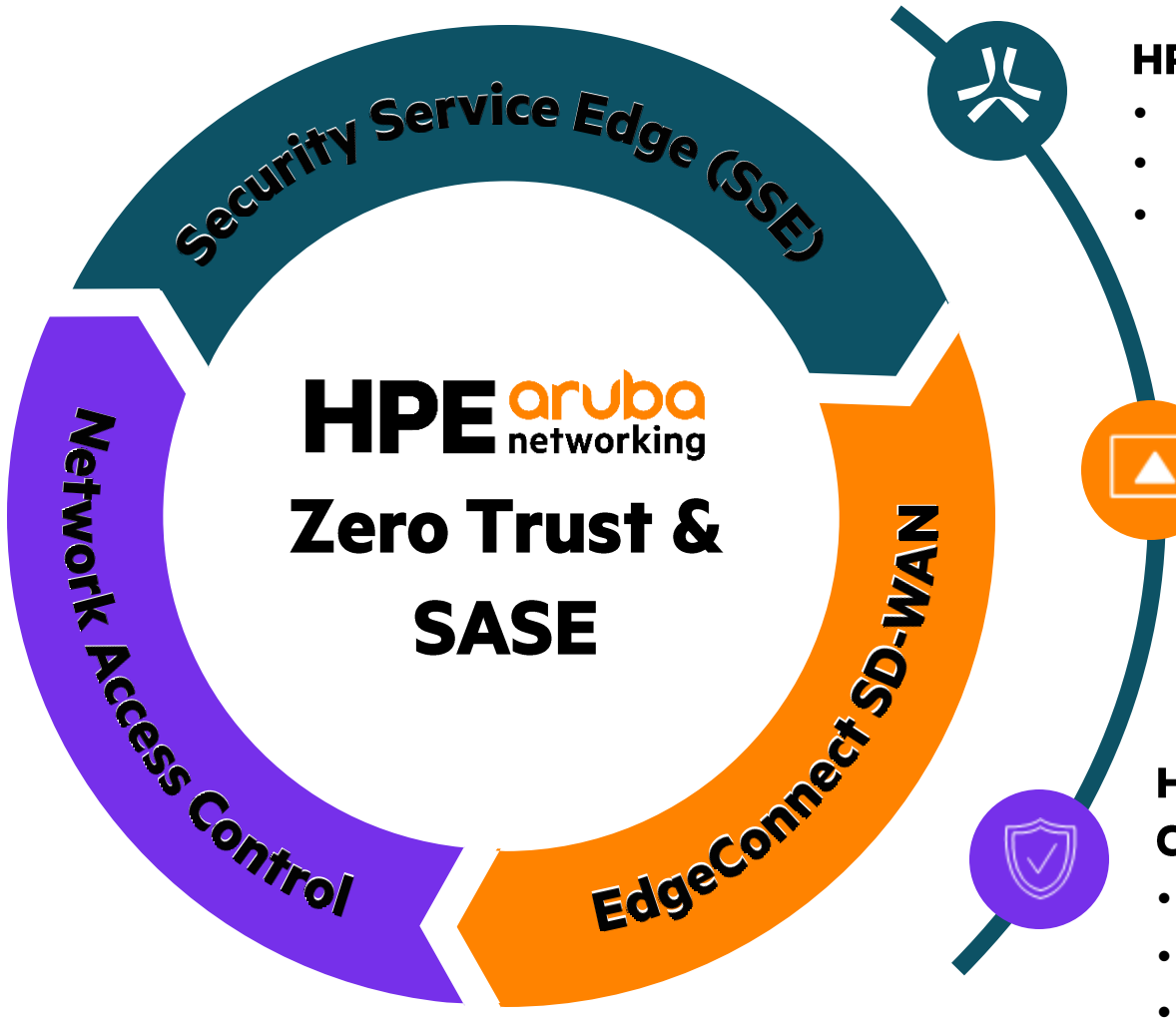
“By 2027, 65% of new software-defined wide-area network (SD-WAN) purchases will be part of a single-vendor SASE offering, an increase from 20% in 2024.”

Gartner®

Magic Quadrant for Single-vendor SASE, July 2024

HPE Aruba Networking Approach to Zero Trust and SASE

Apply zero trust security controls to protect users and applications, no matter where they connect



HPE Aruba Networking SSE

- Agent/Agentless ZTNA
- Unified policy management
- Global PoPs

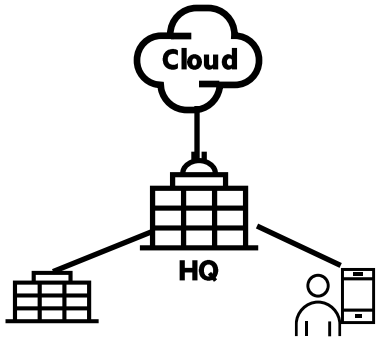
EdgeConnect SD-WAN

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

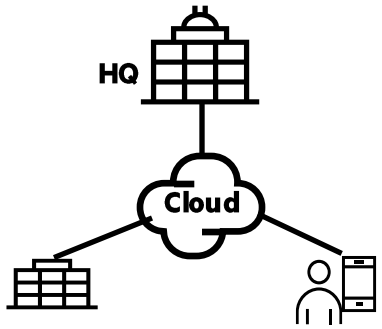
HPE Aruba Networking Central NetConductor & ClearPass Network Access Control

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

Why legacy networks fail to support zero trust



Corporate data center as the central hub

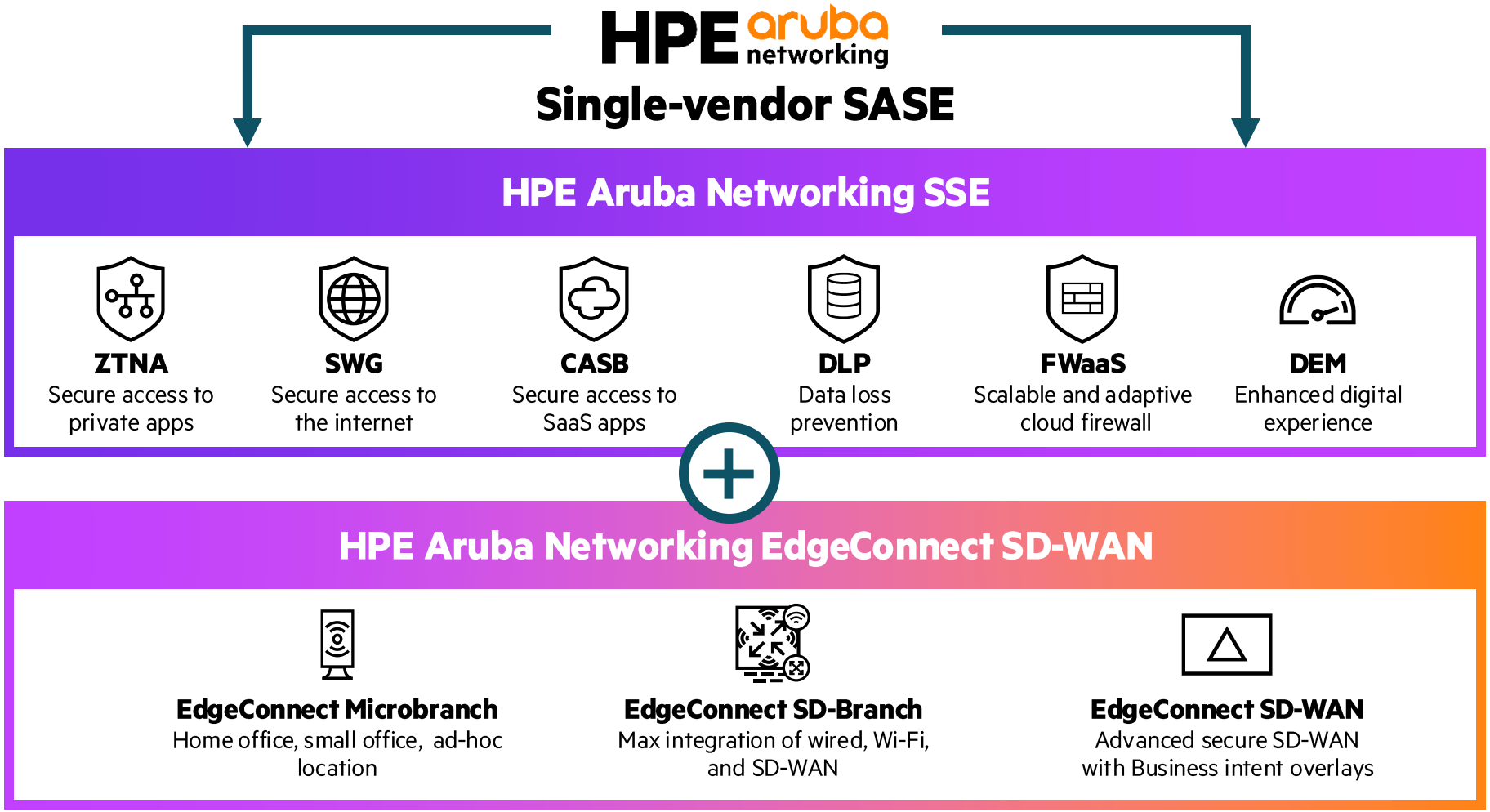


Users and devices connect from anywhere to the cloud

Legacy architecture	Cloud-centric, zero trust architecture
Implicit trust within the network	Continuous authentication and verification
Broad access to all resources	Granular, identity-based control
Flat, segmented architecture	Micro-segmentation to limit movement
Firewall-based perimeter defense	Cloud-first security enforcing least-privilege

HPE Aruba Networking SASE

Deliver zero trust with EdgeConnect SD-WAN and HPE Aruba Networking SSE



Transforming secure business access with HPE Aruba Networking SSE

Zero Trust Network Access (ZTNA)

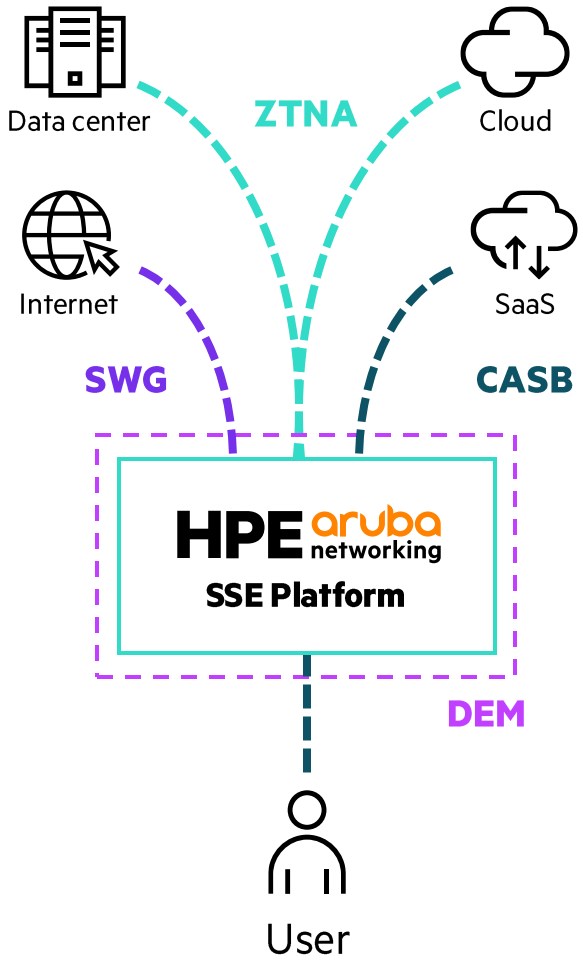
Secure access to private applications in the data center or cloud enforcing zero trust principles.

Secure third-party access, VPN/VDI replacement, Accelerated M&A

Secure Web Gateway (SWG)

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

URL filtering gambling/malware sites, DNS control, SSL inspection for malware



Cloud Access Security Broker (CASB)

Secure access to SaaS applications and protect against data loss.

Control block upload/download from Box, Sharepoint, Facebook, Salesforce

Digital Experience Monitoring (DEM)

Monitor digital experience and troubleshoot user access issues for all traffic.

Network ops for private & public traffic

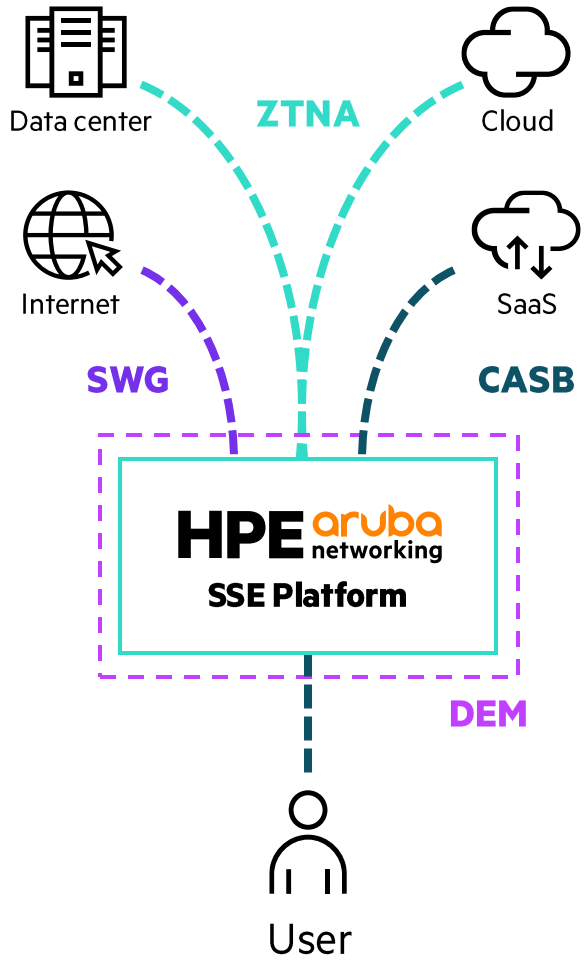
What's so different about HPE Aruba Networking SSE

Focus is on unify – one UI, one policy, one platform (ZTNA, SWG, CASB, FWaaS, DEM)

Goal is to **simplify policy & inspect any traffic** for Internet, SaaS, and legacy apps (SSH, RDP, VOIP, AS400, ICMP etc.)

Ability to **harmonize access across the world** via smart routing and a cloud-backbone on AWS, Azure, Google, and Oracle

Purposely designed to enable users to access resources **with or without an agent**



HPE Aruba Networking ZTNA

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

VPN replacement

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

Single pane of glass

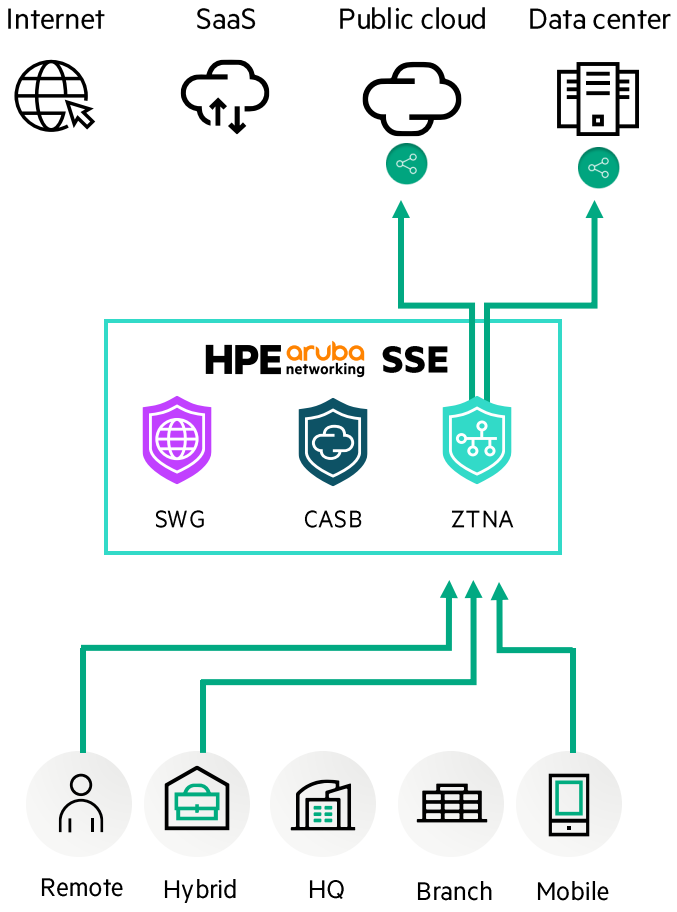
- Configure granular policies for all private applications in a centralized policy engine

Agent and agentless

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

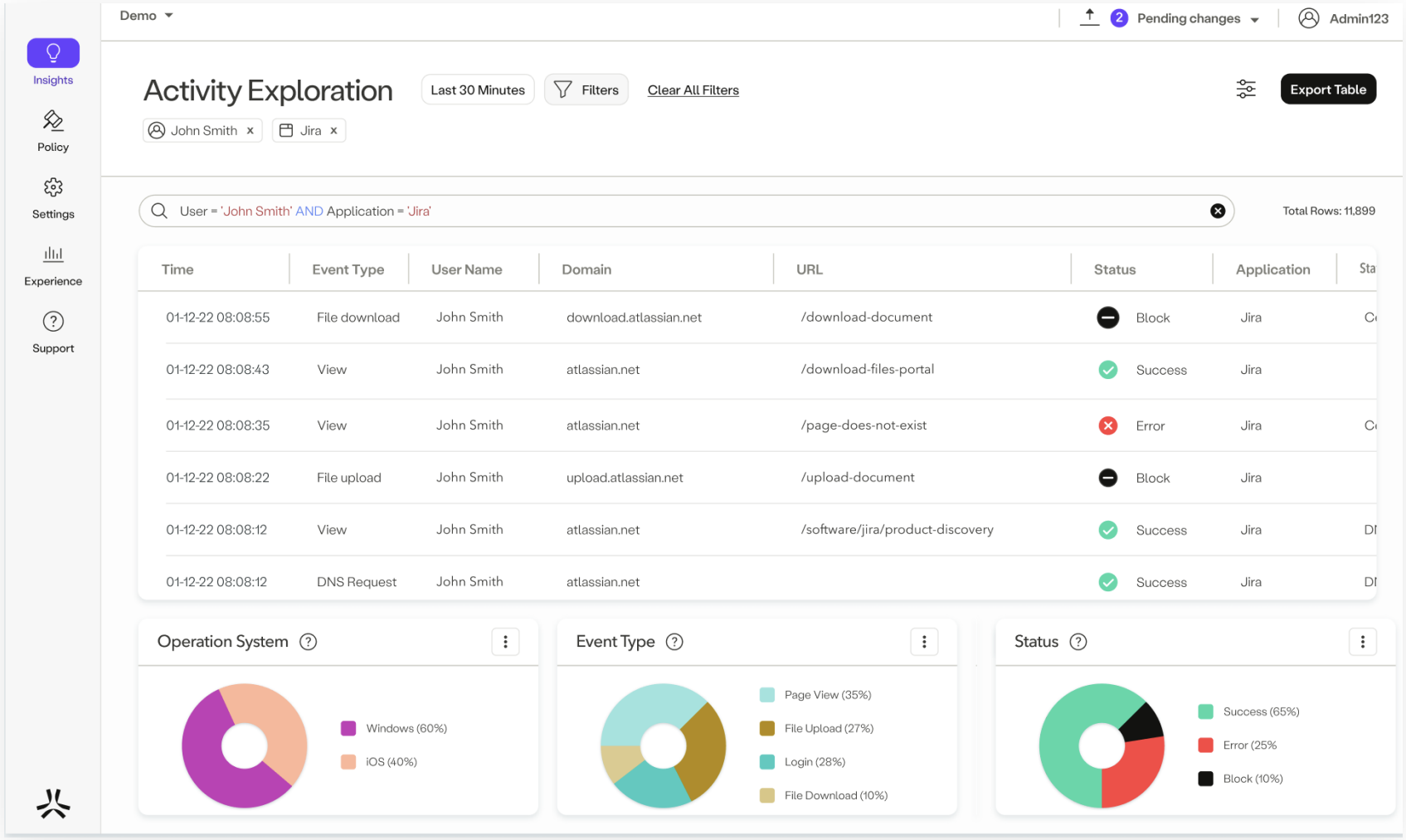
Least privilege access

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



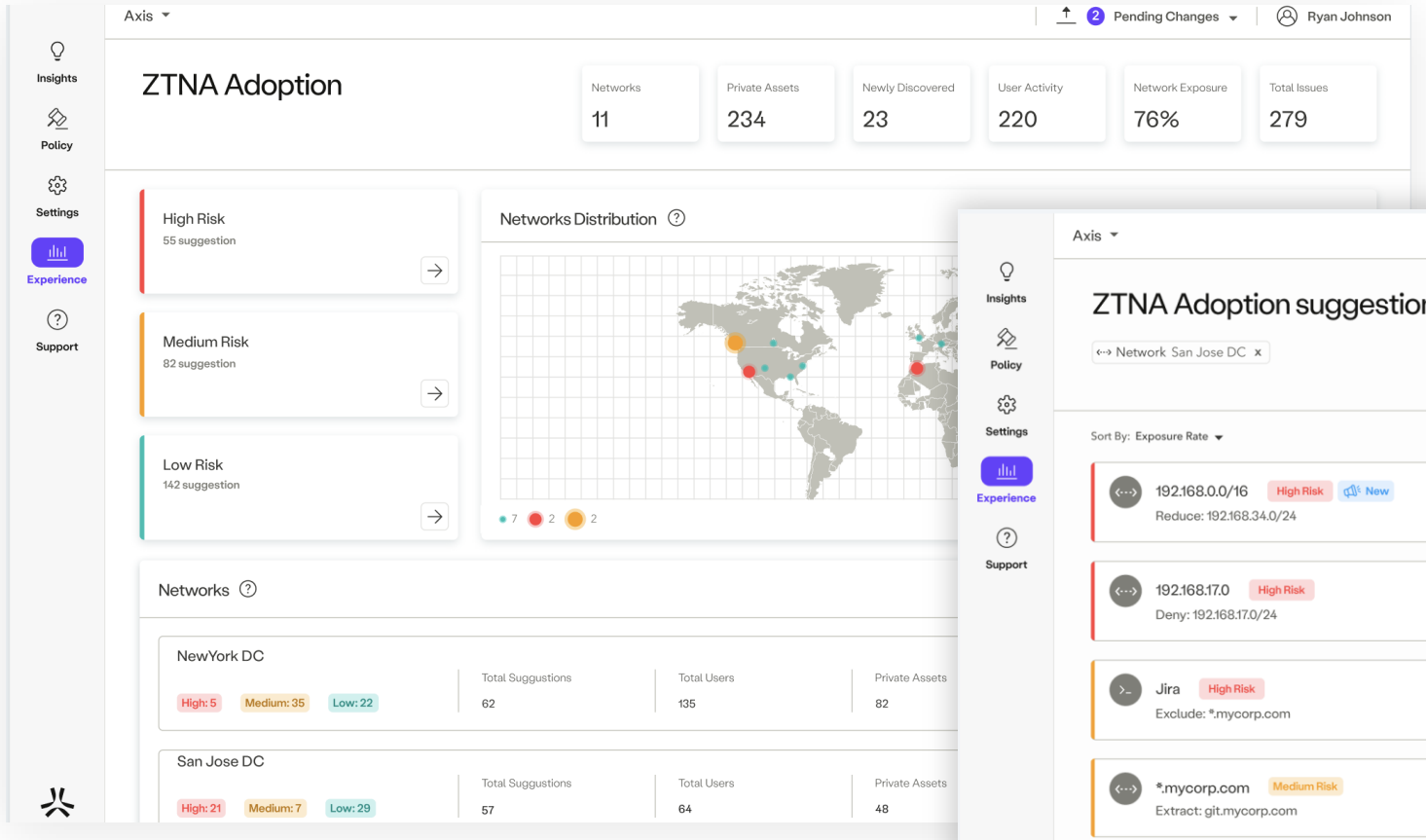
Advanced SSE dashboards: Get a comprehensive view of user activity

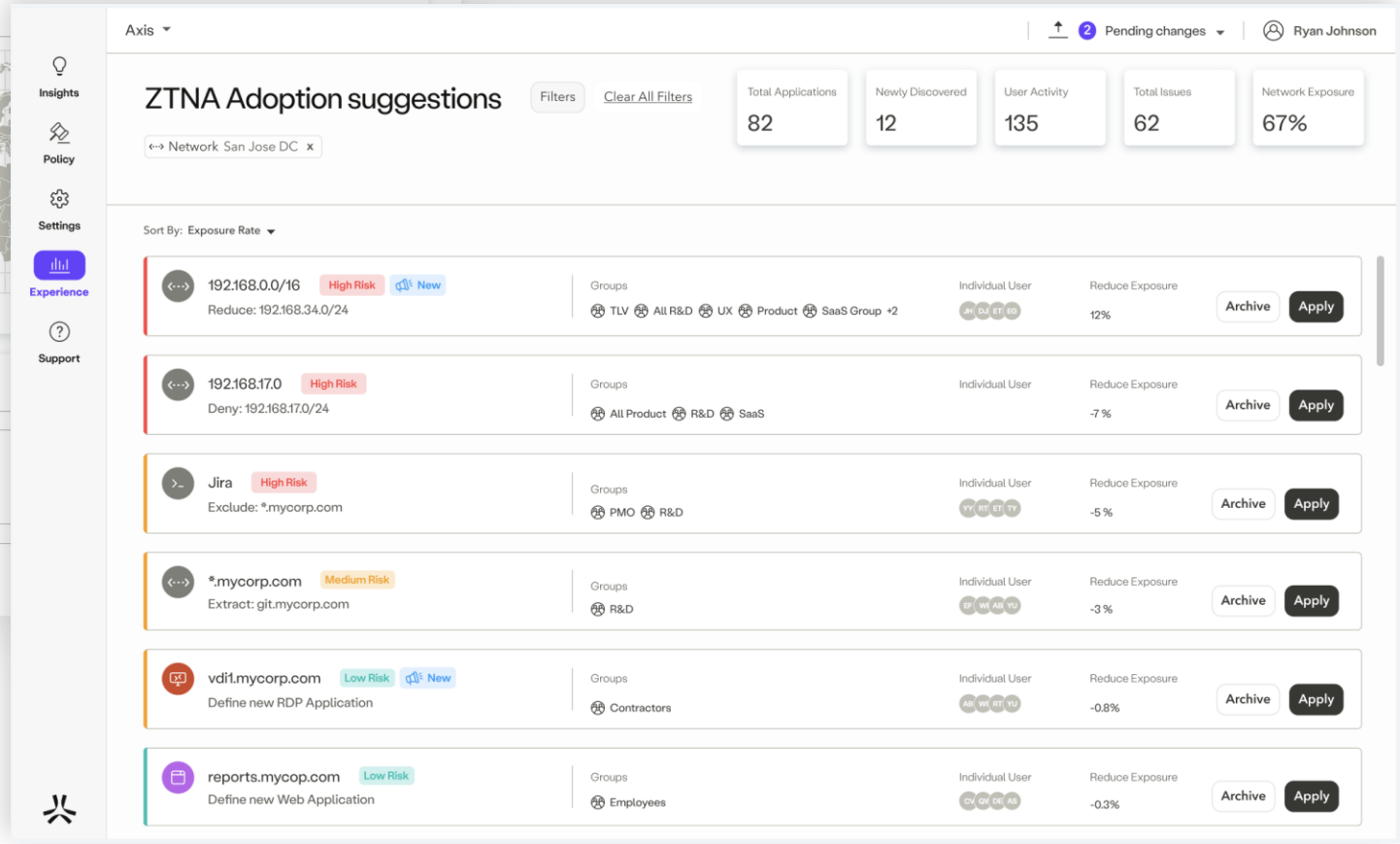
View activities such as uploads/downloads, logins and view activity status



Advanced SSE dashboards: Get recommendation for ZTNA adoption

Analyze exposure risks and provide recommendation for ZTNA



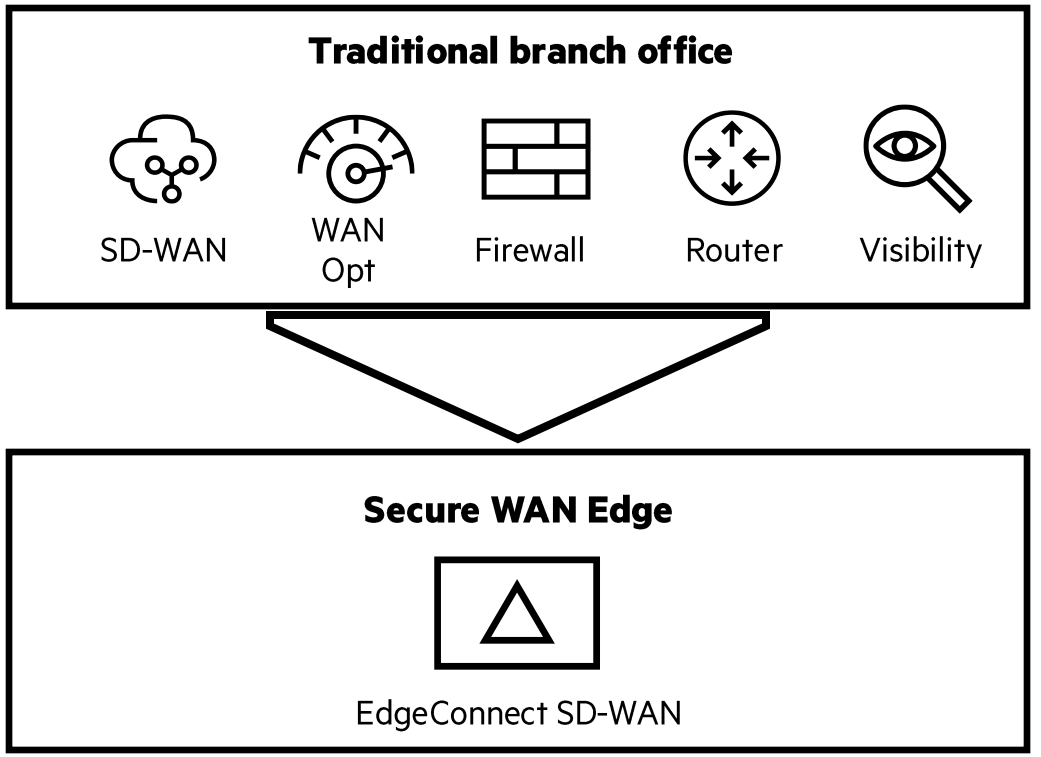


HPE Aruba Networking EdgeConnect SD-WAN

EdgeConnect Secure SD-WAN Platform

Improve app performance, streamline management, reduce hardware footprint

- Built-in next-generation firewall including IDS/IPS, adaptive DDoS and role-based segmentation
- Multi-cloud networking
- Dynamic routing with BGP and OSPF support
- App performance with SaaS and WAN Optimization & Path Conditioning
- Network visibility and reporting
- Automation and zero-touch provisioning



EdgeConnect SD-WAN Key Use Cases

Complement SSE with an advanced secure SD-WAN

Improve app performance over broadband

- 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

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

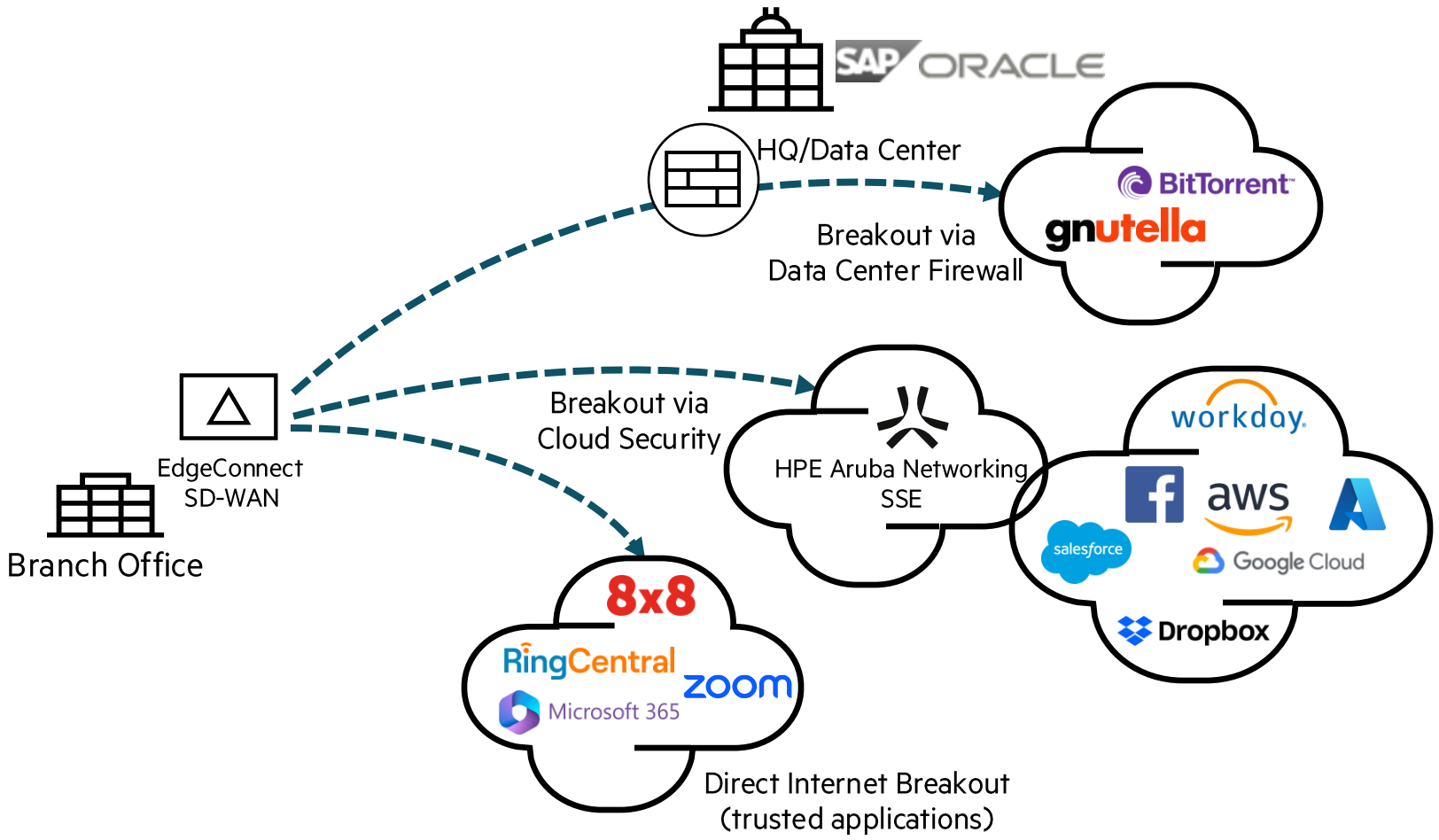
- Consolidate branch network and security functions
- Built-in next-generation firewall with IDS/IPS, Adaptive DDoS protection and role-based segmentation
- Protect data in transit with IPsec tunnels
- Full support for OSPF and BGP

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 role
- Go beyond what is defined by SASE

Architecting a SASE solution

SD-WAN and cloud security for cloud-first enterprises



Steer apps intelligently

- Intelligent breakout of SaaS and trusted internet-bound traffic directly to the cloud

Improve SaaS performance

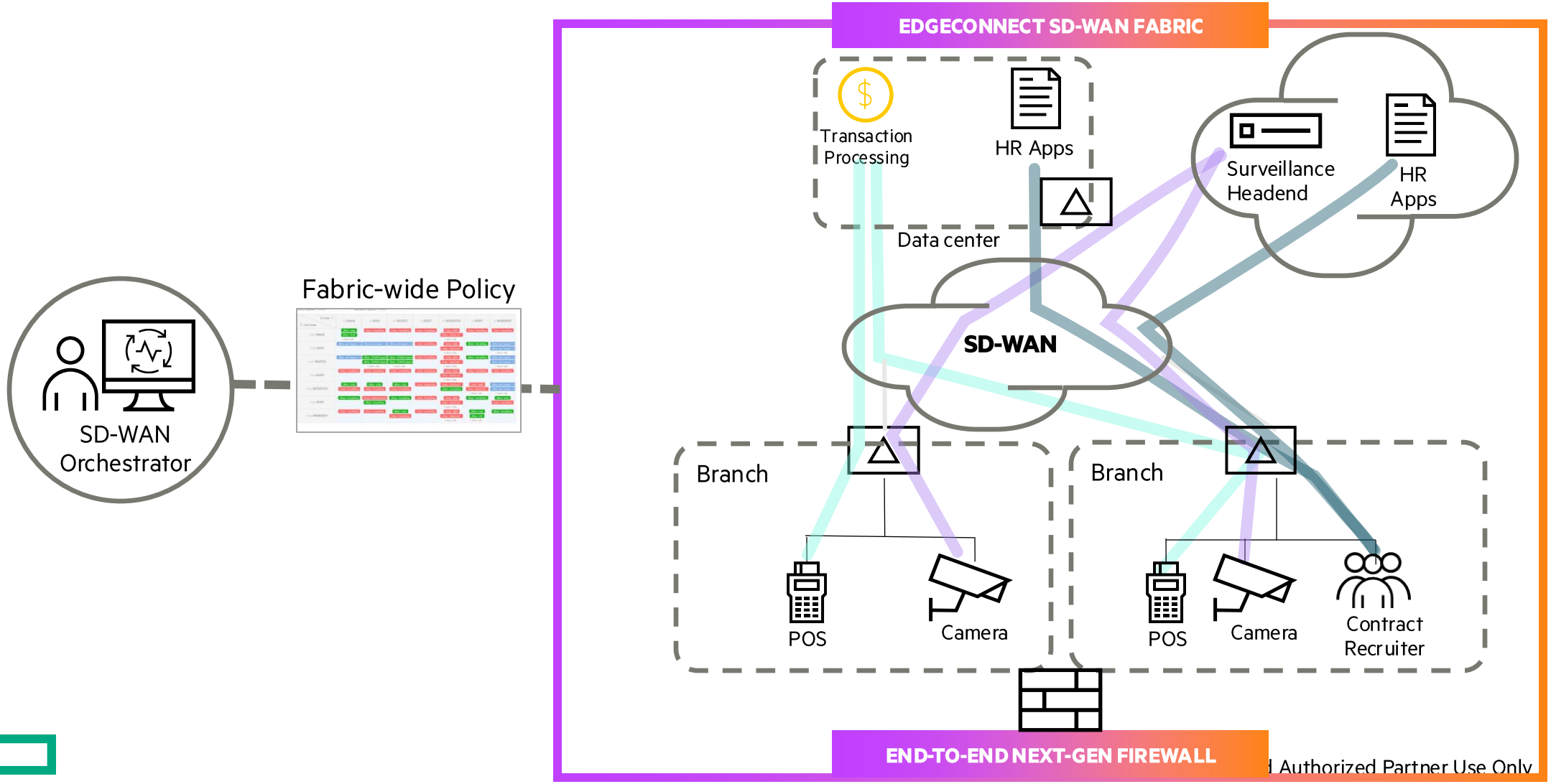
- Avoid backhauling traffic to the data center and improve SaaS application performance

Implement consistent security policies

- Eliminate application security and performance tradeoffs

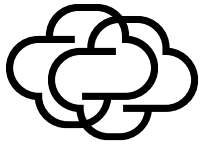
Secure IoT traffic using fine-grained segmentation with EdgeConnect SD-WAN

Seamlessly enforce security policy across the entire fabric creating a single logical firewall



A secure, business-driven SD-WAN edge platform

Delivering the transformational promise of the cloud with a business-first networking model



Multi-Cloud

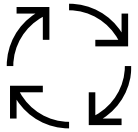
Deployment to any of the cloud providers (AWS, Azure) to enable end-to-end connectivity

Intelligent steering of cloud application traffic

Highest Quality of Experience

Prioritization of mission critical application traffic using Business Intent Overlays

Traffic acceleration with path conditioning, SaaS and WAN optimization



Continuous Adaptation

Automation and centralized orchestration

Best path selection in real time

Business-driven SD-WAN Policies

Secure SD-WAN

Built-in next generation firewall

Role-based segmentation to secure users and IoT

Single-vendor SASE or tight integration with third party SSE vendors

Delivering Highest Quality of Experience and Security for Users and IT

Connect to HPE Aruba Networking partners for an easy integration into existing ecosystem

Secure with various options

Connect to various identity management and end-point security solutions. Benefit from HPE Aruba Networking 360 Security Exchange partners.

SSE with anyone

Open SSE ecosystem allows for full integration with HPE Aruba Networking SSE or through any of our technology partners.

Expand in the cloud

Comprehensive cloud provider integration enabling direct connectivity options wherever applications are.