Hewlett Packard Enterprise

HPE aruba networking

Transforming Security: The Power of SSE for Zero Trust Access

John Spiegel
Field CTO

Jaye Tillson
Field CTO

The enterprise is undergoing the most significant transformation in history.

Adopting cloud services means you need a **new approach to network security** to keep access safe and fast.

The proliferation of IoT devices is driving digital transformation but creates new challenges for IT teams managing the enterprise network.

Hybrid and Remote Work has revolutionized the need for new connectivity solutions.

Access to your **apps and private data must be secure and available** from anywhere.

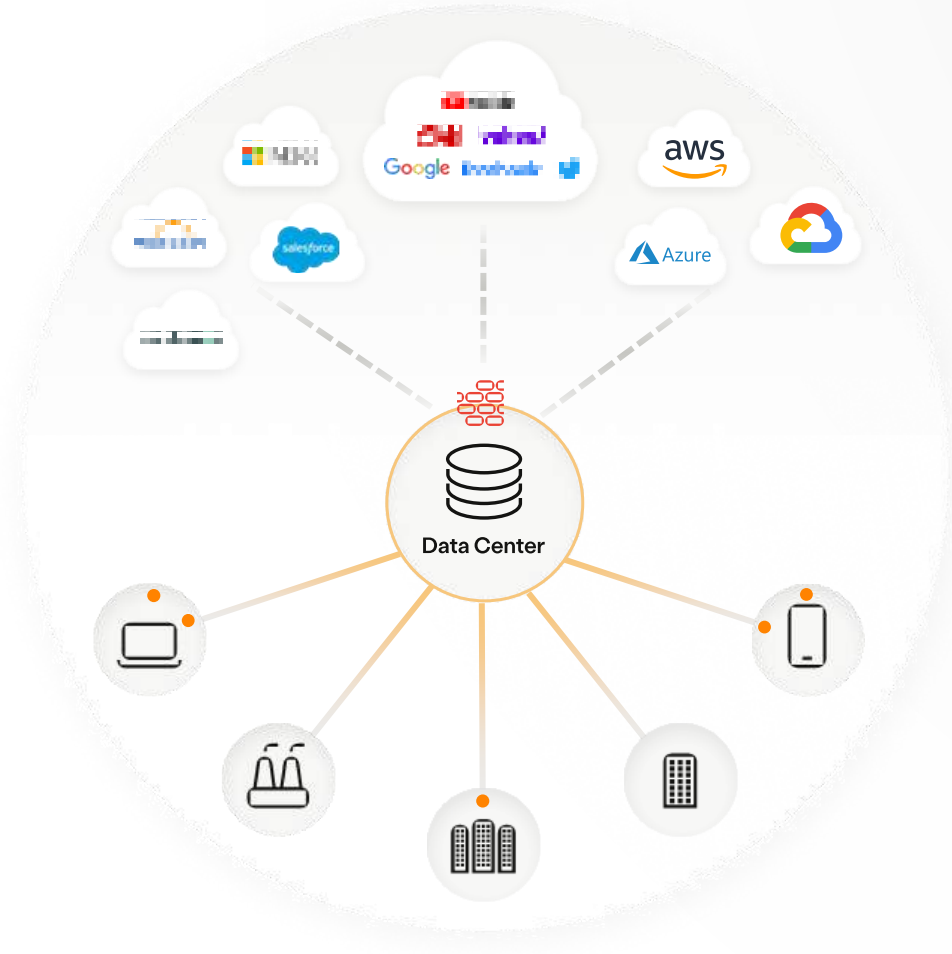
Security is a priority, yet also a challenge

Digital transformation breaks with an old-world approach
Hub & Spoke

Adopting SaaS
Guaranteed level of service, scale and accessibility,
cost effective, simple integration – making SaaS security critical

Adopting Public Cloud
Reduces CapEx, rapid app deployment, high performance and availability – making securing across hybrid cloud key

Adopting Mobility
Workforce can connect from anywhere - making user experience more important than ever



Traditional Security
Appliance-based products tethered to the data center, focused on protecting the network

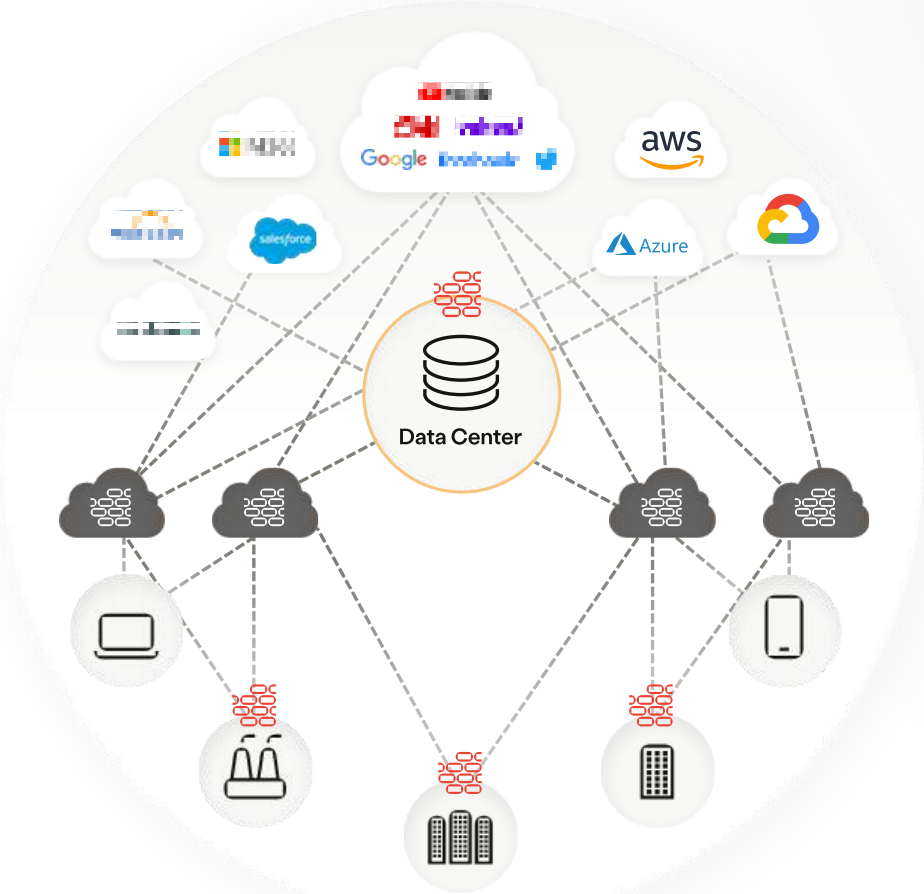
Traditional Network
Built for backhauling traffic to DC from branch and remote sites to network

New Threats
Increase in advanced threats exploiting legacy network security architectures

Virtualizing the same doesn’t work.. Just adds to the problem.

Virtualized Firewall

- **Complexity** of managing more FWs
- **Cost** increases with more appliances and HW needs
- Inherent **risk** due to traffic still being placed on network

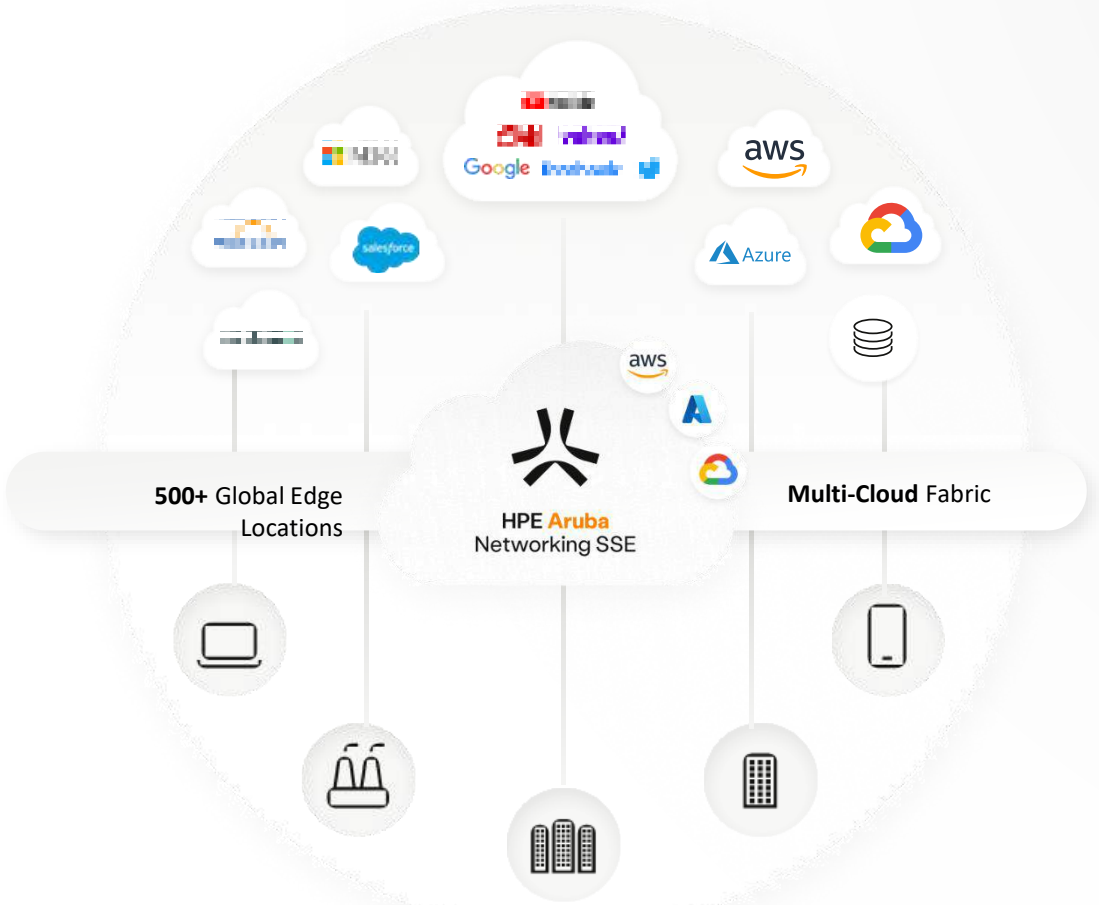


Virtualized FWs don’t solve the problem. Still a need for zero trust access – with a strong user experience

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

Benefits of SSE

Granular, zero trust access to business apps

(Private apps, SaaS apps, & Internet)

- Eliminate attack surface & exposure
- Enforce Least-privilege access
- Protect against Ransomware
- Prevent data loss

Keep end users connected from anywhere. Streamline IT admin workflows.

- End-users receive seamless access to apps and data every time they access a resource due to intelligent smart-routing across 500+ edge locations.
- IT admins can leverage APIs, and AI/ML capabilities to easily set granular policies, and gain visibility into actionable intelligence

Cloud service offloads infrastructure management to the cloud, ensures scale, and makes spend predictable

- Minimize complexity by reducing point-product solutions
- Effortlessly scale with cloud-delivered platform.
- Save money by reducing reliance on appliance-based security solutions

Customers who are already benefiting from SSE

DELTA DENTAL®

Reduced attack surface and risk by eliminating the corporate VPN

UKG

Secured access to 16,000 employees in less than 2 weeks

** HPE Aruba Networking unified SASE customer*

Visionworks

Modernize infrastructure and cut costs by 70%

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

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

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

Digital Experience Monitoring

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

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

HPE Aruba Networking SSE in action.

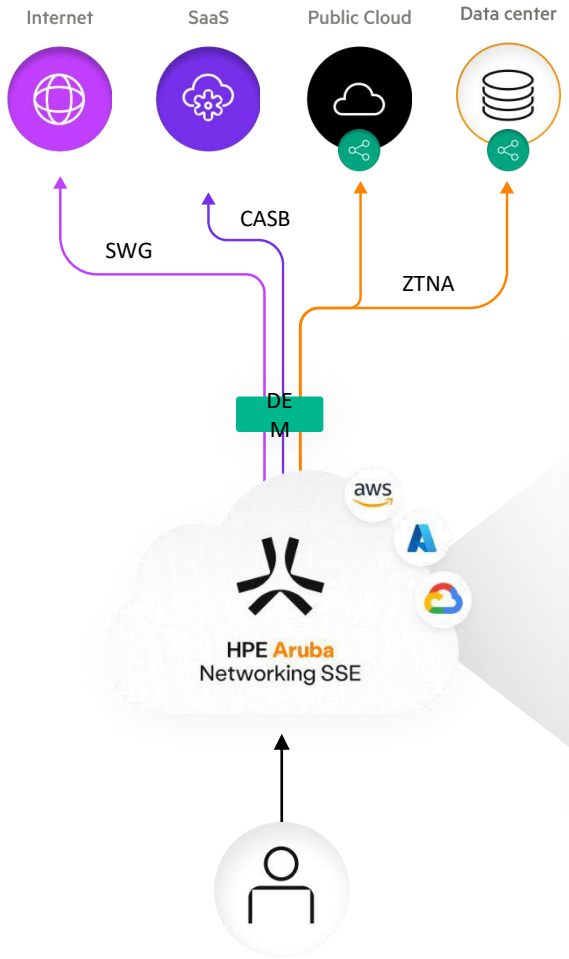
1 **User requests access**
(agent or agentless)

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



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

SSE is part of a broader zero trust ecosystem

POLICY

IDENTITY

ENDPOINT

SIEM

SD-WAN

Pro Tips
What to look for when considering SSE

1. A focus on a unified access platform approach

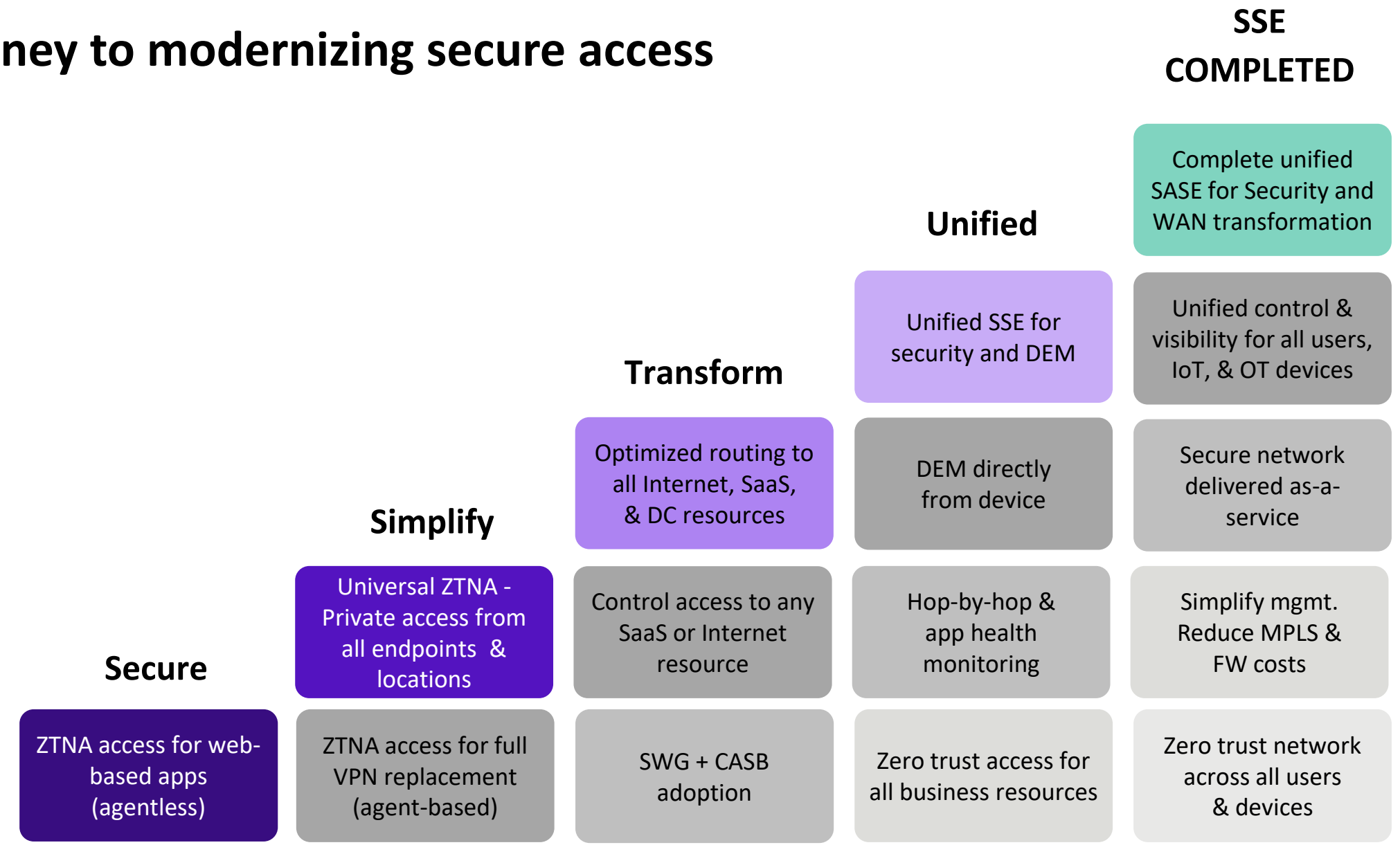
2. Simplified policy & inspect traffic for Internet, SaaS, and legacy apps (SSH, RDP, VOIP, AS400, ICMP, VNC etc.)

3. Harmonizes access across the globe via a cloud-backbone (AWS, Azure, and Google) and local edge capability

4. AI powered detection (anti-phishing engines) and ML-based incident response (deep-level analysis) for sandboxing

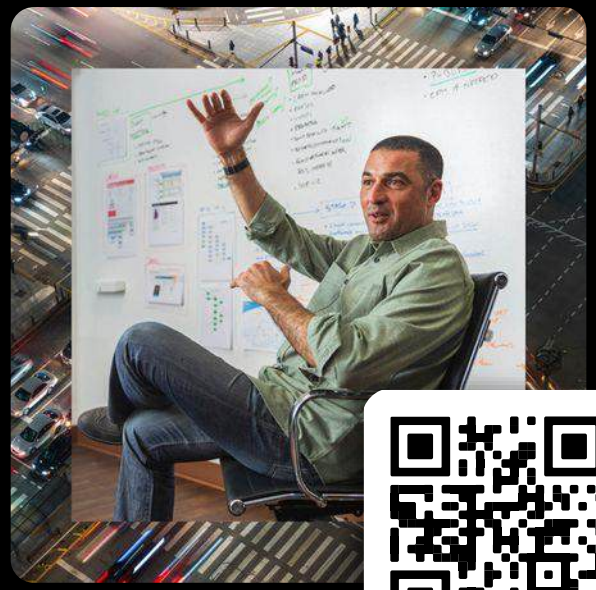
Hewlett Packard Enterprise | HPE aruba networking

The journey to modernizing secure access



Hewlett Packard Enterprise | HPE aruba networking

What now, what next



Speak to an expert

Read the full report

Thank You