Hewlett Packard Enterprise

CONNECT & PROTECT
Cloud-Based Zero Trust Network Access

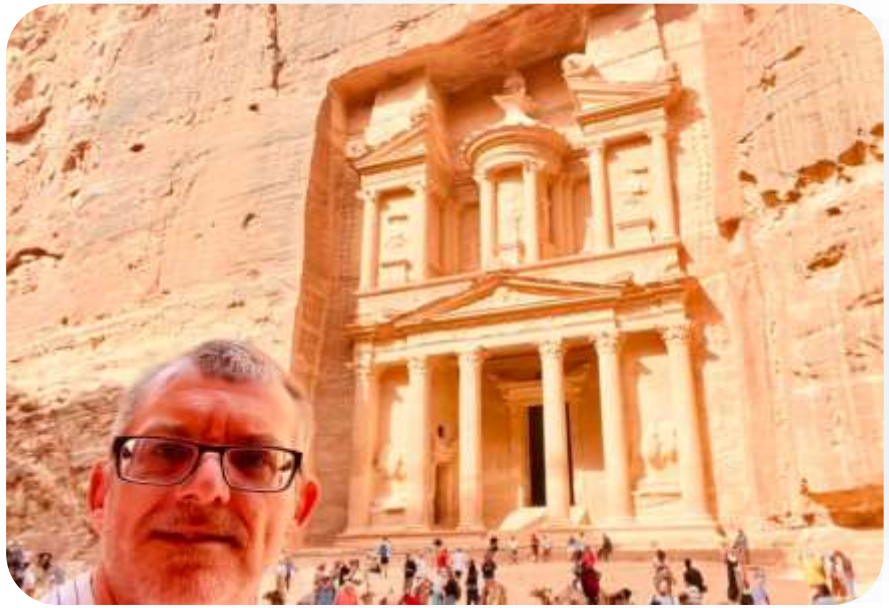
Jaye Tillson, Director of Strategy

October 2023

Hewlett Packard
Enterprise

Jaye Tillson

Director of Strategy / Field CTO
Co-host of the SSE Forum & The Edge Podcast



The workforce of today












Bad actors are targeting our points of weakness

92%

Companies that still use legacy VPN technologies

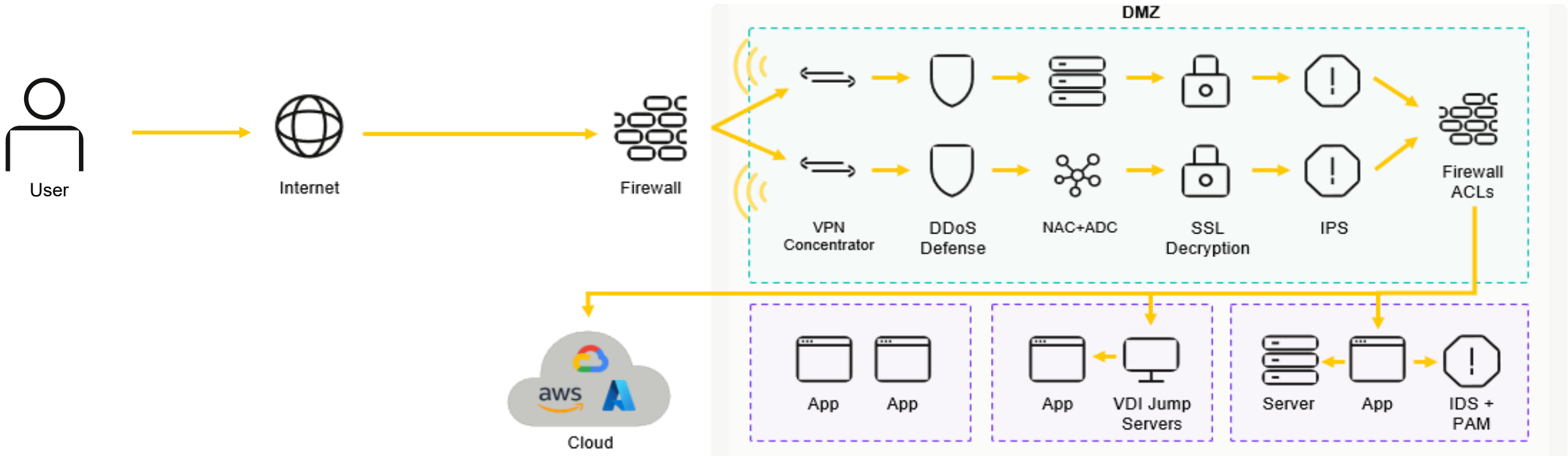
71%

Are concerned that VPN will jeopardize their environments

↑ **92%**

In targeted VPN attacks due to remote work

VPN architectures create poor user experience



Security Risks

VPNs expose IPs

VPNs are like beacons, looking to be found. Consequentially, IPs are exposed creating an attack surface to be exploited.

VPNs over-extend network access

Unknown users from unknown devices are extended network access, increasing attack surface.

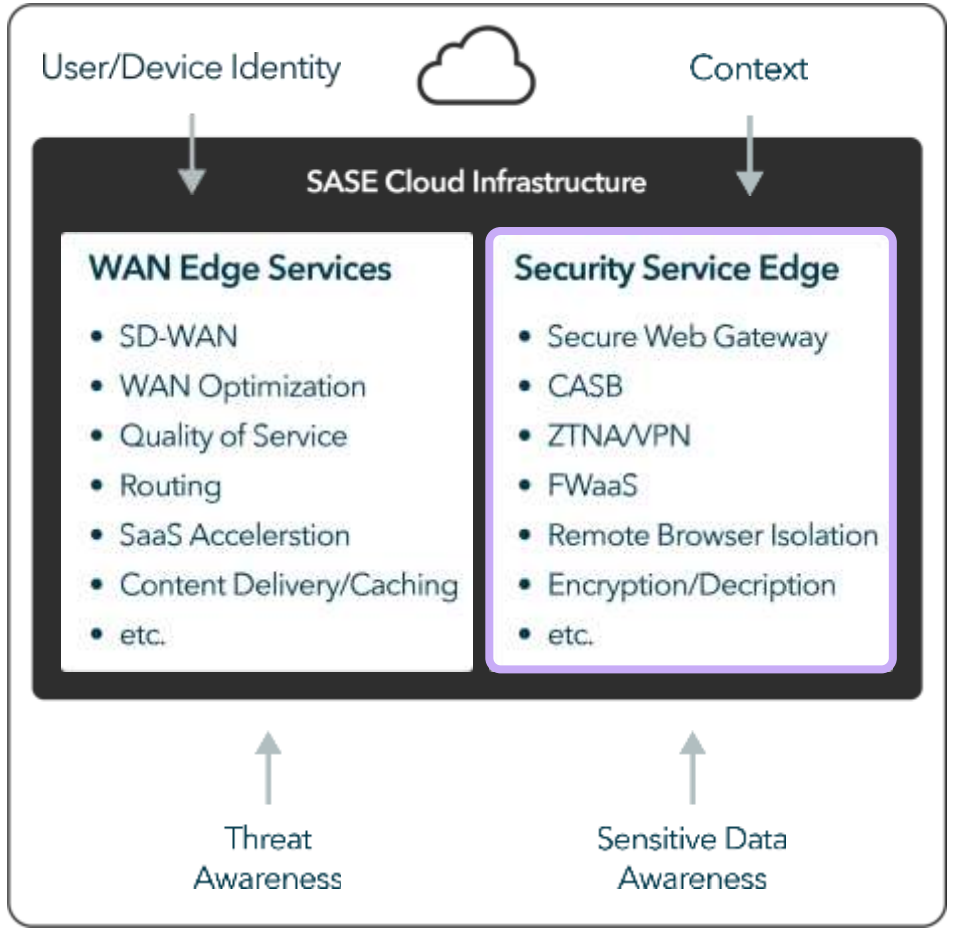
VPNs are complex to manage

Scaling physical VPN gateways adds network complexity and is costly.

Teams managing multiple configurations and policies across several UI's is time-consuming and error prone.

What are all these acronyms?

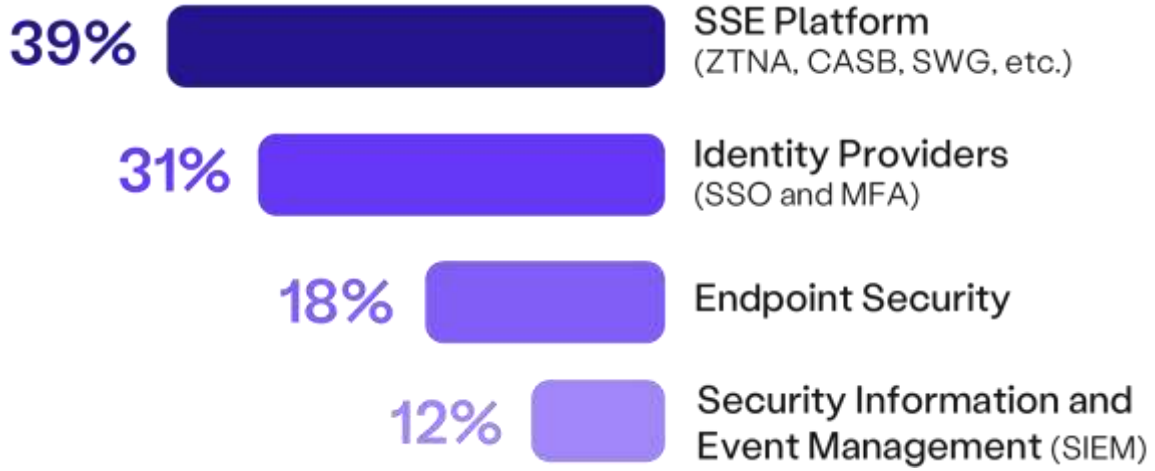
Gartner Consistent Network and Security Policy

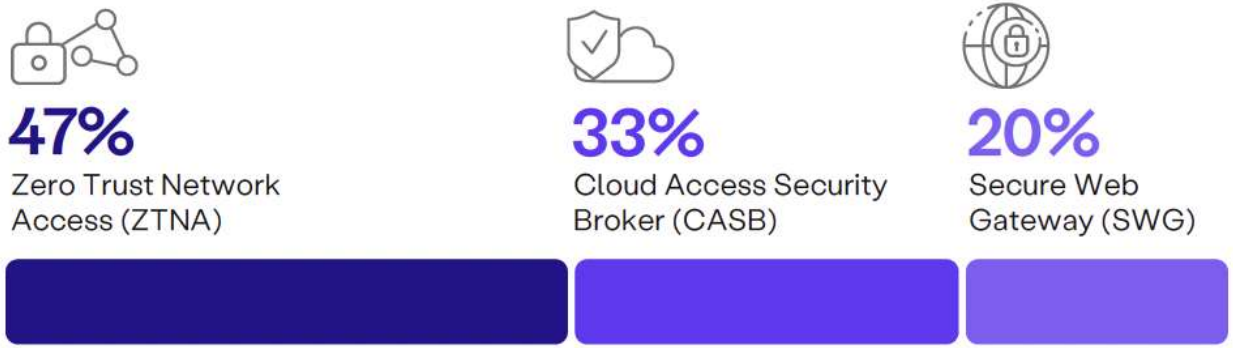


Why start with ZTNA?

67%
SSE Platform
ZTNA, CASB, SWG

33%
WAN Edge Services
WAN Optimization,
SD-WAN, SaaS Acceleration





Transforming secure business access

Zero Trust Network Access (ZTNA)

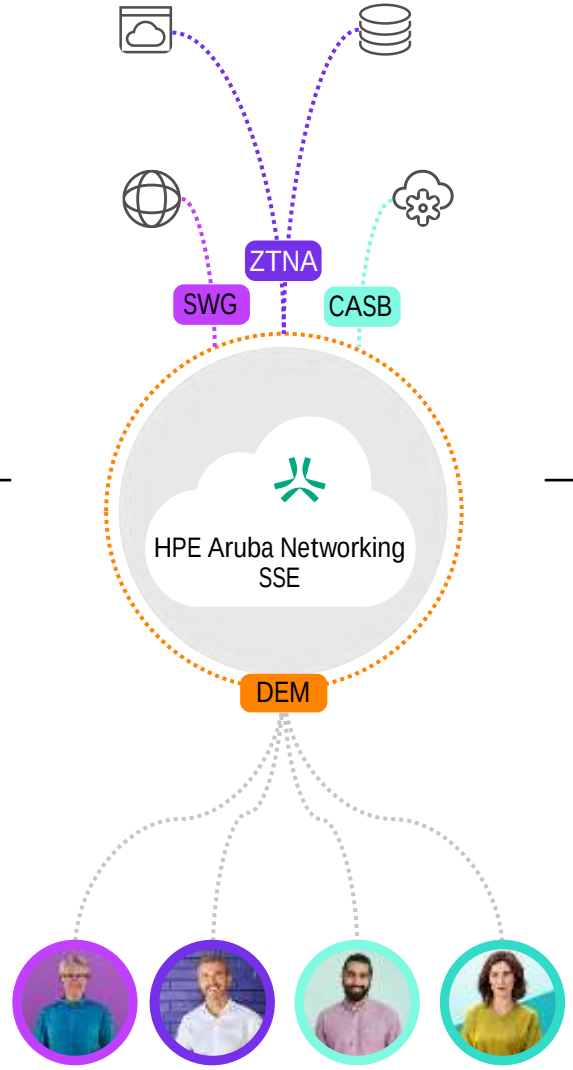
Secure access to private applications in the data center or cloud.

e.g., VPN/VDI replacement

Cloud Access Security Broker (CASB)

Secure access to SaaS applications and protect against data loss.

e.g., Block Upload/Download from Box, SharePoint, Facebook, Salesforce



Secure Web Gateway (SWG)

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

e.g., URL filtering, DNS Control, SSL inspection für Malware

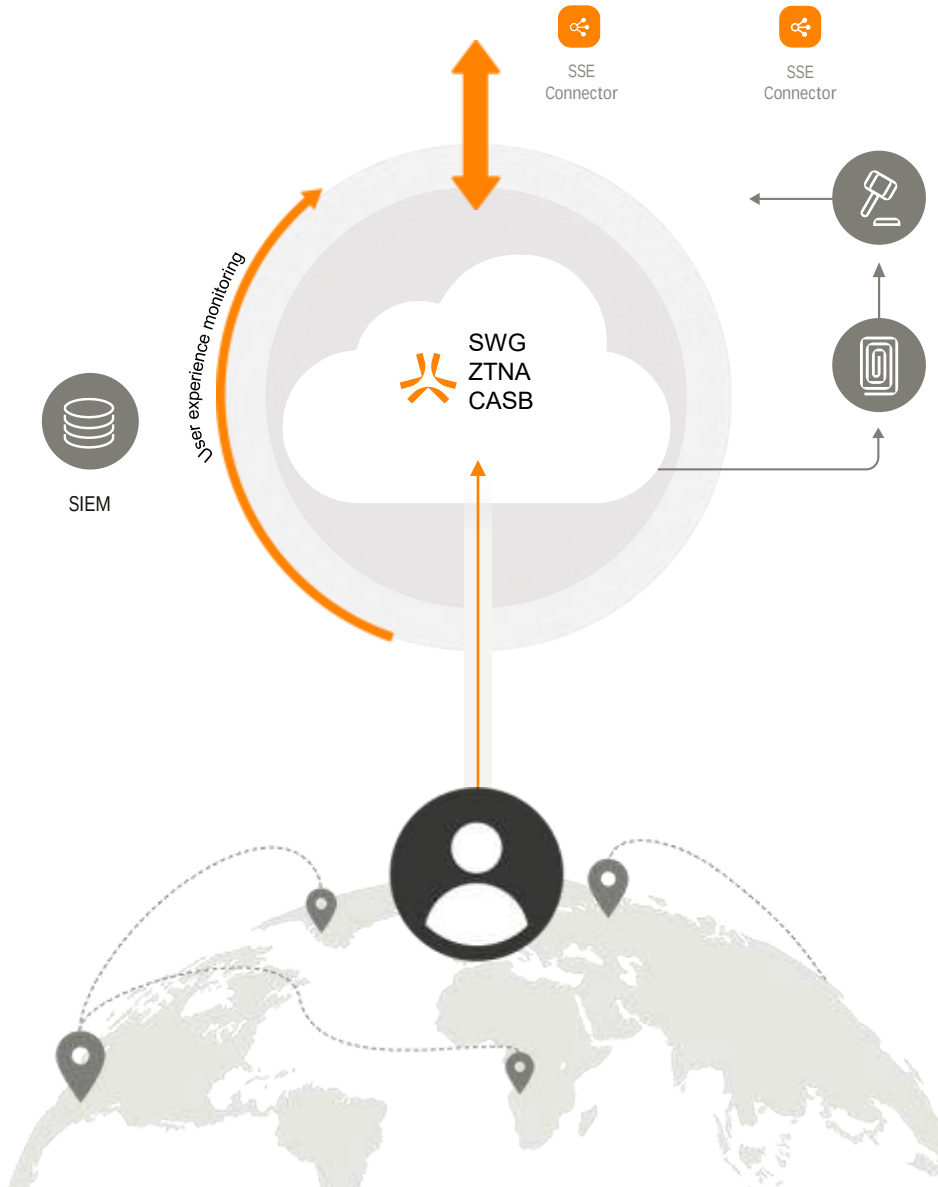
Digital Experience Monitoring (DEM)

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

e.g., Network Ops for private and public traffic

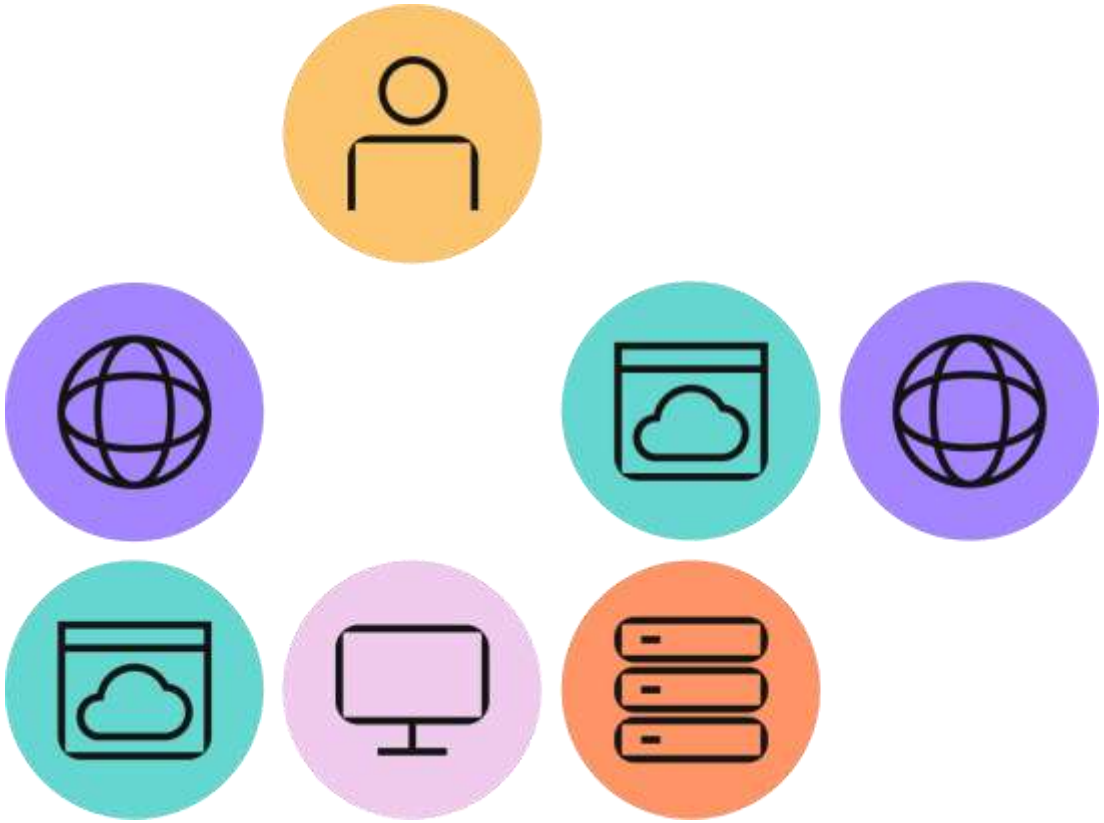
Enable Work from Anywhere

1. User requests access (agent or agentless)
2. Mediates request
3. Identity + MFA verified + Policy evaluated
4. Brokers 1:1 connection
5. Continuously inspects, adapts, and protects



Where do you go from here?

				SASE Complete	Complete unified SASE for security and WAN transformation
			Unified	Complete unified SSE for security and digital experience monitoring	Control and visibility for all user, IoT, and OT device traffic
		Transform	Optimized all routing to Internet, SaaS, and DC resources	Digital experience monitoring directly from device	Simplify Network Underlay
	Simplify	Secure private access from any endpoint	Control access to any SaaS or Internet resource	Hop-by-hop, and app health monitoring	Reduce/Eliminate MPLS
Secure	ZTNA partner access (agentless) for web-based apps	ZTNA for employees (agent) and replace legacy VPN	SWG + CASB adoption	Zero trust on-premises for all business resources w/ advanced security	Modernize & secure the branch network with SSE + ClearPass



Next steps?

Meet with a zero trust consultant.