HPE GreenLake

Overcoming roadblocks to delivering more secure, seamless connectivity

To stay competitive, businesses need to deepen digital acceleration, strengthen hybrid work environments, and evolve strategies to keep up with rapid Internet of Things (IoT) growth. An effective network approach can ensure these needs are met — delivering high performance and uninterrupted access to business-critical tools with the least possible security risk.

However, a recent survey from Hewlett Packard Enterprise of over 2000 IT leaders across 21 markets[1] reveals that the **network's full potential to drive these goals isn't being tapped into**.

Only

43%

of IT leaders say their company's network enables staff to securely work from anywhere[2]

Only

29%

can depend on their network to offer BYOD services[3]

Only

34%

agree that staff benefit from seamless connectivity[4]

A company's choice of devices, tools, and systems has a huge impact on an employee's experience, performance, and productivity. Unfortunately, many companies are still running traditional network setups that don't adequately support BYOD and hybrid work. Without providing the flexibility for employees to work how they like, these businesses will find it increasingly challenging to attract and retain talent.

[1], [2], [3], [4] "Sapio Research survey commissioned by HPE Aruba Networking," February 2023.

Navigating the hybrid access roadblock

Traditional network architectures worked well when business applications were hosted exclusively in the corporate data center. But today's landscape has changed, with most applications and services having migrated to the cloud. In this decentralized environment, the router-centric network presents a roadblock. Cloud-destined traffic must first be backhauled to the data center — slowing application performance and negatively impacting user experience and productivity.

There is a real need for a better way to send traffic directly over the internet from branch locations to trusted SaaS and cloud-based applications while maintaining compliance with enterprise security mandates.

That's where a Software-defined Wide Area Network (SD-WAN) architecture comes in. An SD-WAN provides intelligent application-aware routing across the WAN. The network automatically learns of any changes in conditions that might impact application performance — such as packet loss, latency, and jitter. It then automatically adapts to give every application the network and, crucially, security resources it needs, all in accordance with business needs. The result is the best end-user quality of experience for cloud-hosted applications.

At least it should be. It's important to remember that not all SD-WANs are created equal. Organizations should take care to seek out a business-driven SD-WAN versus just a basic SD-WAN.

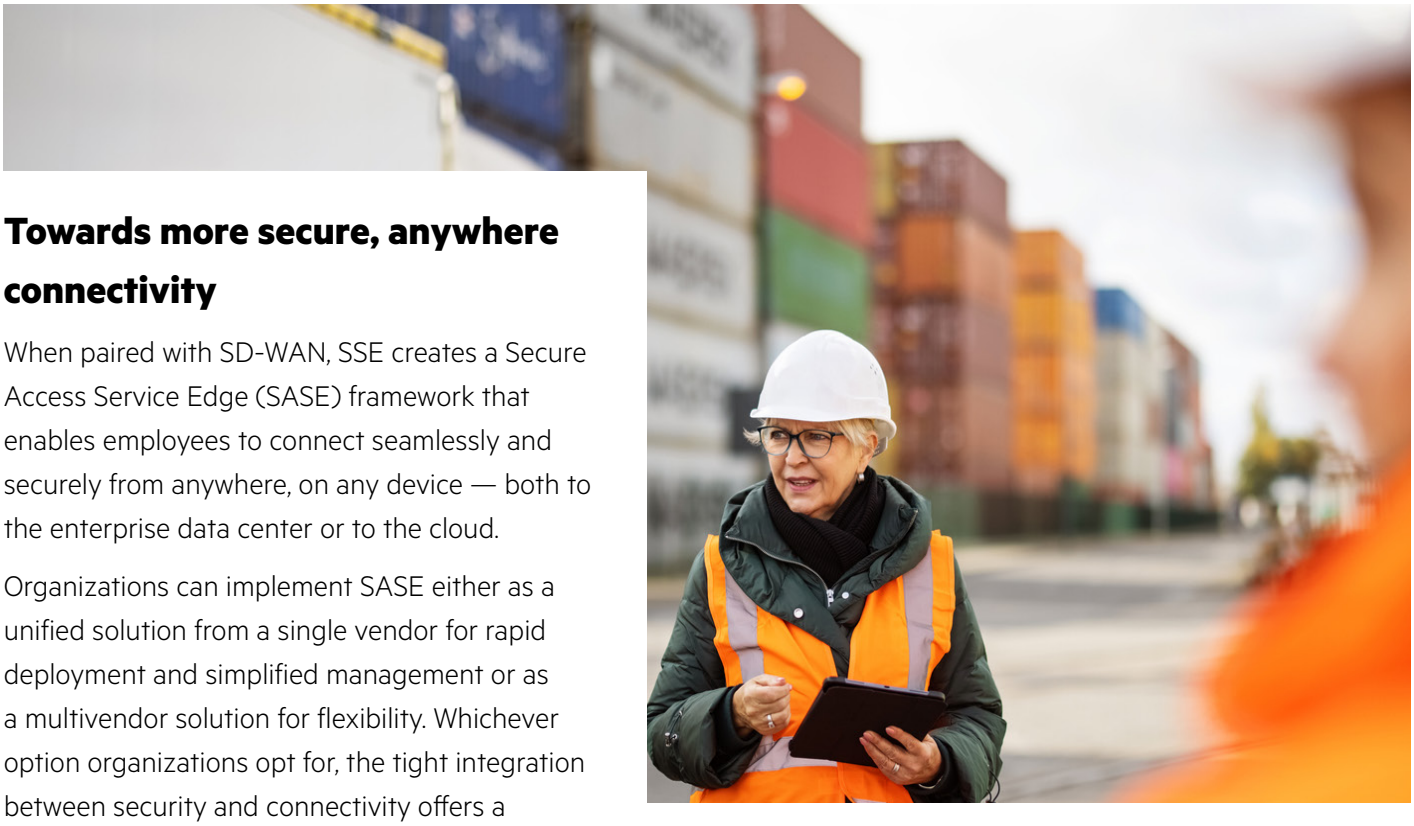
Traditional router-centric model	SD-WAN
Business conforms to constraints of the network	Network enables the business
Bottoms-up, device centric	Top-down: starts with business intent
Network creates a bottleneck	Network is a business accelerant
Manual, elongated delivery	Fully automated, continuous delivery
One size fits all	Gives every application what it needs
Unsustainable economics	10x bandwidth, same budget
Surprises, always behind	Delivers highest quality of experience

Basic SD-WAN	Business-first SD-WAN
Zero Touch Provisioning	Full orchestration and lifecycle automation
Automated templates	Continuous, self-learning, outcome oriented
Path selection	Consistent wow experience, even voice and video over broadband
Encrypted VPN overlay	Continuously enforces end-to-end segmentation
Fixed app definitions, ACLs	Identifies millions of applications on the fly, updated daily
Service-chained VNFs	Seamless, holistic implantation of multiple functions

Removing the roadblock to securely working from anywhere

Unless you can properly secure it, streamlining access to a hybrid, cloud-connected workforce can offer as much risk as reward. The traditional network security approach was laser-focused on protecting the perimeter. However, the perimeter is now a moving target as devices and staff access both on-premises and cloud resources from various locations.

Protecting this new environment calls for security to also move to the cloud. This is where Security Service Edge (SSE) solutions come into play. With SSE, organizations can apply consistent security from the cloud and secure access to applications spread across multiple clouds, data centers, and SaaS applications. SSE creates a more dynamic security perimeter by performing advanced security inspections closer to endpoints, including users and devices.



Towards more secure, anywhere connectivity

When paired with SD-WAN, SSE creates a Secure Access Service Edge (SASE) framework that enables employees to connect seamlessly and securely from anywhere, on any device — both to the enterprise data center or to the cloud.

Organizations can implement SASE either as a unified solution from a single vendor for rapid deployment and simplified management or as a multivendor solution for flexibility. Whichever option organizations opt for, the tight integration between security and connectivity offers a strategic network advantage, delivering a more consolidated connect and protect approach for modern businesses.

Learn more at
HPE.com/edge

Visit **HPE GreenLake**

Chat now

Hewlett Packard Enterprise

a00138260ENW