HPE

Can your network close critical security gaps without adding complexity?

VS

The need for ubiquitous connectivity, the accelerating pace of business, and relentless cyber threats have made it harder than ever for organizations to identify and close security gaps. It's time to start utilizing a new tool to protect users, devices, and applications: the network.

Networking and security have traditionally been perceived as having competing objectives, with increased connectivity often coming at the expense of exposing the organization to unnecessary risk. The reality is that connectivity and protection are not mutually exclusive; both must be satisfied to respond to evolving business needs.

Here's how your network can address the latest security trends, as outlined in research conducted by leading cybersecurity research firm Ponemon Institute and sponsored by HPE.

Expanding zero trust security initiatives

Many organizations have already adopted zero trust models to address rapidly evolving threat landscapes and expanding attack surfaces. Over two-thirds of organizations have adopted or plan to adopt zero trust security within the year.

How the network can help

By choosing a network with zero trust security controls built in, you can turn it from connectivity enabler to cybersecurity defender at every point of connection, consistently enforcing least-privilege access and continuous monitoring from edge to cloud.

Persistent IoT risks

While organizations recognize the critical need to identify and authenticate IoT devices accessing their network from a security perspective, few feel confident in their ability to do so, leaving them exposed to threats and data leakage.

How the network can help

Avoid IoT blind spots with the help of artificial intelligence (AI) and machine learning (ML) tools. Look for a network solution that uses AI and ML for deep visibility and accurate profiling of devices. Having AI-powered behavioral baselines at a per-device level can identify anomalous behavior from IoT devices to help you respond to early signs of potential threats.

Rising SASE adoption

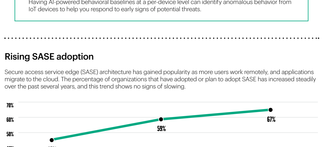
Secure access service edge (SASE) architecture has gained popularity as more users work remotely, and applications migrate to the cloud. The percentage of organizations that have adopted or plan to adopt SASE has increased steadily over the past several years, and this trend shows no signs of slowing.

How the network can help

If you are planning your own SASE adoption, be certain to include secure SD-WAN as a critical component of your strategy. This will enable your network to isolate IoT traffic from mission-critical applications.

Shared decision-making amount teams

Typically, organizations are split when it comes to making security architecture decisions, with either the network or security team taking the lead. But collaborative decision-making is gaining ground—with the two teams coming together to make joint decisions.

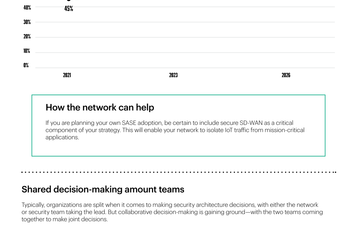


How the network can help

Choose a network that offers a common foundation for networking and security teams. Shared visibility, global policy, consistent enforcement, AI-powered network operations and threat defense can facilitate collaboration and help each team achieve their specific objectives and desired outcomes—without compromising performance or protection.

Prioritizing the use of AI for security

Organizations are increasingly using AI to close cybersecurity gaps. High-performing security organizations—those considered highly effective in keeping up with threats and closing security gaps—are adopting AI at a higher rate than other organizations.



How the network can help

Enlist AI for networking to improve both connectivity and security. Networking that delivers AI-powered profiling, security policies, and threat analysis can help your team protect data, infrastructure, and applications at scale.

About the data

The 2026 Global Study on Closing the IT Security Gap features insights from 2,120 IT and IT security practitioners around the world and examines the critical actions needed to close security gaps and protect valuable data within modern enterprises.

For more insights into how organizations are using AI, network access control, and zero trust network access to close cybersecurity gaps, download your complimentary report from the HPE website.[1]

Secure connectivity from edge to cloud

Enable exceptional experiences with secure, simplified access everywhere. Deliver protection without compromise from edge to cloud with HPE's unified, AI-native secure networking architecture. Unified SASE brings SD-WAN, SSE, and zero trust network access together in one cloud-delivered, AI-powered platform that authenticates, secures, and optimizes every connection. Combined with a hybrid mesh firewall, enterprises can enforce consistent zero trust security for any user, device, or resource, anywhere. AI-driven insights and automation detect threats, strengthen protection, and reduce operational effort—helping organizations move from reactive firefighting to proactive, intelligent security.

Learn more at

HPE.com/networking

[1] HPE.com/security

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development L.P. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00117464ENW

HEWLETT PACKARD ENTERPRISE

hpe.com