Article

WHEN THE NETWORK IS SECURITY

How unified architecture transforms protection and performance

As organizations expand across cloud, edge, and distributed environments, the relationship between networking and security has fundamentally shifted. Networks once had one defining role: connectivity enabler. Now, with users, apps, devices, and data everywhere, its mandate has expanded to include cybersecurity defender, as it offers the most scalable and consistent enforcement point for security. Standalone, bolted-on security tools are simply too slow, too fragmented, and too operationally complex.

But how easy is it to truly converge networks and security? What's required, and what stands in the way? We explore more in this Q&A.

1. What are the biggest challenges faced when trying to converge networks and security?

The biggest challenge isn't just technical. It's also cultural and operational. Networking and security teams have long worked independently, with different tools, workflows, and priorities. Bringing them together requires rethinking how teams collaborate and how the organization governs visibility, policy, and risk.

On the technical side, fragmented infrastructures make it hard to maintain consistent security and user experience as traffic moves across cloud, edge, and on-prem environments. Visibility becomes uneven, policies drift, and teams struggle to keep pace as applications, users, and AI-driven workloads become more distributed.

That's why the industry is shifting toward architectures where **networking and security are unified from the start**—automated, adaptive, and inseparable from one another.

"You can't really think about building a network today without thinking about security," says David Hughes, senior vice president of SASE and security at HPE. "There's a big overlap. What we really need to do is help the two teams work together to deliver great experiences and great protection, by architecting that security into the network from the beginning."

Ultimately, convergence isn't about stitching systems together. It's about creating a single operational model where teams share the same context and the network itself becomes an active security enforcer. Organizations that embrace this approach gain a more resilient, scalable foundation for the next wave of cloud and AI demands.

A lack of collaboration impacts resilience

Collaboration between the network and security teams has declined from 47% in 2024 to 36% in 2026,[1] affecting their ability to effectively close the IT security gap.

2. What are the operational gains of using a single unified model rather than separate tools?

With a single architecture, the silos that force teams to stitch together policies, tools, and identity controls disappear. Disconnected systems inevitably create gaps, slowdowns, and inconsistent enforcement, especially as users and workloads move fluidly across environments.

By contrast, when zero trust, segmentation, SD-WAN, and SSE draw from the same architectural foundation, security becomes intrinsic to the network rather than an add-on. Identity, posture, and policy are applied consistently at every point of connectivity, providing a unified view of risk and reducing the manual coordination that leads to policy drift and blind spots.

NetOps and SecOps can now operate from the same context, streamline workflows, and troubleshoot issues faster because visibility, automation, and enforcement all work in concert. The result is a simpler, more resilient environment that adapts quickly to change without compromising protection or performance.

[1] Ponemon Institute, "The 2026 Global Study on Closing the IT Security Gap," February 2026. hpe.com/security

3. When starting a networking-security convergence journey, what does a realistic transformation look like, from initial quick wins to full maturity?

"There is no right or wrong way for an organization to start or advance a unified connectivity and security journey," explains Eve-Marie Lanza, senior security solutions marketing manager at HPE. "The best first step is to understand the needs of the business and prioritize projects according to a balance of risk and opportunity."

Many times, initial needs focus on reducing costs, improving application experience, or strengthening security posture. Over time, new priorities naturally surface, so it's important to adopt approaches and architectures that remain flexible. Organizations that avoid locking themselves into fixed or brittle paths are better positioned to adapt their security and networking strategy as requirements shift.

Early wins can come from replacing complex VPNs with ZTNA to secure third-party access or accelerating how applications connect across sites and clouds. From there, organizations can work toward deeper convergence by bringing SD-WAN and SSE together into a unified SASE fabric, reducing reliance on point tools and creating a more cohesive operational model. Extending zero trust access everywhere through cloud-native NAC strengthens this foundation, facilitating consistent protection across users, devices, and environments. As automation and AI begin to augment these layers, teams can detect anomalies earlier, refine policies dynamically, and automate posture checks, which reduces risk while easing operational load.

In 2026, cost reduction, improved application performance, and improved security posture are the main drivers of SASE adoption.[2]

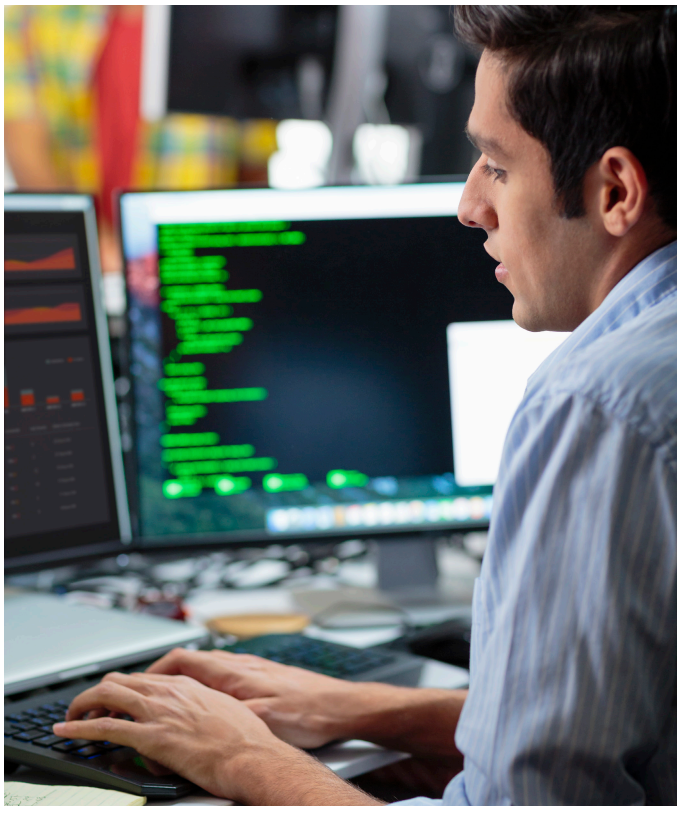
4. With increasing compliance, data control, and global scale requirements, what architectural considerations matter most when unifying networking and security?

Creating a unified model is important. Because hybrid environments evolve unevenly through new applications, cloud expansion, and expanding device footprints, the priority is maintaining consistent identity, access, and policy enforcement across environments that will never be fully uniform.

A unified model applies zero trust principles consistently, keeps policy logic synchronized as traffic moves, and provides continuous visibility into users, devices, and risk.

Tool and vendor sprawl ranks as the single largest barrier to advancing zero trust and SASE, ahead of budget and legacy technology.

78% of surveyed organizations manage secure-access policy across more than two separate systems. Only 17% operate from a unified platform.[3]



[2] Ponemon Institute, "The 2026 Global Study on Closing the IT Security Gap," February 2026. hpe.com/security

[3] Cybersecurity Insiders, "2026 Zero Trust Report. Bridging the Execution Gap—Unifying Security from Edge to Cloud", January 2026. hpe.com/unified-sase

5. In a market crowded with SD-WAN, SSE, and security vendors, what makes HPE's approach different?

Our mission is to make the journey to SASE and zero trust simpler. Instead of disconnected solutions, we offer a single, fully integrated platform that unifies a single-vendor SASE solution with advanced, AI-powered NAC capabilities. With this approach, organizations can enforce a universal zero trust network access model, where zero trust principles follow users, devices, and workloads wherever they operate.

Some other key advantages of our approach include:

- **Fully automated SD-WAN and SSE integration:** Our SASE solution automates the entire orchestration process end-to-end, streamlining operations, configuration and troubleshooting.
- **Cloud-first performance:** Intelligent traffic steering powered by first packet iQ optimizes cloud performance, with best-path selection and built-in acceleration for mission-critical applications.
- **Global scale:** A global cloud footprint with 500+ edge locations delivers low latency, smart PoP selection, and fast-failover worldwide.
- **Advanced security:** SSE services such as ZTNA, SWG, CASB run on a single policy engine, and branches are protected with built-in next-generation firewall.

6. How does HPE's proven security efficacy extend to protect against zero-day attacks?

Zero-day attacks demand protections that can spot emerging threats before signatures exist, which means organizations need an architecture that can detect unusual behavior, not just known indicators. HPE hybrid mesh firewall strengthens this posture by embedding AI-driven detection, behavioral analysis, and continuous global insight directly into how the network and security layers operate. Instead of relying solely on signature-based engines, the architecture looks for deviations in identity, device posture, and traffic patterns, giving teams early visibility into fast-moving or previously unseen threats across both managed and unmanaged environments.

Consistent enforcement across distributed environments is equally critical. By unifying identity, access, and policy under a common framework, protections can be applied consistently across cloud, branch, campus, and remote edges. This helps contain suspicious activity quickly, even as users, applications, and workloads move across environments.

The result is a more proactive and adaptive defense model; one that uses continuous intelligence, shared context, and automation to identify, isolate, and respond to emerging threats at speed. Instead of waiting for known bad indicators, organizations gain a security posture capable of keeping pace with modern adversaries across distributed environments.

A unified architecture for what comes next

As organizations modernize, the advantage will belong to those who treat networking and security as a single, integrated system rather than parallel disciplines. Unified zero trust, AI-native operations, and end-to-end SASE create a foundation that is simpler to run, stronger against evolving threats, and ready for the next wave of digital transformation. By embedding protection directly into the network and aligning policy, identity, and visibility across every edge, HPE helps customers build an architecture designed not just to keep up with change but to lead it. native operations, and end

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

a00156862ENW

HEWLETT PACKARD ENTERPRISE

hpe.com