



# TURN YOUR NETWORK INTO A SECURITY SOLUTION

Built-in protection for a connected,  
AI-driven world

Modern networks are no longer just conduits for data—they're critical infrastructure for business operations, AI workloads, and digital experiences. Which makes them very attractive targets for cybercriminals.

Organizations today face unrelenting security threats and challenges. With more entry points, users and devices, and data in motion than ever, attack surfaces continue to grow, while traditional security perimeters dissolve. IT leaders are expected to protect everything, everywhere, all the time—and all without frustrating users, diminishing productivity, or stalling innovation.

## Time to converge networks and security

It's a lot of pressure, but one the right network can ease. While perimeter-based solutions and bolted-on products like VPNs are no longer effective at keeping the network safe, a network with zero trust security built into its DNA can help keep your organization more secure while simplifying operations.

When connectivity and security converge, you can meet the objectives of both: delivering the high performance users expect, while also making the network a powerful and integral part of your security ecosystem.

### What's driving the changes in network security?

- **Expanding attack surface:** More devices, users, and data mean more opportunities for threats to enter.
- **Complex compliance demands:** Regulatory and data governance requirements are tougher to meet with legacy systems.
- **Fragmented tools:** Disconnected security solutions create gaps and add operational headaches.
- **Pressure to protect it all:** IT teams must safeguard all connections in every location without slowing business down.

## Your network, now a security solution

What does a network with integral security look like? It's about having a network that has:

**SASE readiness:** Combining SD-WAN, SSE, and zero trust into a unified service delivered at the edge, for more secure, scalable access to applications and data from anywhere.

**A foundation for universal zero trust network access (UZTNA):** An advanced framework that applies zero trust principles consistently for users and devices across all environments from edge to cloud.

**Hybrid mesh firewall:** As part of a distributed security architecture, mesh firewalls enforce identity-based, context-aware policies across hybrid and multi-cloud environments. They enable granular, zero trust protection by securing traffic between users, devices, and workloads—regardless of location, with performance that delivers on business needs while easing operational effort and reducing inconsistencies.

**AI-powered threat detection and automated incident response:** As threats become more sophisticated and AI-driven, manually monitoring and plugging security vulnerabilities is no longer feasible. AI-powered analytics and security protections can keep eyes on all areas of the network and support prediction and prevention of breaches.

## The impact of integral security

With this foundation, networks can play a more active role in:

- **Limiting the impact of expanding attack surfaces:** Ensure consistent protection across all domains: cloud, edge, IoT, and remote work.
- **Consistently enforcing zero trust, everywhere:** Remove VPN challenges and enforce real-time access policies at every network touchpoint, for every user and device.
- **Improving visibility and threat detection:** Use AI and advanced analytics to predict and intercept attacks and protect sensitive data in motion and at rest.
- **Simplifying operations:** Reduce complexity with a single policy engine, unified management, and fewer point solutions, and integrate with other elements of your security ecosystem to enhance protection.
- **Supporting compliance:** Enforce data governance and ease compliance with regulations including HIPAA and GDPR.
- **Facilitating resilience and continuity:** Isolate threats and maintain uptime with an AI-native, self-healing network.
- **Strengthening network and security team collaboration:** Make security a natural part of the network management workflow and give teams the benefits of a shared foundation for networking and security.

## Consistent protection across all attack surfaces

HPE offers a secure, self-driving network with integral security designed to simplify the journey to SASE and expand zero trust everywhere. Unlike bolt-on security approaches that add complexity and tackle protection in disconnected, siloed ways, our holistic edge-to-cloud AI-native platform integrates a secure SD-WAN, SSE, cloud-native network access control (NAC), and hybrid mesh firewall capabilities for universal ZTNA with comprehensive protection.

Now you can enforce universal ZTNA with zero trust security principles and experience comprehensive protection everywhere, on any device, for any resource, regardless of location or destination, while leveraging AI for deep insights and automated remediation—giving you the confidence to advance business initiatives without compromise.

### The HPE difference

- A single-vendor SASE platform that integrates a secure SD-WAN, cloud-native SSE, and AI-powered NAC
- Secure access to any internal application with agent and agentless ZTNA
- Leading security efficacy—ranked #1 in every test for over 5 years<sup>1</sup>
- AI-powered profiling and observability across multi-vendor infrastructure
- AI-driven insights, anomaly detection, and automated troubleshooting
- Broad integrations with third-party security solution providers



<sup>1</sup> Juniper SRX Series Firewalls were ranked #1 in performance in the following research and testing programs: NetSecOPEN (2022), CyberRatings.org (2024 Cloud Network Firewall, 2025 Enterprise Firewall)

## Keep every connection more secure

HPE's secure, AI-native network solutions make it easy to adopt zero trust and advanced protection without disrupting business.

Empower your organization to connect without compromise and discover new possibilities for growth and innovation.

Visit [HPE.com](https://www.hpe.com)

Learn more at

[HPE.com/networking](https://www.hpe.com/networking)



[Chat now](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. 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.

a00156064ENW

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

