

4 WAYS TO KEEP YOUR NETWORK ADAPTABLE TO CHANGING NEEDS

And how HPE can help

Network decision makers have a tough job. They need to meet today's connectivity demands—supporting more users, devices, locations, and increasingly data-intensive workloads like AI—while also preparing their networks for whatever comes next.

Technology evolves quickly, business priorities shift, and the threat landscape grows more complex every year. As a result, network modernization can no longer be treated as a one-time upgrade. It's an ongoing journey that requires a more intelligent, flexible, and security-driven foundation.

To stay adaptable, organizations need networks that can learn, optimize, and protect themselves as conditions change. That means embracing AI-driven operations, transitioning to platforms designed to evolve quickly, supporting diverse connectivity needs, and building security directly into the network.

Here are four ways to build a network that's ready for what's next, and how HPE can help.

1. Modernize your network with AI-driven operations, with a journey to self-driving

As networks grow more distributed and dynamic, manual approaches to operations can't scale with them. New users, devices, applications, and AI-driven workloads continually change network conditions, making it harder for IT teams to maintain performance, reliability, and security.

To stay adaptable, organizations are modernizing operations with AIOps. By applying AI to network telemetry, teams gain continuous visibility, can anticipate and address issues earlier, and respond more effectively as conditions change. HPE's approach is designed for this journey: AI-driven support that continuously learns from real operations, combined with rich telemetry and long-standing data science investment, helps advance networks toward self-driving resilience.

How HPE can help

- HPE embeds AI directly into the network management platform, enabling intelligence that can reason across domains, learn from real-time conditions, and automate actions to simplify operations at scale.
- By integrating AI into the core of the platform, not as an add-on, analysis and action happen in near real time, enabling faster response, more accurate insights, and better outcomes.
- Delivered through a cloud-native, microservices-based architecture, HPE's approach allows organizations to adopt automation and self-optimizing capabilities gradually, improving reliability, visibility, and security across wired, wireless, and WAN environments from client to cloud.

2. Transition to AI-native Wi-Fi

Wi-Fi is now the primary access layer for the enterprise, supporting users, devices, IoT systems, and increasingly AI-driven applications across highly distributed environments. Traditional wireless architectures weren't designed for this level of scale and variability, making it difficult to maintain consistent performance and user experience through manual operations alone.

AI-native Wi-Fi addresses these challenges by embedding intelligence directly into the wireless platform. Continuous telemetry enables the network to monitor conditions in real time, anticipate issues, and automatically optimize performance as demands change. This built-in intelligence simplifies deployment, reduces day-to-day operational effort, and allows IT teams to deliver more reliable wireless experiences as environments grow and evolve.

How HPE can help

- HPE delivers AI-native Wi-Fi built from the ground up to support automation, assurance, and self-optimization across enterprise environments.
- Built-in cross-domain AI leverages continuous telemetry from access points, switches, and WAN infrastructure to provide holistic visibility and more accurate insights across wired and wireless networks.
- AI-driven automation helps speed deployments, reduce troubleshooting effort, and maintain consistent performance across campuses, branches, and remote locations.
- A cloud-native management approach enables centralized visibility and control, allowing IT teams to scale Wi-Fi environments confidently as demands grow.

How HPE can help

- HPE offers a cloud native, microservices-based network management platform designed to scale and evolve with enterprise networks.
- Modular architecture provides elastic scalability, seamless fault isolation, and continuous innovation with updates that can be deployed rapidly without disrupting the entire platform.
- Open, standardized APIs and third-party integrations support flexibility and help avoid restrictive vendor lock in.
- Flexible deployment options including SaaS, virtual private cloud, on-premises, and network-as-a-service deliver the same functionality while supporting regulatory, security, and operational requirements.

3. Opt for network management that's cloud-native and microservices-based

As networks expand across campuses, branches, remote locations, and cloud environments, legacy management platforms often become a constraint. Monolithic tools weren't built to evolve quickly, making it harder for IT teams to adapt to new requirements, roll out capabilities faster, or maintain consistent visibility as environments change.

Cloud-native, microservices-based network management offers a more flexible approach. By designing management platforms as modular services that can be updated and scaled independently, organizations can evolve continuously without disruptive upgrades. Just as importantly, cloud-native doesn't have to mean cloud only—flexible deployment options allow teams to modernize at their own pace while maintaining control, compliance, and operational consistency.

4. Turn your network into a security solution

As networks become more distributed, the attack surface expands with them. Users, devices, applications, and data now move across campuses, branches, remote locations, and cloud environments, making traditional perimeter-based security models increasingly ineffective.

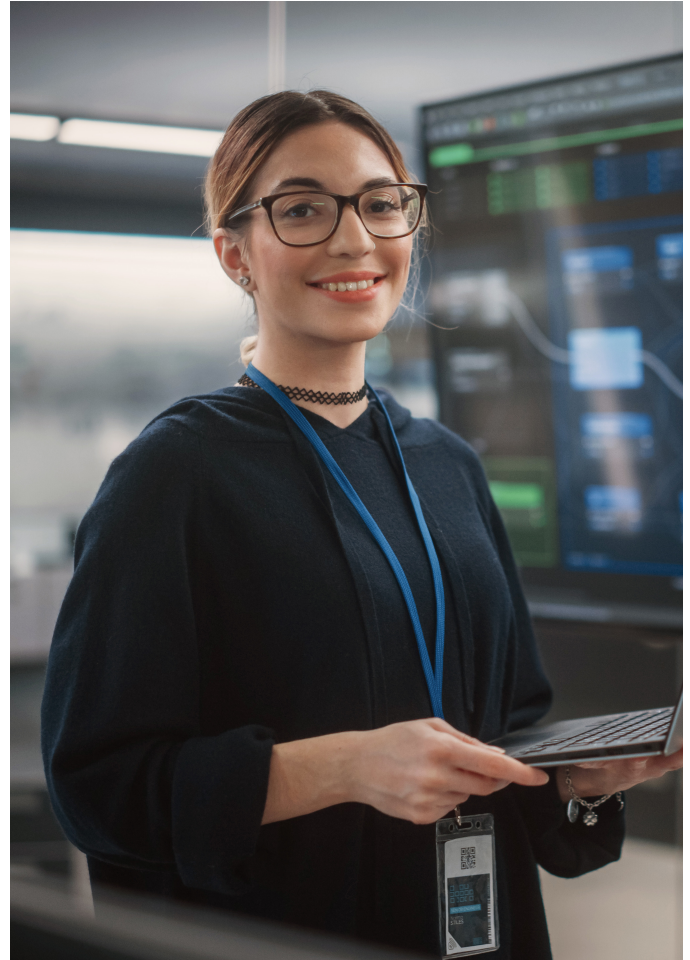
Rather than layering tools on top of the network, organizations should treat the network itself as a security solution. When security is built directly into the network, zero trust principles can be enforced consistently at every point of connection, using identity, context, and real-time conditions to make access decisions. Integrated visibility and AI-driven intelligence help detect unusual behavior earlier, isolate threats faster, and maintain performance as environments change.

How HPE can help

- HPE Aruba Networking unified SASE simplifies the journey to zero trust from edge to cloud by unifying secure SD-WAN and cloud-native SSE under a single platform for consistent protection and access everywhere.
- Paired with cloud-native NAC, HPE helps enable universal ZTNA—supporting identity- and context-based access decisions, even for unmanaged devices such as IoT, leveraging AI-powered visibility and authentication.
- Juniper SRX Series Firewalls provide high performance, next generation firewall protection for campus, branch, data center, and cloud deployments, enforcing granular security policies without compromising performance.
- AI-powered threat intelligence from HPE Threat Labs continuously feeds advanced security insights into SRX firewalls, helping detect and prevent sophisticated and emerging threats in real time.

Learn more at

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



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

[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.

a00148342ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com

