Brochure

HPE aruba networking

Work smarter, not harder

Unleash the power of a security-first, AI-powered network to accelerate business outcomes

Transform your network with modern cloud-native security, automation, and flexible consumption—to ensure your IT teams are prepared to help the business improve user experience, accelerate technology adoption, and reduce cyber risk.

Get started >

HPE GreenLake

The network is the new business imperative

The 2023 business climate was ripe with innovation, disruption, and challenging macro-level conditions, with ever-increasing pressure on IT teams to accelerate business transformation and make IT resources more available to create personalized user experiences. Generative AI (GenAI) and other natural language processing (NLP) technologies continue to reset business expectations and priorities around automation, privacy, security, and resource allocation.

Because of the critical role networks play in enabling data services and the deployment of line of business technology (e.g., IoT), their performance and health is key to business success and providing a consistent experience for connected users and devices. Addressing cloud-native cybersecurity and compliance issues also requires a new strategy—one that embraces Zero Trust Security to stay ahead of evolving threat landscapes and mitigate cyber risk. Advanced AI-powered technology enhances available network tools to ensure continuous network optimization for applications and users—and, critically for network administrators, helps to automate increasingly broad and complex IT processes and procedures to allow for more efficient network operations.

Securely delivering critical business data and services requires a network services architecture that is versatile and flexible enough to meet the needs of both networking and security teams—one that will drive the business further forward into the digital era.

New questions to ask

- Are GenAI and NLP part of your business technology investments?
- How do you anticipate using AI networking and AIOps?
- How often do the network and security teams interact? How much of a focus is there on tools that can improve cross-functional alignment?
- How much time does your IT team spend provisioning new network services for the line of business?
- How much visibility do your IT teams have on users, applications, and client or IoT device traffic on your network?
- How often do your teams focus on new business-critical initiatives vs. monitoring, reporting, and troubleshooting (MRT)?
- What are your new business requirements for connectivity? Are you being asked to support new clients capable of new Wi-Fi and wired access technologies? (e.g., 6GHz for new clients and 10GbE to the desktop)
- Are your current security policies and control sufficient for new cloud-native applications? Do they provide the granularity needed for new compliance requirements?
- Do you plan to increase your investment in campus network and wide area network (WAN) infrastructure to support new data demands?

What can security-first, AI-powered networking do for your business?

- **Improved IT efficiency:** Encourage collaboration between IT teams focused on end-user services, IoT and application development, network operations, and security, risk, and compliance.
- **Consistent end–user experience:** Ensure users and devices are granted access where needed—and the network can proactively optimize and analyze areas of concerns.
- **Reduced cyber risk:** With the appropriate visibility and access controls automatically in place, network teams can more efficiently secure against external actors, identify and mitigate at-risk assets, and meet industry compliance requirements with instant access to appropriate alerts and reports.
- **Accelerated IoT adoption:** Accelerate deployment of line of business technologies such as onsite Wi-Fi and wired networking, point of sale systems, security cameras, Bluetooth and Zigbee sensors, and more.

Building a better network

Networking and security teams must be aligned and have a common network and security foundation to ensure ubiquitous access and to sufficiently address the threat landscape.

The network is the foundation

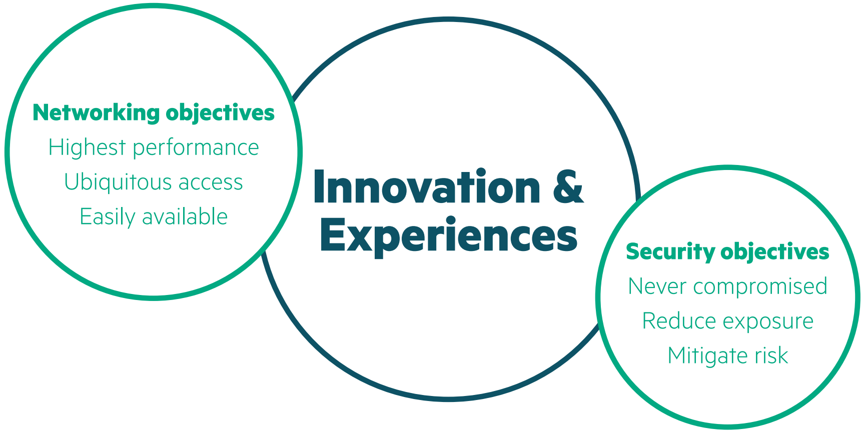


Figure 1. Network and security objectives

A new approach is needed to orchestrate data in a secure, simple, and automated way—one that enables IT to collaborate more productively across networking and security functions and is proactive and reactive where needed—while providing the utmost security and helping meet compliance requirements.

Dynamically applied context-based awareness of user roles, devices, applications, location, and other metadata based on Zero Trust principles empowers the network to provide stringent “deny-first” access control and a customized end-user experience. The ability for the network overlay (i.e. the services platform) to be compatible with IoT services and for the infrastructure to integrate IoT protocols such as Bluetooth, Zigbee, and third-party USB connections help to minimize the time and resources spent implementing new onsite technologies. And to help optimize IT operations, AI networking technology can apply automation when and where it’s needed most—reducing the burden on IT to scale out and support the new on-demand workloads required to deliver cloud-native digital experiences.

What can security-first, AI-powered networking do for your IT teams?

- Enable network and security teams to work more collaboratively using common tools powered by machine learning (ML) and NLP
- Help improve network performance and uptime
- Expand the role of the network to serve as an IoT connector and security solution
- Gain greater visibility and control over client devices and application traffic
- Unlock insights into digital experience and network power consumption
- Multiply human potential and roll out comprehensive cyber protection using AI-driven automation and analytics

Introducing security-first, AI-powered networking

With decades of customer-centric innovation in enterprise networking, HPE Aruba Networking delivers Zero Trust solutions with security-first, AI-powered networking, providing a common foundation for networking and security teams to deliver secure, distinctive experiences and cybersecurity protection for end-user and client devices.

Utilizing shared visibility, global policies that follow the user, edge-to-cloud enforcement, and AI automated operations, security-first, AI-powered networking solutions from HPE Aruba Networking are engineered to deliver high performance and ubiquitous access with the least possible risk. With a single point of visibility and control available in HPE Aruba Networking Central, further advanced visibility, insights, automation, centralized policy management, data protection, and threat defense across campus, WAN, and data center network, become unlocked.

Intelligent automation features also built into HPE Aruba Networking Central offer an improved end-user experience and mitigate security risks. AI insights, profiling, search, and firmware recommendation features deliver optimized network performance, anomaly detection, and enhanced monitoring, diagnostics, and auditing to augment IT capabilities. Central and the access points, switches, and gateways under management are designed to help accelerate IT outcomes and ensure organizations have the flexibility and versatility they need.

Driving line-of-business success

Today's evolving user behavior, environmentally conscious business goals, and the reliance on cloud-native applications require consistent and reliable business, IT, and user experiences.

Networks need to be smart, stable, and simple to manage—and reduce the need to perform disruptive and repetitive moves, adds, and changes that use countless hours of IT resources.

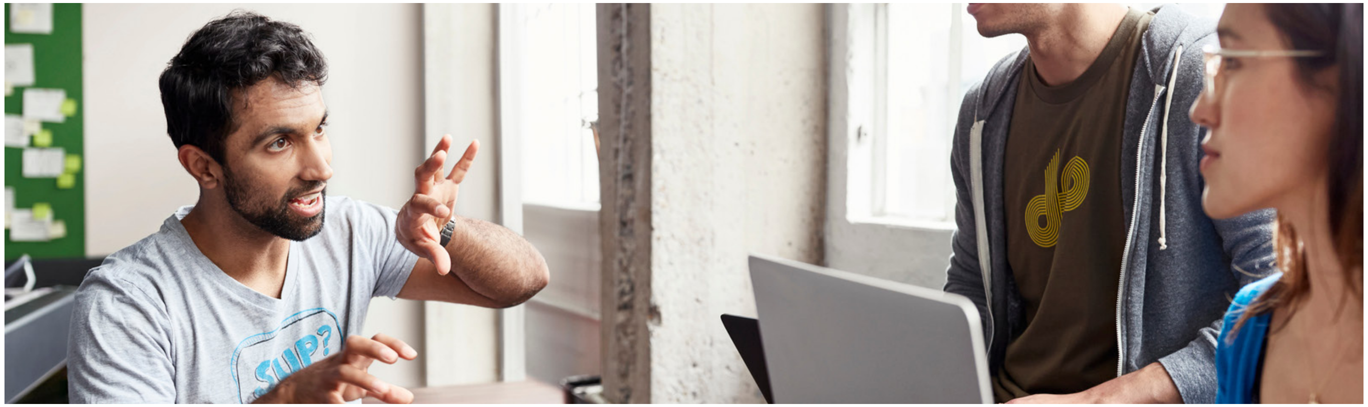
They also need to be aligned with business goals and priorities (e.g., carbon reduction) and directly support line-of-business requirements by efficiently optimizing for digital experiences and IoT technologies. Network automation features need to include:

- **Unified infrastructure operations:** Get lifecycle management for Wi-Fi, switching, SD-WAN, and VPN infrastructure across campus, branch, remote, and data center network operations, using a single point of visibility and control, via a common services platform (HPE Aruba Networking Central). Network agnostic and third-party services (IoT, security, etc.) can be easily integrated and delivered across any connected network device or location. Learn more about unified infrastructure
- **Rapid and accurate onboarding and deployment:** Provide privacy-centric, self-service device registration and service availability to end users at any location needed. Offload repetitive daily tasks from network administrators with cloud-based authentication, MPSK, Bonjour and other zero configuration networking capabilities (e.g., AirGroup). Learn more about enabling a self-service, privacy-first network experience
- **Automated configuration at scale:** Leverage advanced campus switching software like NetEdit, port profiles, and the cloud-native switch management features in HPE Aruba Networking Central to streamline network changes with minimal end-user disruption and reduced IT overhead. Learn more about HPE Aruba Networking CX switches and HPE Aruba Networking Central
- **AI-powered performance optimization and diagnostics:** Identify, diagnose, and automatically perform configurations to ensure the best possible end-user experience, 24x7, using the ML technology within HPE Aruba Networking Central. Learn more about our artificial intelligence operations (AIOps)

How HPE Aruba Networking is prioritizing sustainability

- Hewlett Packard Enterprise (HPE) is committed to achieving net-zero emissions across our entire value chain by 2040, with a 70% reduction in scope 1 and scope 2 emissions by 2030.
- Every element of the product lifecycle, including design, material composition and acquisition, production, packaging, transportation, and post-use disposition is considered to ensure they meet our customers' evolving needs and expectations. New eco-packs are available across our high-volume products to reduce the packaging needed for product fulfillment.
- Our AI-powered network infrastructure and services dashboards deliver zero-touch provisioning, cloud-based lifecycle management, and automated troubleshooting to streamline workflows to drive IT resource optimization and minimize manual, onsite labor needs to enable control of key resource consumption.
- We prioritize innovations that provide visibility and control for maximum power efficiency such as the HPE GreenLake sustainability dashboard, power management and control features, platform operation, built-in intelligence, and standards compliance.
- We enable customers to control their environments with automation features such as IoT Operations (in HPE Aruba Networking Central) to efficiently design and implement IoT services and reduce or eliminate the need for overlay appliances—for decreased costs, carbon emissions, and lifecycle management activity.

Learn more about sustainability at HPE Aruba Networking



- **User experience measurements that increase the value of the network:** Help alert your IT teams of synthetic network and application performance issues by implementing user experience insight (UXI) sensors throughout your network. By testing the network in different locations, UXI sensors can identify and aggregate anomalous issues for potential remediation. Learn more about digital experience monitoring (DEM).
- **NLP technology directly integrated into the network services platform:** Closely monitor the network and identify areas of concern with a more human-oriented approach to network diagnostics, using the NLP-integrated AI search functions in HPE Aruba Networking Central. Learn more about AI tools within Central
- **IoT convergence**: Integrate a vast library of IoT operational products and services with existing IoT-optimized access point infrastructure to simplify physical topology and management overlays. Learn more about access points as IoT platforms
- **IT infrastructure insights and carbon footprint:** Support corporate sustainability initiatives by monitoring and generating environmental impact alerts and reports for visibility into power utilization, carbon emissions, and resource consumption. Learn more about sustainable IT solutions with HPE GreenLake

What is HPE Aruba Networking's approach to Security Service Edge (SSE)?
An SSE solution secures remote access to web, cloud services, and private applications. Security services are uniformly orchestrated through a common platform. SSE includes four core security components:

- ZTNA delivers Zero Trust network access via a trust broker, to only specific applications or microsegments that have been approved for the user.
- Secure web gateway (SWG) protects users from web-based threats through advanced SSL inspection, URL filtering, sandboxing, malware scanning, threat intelligence protection and DNS filtering.
- Cloud access security broker (CASB) mediates secure connectivity to SaaS applications to ensure sensitive data remains protected, data loss is prevented, and the risk associated with shadow IT usage is reduced.
- Digital experience monitoring (DEM) provides in-depth monitoring of device, application, and network performance, as well as the hop-by-hop network path so IT teams can easily pinpoint connectivity issues—and resolve them fast.

Learn more about HPE Aruba Networking SSE.

Protecting the business

With GenAI and hybrid cloud requirements increasingly at the center of business strategy and operations, cybersecurity and privacy landscape threats have grown significantly.

Modernizing security architecture with a Zero Trust Security approach can protect against a variety of cyberattack vectors, enabling businesses to confidently embrace digital acceleration. With HPE Aruba Networking, your network can become an edge-to-cloud security solution that helps ensure compliance and protects user and corporate data, with capabilities that include:

- Unified policy orchestration with automation capabilities that can be globally applied across WLAN, switching, and SD-WAN policy constructs
- AI-powered Client Insights to proactively identify what is on the network
- Secure device onboarding and health checks
- Dynamic segmentation to consistently enforce user, application, client, and network-based least-privilege access controls
- Security Service Edge (SSE) solutions to deliver Zero Trust network access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), and digital experience monitoring (DEM) capabilities

The benefits of an HPE Aruba Networking as-a-service approach to your IT equipment lifecycle

- Flexible financing with upfront and monthly pricing options based on what you have deployed
- Scalable centralized management that aggregates data center, enterprise campus, and WAN infrastructure
- Pre-planning for migrations and upgrades directly into a statement of work
- Proactive advisory and management capabilities to maximize performance and security
- Change management controls based on your compliance needs
- Upcycling to help extend equipment lifecycles and lower environmental impact.

Aligning the network with business outcomes

Network as a service (NaaS) is a flexible way to consume enterprise network infrastructure and keep pace with innovation, meet rapidly changing business needs, and optimize network performance and user experiences through a cloud-like subscription model.

NaaS allows enterprises to consume and optionally outsource the full lifecycle of their enterprise network deployment, with all hardware, software, licenses, and services delivered in a flexible consumption or subscription-based offering.

NaaS also allows organizations to outsource the planning, deployment, and day-to-day operational management of the network, including software upgrades, monitoring, and troubleshooting, as well as decommissioning and end-of-life support. Through this process, organizations get access to the latest and greatest technology while easing the burden on their IT staff.

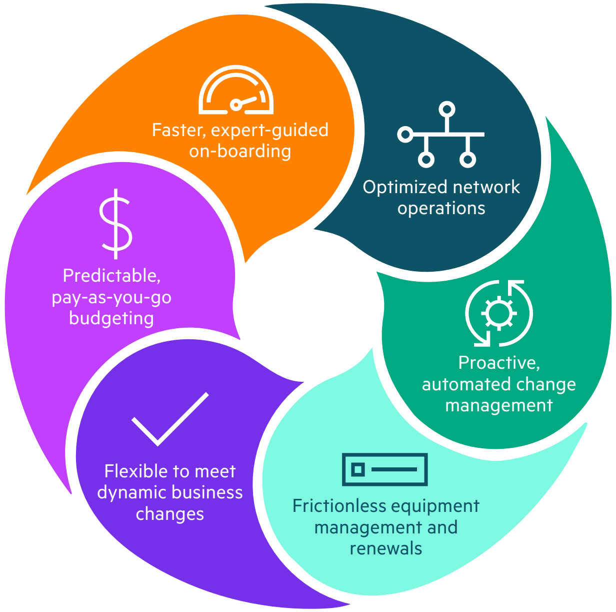

Faster, expert-guided on-boarding
Optimized network operations
Proactive, automated change management
Frictionless equipment management and renewals
Flexible to meet dynamic business changes
Predictable, pay-as-you-go budgeting

Figure 2. Example NaaS outcomes

Work smarter—not harder—on your digital transformation journey. By implementing security-first, AI-powered networking, your business will be strategically positioned to accelerate technology adoption, improve end-user experience, and reduce cyber risk. By leveraging a common network and security foundation with HPE Aruba Networking Central as your services platform, a wide variety of cloud-native technologies built on Zero Trust principles can help you unlock higher network performance, optimize user and IoT experiences, and keep pace with the evolving threat landscape- no matter what industry you are in. What's more, flexible consumption options are available to help accelerate the mean time to value of your network investments.

Make the right purchase decision.
Contact our presales specialists.

✉ **Contact us**

To learn more about security-first, AI-powered networking, please visit the HPE Aruba Networking website and contact us for any questions.

Visit **ArubaNetworks.com**

Hewlett Packard
Enterprise