HPE aruba networking | BlueAlly

Brochure

Four requirements for an AI-powered network

Modern business demands mean networks must connect more applications and Internet of Things (IoT) devices than ever before, all the while staying on top of evolving AI workloads. Can your network deliver?

HPE

Obstacles in an edge-to-cloud era

Despite the shift toward return-to-office mandates, modern enterprise networks still find themselves having to connect dispersed workforces to services that are hosted everywhere — from the cloud to IoT devices at the edge. On top of this, AI continuously transforms the network landscape — AI applications generate a vast volume of data that cannot be confined to a single location and this data must still be protected and secured.

Can existing network infrastructure handle the increasing demands of more sophisticated applications, additional IoT devices, and greater AI adoption? If not, delivering differentiated user experiences and securely connecting IoT devices to support AI and other business needs will be a tall order.

The scale of the challenge that today's enterprises face requires innovation and it can be boiled down to three key issues:

— **Demanding, immersive applications:** Outdated network infrastructure lacks intelligence and is simply too complex and slow to deliver next-generation digital experiences or support evolving AI requirements. Wireless connectivity continues to be needed everywhere — from traditional campus environments to manufacturing facilities and outdoor spaces. But as the use of IoT devices and applications grows at an unprecedented rate, organizations struggle to gain agility and scalability across their already extended networks. Additionally, without real-time visibility into diverse application usage, businesses risk subpar performance that frustrates users.

— **Operational inefficiencies:** In fragmented environments, operational inefficiencies are inevitable. As businesses digitize their operations to improve productivity and gain a competitive advantage, networking teams must be more agile and responsive. Without a unified infrastructure that spans Wi-Fi, private 5G, wired LAN, and SD-WAN — and that is fueled by AI-powered automation — these teams are left with no choice but to carry out independent management of each network with domain-specific tools across campus, branch, remote worker, and data center locations.

— **Security vulnerabilities:** A patchwork setup is complex to manage, and manual and static VLAN-based approaches to securing networks can be error-prone. This leaves network operators needing to consistently define and globally enforce role-based policies across complex, evolving, geographically distributed networks. Added to this, traditional discovery and profiling techniques struggle to accurately identify the growing number of IoT devices that connect to the network. The result is poor visibility and increased risk of unplanned downtime or security incidents.

A fit-for-purpose network should deliver on the performance, security, and coverage that's necessary to manage all users, devices, and workloads — particularly data-heavy AI workloads as the demand here is set to grow exponentially. Moreover, a modern network should not only be simple enough to manage with existing resources and without any downtime but also capable of providing actionable insights.

The network checklist

When modernizing, network investments should focus on delivering a unified infrastructure that can rapidly adapt to changing business needs. To harness this agility, enterprises should move away from multiple management consoles by opting for a broad and innovative networking portfolio that provides built-in security solutions, customer-to-cloud connectivity, and essential AI capabilities, all managed from a single pane with third-party observability to ensure reliability and security across the full stack.

Speaking of AI, businesses must be mindful of both current and future needs, investing in architecture that will support the expansion of AI as well as the growing number of IoT devices needed to fuel AI training and inference. Such infrastructure must also be scalable to accommodate the increasing network traffic generated by AI workloads running from edge to data center to cloud.

A modern network should meet four foundational criteria to ensure you can achieve the top three demands for business agility, IT efficiency, and enhanced security.

1. Is it seamless?
A modern network infrastructure features wireless access points, enterprise-ready private cellular, and programmable switches to prevent any coverage gaps. It supports seamless integration of IoT operations and offers ease of management with comprehensive visibility.

2. Is it AI-powered?
AI-powered management across Wi-Fi, private 5G, wired LAN, and SD-WAN networks gives you the visibility, control, and insights needed to streamline and secure your IT operations. This is boosted by AI-driven troubleshooting and optimization recommendations, enabling you to reduce time-consuming manual management and intervention while automating deployments and updates. A robust set of application programming interfaces (APIs) and webhooks makes integration with private tools frustration-free.

3. Is security built in?
Built-in zero trust security solutions are the key to enhanced security. These include identity-based access control, automated policy enforcement across wired and wireless LAN and SD-WAN, and comprehensive device visibility that spans the network. AI features further amplify security, delivering accurate customer insights for proactive-issue resolution and anomaly detection for threat prevention and response.

4. Is it flexible?
You can optimize resource use (and costs) through flexible acquisition and deployment models (on-prem and in cloud) that offer predictable expenses and faster time to value. Management includes third-party observability for multivendor environments and a robust set of APIs and webhooks for easier interoperability.

Network innovation to meet enterprise needs

The unified infrastructure portfolio offered by HPE Networking is built to help businesses overcome the obstacles that traditional networks present. A secure, flexible, and AI-powered network is what HPE delivers to meet your need for future-ready agility and efficiency. What does this entail?

1

Modern infrastructure for seamless, comprehensive connectivity

HPE offers a comprehensive AI-powered networking portfolio, giving you everything you need to support diverse and growing connectivity needs across various environments.

Our AI-powered portfolio of Wi-Fi access points and HPE Aruba Networking private 5G solutions provide reliable, high performing coverage to support growing numbers of users and devices and the demands of AI. HPE Aruba Networking Wi-Fi 7 access point innovation goes beyond the industry standard to help maximize wireless performance, strengthen network security, enhance location-based services, and act as a secure IoT platform. This enables enterprises to boost the value of their wireless investment and discover operational efficiencies. Meanwhile, our private 5G solution makes it simple for enterprises to augment their Wi-Fi networks with private cellular — providing a complete solution based on mature and proven technology.

When it comes to delivering comprehensive coverage, switches that connect different parts of the network to enable seamless data flow are equally important. Legacy switches can't offer the same high availability and robust data-handling capabilities that CX switches can. HPE Aruba Networking CX Switch Series addresses requirements from access edge to data center, with consistent controls and operations as well as a unified view of the entire switching fabric — all helping to strengthen IT efficiency.

2

AI-powered management for operational efficiency

In the AI era, it's essential that networks can manage and scale alongside increasingly large amounts of data. HPE Aruba Networking Central is a unified management solution for secure wireless, wired, WAN, and IoT networks that helps maximize operator efficiency with an AI-powered, intuitive user experience. With new integration of third-party network device monitoring capability in HPE Aruba Networking Central, customers gain an advantage in their ability to control, predict, and manage their end-to-end network infrastructure.

Delivered on cloud-native, microservices-based architecture, HPE Aruba Networking Central offers zero-touch provisioning for faster deployments and live updates. It helps eliminate manual troubleshooting tasks, reduces resolution time for common network issues, and increases network capacity through peer-based configuration optimization.

It provides IT teams with simpler navigation and enhanced endpoint-to-infrastructure visibility and is designed to more intuitively incorporate AIOps analytics to deliver a best-in-class user experience.

Actionable AI that produces trustworthy outcomes depends on three key ingredients: an extensive volume and variety of data, domain expertise, and experienced data scientists. HPE Aruba Networking AIOps applies over 18 years of proven network innovation when modeling telemetry data from over two million wired, wireless, and SD-WAN devices to identify anomalies and provide prescriptive recommendations that network admins can trust.

3

Built-in zero trust for strengthened security

A security-first, AI-powered network from HPE Networking eases adoption of zero trust security and supports compliance with cybersecurity standards and regulations by allowing teams to use the network as a security solution. The network can now provide advanced visibility and insights, centralized policy management, data protection, threat defense, and access control in a single platform.

Zero trust security starts with visibility. HPE Aruba Networking Central leverages native infrastructure telemetry from access points, switches, gateways, and customers to automatically fingerprint and identify a diverse set of IoT devices across the entire wired and wireless infrastructure offering the most granular profiling and visibility. Cloud-native network access control (NAC) capabilities enable frictionless onboarding of users and devices, automatically assigning to each the right level of network access consistent with identity and role. Dynamic segmentation applies least privilege access to applications and data through role-based access policies that follow the user throughout the network and are applied uniformly across wireless, wired, and remote connections.

Zero trust security models rely on an up-to-date understanding of device behavior to identify and thwart potential compromise and attack. HPE Aruba Networking Central applies AI to comprehensive device telemetry to detect anomalous behaviors and raise alerts for investigation, making it simpler for network and security teams to detect potential compromises of high-risk IoT devices. AI-powered policy optimization tools within HPE Aruba Networking innovation can also help organizations accelerate potential threat response without manual intervention or operational disruption. How? By recommending and previewing role-based policy changes aligned to zero trust principles and least privilege access.

Stay future-ready

Network modernization is a sound investment because it not only supports today's operations, but it also keeps your business ready for what comes next. To deliver a return on this investment, the only real answer is a security-first, AI-powered, unified infrastructure.

With HPE, you not only gain access to a comprehensive cloud-native portfolio for all of your Wi-Fi, private 5G, wired, and SD-WAN needs, but are also able to retain a single point of visibility and control through HPE Aruba Networking Central. This helps to ensure great user experiences and secure IT connectivity across business locations — from home working to the campus, branch, and data center — for organizations of any size in any sector.

By combining cutting-edge hardware, AI-powered management, and built-in security, HPE innovation provides greater performance and seamless connectivity to even the most remote of locations. Our solutions also enable you to increase bandwidth to match business demands — without disrupting the service offered by the network.

HPE innovation provides a comprehensive networking portfolio designed to meet the needs of any scenario and deliver great experiences.

About HPE

HPE is the edge-to-cloud company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open, and intelligent technology solutions, with a consistent experience across all clouds and edges, to help customers develop new business models, engage in new ways, and increase operational performance.

Learn more at

HPE.com/us/en/networking

Visit HPE.com

Chat now

a00148129ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com