



**BUYER'S GUIDE  
TO WI-FI 7 AND  
PRIVATE 5G**



## Key takeaways

1

AI is impacting the network in new and profound ways.

2

Industry standards are evolving to improve performance and reliability, yet innovative wireless solutions go beyond the standard to deliver better support for IoT/OT, location services, sustainability, and more.

3

Wi-Fi and private 5G can and should work together to provide pervasive wireless coverage—without increasing management overhead.

# Introduction

Every five years or so, enterprises typically modernize their wireless networks. Most times, it's because needs have changed and requirements have grown. Other times, it's because the legacy technology is nearing end of support and difficult to maintain.

This buyer's guide examines key trends in networking due to AI—both networking for AI and AI for optimizing the network—and their impact on network modernization. It then delves into the key wireless technologies: Wi-Fi 7 and private 5G. In addition to 802.11 and 3GPP standards that lay the foundation for basic capabilities, it is also important to look at the additional, yet essential capabilities for wireless networks today. Lastly, it considers how private 5G and Wi-Fi should work together to provide pervasive connectivity and how network management can unify and simplify the operator experience, providing observability, ease of configuration, AI insights, and extensibility.

**The private 5G market continues to flourish, offering wider coverage, higher speed mobility, and additional spectrum for mission-critical applications to augment Wi-Fi's ubiquitous reach. Private 5G helps connect mobile endpoints reliably, especially where dedicated performance, data privacy, or wide area coverage is needed. Emerging innovations in both Wi-Fi and private 5G provide a compelling "1+1>2" value proposition for many enterprises.**

**"Unifying wireless: Private 5G and Wi-Fi", IDC Spotlight, August 2024**

## Increasing wireless demands

The demands on wireless are only increasing with AI. Since the earliest days of 802.11, wireless networking has evolved and modernized to meet the growing numbers of user and IoT devices and increasingly bandwidth-hungry and latency-sensitive applications.

## Networking for AI

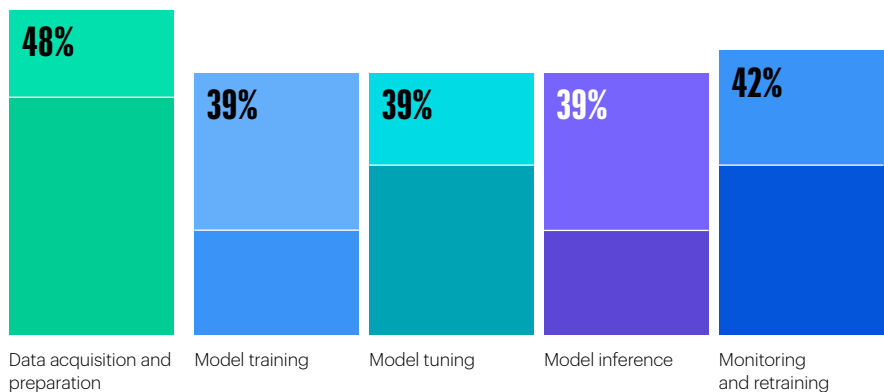
The AI hype and its impact on the network are real. AI is driving more challenges around growth of traffic, performance, and latency. AI generates more data, and that data cannot sit in a single location. It is truly dynamic, and it has to be acted upon multiple times, often in multiple locations, which in turn drives a significant increase in data loads in customer network environments.

To be able to collect all data—no matter where it’s generated—enterprises need to implement the broadest set of connectivity options, including Wi-Fi for IoT and private 5G. They must do so without any loss—all the way from a user device connected to a Wi-Fi access point, to the campus switching infrastructure through the aggregation and core layers, and, finally, back into the data center. And, because of the parallel processing inherent in AI, latency must be kept to a minimum.

However, implementing a broad set of connectivity options can easily lead to siloed infrastructure. Enterprises need a single connectivity fabric from edge to cloud, which enables consistent security policies, centralized management, and contextual visibility into the network from a single pane of glass.

As always, security is a top concern. AI requires stringent data protection to determine who and what devices are allowed to provide information and inform the machine learning algorithms and training models. Unfortunately, because older legacy networks may not be able to handle the demands of AI, IT teams may struggle to meet new business needs with existing resources.

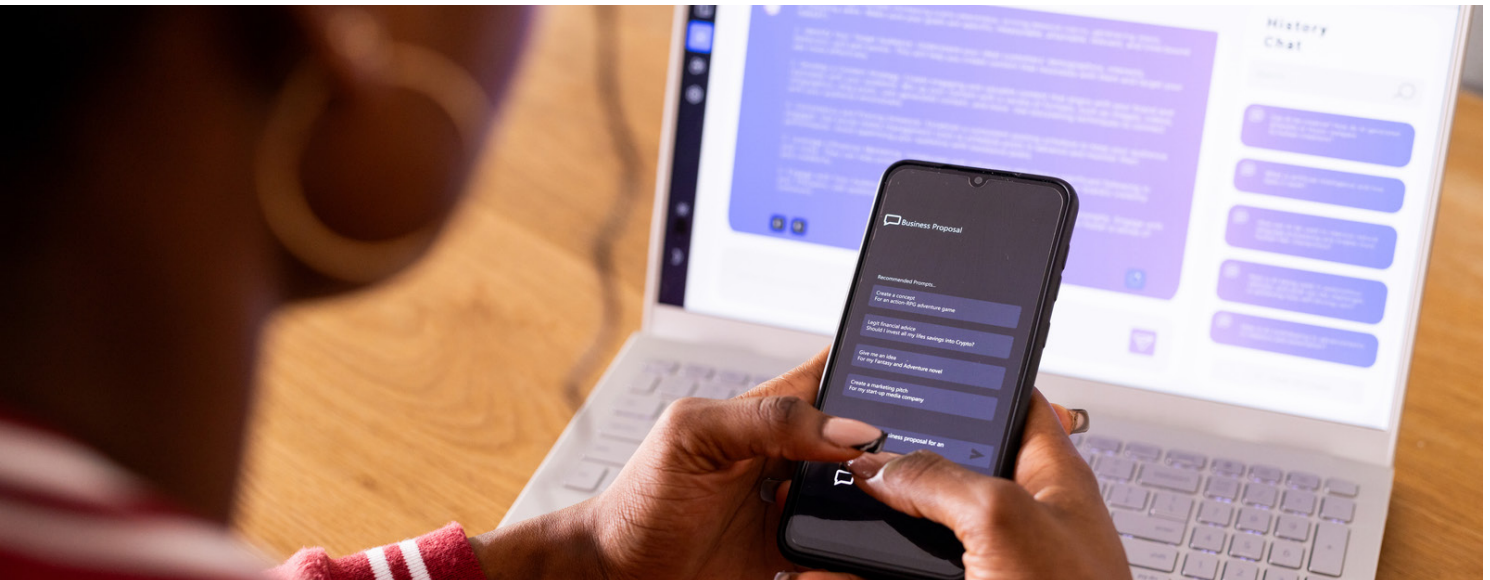
### % of IT decision-makers who fully understand networking needs across the AI life cycle



### Stages of the AI life cycle

<sup>1</sup>“[Architect an AI advantage](#),” HPE, 2024

**Figure 1.** Less than half of IT decision makers understand the networking needs across the AI life cycle.<sup>1</sup>



## Keys to effective AI for networking

- Rich data lake with billions of endpoints and device metrics
- Hardware telemetry to collect the right data to inform models
- Data science that continuously refines recommendations while protecting customer data
- Visualizations that make it easier for operators to apply the insights
- Self-driving automation, where applicable

## AI for networking

Not to be confused with networking that supports AI, AI for networking is gaining traction to make sense of the volume, velocity, and diversity of data that is generated by the network. As networks grow more complex and distributed, AI technologies are becoming critical to network management. Simply put, it is increasingly impractical to manage and protect these environments with traditional manual techniques.

Planning, installing, securing, and operating myriad access points, switches, gateways, and WAN connectivity require the insight and efficiency that AI can provide.

Comprehending network telemetry data leveraging AI is necessary for quickly understanding network operating tolerances and resolving issues, removing the need of IT staffers to constantly monitor and chase problems. AI is also necessary to analyze rapidly changing user, device, application, and network behaviors to quickly spot anomalies that could indicate a threat, with AI-generated recommendations and workflows that could halt or minimize the impact of such threat. (This is especially useful when it comes to headless IoT devices.) Finally, AI-powered large language models (LLMs) can accelerate triage efforts by providing contextual guidance rather than wading through extensive technical support documentation.

But although AI makes things easier, AI itself is not so simple. While anyone can API a question into ChatGPT and generate what looks like a reasonable answer (not with the coverage and accuracy networking practitioners would expect), the source and integrity of the training data often times produce suboptimal or inaccurate results.



## Wi-Fi 7: Innovation in Wi-Fi

Wi-Fi continues to evolve to meet the needs and demands of enterprises. The latest version, Wi-Fi 7 or 802.11be, offers several advancements:

- 320 MHz bandwidth channels (2x the width of the previous generation, although most enterprises rely on 40/80 MHz channels due to density and capacity constraints)
- Multilink operation (MLO) for channel aggregation across different bands to improve resiliency/failover
- 4096-QAM (4k QAM) for higher peak data rates
- Spectrum puncturing to better accommodate interference in wide channels

It's important to note that many of the Wi-Fi 7 innovations will be adopted over time. For example, 320 MHz channels are not practical today in an enterprise environment where 40 MHz channels are prevalent.

The most transformative change to Wi-Fi, however, has been the opening of the 6 GHz band that adds 1200 MHz (or 500 MHz in some countries) of additional spectrum. With the addition of the 6 GHz band, Wi-Fi can support more devices and deliver higher speeds and lower latency. Both Wi-Fi 7 and Wi-Fi 6E (**E** stands for extended) take advantage of the 6 GHz band.

**6 GHz support more than doubles the available spectrum and can be leveraged in both Wi-Fi 6E and Wi-Fi 7.**

## Seven questions to ask before you modernize your wireless network

1

What is driving your Wi-Fi refresh? (End of support, real estate changes, business requirements, and so on.)

2

What will be the role of AI/ML to automate optimization, provide recommendations, and improve troubleshooting?

3

How do you ensure the security of your wireless network?

4

How will you support growing numbers and types of IoT devices?

5

Are you or would you like to use Wi-Fi for location-aware services?

6

Does your organization have sustainability goals to reduce energy consumption?

7

Are you looking for cloud management or NaaS, and will you deploy with gateways?

## Wi-Fi® by the numbers 2024

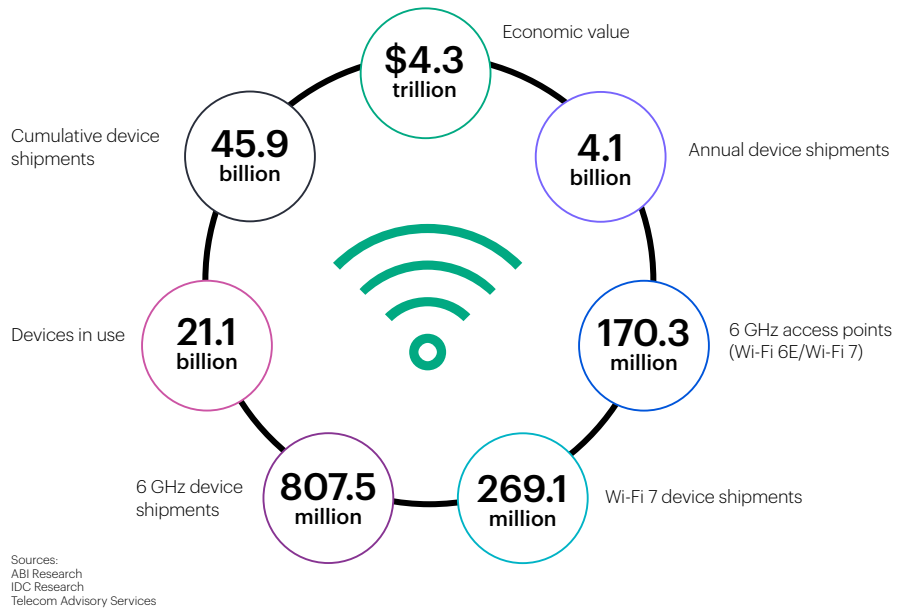


Figure 2. Wi-Fi by the numbers.

## Wi-Fi standards alone are not enough

Wi-Fi certification is important because it provides third-party validation of functionality and interoperability. Yet, meeting the standard is table stakes. Wi-Fi APs must go beyond the standard to deliver:

- **A wide range of IoT support** from BLE to 802.15 (Zigbee) to USB port extensions that allows for IoT connectivity without requiring overlay networks as well as IoT device inspection to eliminate rogue devices and processing power run IoT services on the AP itself.
- **Sustainability automation** to enable APs to dynamically turn off/on to reduce power consumption while still providing reliable coverage.
- **Dynamic prioritization capabilities** that use AI to go beyond best effort and improve quality of service for mission-critical applications.
- **Fine-grained filtering** that prevents interference yet maximizes use of the 5 GHz and 6 GHz bands for higher throughput and lower latency.
- **Embedded security** that is not **bolted on** and enables role-based access control and a unified fabric that extends across wired, wireless, and SD-WAN.
- **Location-aware APs** that can detect their own location on a floor plan (including floor level) and then broadcast the latitude, longitude, and altitude coordinates freely to devices that then calculate their location within 1 meter accuracy for use in wayfinding, asset tracking, safety, and other applications.

## Case study for private 5G

To provide connectivity for a pop-up event that transformed a parking lot into a lively venue for music and food, the organizer recognized that the demands of the fans and vendors would require both Wi-Fi and private 5G. In a matter of days, they deployed private 5G on their SIM-enabled devices to support mission-critical vendor applications for ticketing and for food and beverage purchases. And for their enthusiastic fans, they deployed Wi-Fi access points with support for 6 GHz to support immersive experiences and video live streams.

## Complementing Wi-Fi with private 5G

Private 5G complements Wi-Fi with a flexible type of wireless connectivity. Enterprises adopt private 5G for many reasons, including its strengths in the following areas:

- 1. Wider area coverage.** Due to higher power limits and higher radio receive sensitivity, private 4G/5G can cover more area per access point (albeit at a lower per-AP throughput). Less cabling is needed which lowers costs, minimizes the impact on landscaping, and makes it easier to connect hard-to-reach areas like mines and wind farms.
- 2. High-speed mobility.** Industry 4.0 requires high-speed mobility without any loss of connectivity in order to avoid costly work stoppages. In private cellular, hand-off decisions are controlled by the network and benefit from the wider area coverage that requires fewer handoffs. Private cellular capabilities are ideal for robotics, autonomous vehicles, and warehouse operations.
- 3. Segmentation of mission-critical traffic.** Some enterprises want to deploy a separate network for business-critical applications that operates over relatively clean spectrum alongside existing Wi-Fi networks. For example, a large public venue might deploy private cellular for back-office applications like mobile ticket scanning and reserve the Wi-Fi network for guest use.
- 4. RF complexity.** In areas such as manufacturing sites with non-conforming materials, private 5G can transmit at higher power levels and provide additional, dedicated spectrum for connectivity.
- 5. Deterministic network access.** The private 4G/5G infrastructure coordinates the resources of each forwarding node to guarantee priority, latency, and bandwidth per application per device rather than the client coordinating resources as it does in Wi-Fi. This enables predictable, high levels of QoS for mission-critical applications even in crowded environments.

## What's slowing private 5G adoption?

Despite compelling use cases for private cellular, enterprises have struggled to implement networks due to the complexity. Traditionally, private cellular networks have relied on technology from up to seven vendors, plus assistance from a service provider.

Vendors make it easier to deploy and manage private cellular by delivering pre-integrated, all-in-one solutions that include:

- Cloud-based core and radio management (with on-prem options)
- Core software that supports both 5G as well as 4G (LTE)
- Spectrum access systems, as needed, to protect incumbents using the CBRS band in the US
- Appliances to run the core software on prem
- Indoor and outdoor small cell radio options
- SIM or eSIM for client devices



## AI-powered network management

Maintaining a network today requires full-time observability and automation. AI for networking can help automate network operations to improve performance and efficiency:

- Identify network, security, and application performance issues before they affect users or business applications.
- Eliminate much of the manual troubleshooting tasks that keep your IT team buried in busy work.
- Provide optimization tips as your network experiences changes, like an increase in IoT or more apps like Zoom or Teams.
- Classify and see Wi-Fi and wired clients (IoT, laptops, cameras, phones) to identify security threats and to grant access privileges for security and bandwidth demands.
- Find more intelligent answers faster using large language models (LLMs).



Private cellular management

Mobile core as appliance or VM

Indoor & Outdoor radios  
Spectrum access systems (US)

SIM/eSIMs

### One end-to-end offering

Everything you need  
to deploy a cellular network

## The need for unified management

Are you one of the 75% of organizations that use four or more management tools? If so, there is an opportunity to simplify how you manage your network and streamline troubleshooting tasks. With the right solution, you can unify cloud-native network management and drive greater operational efficiencies across branch, remote, campus, data center, and IoT networks with AI-powered insights, workflow automation, and edge-to-cloud security.

A unified network management solution should provide:

- **Contextual observability:** Intuitively deliver a holistic view into the entire connectivity experience
- **Streamlined configurability across device types:** Speed up deployment and reduce configuration-related errors
- **Purpose-built AI:** Create data-driven insights and analyses to improve cybersecurity and reduce threats, increase network domain expertise, and make teams more efficient
- **Architectural openness:** Bring platform scale and modularity to fuel future innovation

## Before you start: Deployment considerations

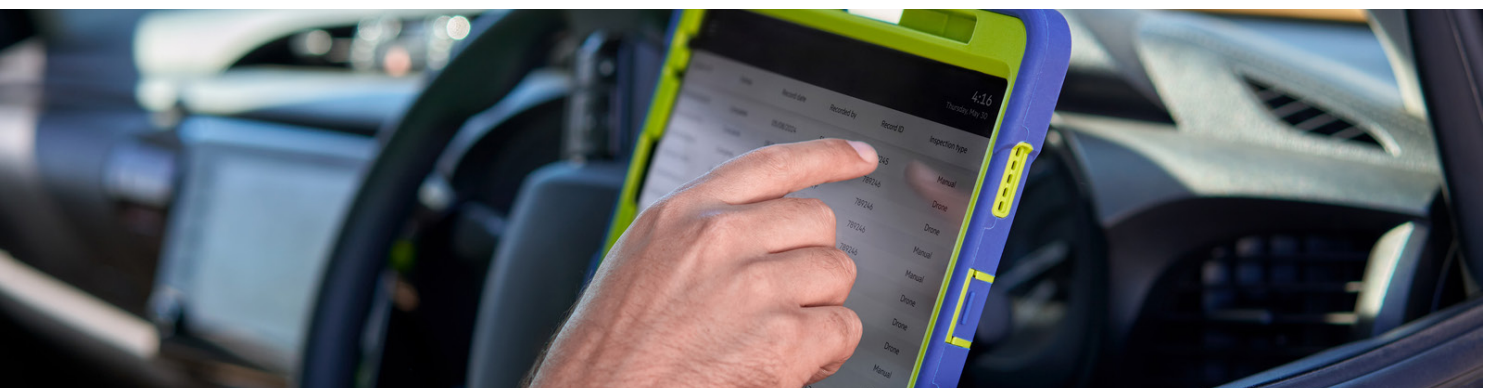
When refreshing your wireless network, it's critical to first take stock of your existing footprint. If you deployed access points using RF models for 5 GHz, you'll probably have good coverage when you move to either Wi-Fi 6E or Wi-Fi 7 and begin using the 6 GHz band. You may, however, need to reevaluate your power sources as newer access points may require switches that support IEEE 802.3bt with 30W of PoE power or more.

For greenfield implementations, such as 4G/5G private cellular networks, it's important to clearly identify your use case such as wide outdoor coverage or high-speed mobility within a warehouse. Outdoor coverage is typically 8–10x that of Wi-Fi due to the higher power levels, whereas indoor models can range up to 4–5x depending on the materials used and propagation.

Refreshing or deploying a new network is also an opportunity to reevaluate your network management. Consider whether this is a good time to move to cloud-based management to enable effortless upgrades and access to the latest innovations so that your team can focus on running the network, not running the network management system. Also consider how AI can help your team become more effective.

## Checklist for Wi-Fi 7 & private 5G

- ✓ **Wi-Fi + private 5G:** Single vendor solution for Wi-Fi and private 5G to serve a wide range of use cases from high-density indoor connectivity to IoT support, to wide area coverage outdoors, to high-speed mobility.
- ✓ **AI-powered:** Insights and recommendations based on a large data lake and 95%+ level of certainty to streamline routine tasks and optimize network performance and reliability.
- ✓ **IoT platform support:** Support for large numbers of IoT devices that connect through Wi-Fi, Bluetooth, Zigbee, and USB ports that avoid the need for overlay networks and add the ability to process IoT data at the edge.
- ✓ **Traffic segmentation:** Detection and dynamic segmentation of users and malicious IoT devices to address headless device security threats, plus role-based access control based on application, device, or location.
- ✓ **Ease of use:** Operator-centric interface that makes it easier to onboard new IT professionals and to go back in time to investigate complex problems.
- ✓ **Broad portfolio:** Wide range of access points and small cell radios to support indoor, outdoor, ruggedized, and hospitality use cases and APs that have been Wi-Fi certified to ensure interoperability.
- ✓ **Unified management:** Wireless infrastructure with network switches and SD-WAN gateways provide uniform visibility and control that drives greater operational efficiency and end-to-end network optimization.
- ✓ **Scalability:** Wi-Fi and private 5G that is highly scalable to support hundreds of thousands of devices that can grow as your business grows to support future requirements, including AI.
- ✓ **Mobility access switching:** With ever expanding AI, IoT, and wireless requirements, a wide range of intelligent, high-performance switches to optimize connectivity.
- ✓ **Global support and services:** Both direct and through partners with an award-winning Partner Advantage Program.



Learn more about [wireless solutions](#) from HPE Aruba Networking.

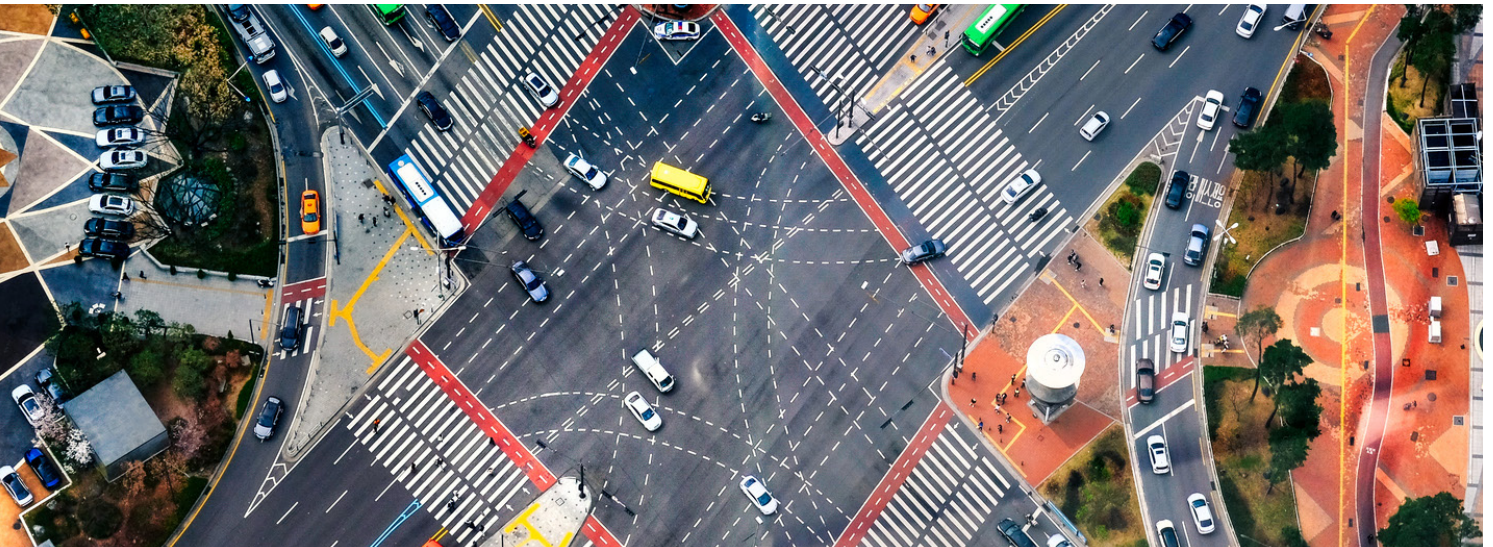
Visit [HPE.com](#)

## HPE Aruba Networking solutions

HPE Aruba Networking delivers Wi-Fi and private 5G to provide pervasive connectivity for even the most demanding use cases. We have been recognized as a leader in the Gartner® Magic Quadrant® for Enterprise Wired and Wireless LAN Infrastructure 18 consecutive times for our innovation and ability to execute. Our Wi-Fi 7 and Wi-Fi 6E access point portfolio spans indoor, outdoor, ruggedized, and hospitality form factors, all backed by a limited lifetime warranty and certified by the Wi-Fi Alliance. They are the only APs to use ultra triband filtering to eliminate interference and unlock up to 30% more channels for faster speeds and lower latency. Enterprises can take advantage

of HPE Aruba Networking private 5G to augment their existing Wi-Fi deployments for wider area coverage, high-speed mobility, and predictable QoS for mission-critical applications. Our end-to-end private 5G solution simplifies the purchasing, deployment, and management of private cellular and can be managed by IT teams the same way that they manage their Wi-Fi networks today.

HPE Aruba Networking Central, our security-first, AI-powered network management solution, has been significantly enhanced with more AI generated insights, simplified device configuration workflows and APIs, and third-party network device monitoring capabilities built upon a refreshed user interface that delivers class-leading AI-powered network automation and observability.



### [Chat now](#)

© Copyright 2025 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.

Bluetooth is a trademark owned by its proprietor and used by Hewlett Packard Enterprise under license. All third-party marks are property of their respective owners.

a00142500ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

