

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure



Note: This document is based on the Gartner *Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure (March 2024)* and has been updated to reflect major industry developments through July 2026, including the completion of Hewlett Packard Enterprise's acquisition of Juniper Networks.

Automation, security and migration strategies are the primary drivers for infrastructure strategies as the market continues to move away from hardware. I&O leaders must use this research to deliver wired and wireless infrastructure to their campus, branch and remote-office environments.

Strategic Planning Assumption

Through at least 2026, over 70% of wireless local-area network (WLAN) deployments will lack a tangible use case for organizations to deploy Wi-Fi 7, as most business applications do not require the enhanced capabilities of the new standard.

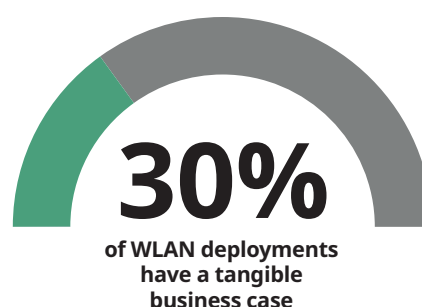
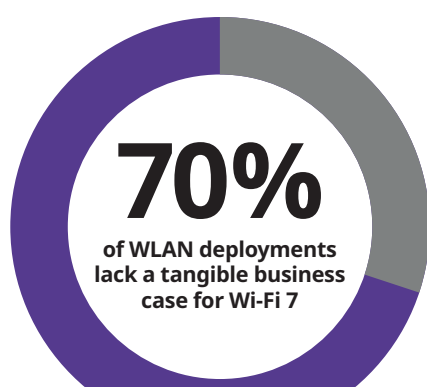
By 2027, 70% of enterprises refreshing and/or expanding their WLAN will upgrade to Wi-Fi 7, due to future proofing aspirations and vendor push combined with aggressive product marketing.

THE WIFI 7 ADOPTION GAP

**Most organisations don't need Wi-Fi 7 today –
but most will buy it anyway.**

THROUGH 2026

TODAY'S EARLY ADOPTERS



Source: Gartner Strategic Planning Assumptions, March 2024



2027

70% of enterprises refreshing and/or expanding their WLAN will upgrade to Wi-Fi 7

Market Definition/Description

This document was revised on 11 March 2024. The document you are viewing is the corrected version.

Gartner defines the enterprise wired and wireless LAN infrastructure market as wired and wireless networking hardware and the related network software. Related components of the solution include enterprise switches, access points and the requisite tools to secure, manage, test and optimize the network infrastructure that provides connectivity for users, devices and applications that may reside on the network or on other networks.

Enterprises in all vertical markets use enterprise wired and wireless networks to connect and transport data for fixed and end-user devices to applications that may be local or remote to the physical end user. In addition to physical connectivity, these solutions provide the following capabilities in diverse markets, including the ability to:

- Discover, identify, secure, manage and segment Internet of Things (IoT)/operational technology (OT) devices
- Support, test and maintain network infrastructure components
- Provide a resilience infrastructure
- Secure the network infrastructure
- Provide scalability and flexibility for management and control plane communication processes
- Provide no-touch/low-touch Day 2 environment

The must-have capabilities of this market include:

- IEEE 802.11 Wi-Fi-certified access points that support 2.4GHz, 5GHz and 6GHz.
- Ethernet network switches suitable for deployment at the network access, distribution and core network layers.
- Wi-Fi process control and management plane functionality placed on a physical appliance, virtual machine, which can be located at the edge, in the data centre or cloud-based.
- A network management application.
- Secured and managed third-party devices on the network.
- Security for device authentication and authorization, such as 802.1X.
- Security policy enforcement application.
- A wired and wireless intrusion detection.
- Telemetry for troubleshooting and optimization of the network.

The standard capabilities for this market include:

- Access points that support indoor and outdoor environments with optional external antennas and that support Wi-Fi 5, 6 and 6E certifications.
- The ability to provide Power over Ethernet (PoE) to all components.
- A guest access portal that allows for guests to be directed outside of the firewall for internet connectivity.
- The ability to view network analytics for the end users and applications they use on their devices.
- A network fabric that can create dedicated channels of communication across the end-user connection to its destination that are governed by a policy. The fabric should be able to extend across competitive equipment (i.e., access points and switches).
- Network monitoring, such as user and entity behaviour analytics (UEBA), that can be integrated with the network security policy to take that appropriate action.
- The ability to collect and export telemetry data that allow AI-native networking, AIOps and Agentic AI network assurance tools to troubleshoot and optimize the network.
- The ability to detect and report configuration drift.
- The ability to discover, identify, secure and manage non-user devices (IoT/OT).
- Application visibility and/or performance management.
- The ability to manage through exported API, Simple Network Management Protocol (SNMP) and other methods of legacy competitive access points and switches.

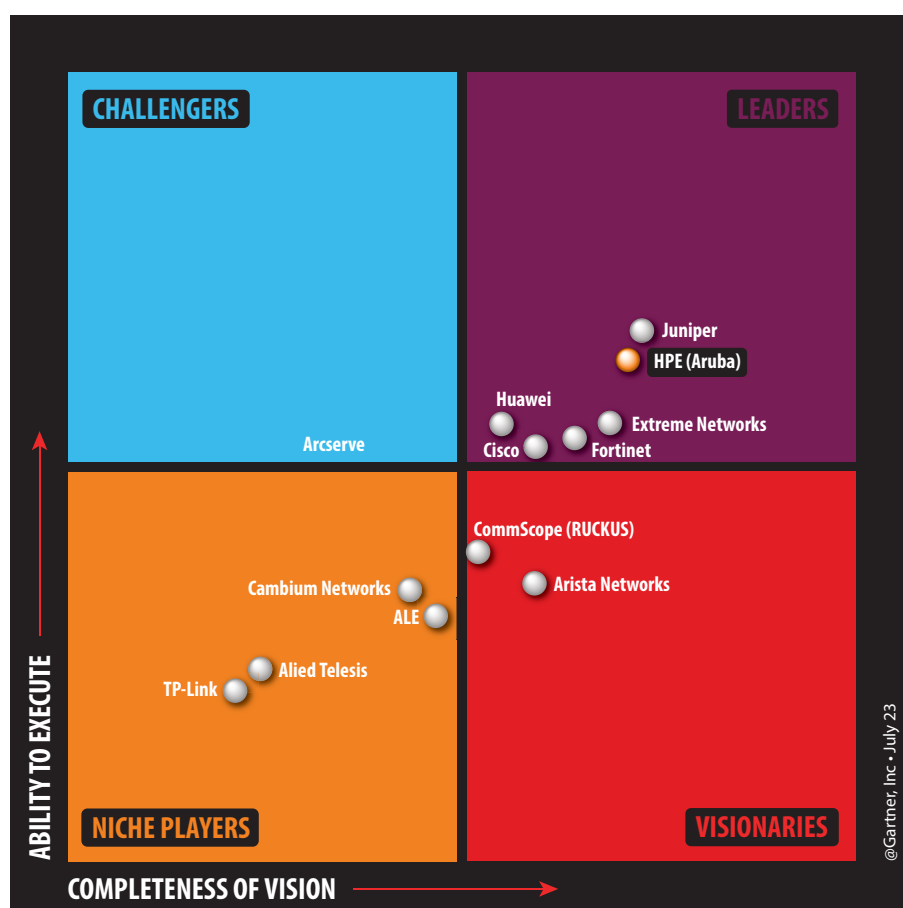
It is important to note that this research is not inclusive of wired and wireless networking infrastructure devices that are primarily used to support adjacent markets, such as point-to-point WAN offerings.

Optional capabilities for this market include:

- Indoor location services
- Natural language troubleshooting interface
- Consumption-based pricing models (NaaS)
- Ability to collect and use telemetry data from competitive access points and switches
- Integration with ITSM applications, including ticketing
- Private/public 5G integration and offloading
- The ability to apply full zero trust principles to all connected users and devices

Magic Quadrant

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure



Vendor Strengths and Cautions



Alcatel-Lucent Enterprise (ALE) is a Niche Player in this Magic Quadrant. Its OmniSwitch switches, OmniAccess Stellar wireless access points and OmniVista management products broadly address the enterprise network market. ALE's portfolio includes on-premises and cloud-native management options with network fabric segmentation and universal network policy for IT and IoT provisioning. The company prioritizes the mid-size enterprise (MSE) business market segment, and its clients are primarily in the government, healthcare and transportation verticals. Gartner expects ALE to continue investing organically in software capabilities for network security, visibility and assurance, with inorganic investment in vendor technology partnerships to continue filling out solutions for the portfolio offering.

Strengths

- **Campus networking fabric:** Clients in ALE's key target verticals (government, healthcare, transportation and education) looking for simplified management and streamlined automation will benefit from ALE's fabric architecture and industry-specific expertise.
- **Universal network policy – UPAM/NAC:** ALE's Intelligent Fabric and OmniVista management solutions include onboarding, segmentation and secure policy provisioning across the wired and wireless network edge for customers with IT, IoT and OT requirements.
- **Technology partnerships and solutions:** ALE has strong partnerships for SASE solutions, SSE cloud-native security solutions, and video management systems to provide customers with extensible systems.

Considerations

- **Lack of parity between cloud and on-premises offerings:** OmniVista 2500 Network Manager System and OmniVista Cirrus do not ship with feature parity. ALE plans continued investment in development, however, customers must ensure that the required functionality is available in their preferred deployment model today..
- **Limited AIOps functionality:** ALE is trailing leaders in this research for advanced visibility and assurance functions. The OmniVista Network Advisor, and separate Rainbow collaboration platform, have limited use-case outputs and autoremediation. Customers are advised to test functionality as part of a proof of concept before buying.
- **NaaS product offering:** ALE offers a buying model for customers that includes some capex in the initial purchase. This product offering doesn't not meet Gartner's definition for NaaS; however, it may appeal to buyers that seek some reduction in initial capital outlay.



Allied Telesis is a Niche Player in this Magic Quadrant. The company has a broad switching portfolio led by the x9x0 series switches and a WLAN offering that can address most use cases, but is currently missing a Wi-Fi 6E model. The portfolio is governed by Vista Manager EX, the Autonomous Management Framework Plus (AMF Plus), the AMF-Security Controller and the Autonomous Wave Control (AWC) wireless controller. Allied Telesis focuses on customers in the healthcare, education, government and healthcare sectors, and its operations are geographically diverse. Gartner expects Allied Telesis to start adding AI-native networking, AIOps and Agentic AI analytics to its network management solution in 2024, to ease off network operations with features such as guided troubleshooting.

Strengths

- **Enterprise-grade network management features:** AMF Plus and the AMF Security Controller are optional add-ons to Vista Manager EX, resulting in a breadth of features that include quality of service (QoS) traffic prioritization, endpoint policy enforcement and malware protection.
- **Multi-vendor management:** AMF Plus provides support for third-party network devices, simplifying the administration of wired and wireless infrastructure.
- **Unified operating system:** Allied Telesis has a single OS, AlliedWare Plus, which eases management and configuration capabilities across all products, including routers and firewalls.

Considerations

- **Lack of network fabric:** Allied Telesis lacks a native network fabric, which limits segmentation and policy enforcement and may require a partner product.
- **Lack of AIOps features:** Allied Telesis does not yet have AI-native networking, AIOps and Agentic AI analytics for network assurance services, such as root cause analysis of issues arising from baselined application performance, guided troubleshooting and a natural language interface.
- **Limited market visibility:** Allied Telesis has limited wired and wireless LAN market visibility among customers and prospects outside of Japan, based on end-user Gartner interactions, gartner.com searches and social media conversations.

ARISTA

Arista Networks is a Visionary in this Magic Quadrant. The company addresses the enterprise networking market with its 700 series leaf switches and 7000 series enterprise spine switches; Cognitive Wi-Fi access points that include Wi-Fi 6E; and its CloudVision management platform. Most of Arista's customers are located in North America and are in the financial, healthcare and higher education sectors. Gartner expects Arista to continue to invest in its CloudVision integrated security and AI-native networking, AIOps and Agentic AI capabilities, with functionality further extending to the data centre. This architecture expansion will aim to deliver proactive network performance monitoring, application visibility and policy enforcement across the campus, WAN and data centre.

Strengths

- **Network management tools that simplify operations:** Arista's CloudVision platform is unified for both campus and data centre management; it also supports digital twin capabilities for testing and validation of configuration/connectivity changes to the campus network.
- **Differentiated network security strategy:** Arista is one of the few vendors in this research with a NDR offering for advanced threat detection and incident response use cases. The launch of CloudVision Arista Guardian for Network Identity (AGNI) in 2Q23, a NAC product, adds risk and behaviour assessment of endpoints.
- **AI-native networking, AIOps and Agentic AI capabilities:** Arista's CloudVision AIOps includes the Autonomous Virtual Assist (AVA) platform for natural language processing, in addition to automated trouble ticketing, incident severity classification and issue remediation, and predictive analytics.

Considerations

- **Limited exposure outside its data centre customer base:** Arista's strategy targets its data centre customer base to grow its campus networking business, limiting market visibility, especially in the mid-market.
- **Price premiums:** Arista's campus switching portfolio, predominantly targeted at large enterprises, has a price premium. Measured in the average revenue per port, it is among the highest in the industry.
- **Limited exposure outside North America:** This region accounted for more than 60% of Arista's wired and wireless LAN revenue in 2023. Organisations considering Arista should verify product and service availability in their geography.



Cambium Networks is a Niche Player in this Magic Quadrant. Cambium's ONE Network solution addresses the enterprise market with wired switches (via its cnMatrix product line) and access points with software-defined radios. cnMaestro X manages the entire Cambium product family. Cambium focuses on customers in the hospitality, education, government and healthcare sectors, and its operations are geographically diverse. Gartner expects Cambium to enhance its ePSK technology for simplified device onboarding, including IoT endpoints, and to continue to invest in its AIOps capabilities.

Strengths

- **Broadened network management capabilities:** Cambium's recently introduced Network Service Edge (NSE) solution extends cnMaestro's network management to include SD-WAN, network security and outdoor fixed wireless.
- **Cambium's 'assists' feature:** This application provides a security auditing capability that continually scans the network, and reports and provides resolution of misconfigured products, as well as identification of the potential risk.
- **Flexible software-defined radios:** The software-defined radios in Cambium's access points allow for enterprises to change the radio frequencies (2.4 GHz, 5 GHz or 6 GHz). Up to five radios can be configured for high-density requirements or for the need to simultaneously support different WLAN installations.

Considerations

- **Fragmented IoT segmentation capabilities:** NSE supports segmentation of wired IoT endpoints, while cnMaestro X leverages Cambium's ePSK technology for wireless IoT onboarding. Additionally, Cambium does not have a campus fabric, limiting its ability to segment devices as a unified construct to the access layer, with no support of VXLAN.
- **Limited enterprise vertical exposure:** Cambium has limited visibility in the enterprise space outside the hospitality, education and healthcare verticals. Cambium's exposure at deployment scales above MSE is also very limited.
- **Lack of modular chassis switch:** This portfolio gap prevents Cambium from adequately addressing high-density access or high-speed core/distribution use cases, in which a common high-speed backplane and redundant management and power supplies in a single chassis are highly desirable.



Cisco is a Leader in this Magic Quadrant. Its Catalyst and Meraki products deliver a broad portfolio of wired and wireless access products, network applications and services. Its operations are geographically diversified, and Cisco services clients in all markets, from small and mid-size businesses (SMBs) to large enterprises. Cisco's vision for Networking Cloud is to unify the on-premises catalyst hardware with the simplicity of the cloud-based Meraki management to deliver flexible options for its customers. Gartner expects Cisco will continue to invest in its on-premises management (DNA Centre, now Catalyst Centre), NAC (Identity Services Engine [ISE]), and SDA Fabric solutions as they strive to achieve use-case parity and experience consistency across the two portfolios.

Strengths

- **Portfolio breadth:** The scope of Cisco's wired and wireless hardware and software product portfolio addresses use cases across market verticals, business organizations of all sizes and network deployment scenarios of any type.
- **Advanced network assurance:** Cisco's integration of ThousandEyes throughout the portfolio, along with its deep relationship with device vendors (Apple, Intel, Samsung), is delivering real-world insights for IT and security operational use cases.
- **Geographic reach:** Cisco's extensive global reach within direct and indirect sales channels positions it as a campus networking vendor capable of delivering and supporting effective solutions to clients worldwide.

Considerations

- **Rising prices:** Cisco customers cite high prices to obtain, refresh and maintain Cisco wired and wireless infrastructure.
- **On-premises and cloud lack parity:** Cisco buyers must make a decision on the management solution they intend to deploy – Meraki in the cloud, or Catalyst Centre on-premises. Differences in solutions create a buying gap for key generative AI, AIOps and security analytics features.
- **Security portfolio decision:** Cisco's vast security portfolio creates buyer confusion, with an increase in the total cost of ownership (TCO), as customers choose from optional software components such as XDR, ISE, Umbrella and Secure Network Analytics.



RUCKUS Networks, owned by CommScope, is a Visionary in this Magic Quadrant. The company addresses the market with its RUCKUS brand ICX wired switches, R series wireless access points and RUCKUS One – its network management and AI Ops platform. RUCKUS operates globally and focuses primarily on the federal, state and local government segments of the enterprise network market, as well as the education segment. Gartner expects that RUCKUS will continue to invest in the AI Ops capabilities of its RUCKUS One platform, its network security and segmentation capabilities, and in expanding its integration with WAN edge capabilities.

Strengths

- **Network management with AI Ops features:** The RUCKUS One platform has several strong capabilities, including network assurance services, profiling and policy enforcement of endpoints (including IoT), and digital twin features for testing and validation of Wi-Fi upgrades.
- **Detailed root cause analysis tools:** RUCKUS AI, the AI engine of RUCKUS One, offers detailed analysis across the wired and wireless network. Users can see the root cause assessment data and apply resolution suggestions.
- **Security strategy:** RUCKUS One comes with integrated NAC functionality at no extra cost, and the RUCKUS WAN Gateway provides network services such as micro-segmentation, DNS and fire-walling to switches and WLAN access points.

Considerations

- **Limited experience in large complex network requirements:** RUCKUS has limited experience in large enterprise network environments, especially in complex core layer network deployments.
- **Digital twin functionality gaps:** RUCKUS One does not support the verification of switching network configurations in a virtual testing environment, since its digital twin capabilities are limited to wireless.
- **Lack of modular chassis switch:** This portfolio gap prevents RUCKUS from adequately addressing high-density access or high-speed core/distribution use cases, in which a common high-speed backplane and redundant management and power supplies in a single chassis are highly desirable.



Extreme Networks is a Leader in this Magic Quadrant. Extreme Network's Infinite Enterprise portfolio ties wired, wireless and SD-WAN products together into a single end-to-end solution underpinned by Extreme Fabric, a zero touch, automated network fabric. This fabric is managed by a unified management platform available in the cloud or on-premises. Extreme's operations are geographically diversified and the company services clients in all markets, from SMBs to large enterprises, with a specific focus on state and local government, education, healthcare, manufacturing, and retail. Gartner expects Extreme Networks to continue to invest in its ExtremeCloud IQ CoPilot AI capabilities, as well as cloud-native universal ZTNA, fabric innovation and digital twin initiatives.

Strengths

- **Zero touch network fabric:** Extreme Networks has continued investment in Extreme Fabric, its single secure end-to-end fabric technology. Zero touch provisioning and automation reduces the deployment burden for customers.
- **Universal licensing:** Extreme's universal licensing gives the customer a flexible licensing approach. Licenses are not tied to specific hardware and can be moved from one device to another, irrespective of device type. The licenses are tied to the network.
- **Third-party network management:** Multi-vendor integration streamlines deployment into brownfield environments. Configuration, firmware updates, backups, alarms and events can all be handled by ExtremeCloud IQ.

Considerations

- **Global reach challenges:** Extreme Networks has gaps in its presence in regions such as Asia and Latin America.
- **Pricing:** Extreme Networks' pricing for switches is higher compared to most vendors in this research, based on our market statistics that measure the average revenue per port (after discount).
- **No NaaS offering:** Extreme does not directly offer a consumption-based NaaS offering, with pricing delivered on a pay-for-use basis or as a subscription based on usage metrics.



Fortinet is a Leader in this Magic Quadrant. The Fortinet Security Fabric, unified by FortiOS, allows extremely tight integration between its wired and wireless products. Through its proprietary FortiLink protocol, FortiAPs and FortiSwitches can become an extension of the FortiGate security appliance. Fortinet's operations are geographically diversified, and its clients range from MSEs to large enterprises across various sectors. Gartner expects Fortinet to continue to invest in its network AIOps capabilities, including incorporating enhanced third-party management and network performance monitoring. We also expect Fortinet to improve its threat detection capabilities through correlation and user and entity behaviour analytics (UEBA) at the network level.

Strengths

- **Differentiated LAN offering with a strong security focus:** Fortinet delivers an architecture in which wired, wireless and security are integrated under a single unified operating system (FortiOS) and cloud-native management platform.
- **Dedicated AI operations module:** The FortiAIOps AI engine provides network assurance (event correlation and issue re-mediation) across security, wired and wireless by leveraging data feeds from the FortiGate portfolio.
- **Effective microbranch solution:** Fortinet has a well-thought-out solution for microbranch sites. The solution allows FortiAP to act as an endpoint for Unified SASE. Unified SASE, together with digital experience monitoring (DEM), provides converged access for a hybrid workforce.

Considerations

- **Lagging influence with security buyers:** Most of Fortinet's firewall customer base deploys switches and WLAN products from a competitor, since security and networking are commonly separate buyer centres. Fortinet's revenue market share in campus networking is almost 10 times smaller than that in the firewall market.
- **Multiple management interfaces:** Fortinet has several management options: FortiGate manager, FortiManager (on-premises and cloud), FortiLAN and FortiMonitor, which are used to manage the different deployment architectures. This can result in a confusing mix of management options.
- **Lack of modular chassis switch:** This portfolio gap prevents Fortinet from adequately addressing high-density access or high-speed core/distribution use cases, in which a common high-speed backplane and redundant management and power supplies in a single chassis are highly desirable.



HPE Aruba Networking

HPE Networking (HPE) continues to be recognised as a Leader in enterprise wired and wireless networking. Building on the strengths of the HPE Aruba Networking Edge Services Platform (ESP), HPE Networking now offers an expanded AI-native networking portfolio following the completion of its acquisition of Juniper Networks on 2 July 2025. The combined organisation brings together Aruba's enterprise networking expertise with Juniper's AI-driven Mist platform, creating one of the industry's most comprehensive networking portfolios spanning campus, branch, data centre, WAN and security.

Aruba Central remains HPE Networking's flagship cloud-native network management platform for Aruba deployments, while HPE Networking is actively converging Aruba Central and Juniper Mist through shared AI services, common cloud microservices and a unified AI-native networking strategy.

Operating globally, HPE Networking serves organisations of all sizes, from small and medium-sized businesses to the largest enterprises. The acquisition of Juniper significantly expands HPE's market presence, doubles the size of its networking business, and strengthens its position in AI-native networking, Zero Trust security and cloud-delivered network management.

Strengths

- **Comprehensive AI-native networking portfolio:** The combination of Aruba ESP and Juniper Mist delivers a market-leading portfolio across wired, wireless, SD-WAN, data centre networking and AI-driven operations, enabling simplified management and enhanced user experiences.
- **Campus fabric and Zero Trust security:** Aruba ESP continues to provide automated, secure wired and wireless networking with integrated device onboarding, policy enforcement, network segmentation and UEBA capabilities that support Zero Trust architectures.
- **Advanced AIOps and automation:** Aruba Central includes AI-powered network assurance, proactive monitoring and automated troubleshooting within its standard licensing model. Ongoing integration with Juniper's Mist AI and Marvis technologies further enhances predictive operations, natural language interactions and autonomous network management.
- **Innovative switching platform:** Aruba's switching portfolio continues to differentiate itself through capabilities such as In-Service Software Upgrades (ISSU) for switch stacks, Layer 7 application visibility and policy enforcement at the network edge.
- **Broad cloud and consumption offerings:** HPE continues to expand its Network-as-a-Service (NaaS) capabilities through HPE GreenLake, providing flexible consumption models alongside integrated networking, security and infrastructure services.
- **Unified networking strategy:** HPE's acquisition of Juniper significantly expands its networking capabilities by combining Aruba ESP with Juniper Mist AI, enabling customers to adopt a common AI-native architecture across campus, branch, WAN and data centre environments.

Considerations

- **Platform convergence:** While HPE has announced a unified networking strategy, Aruba Central and Juniper Mist continue to evolve toward greater integration. Organisations should understand the roadmap for management platforms and feature alignment when planning long-term investments.

Customers with existing Aruba Central or Juniper Mist deployments should understand HPE's published migration and platform convergence roadmap before making long-term architectural decisions.

- **Multiple management options:** Customers with mixed Aruba, Juniper and legacy deployments may encounter multiple management platforms during the transition period. HPE has committed to convergence, but organisations should evaluate which platform best aligns with their operational requirements.
- **Licensing complexity:** The expanding portfolio introduces a broader range of licensing and consumption options across Aruba Central, Juniper Mist and HPE GreenLake. Buyers should carefully assess licensing models and total cost of ownership to ensure they select the most appropriate solution for their environment.

NOTE: Update (July 2026): Hewlett Packard Enterprise completed its acquisition of Juniper Networks on 2 July 2025. Product strategies, management platforms and AI capabilities referenced in this document should be considered in the context of HPE's unified networking roadmap announced following the acquisition.



Huawei is a Leader in this Magic Quadrant. Huawei's CloudCampus solution consists of CloudEngine S-series switches, AirEngine wireless APs and iMaster NCE applications that are broadly focused on addressing a wide range of use cases. Huawei's operations are globally diverse, with clients across multiple verticals and significant growth in Europe, the Middle East and Africa. However, geopolitical issues cause Huawei to have virtually no presence in North America and limited penetration in a few other countries, such as Australia and the U.K., where it ceased operations of its own accord. Huawei has continued to invest in its Wi-Fi 7 portfolio and antenna technology, and in its network assurance capabilities for high-quality user experience in popular audio and video applications.

Strengths

- **Strong product portfolio:** Huawei has a robust wired and wireless product portfolio that continuously monitors connectivity to increase performance and stability.
- **Experience-centric network configuration and management:** The iMaster NCE-Campus network management platform provides experience-centric wired and wireless LAN service quality and network assurance services.
- **Simplified architecture for OT to IT migration:** Huawei has introduced a converged campus network architecture that integrates OT capabilities into traditional enterprise products and simplifies the migration of OT to IT.

Considerations

- **Global sales reach challenges:** Huawei continues to have ongoing geopolitical issues that limit Huawei's exposure in some geographies and vertical markets. Its presence in North America, the U.K. and Australia is limited.
- **Limited market messaging:** Compared to other vendors in the market, Huawei marketing focuses on its technical capabilities and less on client business values and issues.
- **No NaaS offering:** Huawei does not have a NaaS offering, with pricing delivered on a pay-for-use basis or as a subscription based on usage metrics.



Since the publication of this research, Juniper Networks became part of Hewlett Packard Enterprise on 2 July 2025. Juniper's Mist AI platform, AI-driven operations, Campus Fabric and cloud-native networking capabilities are now part of HPE Networking's unified networking strategy. HPE Networking has announced plans to converge Aruba and Mist through shared AI services, common cloud microservices and unified networking innovation while maintaining investment in both product families during the transition period.

Strengths

- **AI-driven automation:** Juniper leads with AI-native networking, AIOps and Agentic AI capabilities, including performance monitoring based on customizable SLEs, to deliver improved end-user experience. Guided troubleshooting and the ability to automatically fix routine issues simplify network operations.
- **Strong security:** Juniper's WxLAN framework provides network wide policy enforcement for users and IoT endpoints, and the recently introduced Juniper Mist Access Assurance service further provides agentless NAC capabilities.
- **Simplified network management with fabric technology:** Juniper's Campus Fabric, based on a VXLAN overlay with an EVPN control plane, can ease campus and branch management of Juniper devices by reducing network complexity and deployment inconsistencies.

Considerations

- **Cloud-dependent management platform:** While Mist Edge handles some network functions on-premises, to get the most value (e.g., access to real-time statistics and device updates) it requires a connection to the Mist Cloud. The legacy Junos Space Network Management Platform lags functionality as a fully centralized (on-premises) alternative.
- **Campus fabric lacks third-party support:** While Juniper's fabric is built on a standards-based EVPN-VXLAN architecture and interoperates with third-party infrastructure, it does not manage third-party network devices natively.
- **Limited customer traction of NaaS solution:** Juniper has announced its NaaS offering, but Gartner barely sees it come up during inquiry.



TP-Link is a Niche Player in this Magic Quadrant. Its Omada, Omada Pro and associated network software products mainly focus on addressing the needs of the small and mid-size enterprises (SMEs). Its operations are geographically diversified, with the bulk of its revenue generated from EMEA, followed by Asia/Pacific and North America. Gartner expects that TP-Link will continue to invest in SME customers' requirements for ease of configuration and operations by adding to the capabilities of its GUI web-based configuration and cloud management platforms.

Strengths

- **Scalable network management offering:** The Omada network management offering is bundled with its access network hardware, which provides unified monitoring for an unlimited number of TP-Link APs, campus switches and security gateway products.
- **Wi-Fi 6 and 7 portfolio:** TP-Link offers a comprehensive portfolio of enterprise Wi-Fi 6 and Wi-Fi 7 access points, all supported by advanced RF optimisation features that enhance wireless performance, improve client experience and simplify network troubleshooting. The company has significantly expanded its Wi-Fi 7 portfolio, providing solutions for a wide range of enterprise deployments. These access points are managed through the Omada platform, enabling centralised cloud or on-premises management, AI-assisted optimisation and consistent policy enforcement across wired and wireless environments.
- **Competitive pricing:** TP-Link's pricing is among the lowest of its competitors, which aligns with the needs of most MSEs. More broadly, this strategy is particularly attractive to organizations with basic network connectivity needs and where cost is the primary determinant.

Considerations

- **Lack of enterprise focus on software innovation:** Despite products that meet all traditional levels of enterprise network technology, TP-Link lags behind other vendors in its support of advanced network operations technologies, such as network assurance, automation and AIOps functionality.
- **Basic network security and location features:** TP-Link provides only basic network policy enforcement, and limited IoT containment and indoor location services.
- **Limited product capabilities:** TP-Link's enterprise network portfolio lags the competition, with limited AI-native networking, AIOps and Agentic AI capabilities. Additionally, TP-Link's portfolio lacks support for next-generation networking features such as network fabrics, leaf-spine topologies and dynamic segmentation.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Allied Telesis was added to this Magic Quadrant.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

For Gartner clients, Magic Quadrant and Critical Capabilities research identifies and then analyses the most relevant providers and their products in a market. Gartner uses by default an upper limit of 20 providers to support the identification of the most relevant providers in a market. On some specific occasions, the upper limit may be extended by Methodologies where the intended research value to our clients might otherwise be diminished. The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, providers must:

- Demonstrate relevance to Gartner clients in the wired and wireless networking market by offering an Ethernet switching and wireless LAN (Wi-Fi) hardware portfolio that minimally addresses the "must-have" capabilities identified in the market definition.
- Produce or OEM networking products that provide mechanical and/or virtual stackable wired networking for general availability as of 31 July 2023. All components must be publicly available for purchase, exist in inventory, be available for shipping and be included on the vendor's publicly published price list. Products shipping after this date will only have an influence on the Completeness of Vision axis.
- Vendors are required to meet one of the following (reported as constant currency):
 - At least \$200 million in annual revenue and have at least 200 customers that use its enterprise wired and wireless LAN solution in the twelve months from 1 July 2022 to 1 July 2023, where "customer" is defined (per Gartner Methodologies) as a net new installed logo that has paid for the equipment and/or is additionally paying (for subscription services), depending on the purchasing model.
 - At least \$10 million in revenue in the twelve months from 1 July 2022 to 1 July 2023, and 50% growth compared to the previous 12 months.
- Have a cloud- and on-premises-capable network discovery, identification, configuration, security, management, and monitoring platform that includes integrated network automation tools.

- Offer integrated network security tools that offer, at a minimum, device and user segmentation, with specific re-mediation for guest users/devices and IoT devices.
- Have no more than 70% of revenue generated in a single region (of the seven regions mentioned below).
- Have customers in at least four of the seven global regional sales (APAC/Japan, North America, South America, Western Europe, Eastern Europe, Middle East, Africa).

HONOURABLE MENTIONS

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on their ability to deliver products or services that meet the requirements of the market. We also evaluate the vendor's ability to articulate differentiation and core competencies in their market message and the receptivity of the market. As a more mature market, criteria such as operations are not rated because we feel that it does not affect the ability of vendors to deliver solutions to the market, compared to the other criteria.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Low
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	High
Customer Experience	Medium
Operations	NotRated

Source: Gartner (March 2024)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to communicate that they understand client business issues in their target markets and have the products, services, vision and strategies to address these issues.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Low

Source: Gartner (March 2024)

Quadrant Descriptions

Leaders

A vendor in the Leaders quadrant will have demonstrated an ability to fulfil a broad variety of customer requirements through the breadth of its enterprise network product family. Leaders will have the ability to shape the market and provide complete and differentiating enterprise network applications, as well as global service and support. Leaders should have demonstrated the ability to maintain strong relationships with their channels and customers, and have limited gaps in their portfolios or are very strong in specific areas.

Challengers

A vendor in the Challengers quadrant demonstrates sustained execution in the marketplace. It will have clear and long-term viability in the market, but may not have a complete enterprise network portfolio for either products or network applications. Additionally, Challengers may not have shown the ability to shape and transform the market with differentiating innovation or functionality, or have the ability to serve a broad, global customer base.

Visionaries

A vendor in the Visionaries quadrant demonstrates an ability to increase features in its offering to provide a unique and differentiated approach to the market. A Visionary will have innovated in one or more of the key areas of enterprise network technologies (for example, security, management or operational efficiency). The ability to apply differentiating functionality across an entire enterprise network infrastructure will affect its position.

Niche Players

A vendor in the Niche Players quadrant demonstrates a near-complete product offering. However, it may not be able to control development or provide differentiating functionality because it relies on a strategic partner to offer part of the offering, whether it is a hardware component or a network application. Niche Players may also lack strong go-to-market capabilities that would enhance their regional or global reach or service capabilities in their product offerings. Niche Players often have deep vertical knowledge and will be an appropriate choice for users in the specific vertical markets where they have specialized offerings and knowledge.

Context

Gartner's perspective on the enterprise wired and wireless LAN infrastructure marketplace emphasizes the continued and accelerating shift from merely providing foundational network connectivity to applications and technologies that address business issues such as technical debt, lack of IT resources and digital transformation. It also includes application performance, end-user experience and the overall support of business requirements across the entire network fabric. This market view is based on the preceding 12-month time period ending August 2023.

Gartner's research indicates that investments in campus-switching products have slowed down in the past year, with global port shipments registering a decline of 1% in the period 1Q23 through 3Q23, year over year (see Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 3Q23). Worldwide unit shipments of WLAN APs, however, increased by 10%. This indicates that organizations continue to "rightsize" investments in wired infrastructure, while favouring a more aggressive push to Wi-Fi connectivity. The increase in work-from-anywhere initiatives is creating opportunities for enterprises to reduce their footprint of switching and cabling infrastructure, since Wi-Fi connectivity better suits flexible office space arrangements.

From a global market revenue perspective, campus switching grew 31% and WLAN 27% in the period 1Q23 through 3Q23, year over year, hence significantly outpacing shipment growth. This was predominantly due to price increases, as a result of the supply issues that have been impacting the market since late 2021. Most vendors have raised their pricing to counterbalance higher component and freight costs, albeit these increases have also impacted software licensing. The outlook for 2024 is that of supply conditions continuing to improve, as most vendors have voiced, allowing them to carry on releasing backlog as inventory levels normalize. While it is unlikely that vendors will reduce their pricing in the next 12 months as supply conditions stabilize, today's economic environment will foster more aggressive price

competition. The value proposition of more attractive lead times has begun to slowly fade away as a differentiator, and we expect will force vendors to more aggressive discounts.

Even though core connectivity technologies are also driving network refresh projects, the most visible of the connection-oriented technologies is Wi-Fi 6 (802.11ax), which operates at 2.4 and 5 GHz, and Wi-Fi 6e (802.11ax; 6 GHz), which is still a draft standard and operates in the less-crowded 6 GHz spectrum. It is important to note that the majority of contemporary end-user devices, such as laptops, tablets and smartphones, are still limited to 802.11ac and 802.11ax, and cannot use the 6 GHz spectrum.

Wi-Fi 6E APs accounted for 1.7 million units shipped in the period 1Q23 through 3Q23, equivalent to 6% of overall AP shipments. Wi-Fi 6E adoption is led by customer interest in the performance improvements from the newly allocated 6 GHz band, combined with future-proofing aspirations. We believe that some of these deployments have been influenced (and will continue to be, in the short term) by the supply issues affecting the market. Gartner has observed Wi-Fi 6E AP sales benefiting from shorter lead times. This is because Wi-Fi 6E APs have new semiconductor components, altering supply differently, and shipments only started to pick up at the end of 2022, limiting the impact on inventory levels. The arrival of Wi-Fi 7 will change many of these dynamics, diminishing the value proposition of Wi-Fi 6E.

The reliance on diverse suites of technologies to support digital business has placed significant emphasis on understanding application performance, user experience requirements and security postures across the entire network fabric. Disruptive network technologies that focus on application performance and end-user experience continue to drive the majority of innovations in the overall enterprise networking market.

What Has Changed?

Focus on Business Outcomes

AI-Native Networking: Since publication, enterprise networking has rapidly evolved beyond traditional AIOps toward AI-native operations incorporating generative AI, natural language assistants and autonomous remediation. Vendors now differentiate themselves through AI-driven operational efficiency rather than hardware capabilities alone.

Lack of Personnel and Skills Continue to Drive a Push to Automate

In the last couple of years, Gartner's Leadership Vision for Infrastructure and Operations survey has found that enterprises continue to have personnel shortages and skill deficiencies in their organizations. From client inquiries, enterprises are using automation to not only provision equipment and monitor but also to troubleshoot issues when the network functionality is not meeting defined service levels.

The widespread adoption of AI-assisted operations reflects continued skills shortages within IT organisations. Vendors increasingly offer natural language interfaces, predictive analytics and automated remediation to reduce operational overhead.

ZTNA Creates New Experiences

Remote clients are using the connectivity that is available, such as public internet, in conjunction with cloud-based zero trust network access (ZTNA) services to provide security, visibility and flexibility in an as-a-service model. This allows vendors to deliver the same offering in their on-premises campus and branch environments that they're using to secure connectivity to their remote employees. The result would be a single software offering, versus disparate offerings for campus and remote workers, with the goal to deliver a "coffee shop" network, whereby the user experience is: grab a seat, connect and work.

The convergence of networking and security continues through Secure Access Service Edge (SASE), Security Service Edge (SSE), Zero Trust Network Access (ZTNA) and AI-driven policy management. Vendors are increasingly delivering unified networking and security services through cloud-native platforms.

Market Overview

The enterprise wired and wireless LAN infrastructure market is now composed of vendors not only delivering wired and wireless Ethernet networking hardware, but also tightly integrating network management applications that reside on-premises or in the cloud. This combination of network hardware and powerful software is integral for addressing organizational mission agility, the need to automate, pervasive security and the increased levels of performance required by end users across all categories of connected applications and devices.

These integrated software tools speed time to completion for enterprise network deployments, reduce time to identify and resolve network and application issues, and deliver pervasive automation tools that reduce network administrator workloads.

Additionally, core integration of AI-native networking, AIOps and Agentic AI is integral to organizing the flood of telemetry data, thereby presenting key data points necessary to optimize the network in support of digital business requirements. This technology is also becoming a valuable source of business-relevant data that is useful to I&O and overall business leadership.

How Buyers Shape Their Buying Decisions

Traditional Network Technology Capabilities

Enterprise networking has been shaped by more than 30 years of primarily delivering connectivity and resiliency at Layer 2 and Layer 3 of the OSI network model. As a result, buyers expect robust traditional Layer 2 switching features, appropriate power over Ethernet to support VoIP and AP hardware, QoS, and sufficient uplink speeds to support various traffic requirements. At the wired access layer of the network, customers expect the Wi-Fi power, performance and throughput that is necessary to support the client connection densities and bandwidth requirements. Finally, the network core and distribution layers must deliver the redundancy and high-speed routing and switching capacity to support dramatically increased north-south traffic, much of which is destined for the cloud and other off-network locations.

Perpetual and Subscription License Pricing

Network hardware continues to be relatively commoditized, and true differentiation across vendors is reliant on the capabilities of network software features and functionality. However, as network vendors adopt the stance of software vendors, there are diminishing options for traditional perpetual licensing. Vendors realize new revenue streams by shifting to subscription-based licensing, but the shift is often confusing and continues to be a source of frustration for I&O leaders. Subscription licensing may make sense for some organizations. However, a preponderance of Gartner clients continue to express a preference for having a choice of licensing options, instead of being forced into licensing that is often inclusive of features they don't need.

AI-native networking, AIOps and Agentic AI

Enterprise network vendors now offer tools using various degrees of artificial intelligence, machine learning, a natural language interface, automatic issue identification, and remediation to reduce network administration and operational workloads. However, adoption of these essential toolsets in production environments is very slow. Initially, there were concerns about the maturity of the tools, as well as their ability to increase the productivity of network operations teams. As tools mature, there is less concern about their capabilities to operate in the production network environment.

AI capabilities have matured significantly beyond traditional AIOps. Enterprise networking vendors now provide AI copilots, conversational interfaces, autonomous troubleshooting, predictive optimisation and self-driving network operations. These capabilities have become primary differentiators in enterprise networking evaluations.



Management Suite

As managing technical debt is one of the top challenges that IT infrastructure and operations organizations face. Per the 2023 Gartner *I&O Leaders Signature Role Survey*, the ability to provide a migration strategy that includes managing the legacy solution, if applicable, is an important decision criterion. Clients have expressed through inquiry that they don't want two or three different management applications for their equipment. The mantra of a 'single pane of glass' extends to the entire campus environment.

Incumbency

Organizations tend to stay with their current enterprise network vendor if it offers a technology portfolio that is "good enough" to meet their needs and functions within reasonable expectations. Since the network market is relatively conservative and risk-averse, incumbent relationships often survive even when technology alignment is suboptimal. Clients that switch vendors tell us through inquiries that a significant difference in pricing from the average market price, especially on hardware such as access points and switches, will affect their decision to move to another vendor. Additionally, an often-unseen driver is the support that is received during the relationship. Clients who have bad support experiences, whether it is directly with the vendor or through a reseller, are often motivated to switch vendors.

How Providers Package, Market and Deliver

Traditional Consumption

Buyers generally source their wired and wireless LAN infrastructure through an authorized vendor channel partner, with relatively few purchases occurring directly from the network vendor. Hardware expenditures are usually a one-time cost, which is inclusive of a firmware end-user licensing agreement. These initial costs include updates to resolve certain firmware bugs that adversely affect the use of the hardware, or security vulnerabilities that would expose the end user to significant damage if left unpatched. Future operating system updates, feature upgrades or security patches are functions of a firmware maintenance contract that is purchased separately, either at the time of purchase or at a future date. Vendors charge for hardware and software licenses either as a perpetual license or as a subscription license but, as mentioned previously, the market is trending away from perpetual licensing.

Network management platforms have become ubiquitous, so access usually requires separate management licensing with various functionalities assigned to higher levels. However, some vendors offer enterprise networking solutions that are 100% reliant on the management platform for all functionalities. In such cases, the network management platform is included, and various security and/or feature license levels are offered.

Network as a Service

NaaS has slowly emerged in the enterprise networking market over the last 18 months. NaaS is based on a term subscription consumption model and includes deployment and managed services, flexible feature licensing and specific performance SLAs, and the vendor or partner maintains ownership of the equipment throughout the subscription period. True NaaS should present a transparent backbone infrastructure model, similar to cloud, thereby making the

ACRONYM KEY AND GLOSSARY TERMS

Evidence

1 2023 Gartner *I&O Leaders Signature Role Survey*: The survey was conducted to understand I&O organizations' burning issues and priorities, as well as to explore their current and planned services and talent management practices. The research was conducted online from June through July 2023. In total, 202 respondents were interviewed across the U.S. (n = 89), India (n = 46), the U.K. (n = 37) and Germany (n = 30). Qualifying organizations operated in multiple industries and reported enterprisewide revenue for fiscal year 2022 of at least \$50 million or equivalent. Qualified participants belonged to the functional areas of executive leadership and infrastructure and operations. All respondents led, participated or influenced strategies and investment decisions for infrastructure and operations. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

This research was informed by more than 1,500 client interactions in enterprise wired and wireless networking technologies from 2022 through 2023, data from vendor briefings, vendor surveys, vendor demos, Peer Insights, practitioner interviews and previously published Gartner research.

Note 1: Gartner's Definition of Network as a Service

NaaS is a standardized and highly automated delivery model for networking functionality. It offers support for dynamic scaling up and down of network resources. The NaaS vendor primarily owns and operates NaaS offerings. Pricing is on a pay-for-use basis or as a subscription based on use metrics.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the sub-criteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organisational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organisation and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Contact Centerprise International today and
discover how our expertise can help you.

centerprise.co.uk

SOURCE: GARTNER *MAGIC QUADRANT FOR ENTERPRISE WIRED AND WIRELESS LAN
INFRASTRUCTURE* 6TH MARCH 2024



info@centerprise.co.uk



centerprise.co.uk



01256 378 000



[centerprise international](#)