# Critical Capabilities for Enterprise Wired and Wireless LAN Infrastructure

Published 17 November 2021 - ID G00740375 - 33 min read

By Analyst(s): Christian Canales, Tim Zimmerman, Mike Toussaint

Initiatives: Cloud and Edge Infrastructure; IT Services and Solutions

Vendors serving this market provide needed functionality for basic connectivity needs; however, I&O leaders require capabilities for such functionality as network management and assurance, automation, policy enforcement, Internet of Things containment, and locationing, which can vary significantly.

**This Critical Capabilities is related to other research:**

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

View All Magic Quadrants and Critical Capabilities

## Overview

### Key Findings

- Our scores in the five defined use cases point to a lack of variance for the top five vendors, indicating that their portfolios can address a wide variety of enterprise use cases, independent of company size and vertical market.
- Many organizations are seeing a growing number of Internet of Things devices converging onto the corporate network, raising the importance of IoT device visibility and security.
- Network management platforms and product roadmaps point to a growing emphasis on artificial intelligence/machine learning-driven analytics, aimed at baselining, monitoring and proactively resolving network performance issues.

### Recommendations

Infrastructure and operations leaders responsible for planning, sourcing and managing wired and wireless networks and related services should:

- Prioritize their requirements around management, security, automation and locationing capabilities, as relevant, to fulfill their use cases. Hardware capabilities are increasingly commoditized, with declining differentiation among network providers.
- Assess security capabilities for IoT use cases, because IoT endpoints are prone to weak or nonexistent authentication. Key capabilities should include discovery and classification of IoT devices, virtual segmentation and continual monitoring.
- Apply best practices for wireless local-area network implementation, such as identifying bandwidth, latency and mobility requirements for end users. Although the use of analytics leveraging AI for IT operations can simplify troubleshooting and improve service assurance, poorly designed and implemented WLANs will cause a poor user experience.

## What You Need to Know

This Critical Capabilities research is the companion to Gartner's Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure. It scores 14 vendors across five use cases designed to reflect the primary evaluation criteria that Gartner recommends for infrastructure and operations (I&O) leaders responsible for planning, procuring and managing enterprise wired and wireless access networks.

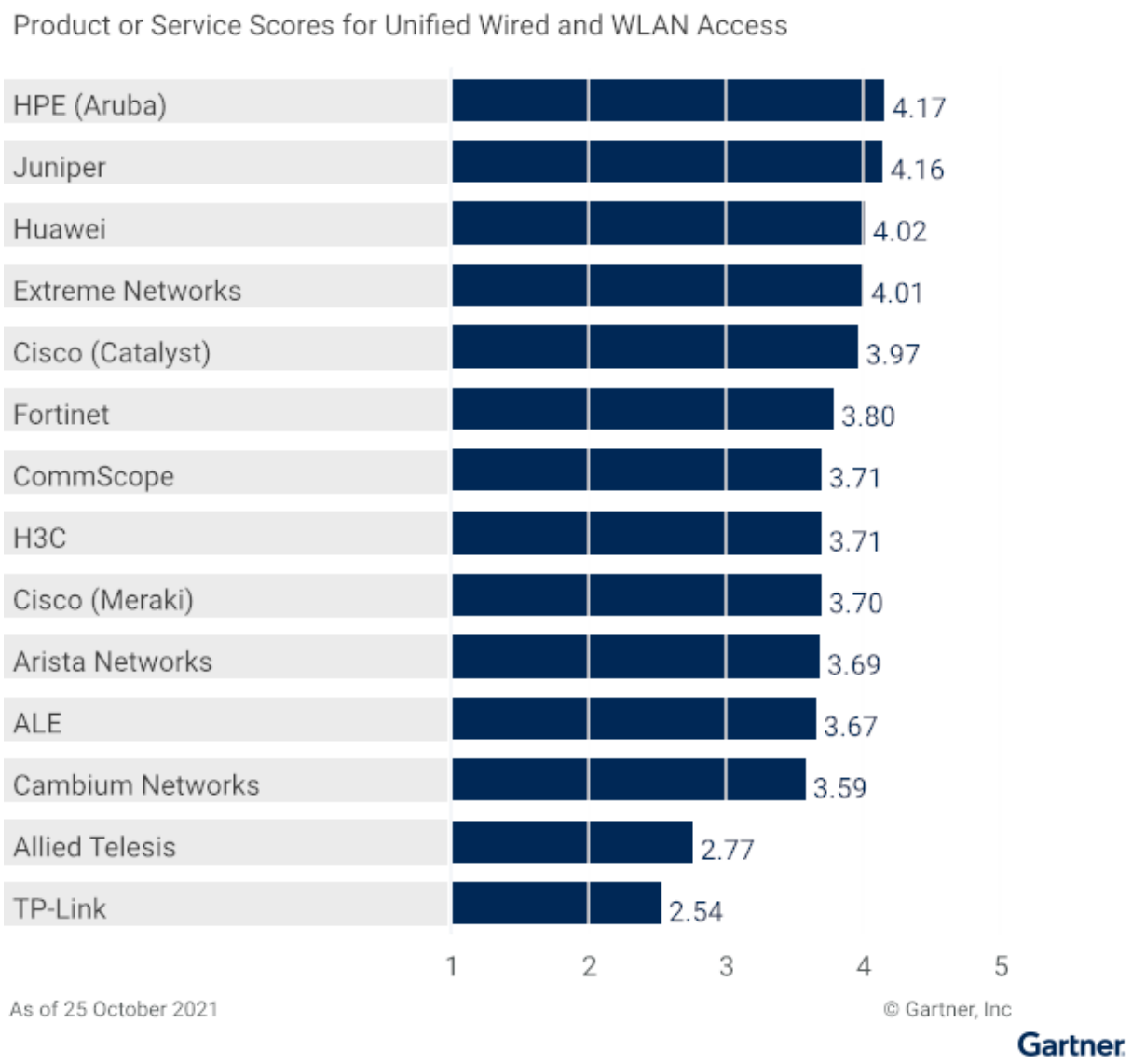
I&O leaders responsible for networking can use the critical capabilities assessed in this research to inform their search for appropriate solutions that more closely meet their specific use cases.

As the market has evolved, standards-based access networking hardware has become less differentiated. Many enterprises now focus more on the features and functionality of network service applications, when evaluating which vendors best meet their network requirements. In addition, enterprises are scrutinizing network service applications for wireless local-area network (WLAN)-only and remote branch office connectivity, either on-premises or in a public or private cloud.

# Analysis

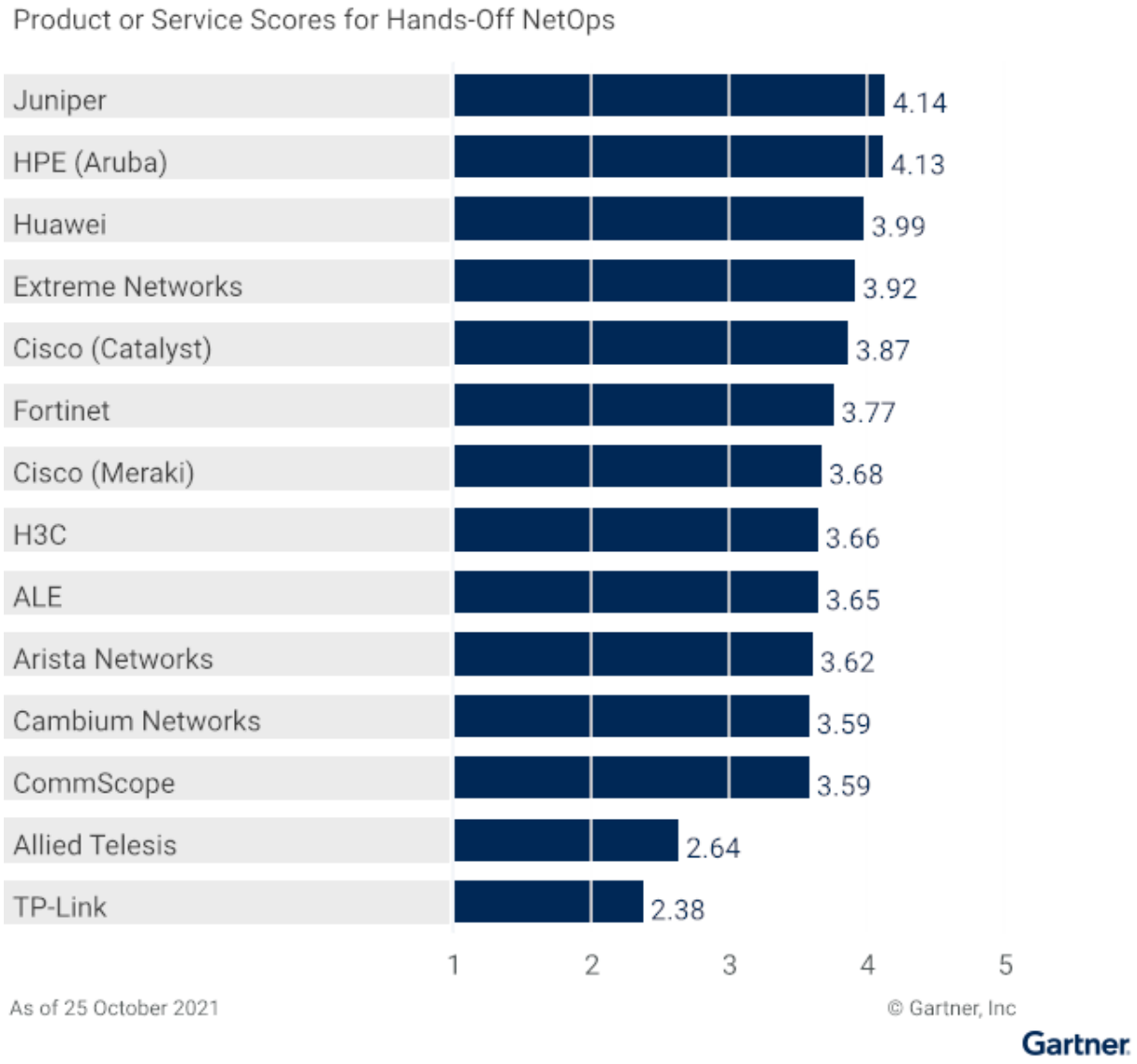
## Critical Capabilities Use-Case Graphics

### Vendors' Product Scores for Unified Wired and WLAN Access Use Case



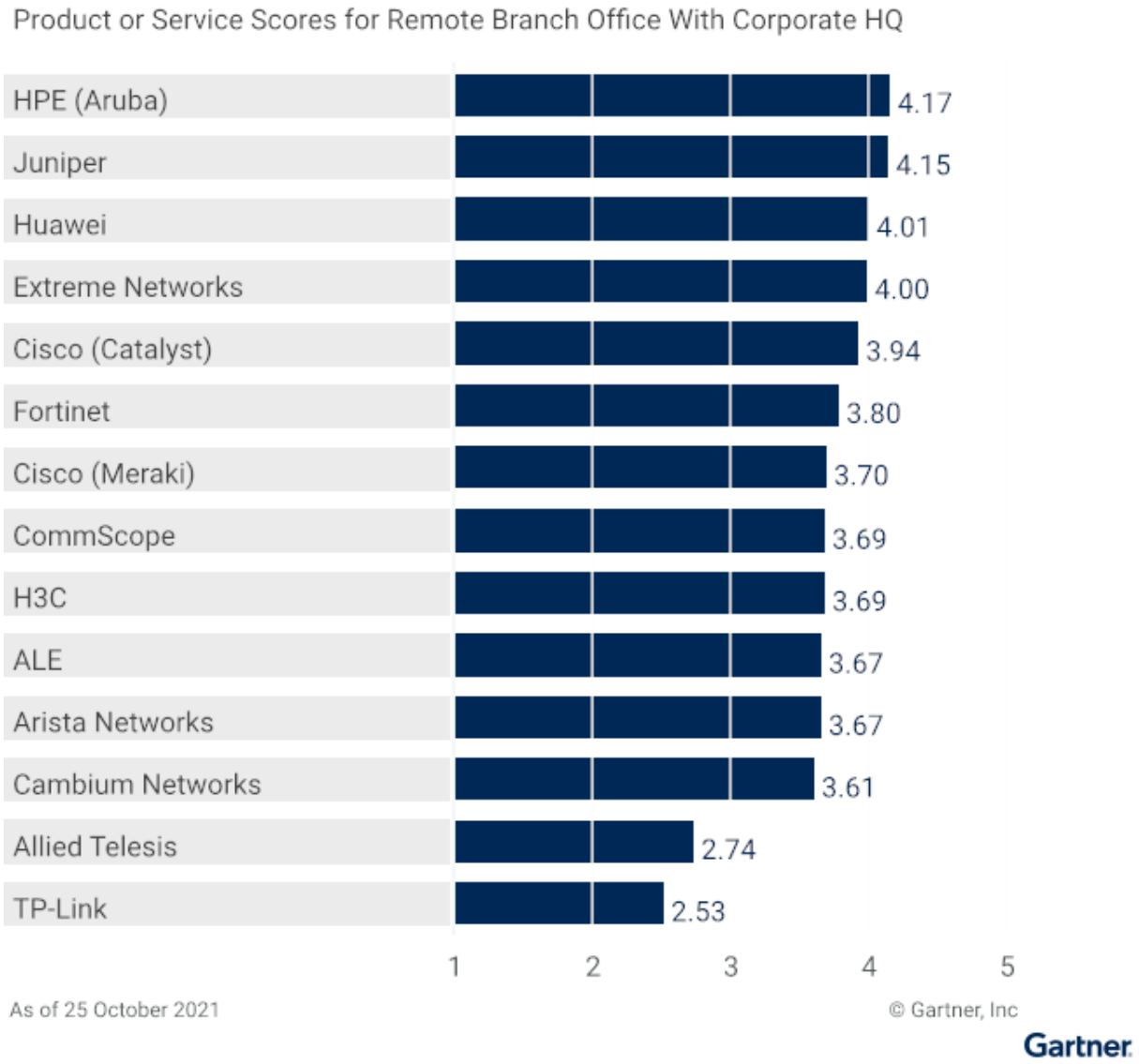

Source: Gartner (November 2021)

## Vendors' Product Scores for Hands-Off NetOps Use Case



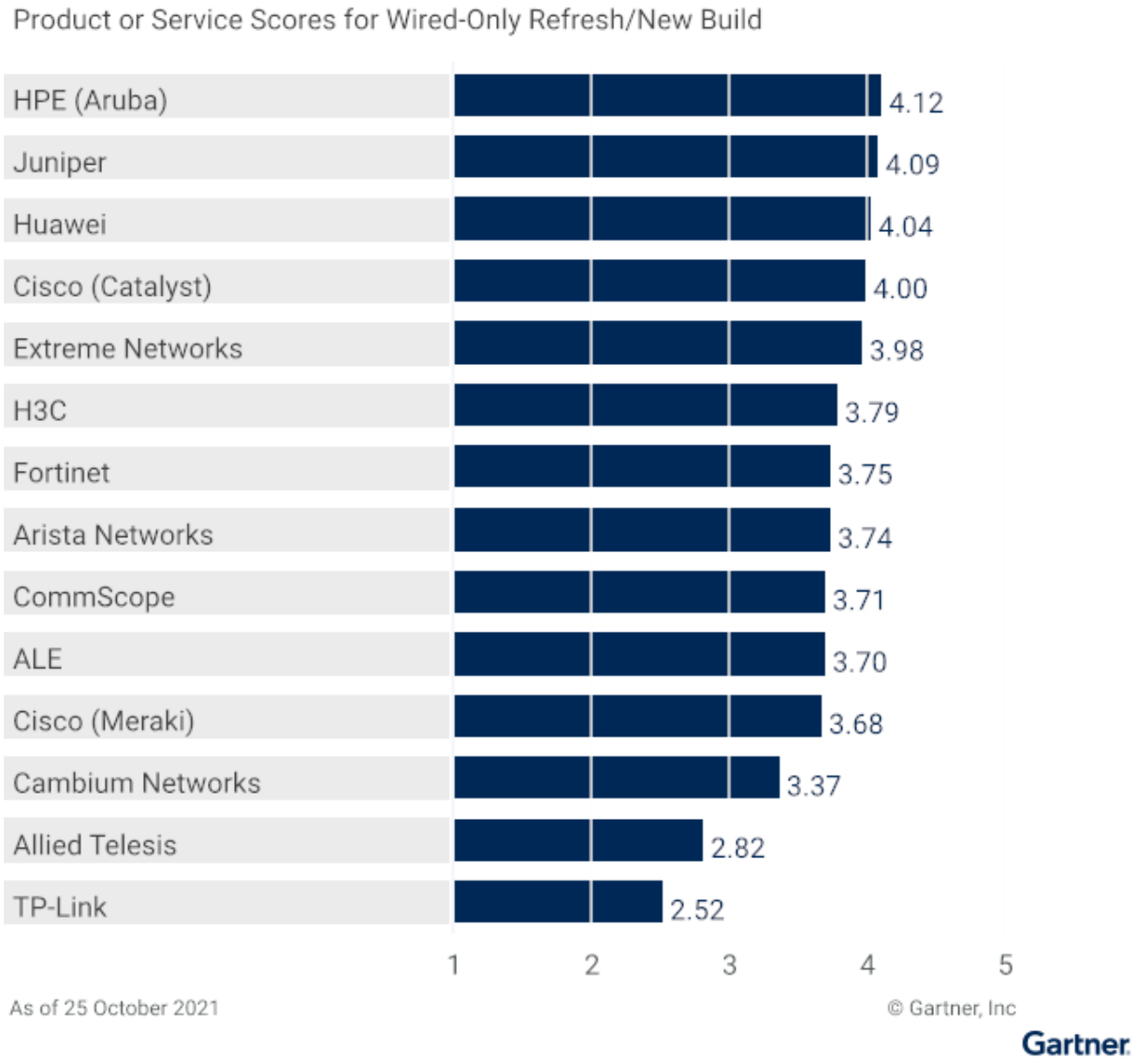

Source: Gartner (November 2021)

## Vendors' Product Scores for Remote Branch Office With Corporate HQ Use Case



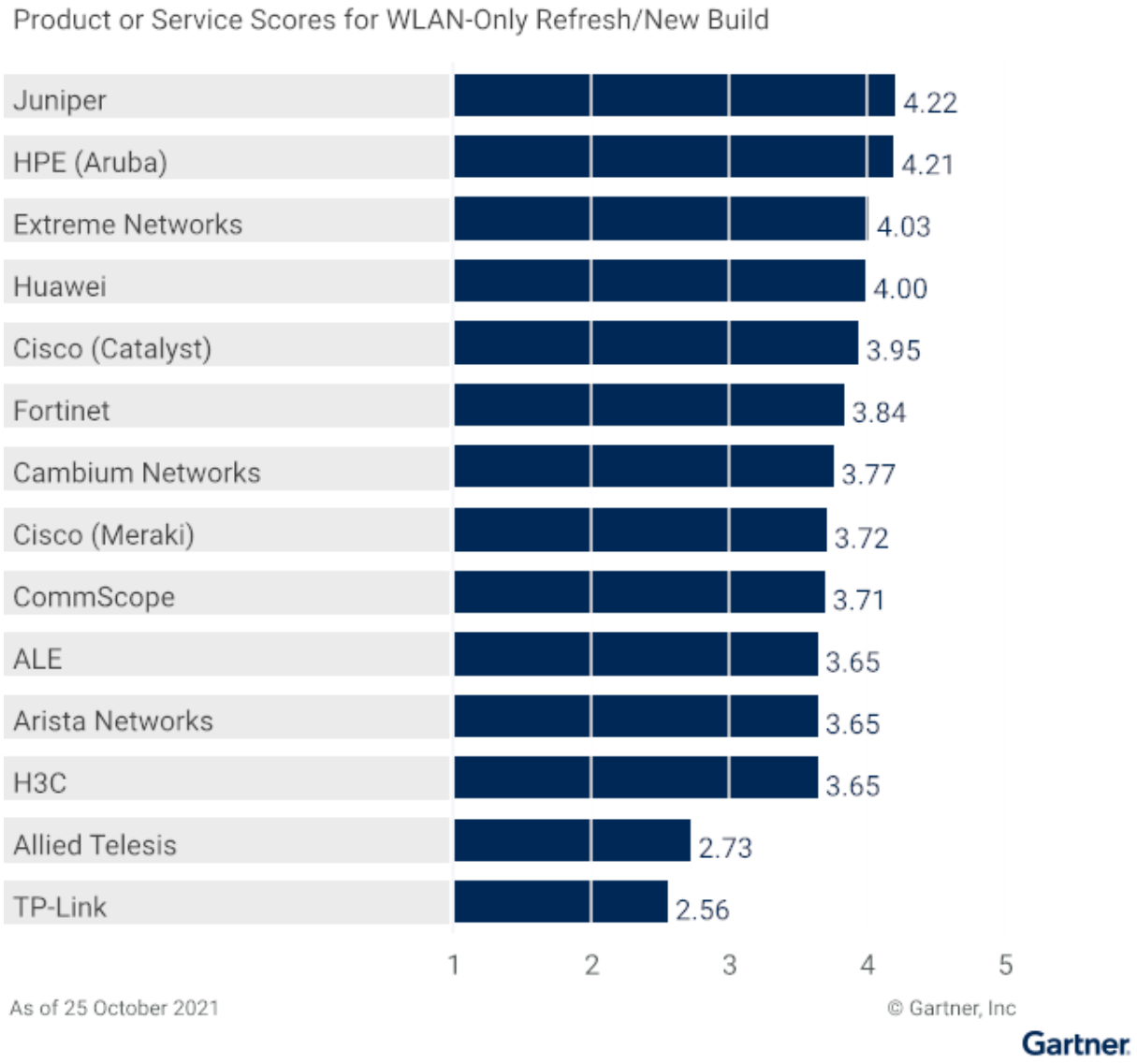

Source: Gartner (November 2021)

## Vendors' Product Scores for Wired-Only Refresh/New Build Use Case




Source: Gartner (November 2021)

## Vendors' Product Scores for WLAN-Only Refresh/New Build Use Case




Source: Gartner (November 2021)

## Vendors

### ALE

Marketed as Alcatel-Lucent Enterprise, ALE provides a wired and wireless LAN portfolio suitable for most requirements. Although the company still sells rebranded Aruba WLAN access points (APs) under its strategic partnership with HPE, ALE now generates most of its revenue from its lower-cost OmniAccess Stellar line of APs.

ALE provides a common orchestration system for wired/WLAN via its OmniVista network management system or its Cirrus cloud-based version, paired with its Unified Policy Access Manager module or with Aruba's ClearPass Policy Manager solution. ALE's Intelligent Fabric technology simplifies network deployment, moves, adds, changes and network monitoring/management, enabling a more automated framework, including for Internet of Things (IoT) devices. The Rainbow Workflow rule engine further complements overall network management with automation and security enforcement capabilities, based on events driven by business processes or triggered by ALE location-based services. IoT containment features identify and classify endpoints with a fingerprinting database, complemented by a deep packet inspection (DPI) engine for device visibility, authentication and authorization. ALE supports artificial intelligence/machine learning (AI/ML) functionality through analysis of logs, though its capabilities are less feature-rich, compared with some of its competitors.

Enterprises in North America, Latin America, Europe and the Asia/Pacific (APAC) region should consider ALE, particularly in its priority vertical enterprise markets of education, healthcare, transportation, hospitality and, outside of North America, government.

**Note:** *The Critical Capabilities scores of ALE reflect an assessment of ALE's own products, and exclude those from its original equipment manufacturer (OEM) partnership with HPE (Aruba).*

### Allied Telesis

Allied Telesis offers a LAN portfolio predominantly suitable for small and midsize businesses (SMBs). Although the switching portfolio is broad, its wireless offering remains limited, with only one access point (AP) model (at the writing of this research) supporting Wi-Fi 6 (802.11ax). Wi-Fi functionality includes indoor location-based services and integrated security for endpoints and IoT devices. The switching portfolio includes stackable and chassis-based switches, with multigigabit ports and Virtual Extensible LAN (VXLAN) support. Allied Telesis runs a common OS, AlliedWare Plus, which is relied on for configuration tasks, despite the availability of the graphical user interface (GUI)-based configuration tools.

Allied Telesis' network management and automation is offered via a suite of tools: AMF for wired automation and AWC for wireless optimization and automation. These tools are integrated via Vista Manager, enabling a centralized management interface. Automation and optimization functionality can reduce the burden of manual provisioning and configuration, although the platform has limited AI/ML-driven capabilities. It lags in delivering data-to-incident correlation, which is necessary to self-drive problem identification and resolution.

Although Allied Telesis has a portfolio that can address a wide variety of network use cases, the company has little exposure to the large-enterprise market. This limits its ability to address and support complex network requirements.

Predominantly SMBs in the APAC region; North America; and Europe, the Middle East and Africa (EMEA) should consider Allied Telesis.

**Arista Networks**

Arista Networks offers its Cognitive Campus strategy, which extends its data center focus and CloudVision management application to the campus and cloud. Arista made enhancements to its Cognitive Wi-Fi software in 2020, including AI/ML capabilities, in addition to launching Wi-Fi 6 (802.11ax) APs and extending its wired portfolio. Other product improvements included the "P-Tracer" dashboard for proximity and contact tracing use cases.

Arista is focusing on meeting NetOps requirements through its prescriptive insights, which are delivered through the CloudVision platform, as well as Ava. The natural language virtual assistant drives remediation recommendations/actions for improved network assurance and user/device experience.

For better security, Arista acquired Awake Security, which solidifies its campus security with anomaly detection capabilities, including a dedicated external sensor offering. CloudVision can now be offered as a fully managed cloud service and has a new endpoint dashboard, IoTvision, which consolidates the view of all wired and wireless endpoints connected to the network. To address IoT visibility and separation requirements, Arista provides its Macro-Segmentation Services solution, as well as a VXLAN fabric with Ethernet VPN (EVPN). For network access control (NAC), Arista does not have its own offering. Instead, it relies on a partnership with Forescout.

Enterprises should evaluate Arista Networks in North America and Europe for most cloud-based access layer connectivity projects and globally through partners that provide the required functionality.

**Cambium Networks**

Cambium Networks' access layer offering emphasizes ease of deployment and operation. WLAN APs consist of the cnPilot brand and the Xirrus product line, with three AP Wi-Fi 6 (802.11ax) models. Cambium's controllerless architecture places application and policy control, locationing, analytics and firewall capability in the APs. Some models have up to five integrated radios for high-density coverage, and APs with multiple, software-defined radios provide a migration path to changing Wi-Fi requirements. The cnMatrix switches provide access layer connectivity options, although high-capacity core and distribution capabilities are missing.

cnMaestro offers unified wired and wireless management (on-premises and in the cloud), location-based services, policy-based segmentation and recent enhanced automation capabilities. cnMaestro is free (Essentials) or licensed (X) with additional features, such as automation. From an AI/ML perspective, Cambium's insight engine provides actionable insights on a number of simple use cases, such as AP low signal strength, misconfigured VLANs and point of entry (POE) issues. Cambium's architecture supports IoT device fingerprinting via policy-based automation, and APs with integrated firewall perform traffic filtering. EasyPass provides automated onboarding for IoT devices, as well as employees and guests.

SMBs should assess Cambium globally for their wired and wireless networking requirements.

**Cisco (Catalyst)**

Cisco has a broad wired and wireless LAN portfolio that addresses all use cases, and the largest worldwide revenue share and geographic reach through its two enterprise brands: Catalyst and Meraki. Most Cisco campus switches and WLAN APs require a compulsory term-based license (DNA Essentials, Advantage or Premier), starting with a minimum three-year subscription. Although Essentials provides basic automation, more advanced capabilities (e.g., NAC, locationing and anomaly detection) require a higher license. This can be a source of indecision for buyers, in terms of whether many of the advanced features are needed, combined with the concern regarding purchasing an inappropriate license, for a specific number of years.

All Catalyst APs require the Catalyst 9000 series WLAN Controller or the virtual/Cloud Controller. Popular extended WLAN features, such as location-based services, are provided through DNA Center/Spaces, with the appropriate licensing.

Cisco has invested heavily in consolidating wired and wireless management via Cisco DNA Center (DNA-C) Server. DNA-C serves a dual role as an AI- and ML-enabled network management platform, and the control plane for the software-defined access, policy-based networking architecture. Large enterprises will find DNA-C useful for reducing cumbersome traditional switch provisioning and configuration tasks. However, DNA-C is an on-premises-based platform only.

Cisco is one of the more expensive providers in this analysis.

Global midsize and large enterprises should consider Cisco for most wired or wireless enterprise network use cases.

**Note:** *Historically, Cisco used the Catalyst brand in reference only to its enterprise switching portfolio. However, it has recently expanded the brand to include its WLAN products (albeit the 802.11ac and outdoor APs have retained the legacy Aironet brand).*

**Cisco (Meraki)**

Cisco Meraki is a portfolio of wired and wireless networking products, which Cisco has traditionally marketed to customers looking for cloud-managed environments. All Meraki products are configured solely through the cloud-based Meraki dashboard, which unifies the management of all wired switches and Wi-Fi APs under a single graphical user interface (GUI). Although the choice of access switches is broad, Meraki has a limited selection of aggregation switches, although, in some scenarios, they can perform both distribution and core functions. Support for Cisco's EIGRP routing protocol is still missing, and multicast support is limited.

Meraki's Layer 7 device fingerprinting and traffic shaping deliver control over devices, applications and users accessing the network. Integration with Cisco Umbrella enhances content filtering and the management of security policies. WLAN device segmentation and traffic encryption, necessary for IoT deployments, is supported natively or through integration with compatible Cisco Catalyst switches.

Although the Meraki Dashboard reduces the operational burden for Meraki network devices, AI/ML-based automated trouble resolution is limited. Meraki's dashboard can't manage Cisco Catalyst devices; therefore, Cisco customers with a compelling reason to consume both platforms must use multiple methods of operation and configuration. Meraki's indoor location-based services are part of its standard license, as well as integrated with Cisco's DNA Spaces.

Global midsize enterprises (MSEs) should consider Cisco Meraki for cloud-based wired and wireless LAN deployments, and for large enterprises with multiple small branch office locations.

**CommScope**

CommScope delivers an end-to-end wired and wireless offering, sold under the RUCKUS brand. Its switching portfolio can support most enterprise requirements, although it lacks VXLAN dynamic segmentation capabilities and a chassis-based distribution/core switch. WLAN deployments can be accomplished using controllerless (RUCKUS Unleashed), controller-based (RUCKUS SmartZone) or cloud-based (RUCKUS Cloud) mechanisms.

RUCKUS Cloud uses AI and ML technologies to reduce time to issue identification and correlation. However, RUCKUS Analytics offers no mechanism for automatic issue resolution, and issues that have been identified cannot be remedied from within the interface. In addition, although most configuration tasks for both ICX switches are accomplished through the GUI, the command line interface (CLI) is still required for many complex routing and switching tasks. To mitigate this requirement, RUCKUS includes dozens of prebuilt Ansible playbooks, which can be quickly edited to automate repetitive tasks, decrease time to device provisioning, and reduce the chances of human error by reducing the manual configuration burden. CommScope's management software includes a policy engine that recognizes and prioritizes as many as 3,500 applications. It uses AI, ML and automation to optimize wireless network settings, as well as networkwide problem identification and guided remediation.

Enterprises located in North America, EMEA and the APAC region (especially in its key verticals of hospitality, education and healthcare) should consider CommScope for all wired and wireless LAN use cases.

**Extreme Networks**

Extreme Networks delivers a broad portfolio of cloud and on-premises managed network applications and services, in conjunction with its end-to-end wired switching and WLAN products.

Extreme's new 5520 and 5420 switches support a campus fabric — Storage Policy-Based Management (SPBM) or VXLAN EVPN — as well as a traditional network with cloud or on-premises-based management. Its Fabric Connect technology enables switches to extend to branch environments across public or private WANs, while Fabric Attach allows non-network-enabled devices to use the fabric. This supports the automation of the wiring closet's connectivity, by allowing "client" switches to be reconfigured automatically. The fabric also supports granular segmentation of users, applications and services, including IoT devices. Extreme has a product line of Wi-Fi 6 (802.11ax) APs, in addition to offering poolable and portable licenses across its platforms and portfolio, making migration easy and cost-effective.

ExtremeCloud IQ provides unified management of Extreme wireless APs and switches, as well as third-party management with unlimited data retention options through ExtremeCloud IQ. ExtremeCloud IQ Access Control and AirDefense are part of a portfolio of security offerings that provide extensive end-to-end security. Extreme has released its CoPilot platform, which offers proactive anomaly detection and ML/AI recommendations that can be immediately acted on, based on deviations in their baseline environment.

Enterprises should consider Extreme globally for all wired and wireless LAN opportunities.

**Fortinet**

Fortinet's wired and wireless LAN products emphasize security. Fortinet's FortiSwitch switches and FortiAP wireless APs scale from SMBs to large-enterprise use cases. The company differentiates itself by integrating its networking products as an end-to-end security-centric fabric, which is anchored by its FortiGate firewalls. This integration offers simplified security and management through its FortiManager management platform and application performance management with FortiMonitor. End-user profiling capabilities can be further enhanced across the network fabric by leveraging onboard NAC services or its overlay product FortiNAC, which further simplifies IoT onboarding requirements. The FortiAIOps introduced in 2021 gathers data from Fortinet's fabric and single OS, improving its network health and performance analytics.

Fortinet has a considerable selection of Wi-Fi 6 (802.11ax) APs, supporting two operational modes: SaaS with FortiAP Cloud and controllerless (the FortiGate appliances have an integrated WLAN controller). To supplement its Wi-Fi 6 AP portfolio, the company also offers various multigigabit Ethernet switches. Fortinet does not have a chassis form factor switch — required to support high-speed core and high-density network access use cases — although it has plans to address this portfolio gap following the acquisition of Alaxala. FortiPresence provides indoor location services.

Enterprises of all sizes and in all geographies should consider Fortinet, especially when network security is a primary use case.

**H3C**

H3C provides a full portfolio of wired and wireless networking solutions, primarily to customers in its home market of China, including Wi-Fi 6 (802.11ax) APs. Its new Application-Driven Campus (AD-Campus) cloud-native architecture provides unified wired/wireless management. AD-Campus uses H3C's new network architecture, which includes a series of modules such as SeerAnalyzer and Endpoint Profiling System. This solution addresses key components, such as network management, access control and analytics, and provides service integration and unified orchestration for campus, data center and WAN networks.

H3C's SeerAnalyzer module builds a granular data lake, whereas the AI analytics capabilities address potential issues and recommend actions to network administrators. These can reduce operations and maintenance costs, predominantly for wireless, based on the analysis of connection, authentication and interference issues. AD-Campus also works with the Oasis IoT Center, SecCenter and AD-NET to provide additional functionality and supports multivendor management of more than 7,000 devices models from Cisco, Huawei and Ruijie. The Oasis IoT platform offers management and automatic onboarding of IoT devices with encrypted traffic.

Enterprises in the APAC region, especially in China, should consider H3C for enterprise campus and branch office deployments, as well as in EMEA, if partners can provide the needed functionality and postsale support.

**HPE (Aruba)**

Aruba ESP (Edge Services Platform) is a cloud-driven platform that automates and secures the campus, branch and remote networks, with additional customer flexibility provided by open, programmable APIs. Aruba ESP uses Aruba Central to deliver a broad portfolio of cloud-based and on-premises managed network applications and services, in conjunction with its access switches and WLAN products. Aruba provides Wi-Fi 6 (802.11ax) support through its AP-500 and AP-600 Series APs and recently extended its broad CX switching portfolio with the CX 6100 for the midmarket.

Aruba's primary management platform is Aruba Central, which can be deployed in the cloud and on-premises. Aruba continues to support AirWave, but expects customers to migrate to Central over time. In addition, Aruba continues to offer ClearPass Policy Manager, while building services such as authentication and policy into Central. It is important for enterprises to evaluate their use cases to understand the functionality differences that exist when determining the outcomes they are trying to achieve.

AI Insights provides self-tuning notifications with root cause analysis and recommended fixes for issues across wired, wireless and WAN connectivity to support enterprise NetOps requirements. With natural language capabilities through AI Search, AI Insights provides AI-based multivendor wired and wireless device visibility and profiling that is now natively integrated into Aruba Central. Aruba's Dynamic Segmentation provides strong capabilities for segmenting wired and wireless traffic, including IoT devices.

Enterprises should evaluate Aruba globally for all wired and wireless LAN opportunities.

**Huawei**

Huawei has a broad wired and wireless LAN offering, with its CloudEngine S Series switches, in addition to its AirEngine wireless APs, broadly supporting Wi-Fi 6 (802.11ax). Huawei delivers a unified, AI/ML-enabled cloud management platform via its CloudCampus 3.0 solution, which was released in March 2021. This is an upgrade to its iMaster NCE-Campus (available as SaaS or an on-premises solution). CloudCampus enables automated and secure management across the LAN and WAN, plus the ability to simulate, test and verify network planning. This includes access authentication, virtual segmentation and network assurance capabilities. However, on-premises deployments of CloudCampus/iMaster NCE-Campus can be complex and/or costly for some midsize enterprises (MSEs), especially those with simple network requirements.

Huawei supports IoT onboarding through a fingerprint library that identifies IoT endpoints connecting to the network. Huawei's HiLink IoT Protocol can be used for more-secure and simpler IoT management, although this entails integration with its IoT module or the use of Huawei's open API and software development kit (SDK). This can limit its relevance to organizations standardizing on other endpoint platforms.

Location capabilities support a large ecosystem of application providers, such as Purple, Cloud4Wi and Pointr, using either Wi-Fi, BLE beacons, radio frequency identification (RFID) or ultrawideband hardware in Huawei APs, WLAN controllers, and RFID terminals or tags.

Enterprises with a presence in Huawei's focus areas of China, the Middle East, Europe, Latin America, Africa, Japan, South Korea and other APAC region areas should evaluate the vendor for all wired and wireless LAN network requirements.

**Juniper**

Juniper Networks offers a full-stack wired and wireless network portfolio, which supports most use cases ranging from SMBs to large enterprises, with a differentiated AI/ML-driven architecture.

Juniper has invested heavily in its Juniper Mist Cloud platform, which is a cloud-based NetOps management suite with integrated automation, AI and ML. The Marvis Virtual Network Assistant and its natural language interaction and self-driving issue resolution capabilities are part of the Juniper Mist Cloud. In addition, the Juniper Mist Cloud includes indoor location and Wi-Fi, wired and WAN assurance services, and analytics, which enable network optimization, application performance, end-user experience metrics, and real-time measurement of targeted SLA compliance metrics. Juniper runs Junos OS across its routing and switching portfolio, which supports traditional CLI device access and configuration, in addition to J-Web, which is self-contained GUI individual device management. Juniper Mist Cloud is now capable of integration with various EX and certain QFX models.

Juniper's indoor location-based services use unsupervised AI/ML to deliver high-accuracy location without requiring any manual calibration and/or fingerprinting of the network, although it is a single vendor solution that requires Mist APs and cloud subscription licenses. Juniper relies on third-party ecosystem partners for advanced NAC functionality, although it is developing an onboarding and microsegmentation solution for bring your own device (BYOD) and IoT devices.

Juniper should be evaluated globally for all wired and wireless LAN opportunities.

**TP-Link**

TP-Link provides a broad portfolio of campus switches and wireless APs. Its aggressive pricing aligns with the needs of SMBs or, more broadly, with those of organizations with basic connectivity needs looking for a cost-effective solution.

The Omada cloud network management solution is bundled with its access network hardware at no charge, providing unified monitoring for an unlimited number of TP-Link APs, campus switches and secure gateways. Network analytics include limited automation and security features. In addition to the Omada cloud-based controller, TP-Link has a free, virtual machine (VM)-based version of Omada (that manages as many as 1,500 network devices), and a hardware WLAN controller that can be remotely configured with a mobile app. Omada cloud can act as an intermediate agent to the on-premises WLAN controller, allowing administrators to have access from anywhere. Although TP-Link provides simple functionality to optimize network performance, the AI/ML-driven analytics are lagging, compared with other vendors profiled in this research, and IoT onboarding capabilities remain basic. TP-Link's WLAN APs do not support integrated BLE, and the company does not have an indoor location services offering.

Enterprises in EMEA, China and the APAC regions where TP-Link has its largest business presence should consider the vendor a low-cost option for wired and wireless LAN implementations, with basic connectivity and management requirements.

## Context

WLAN hardware has become largely commoditized, with the major vendors offering 802.11ax APs. For switching hardware, a growing number of switch models support 2.5/5 Gbps (multigigabit), even though availability of the technology has made rather slow progress since the ratification of the 802.3bz standard in September 2016. The need for multigigabit switching is nonetheless becoming more important, as adoption of 802.11ax APs continues to ramp up (since Wi-Fi 6 requires multigigabit connections to realize its full technical capabilities).

Market maturity in the WLAN and switching hardware means that vendor differentiation continues to predominantly rely on software capabilities used to configure, secure, manage and operate the network. This is a source for the different "software-defined" marketing terms that have evolved in the past couple of years, such as "SD LAN" or "SD Campus" (or SD-Access in the case of Cisco). These terms largely define an architecture that separates hardware and software layers to form an application-driven fabric. Here, policy enforcement and management can be operated at scale and with greater flexibility, from the cloud or via a central orchestration platform.

NetOps is an emerging use case, driven by recent advances in analytics, AI and ML. At the access layer, NetOps applies predominantly to Wi-Fi, although it has begun to extend to wired networking. For too long, Wi-Fi has been one of the “pain points” for organizations, because it comes with inherent challenges associated with interference and distance, and it’s a shared medium. Although these challenges can be addressed, improperly implemented Wi-Fi installations continue to result in a poor end-user experience. Moreover, enterprises have the issue that IT personnel staffing levels are likely to remain flat or decline in years to come.

By leveraging AI/ML, the resolution of network issues can improve from generating alerts to changes that reduce human intervention, depending on the solution. This can affect tasks encompassing policy enforcement, troubleshooting and network automation, ultimately helping to make network performance more predictable. Customers can focus on network assurance capabilities and on the SLAs for supporting a specific user experience more than on the listed throughput, capacity or antenna specs for the deployed infrastructure.

The convergence of the “traditional” IT and building automation networks has increased the number of IoT devices that many organizations need to manage. The additional “blending” of operational technology (OT) connectivity, for monitoring and/or control of industrial equipment, under the same enterprise network, further adds complexity. Lack of IoT device visibility has become a pressing issue for many organizations, leading to a bigger problem, which is IoT security. The ability to discover and classify IoT endpoints is the first step in taking control of the enterprise network and identifying compromised devices.

## Product/Service Class Definition

The rated vendors provide some or all of these elements:

**Hardware** — Physical network elements, including:

- Wi-Fi APs
- Ethernet network switches suitable for deployment at the network access, distribution and core network layers
- Wi-Fi controllers — physical, virtual or cloud-based

**Software** — Network service applications: cloud, appliance or virtual-appliance-based. These applications include:

- Network management interface
- Network monitoring
- Guest access portals
- Self-service device onboarding services
- Network security integration — intrusion prevention system (IPS), intrusion detection system (IDS), cost-effective Domain Name System (DNS) security, etc.
- Network policy enforcement/integration
- WLAN location services
- Application visibility and/or performance management
- AI- and ML-enabled network assurance tools
- Network automation tools
- Dedicated nonuser device (IoT) management and security mitigation
- Natural language troubleshooting interface

This research does NOT include wired and wireless networking infrastructure devices, the primary purpose of which is to support adjacent markets, such as public venues, commercial and industrial settings, or point-to-point WAN solutions.

As the market has evolved, standards-based access networking hardware has become less differentiated. Many enterprises now focus more on the features and functionality of network service applications when evaluating which vendor will best meet the organization's access network requirements. In addition, enterprises are scrutinizing network service applications for WLAN-only and remote branch office connectivity, either on-premises or in a public or private cloud.

## Critical Capabilities Definition

**Wired Access**

This accounts for the vendor's wired switching solution hardware (fixed-form-factor and modular) and integrated software, which may include port-extension capabilities. Key components include performance, availability, scalability, interoperability, cost, support and the portfolio architecture.

Capabilities also include:

- Form factors and port densities that meet specific wired switching requirements. These include fixed-form-factor, port-extension and chassis-based switches.
- 802.3bz capabilities that enable 2.5/5Gb links to wireless APs for supporting high-density Wave 2 802.11ac and 802.11ax deployments, without the need to replace existing Cat 5e or Cat 6 cables.
- Single-application management of hardware from differing vendors, including end-user security and policies.
- Flexibility to deploy access network applications on-premises or in a private or public cloud to address implementation scenarios, such as remote or branch offices.
- Network application innovation to support security, policy enforcement and other access layer functionality.

**WLAN Access**

This accounts for the vendor's wireless-access solution in a traditional, carpeted enterprise, which includes hardware (such as APs in a variety of configuration and antennas) and integrated software.

Key capabilities include:

- A range of wireless AP form factors to support different indoor and outdoor enterprise and campus environments.
- The ability to measure latency for voice and data applications and to provide sufficient data for mean opinion score (MOS) calculations to support toll-quality voice over WLAN (VoWLAN).

- AP hardware that can support OS from different acquired vendors (e.g., as part of an integration roadmap for acquired WLAN assets), including end-user security and policies.
- Ability to scale from hundreds to several thousand APs. The network retains active ability of connectivity to the controller, whether on-premises, virtualized or cloud-based.

**Identification and Network Access**

This includes NAC functionality and/or the ability to provide captive portals to onboard guests and employees for BYOD situations by defining roles of varying access to the network.

Access roles will use device, device profile, user, location, time/date, duration and application access as elements to consistently determine access to the wired or wireless network, regardless of device or location.

**Management and Administration**

This refers to the deployment, configuration and ongoing management/administration capabilities of the vendor's products and other access layer networking products.

It includes functionality embedded into individual network elements, vendor-provided network management system software/hardware and integration with existing management tools (e.g., network performance monitoring and diagnostics [NPMD] and network configuration and change management [NCCM]) via standardized protocols or APIs.

Other capabilities include:

- Policy-based management and configuration
- Network monitoring (e.g., multivendor), including reporting, predictive analytics and troubleshooting tools
- On-premises and cloud-based management options
- Physical and virtual controller or controllerless options
- Digital twins as a management model to improve situational awareness and reduce network downtime

- AI/ML-driven analytics for root cause analysis and problem resolution, which ease management tasks and troubleshooting

**Additional Network Service Apps**

This includes a broad, growing set of network service applications, which include analytics, AI/ML-driven analytics, automation capabilities, forensics, LAN security services (e.g., anomaly detection) and Wi-Fi-to-5G handoff.

It also includes video services that enhance the application, as well as location-based services, which may be vertical-market-specific. Network analytics applications look at the network, as well as the end-user data. Network forensics tools determine what's happening across the entire access layer, in addition to security functionality and fixed mobile convergence capabilities. Location services include the ability to provide Wi-Fi-based or active RFID/beacon location, as well as an application toolkit for zonal or real-time location services (RTLS).

**IoT Device Containment**

This ensures security of the network using virtual segmentation, access control and device containment, including "headless" IoT endpoints. The vendor's network management solution contains IoT devices from the access network connection to the data center, which is a software development focus area.

Solutions typically:

- Discover endpoints (IoT or other) once they are attached, whether they are IP-based or non-IP-based
- Identify/profile any device, including IoT that attaches to the network
- Identify the application and how it secures the device through virtual segmentation
- Identify the application and how it assigns a role, if applicable
- Monitor any device, including IoT and whether it is at line rate or other sampling

## Use Cases

### Unified Wired and WLAN Access

This is an enterprise facility or campus environment, with more than 500 users, requiring wired and WLAN access networking components deployed across carpeted office spaces.

Unified wired and WLAN access will provide the ability to monitor and manage the network from one integrated network management solution.

Users are typically badged employees, although contractors and guests also require connectivity. Employees are usually issued corporate-owned devices. However, the network may also support BYOD for mobile devices, such as smartphones, tablets and, possibly, laptops. This buyer is typically technically competent and/or routinely makes granular changes to wired/WLAN infrastructure components. This is the most common use case for newly constructed office space, although it's often initiated by a campus refresh.

### Hands-Off NetOps

This is an enterprise facility or campus environment that wants to improve the operational experience.

In this use case, the primary driver is to reduce the operational burden and costs associated with managing network infrastructure. This is an emerging use case, driven by the advances in analytics, AI and ML. This applies predominantly to WLAN, although it has begun to extend to wired networking as well. This use case applies to SMB and large-enterprise networking environments. The primary driver for buying LAN equipment is achieving a hands-off operational experience. Users want the vendor's management system to configure itself, monitor itself and self-remediate/optimize, without human intervention. Monitoring WLAN performance remains a key sought-after capability, due to the challenges associated with controlling the RF environment.

### Remote Branch Office With Corporate HQ

This requires wired/WLAN access networking components and knowledge of WLAN connectivity.

This use case involves a single physical facility of 10 to 50 users. It is typically observed for remote small offices of enterprises with central corporate headquarters. This use case also involves SMBs with up to 499 employees. Users are typically badged employees, but contractors and guests also require connectivity. There is usually little or no on-site technical support in the remote locations; however, an IT organization typically supports these locations at the central headquarters.

**Wired-Only Refresh/New Build**

This is a physical facility or campus environment with more than 500 users; it requires only wired LAN networking components.

This use case mostly applies to brownfield and refresh opportunities, often when an incumbent wired solution is in place, and there is no desire to replace it, or it serves a highly risk-averse environment where no wireless has been deployed. This network also may provide connectivity for IoT endpoints, including headless devices. Most users are typically badged employees. However, contractors and guests also require connectivity. This buyer is typically technically competent and/or routinely makes granular changes to wired/WLAN infrastructure components.

**WLAN-Only Refresh/New Build**

This applies to refresh opportunities or new builds in which wireless was the primary or predominant connection to the enterprise network.

This use case can encompass single, small locations or large, campus-based enterprises and may include limited wired components to provide connectivity for WLAN or as incremental updates to expand an existing infrastructure. This network also may provide discovery, connectivity and security IoT endpoints, including headless devices. In addition to data connectivity, the implementation supports the use of the WLAN for voice calls, either from cellular smartphones or from softphones on desktop, laptop or tablet computing devices. This use case is typically observed for brownfield and refresh opportunities. Most users are typically badged employees, but contractors and guests also require connectivity. This buyer is typically highly technically competent and/or routinely makes granular changes to wired/WLAN infrastructure components.

## Vendors Added and Dropped

### Added

Gartner has split Cisco into two separate entities: Cisco (Catalyst) and Cisco (Meraki), because the two product lines differ broadly in functionality, architecture and customer base/target.

### Dropped

The following vendors have been dropped:

- D-Link — Gartner was unable to validate inclusion criteria for this year's Magic Quadrant.
- Dell — Gartner was unable to validate inclusion criteria for this year's Magic Quadrant.
- Rohde & Schwarz (LANCOM Systems) — Rohde and Schwarz did not meet the revenue criterion for this year's Magic Quadrant.
- Ruijie Networks — Ruijie did not meet the revenue criterion for this year's Magic Quadrant.
- Ubiquiti Networks — Gartner was unable to validate inclusion criteria for this year's Magic Quadrant.

# Inclusion Criteria

Table 1 lists the importance weighting associated with each capability present in the various use cases based on a percentage.

### Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

| *Critical Capabilities* | *Unified Wired and WLAN Access* | *Hands-Off NetOps* | *Remote Branch Office With Corporate HQ* | *Wired-Only Refresh/New Build* | *WLAN-Only Refresh/New Build* |
|---|---|---|---|---|---|
| Wired Access | 20% | 10% | 15% | 45% | 0% |
| WLAN Access | 25% | 20% | 25% | 0% | 45% |
| Identification and Network Access | 15% | 10% | 15% | 15% | 15% |
| Management and Administration | 15% | 20% | 20% | 15% | 15% |
| Additional Network Service Apps | 15% | 30% | 15% | 15% | 15% |
| IoT Device Containment | 10% | 10% | 10% | 10% | 10% |
| As of 25 October 2021 | | | | | |

Source: Gartner (November 2021)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

## Critical Capabilities Rating

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

### Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

| Critical Capabilities | ALE | Allied Telesis | Arista Networks | Cambium Networks | Cisco (Catalyst) | Cisco (Meraki) | CommScope | Extreme Networks | Fortinet | H3C | HPE (Aruba) | Huawei | Juniper | TP-Link |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Wired Access | 3.8 | 3.3 | 3.9 | 3.2 | 4.3 | 3.7 | 3.9 | 4.1 | 3.7 | 4.0 | 4.1 | 4.2 | 4.2 | 3.0 |
| WLAN Access | 3.7 | 3.1 | 3.7 | 4.1 | 4.2 | 3.8 | 3.9 | 4.2 | 3.9 | 3.7 | 4.3 | 4.1 | 4.5 | 3.1 |
| Identification and Network Access | 3.6 | 2.5 | 3.8 | 3.5 | 3.9 | 3.7 | 3.8 | 4.0 | 4.0 | 3.7 | 4.3 | 3.8 | 3.8 | 2.5 |
| Management and Administration | 3.7 | 2.8 | 3.5 | 3.5 | 3.6 | 3.7 | 3.6 | 3.9 | 3.6 | 3.6 | 4.1 | 4.1 | 4.0 | 2.7 |
| Additional Network Service Apps | 3.6 | 2.3 | 3.5 | 3.5 | 3.7 | 3.6 | 3.2 | 3.6 | 3.7 | 3.6 | 4.0 | 3.9 | 4.1 | 1.9 |
| IoT Device Containment | 3.5 | 1.9 | 3.6 | 3.5 | 3.8 | 3.6 | 3.6 | 4.1 | 3.9 | 3.5 | 4.1 | 3.8 | 4.1 | 1.0 |
| As of 25 October 2021 | | | | | | | | | | | | | | |

Source: Gartner (November 2021)

Table 3 shows the products/services scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the Critical Capabilities are met for each use case.

### Table 3: Product Score in Use Cases

(Enlarged table in Appendix)

| Use Cases | ALE | Allied Telesis | Arista Networks | Cambium Networks | Cisco (Catalyst) | Cisco (Meraki) | CommScope | Extreme Networks | Fortinet | H3C | HPE (Aruba) | Huawei | Juniper | TP-Link |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unified Wired and WLAN Access | 3.67 | 2.77 | 3.69 | 3.59 | 3.97 | 3.70 | 3.71 | 4.01 | 3.80 | 3.71 | 4.17 | 4.02 | 4.16 | 2.54 |
| Hands-Off NetOps | 3.65 | 2.64 | 3.62 | 3.59 | 3.87 | 3.68 | 3.59 | 3.92 | 3.77 | 3.66 | 4.13 | 3.99 | 4.14 | 2.38 |
| Remote Branch Office With Corporate HQ | 3.67 | 2.74 | 3.67 | 3.61 | 3.94 | 3.70 | 3.69 | 4.00 | 3.80 | 3.69 | 4.17 | 4.01 | 4.15 | 2.53 |
| Wired-Only Refresh/New Build | 3.70 | 2.82 | 3.74 | 3.37 | 4.00 | 3.68 | 3.71 | 3.98 | 3.75 | 3.79 | 4.12 | 4.04 | 4.09 | 2.52 |
| WLAN-Only Refresh/New Build | 3.65 | 2.73 | 3.65 | 3.77 | 3.95 | 3.72 | 3.71 | 4.03 | 3.84 | 3.65 | 4.21 | 4.00 | 4.22 | 2.56 |
| As of 25 October 2021 | | | | | | | | | | | | | | |

Source: Gartner (November 2021)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

## Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

## Document Revision History

Critical Capabilities for Wired and Wireless LAN Access Infrastructure - 10 November 2020

Critical Capabilities for Wired and Wireless LAN Access Infrastructure - 26 September 2019

Critical Capabilities for Wired and Wireless LAN Access Infrastructure - 21 August 2018

Critical Capabilities for Wired and Wireless LAN Access Infrastructure - 3 November 2017

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

How Products and Services Are Evaluated in Gartner Critical Capabilities

Navigating Emerging Network-as-a-Service Promises and Challenges

Three Ways to Improve Network Automation

## Table 1: Weighting for Critical Capabilities in Use Cases

| *Critical Capabilities* | *Unified Wired and WLAN Access* | *Hands-Off NetOps* | *Remote Branch Office With Corporate HQ* | *Wired-Only Refresh/New Build* | *WLAN-Only Refresh/New Build* |
|---|---|---|---|---|---|
| Wired Access | 20% | 10% | 15% | 45% | 0% |
| WLAN Access | 25% | 20% | 25% | 0% | 45% |
| Identification and Network Access | 15% | 10% | 15% | 15% | 15% |
| Management and Administration | 15% | 20% | 20% | 15% | 15% |
| Additional Network Service Apps | 15% | 30% | 15% | 15% | 15% |
| IoT Device Containment | 10% | 10% | 10% | 10% | 10% |
| As of 25 October 2021 | | | | | |

Source: Gartner (November 2021)

## Table 2: Product/Service Rating on Critical Capabilities

| *Critical Capabilities* | *ALE* | *Allied Telesis* | *Arista Networks* | *Cambium Networks* | *Cisco (Catalyst)* | *Cisco (Meraki)* | *CommScope* | *Extreme Networks* | *Fortinet* | *H3C* | *HPE (Aruba)* | *Huawei* | *Juniper* | *TP-Link* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Wired Access | 3.8 | 3.3 | 3.9 | 3.2 | 4.3 | 3.7 | 3.9 | 4.1 | 3.7 | 4.0 | 4.1 | 4.2 | 4.2 | 3.0 |
| WLAN Access | 3.7 | 3.1 | 3.7 | 4.1 | 4.2 | 3.8 | 3.9 | 4.2 | 3.9 | 3.7 | 4.3 | 4.1 | 4.5 | 3.1 |
| Identification and Network Access | 3.6 | 2.5 | 3.8 | 3.5 | 3.9 | 3.7 | 3.8 | 4.0 | 4.0 | 3.7 | 4.3 | 3.8 | 3.8 | 2.5 |
| Management and Administration | 3.7 | 2.8 | 3.5 | 3.5 | 3.6 | 3.7 | 3.6 | 3.9 | 3.6 | 3.6 | 4.1 | 4.1 | 4.0 | 2.7 |
| Additional Network Service Apps | 3.6 | 2.3 | 3.5 | 3.5 | 3.7 | 3.6 | 3.2 | 3.6 | 3.7 | 3.6 | 4.0 | 3.9 | 4.1 | 1.9 |
| IoT Device Containment | 3.5 | 1.9 | 3.6 | 3.5 | 3.8 | 3.6 | 3.6 | 4.1 | 3.9 | 3.5 | 4.1 | 3.8 | 4.1 | 1.0 |

As of 25 October 2021

Source: Gartner (November 2021)

## Table 3: Product Score in Use Cases

| *Use Cases* | *ALE* | *Allied Telesis* | *Arista Networks* | *Cambium Networks* | *Cisco (Catalyst)* | *Cisco (Meraki)* | *CommScope* | *Extreme Networks* | *Fortinet* | *H3C* | *HPE (Aruba)* | *Huawei* | *Juniper* | *TP-Link* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Unified Wired and WLAN Access | 3.67 | 2.77 | 3.69 | 3.59 | 3.97 | 3.70 | 3.71 | 4.01 | 3.80 | 3.71 | 4.17 | 4.02 | 4.16 | 2.54 |
| Hands-Off NetOps | 3.65 | 2.64 | 3.62 | 3.59 | 3.87 | 3.68 | 3.59 | 3.92 | 3.77 | 3.66 | 4.13 | 3.99 | 4.14 | 2.38 |
| Remote Branch Office With Corporate HQ | 3.67 | 2.74 | 3.67 | 3.61 | 3.94 | 3.70 | 3.69 | 4.00 | 3.80 | 3.69 | 4.17 | 4.01 | 4.15 | 2.53 |
| Wired-Only Refresh/New Build | 3.70 | 2.82 | 3.74 | 3.37 | 4.00 | 3.68 | 3.71 | 3.98 | 3.75 | 3.79 | 4.12 | 4.04 | 4.09 | 2.52 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| WLAN-Only Refresh/New Build | 3.65 | 2.73 | 3.65 | 3.77 | 3.95 | 3.72 | 3.71 | 4.03 | 3.84 | 3.65 | 4.21 | 4.00 | 4.22 | 2.56 |
| As of 25 October 2021 | | | | | | | | | | | | | | |

Source: Gartner (November 2021)