Magic Quadrant for the Wired and Wireless LAN Access Infrastructure

Published 24 September 2019 - ID G00368944 - 65 min read

Consolidation continues shaping enterprise choices for suitable campus and branch office access networking solutions. Infrastructure and operations leaders should use this research to identify vendors positioned to meet changing requirements for access network connectivity, services and management.

Strategic Planning Assumptions

By 2023, large enterprise exclusive use of artificial intelligence for IT operations and digital experience monitoring tools to monitor modern applications and infrastructure will rise from 5% in 2018 to 30%.

By 2022, 95% of organizations will still not know the connectivity requirements of all the IoT devices accessing their applications.

Market Definition/Description

Vendors covered in this research, which is intended for use by enterprise I&O leaders responsible for wired and wireless LAN access network infrastructure, provide hardware and software solutions to deliver connectivity to enterprise campus and branch location environments.

Gartner defines this market of vendors as supplying wired and wireless networking hardware and software that enable devices to connect to the enterprise wired LAN or Wi-Fi network. These devices include:

- Laptops
- Smartphones, tablets and other mobile smart devices

- Networked office equipment
- Sensors and other Internet of Things (IoT) endpoints
- Other fixed or mobile devices that communicate to a wired switch port or a wireless access point at the edge of the enterprise infrastructure

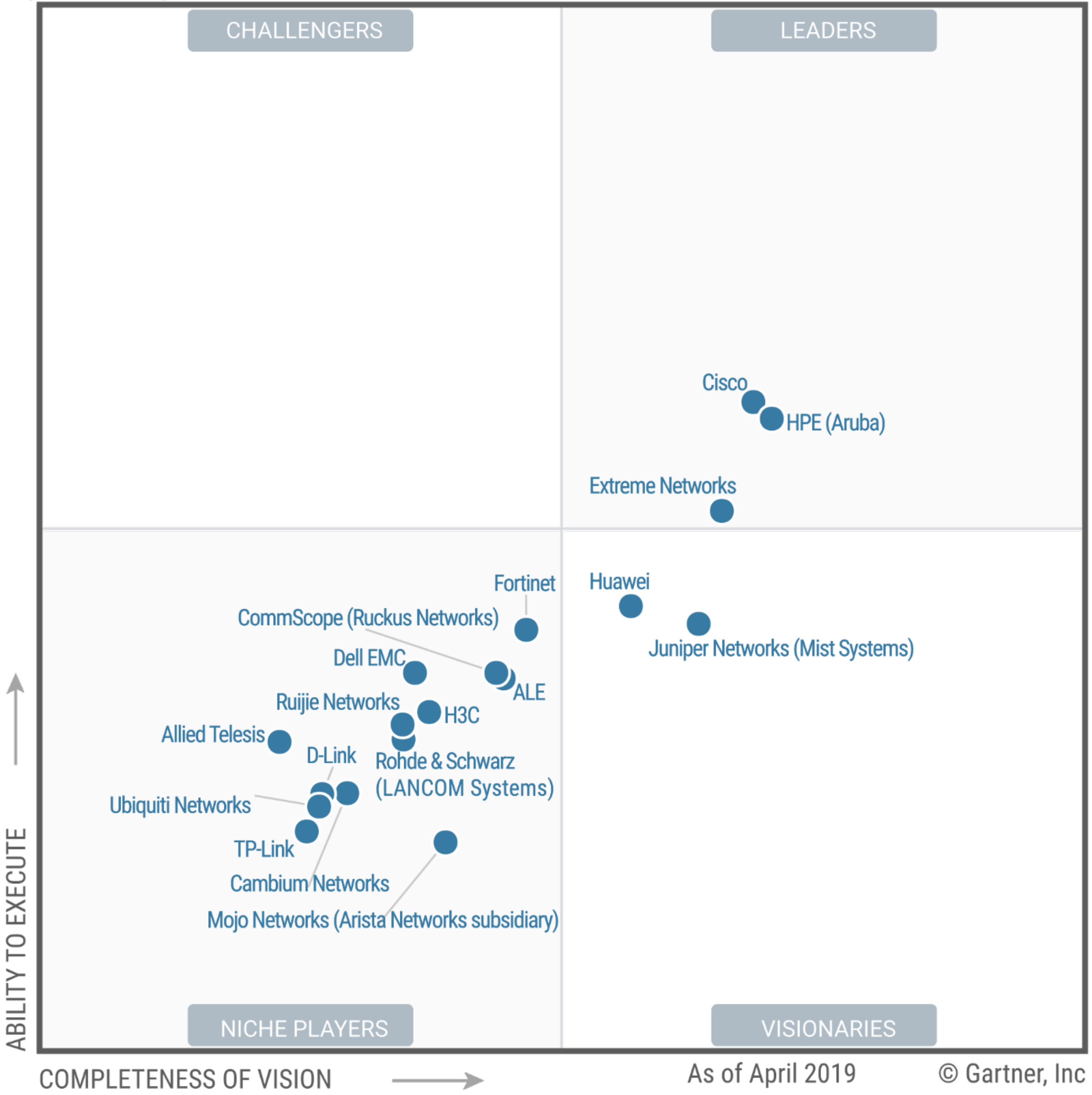
Wireless LAN (WLAN) infrastructure for most large enterprises (1,000-plus employees) is a “must have” for employee and guest or contractor network connectivity, especially as an organization expands to new facilities or plans a migration to “wireless-first” networking scenarios. The underlying technology — now at “Wi-Fi 6” branding for the 802.11ax current state-of-the-art technical standard — continues to evolve through an international standards process supporting ever-greater network throughput, client device density and granularity of network management. These attributes will grow in importance as consolidation of enterprise networks formerly managed as operating technology (OT) become critical elements of the IT domain. Driving this is proliferation of IoT endpoints for building control, security and other applications attaching to the access network. Most innovation, beyond the continuing iteration of standards-based hardware technology, is occurring in network service applications for configuration, provisioning, management and security of the access network, along with support for location-based services and other applications that the network enables. This includes applying machine learning and artificial intelligence to the huge datasets now generated by the access network and connected endpoints and applications, in order to incorporate more automation to network management, assurance, security and troubleshooting.

This research evaluates wired and wireless LAN access infrastructure solutions for enterprises that procure and manage their own access networks (i.e., “do it yourself” [DIY]). It does not cover wired and wireless access networking infrastructure for service providers such as telecom or other managed network service (MNS) providers. It also does not evaluate vendors based on their products for adjacent markets such as public venues, small office/home office, commercial and industrial settings, or point-to-point solutions.

Avoid limiting your choices solely to the vendors in this research. Supplement this analysis by including a regional or vertical-market-focused vendor that may be a good fit or that provides a competitive lever for your organization’s size or vertical industry.

Magic Quadrant

Figure 1. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure



Vendor Strengths and Cautions

ALE

ALE, based in Colombes, France — with its unified wired and WLAN infrastructure portfolio branded as Alcatel-Lucent Enterprise — continues to increase the emphasis on the vendor's homegrown product lines. Products primarily are OmniSwitch fixed format campus switches, OmniAccess Stellar wireless access points, and OmniVista on-premises and software as a service (SaaS) network management systems. The company, which is controlled by the investment firm China Huaxin, continues to offer WLAN hardware and management software provided by OEM HPE Aruba Networks, which, like its own product lines, are marketed under the Alcatel-Lucent Enterprise brand. The OmniVista Cirrus cloud-managed network solution has the same capabilities as the OmniVista 2500 on-premises network management system (NMS) for policy enforcement, network assurance, IoT device management and containment. ALE's network fabric technology enables automated network provisioning, segmentation and unified policy management based on the requirements defined by IT, rather than requiring manual command line interface (CLI)-based configuration.

The ALE market share for campus switches and WLAN equipment falls outside of the global top 10, based on Gartner figures. It should be included in evaluations for wired and wireless LAN implementations for the vendor's priority enterprise markets of transportation, hospitality, healthcare, education and government in its targeted national markets within the North America, Europe and Asia/Pacific (APAC) regions.

Strengths

- OmniVista 2500's network assurance features include predictive analytics that can suggest network configuration changes or firmware updates for uses such as capacity planning or incident management. The solution identifies anomalies in network performance based on KPIs such as network status and availability, or WLAN access point (AP) throughput.
- Customer feedback among vendor references and in other comments to Gartner is generally positive for performance stability of switches and APs, OmniVista 2500 features and functionality, and ALE customer support, with some mixed reviews regarding ease of implementation and configuration.

- ALE accredited channel partners will support a service-level agreement ensuring that the partner will remediate an ALE access network that does not meet the customer's documented performance requirements for KPIs, such as round-trip latency, jitter and packet loss.

Cautions

- ALE and its partners serve customers in more than 50 countries globally, but ALE realizes most of its business in 30 countries. Clients outside of those markets, such as in Latin America outside of Brazil, Argentina or Mexico, should ensure ALE or its partners can provide sufficient local postsale support.
- ALE has targeted midsize enterprises for its go-to-market and promotional efforts in wired and wireless LAN infrastructure, and has generated little client inquiry with Gartner. Combined with its small shares of the campus switch and WLAN access point markets, this indicates low overall market visibility that could affect the vendor's capability to grow.
- The OmniVista 2500 management system supports discovery and monitoring of non-ALE third-party wired and WLAN devices using Simple Network Management Protocol (SNMP) capabilities, in addition to management APIs and automation technology (iFab) to simplify interoperability with third-party devices. Customers who want to manage a multivendor network infrastructure must verify if any additional integration efforts are necessary.

Allied Telesis

Allied Telesis, headquartered in Tokyo, Japan, offers an end-to-end wired and wireless LAN portfolio. Enterprises can manage the switching and WLAN product portfolio on-premises with Vista Manager EX or in the private or public cloud using Autonomous Management Framework (AMF) cloud. Customers requiring a controller-based architecture must use the Autonomous Wave Control (AWC) plug-in with the vendor's Vista Manager EX unified management solution or integrated with Allied's AR-Series Firewall products. Vista Manager EX provides the SNMP plug-in for multivendor management support, and an SD-WAN plug-in is planned for late 2019. The Allied Telesis AMF delivers a suite of features to automate configuration management and simplify network management. All Allied Telesis products, including industrial-grade switches, use the same operating system (AlliedWare Plus) for uniform functionality, support, migration and upgradability. The WLAN portfolio includes the TQ Series APs based on the AWC and the TQm/MWS series with basic management for smaller networks.

Allied Telesis sells predominantly through channels, generating more than 50% of its revenue in Japan. Although it ranked No. 9 and No. 10 in global campus switch revenue and port shipments during 2018, it was outside the top 10 in market share for WLAN equipment, according to Gartner figures. Although it has a global footprint, Allied Telesis mainly targets the public sector, education, healthcare and hospitality vertical markets. Predominantly small and midsize enterprises in the Asia/Pacific, North America and EMEA regions should assess Allied Telesis to meet their wired and wireless LAN infrastructure needs.

Strengths

- Vista Manager EX/AMF can also be integrated via an API with Allied Telesis Secure Enterprise Software Defined Networking (SES), an SDN controller that integrates with the firewall to manage policy enforcement and automate endpoint isolation.
- Allied Telesis has APs that support its “channel blanket” architecture, which can simplify channel planning and enable seamless roaming in high-density environments by eliminating co-channel interference.
- Allied Telesis’ roadmap with Vista Manager EX, which will include an add-on for SD-WAN in late 2019, aligns with customers’ growing needs for platforms that integrate LAN, WLAN and WAN network management.

Cautions

- Allied Telesis has limited capabilities for real-time traffic analysis, security behavioral analytics and network assurance through AI/ML. Indoor location-based services through Vista Manager EX are planned for late 2019.
- Although AMF supports IoT endpoint discovery, Allied Telesis does not have the range of profiling capabilities (e.g., fingerprinting libraries) compared with other leading solutions in the market.
- The vendor’s single-channel architecture has its limitations. To avoid interference in different parts of a building requires APs to be grouped, with each group operating on its own channel, although this can still be managed as a single wireless network.

Cambium Networks

Cambium Networks is a publicly held vendor based out of Rolling Meadows, Illinois. Focused primarily on wireless infrastructure products for carriers and managed network service providers, its wired and wireless enterprise business targets primarily the retail and hospitality verticals. Cambium announced on 8 August 2019 that it had acquired the Xirrus WLAN infrastructure business from Riverbed Technology. The enterprise-focused product ecosystem it had before the acquisition, during the evaluation period of this research, consisted of cnPilot wireless, cnMatrix access switching and cnMaestro, a cloud-based management platform that provides single-pane-of-glass visibility into Cambium products and zero-touch provisioning. Cambium's cnMaestro product supports multitenancy and integration with billing and ticketing systems. The only Cambium cnPilot enterprise access points available before the Xirrus deal were 802.11ac Wave 2.

Before the acquisition, Cambium's enterprise wireless business accounted for only about 10% of its overall revenue but had grown at a 24% rate from the previous year. The vendor ranked below the top 10 in market share for campus switches and WLAN equipment in 2018, according to Gartner figures. Gartner recommends that small and midsize entities in the hospitality, retail and K-12 verticals, as well as government organizations, consider Cambium Networks for basic small and midsize wired and wireless deployments.

Strengths

- The Xirrus acquisition significantly expands Cambium's portfolio, with Xirrus' controllerless, distributed architecture that places application and policy control, locationing, analytics and firewall capability in the AP.
- The cnMatrix switching platform, although focused on small and midsize edge deployments, includes advanced capabilities such as policy-based automation and network segmentation, and it enables policy integration between the wired and wireless segments.
- Cambium's enterprise wireless and wired portfolio includes advanced features such as automation, policy-based segmentation and zero-touch provisioning, all managed through cnMaestro, which is a simple, yet powerful, GUI interface.

Cautions

- In Xirrus, Cambium is acquiring a WLAN infrastructure portfolio suitable for large-enterprise requirements, but it has very little enterprise experience itself above small and midsize deployments. Clients must conduct appropriate due diligence to ensure Cambium is effectively addressing challenges related to integration with Xirrus' sales channel, technologies and product portfolio.
- Cambium's own product line has yet to deliver 802.3bz support. Although the markets for these technologies are still nascent, this product gap puts its current wired and wireless portfolio at a technology disadvantage versus competitors offering numerous APs and switches with the feature.
- Cambium's own product line lacks key features such as security behavioral analytics, application SLAs and anomalous behavior detection, which places it behind all of its closest competitors in the enterprise space.

Cisco

Cisco, based in San Jose, California, continues to deliver a broad portfolio of access wired switching, WLAN products, network applications and services. Its "wireless-first" initiative in 2018 and early 2019 saw the introduction of multigigabit Ethernet (mGig) switches, prestandards-based Wi-Fi 6 and a new line of wireless controller platforms. The Cisco management team effectively is leveraging core competencies across Catalyst and Meraki product lines. The introduction of an access layer "fabric in a box" and the expansion of SD-Access are a foundational strategy as Cisco continues to build its ability to self-optimize the access layer with machine learning. Cisco has struggled in the past with its licensing schema, but in 2018, it launched a simplified structure. However, Gartner client feedback has been mixed, including some confusion about its actual costs and features, such as mandatory subscription licenses for some hardware.

Cisco continues to be the market share leader for campus switch and WLAN access layer connectivity. Cisco switch revenue and ports increased approximately 10% but slipped market share by 1% in 2018. WLAN revenue increased year over year (YoY) by 10%. Cisco's access point market share grew 1.5%. Cisco continues to offer two access layer solutions: Aironet/Catalyst and Meraki, which are loosely tied together through Cisco DNA Center. Clients should consider Cisco globally for all enterprise on-premises and cloud-based access layer opportunities.

Strengths

- Cisco DNA Center is able to address multivendor network management through device packs, which allow a single pane of glass for access layer wired and wireless management.
- The vendor is improving connections between divergent product families via DNA Center. DNA Center provides a single touchpoint that provides automation, analytics, policy management, the ability to tie the Aironet/Catalyst and Meraki product lines together, and the ability to deploy either in the cloud or on-premises.
- Meraki's video capabilities and advanced personnel-counting functionality enhance many of the expanded requirements for location-based services.

Cautions

- Although Cisco plans to merge its cloud and on-premises product lines, clients need to assure that the required functionality is being delivered for the solution they are deploying, such as Cisco DNA Center on-premises DNA Assurance versus cloud-based Meraki Wireless Health.
- Cisco's sales organization includes representatives that specialize in Meraki cloud-managed products rather than the Catalyst on-premises line, so end users must assure that desired network application capabilities are available in their chosen solution.
- Clients must be aware that addressing core issues such as IoT requires advanced licensing, such as DNA Premier, or a separate purchase of Cisco Identity Services Engine (ISE), for policy enforcement.

CommScope (Ruckus Networks)

Ruckus Networks is headquartered in Sunnyvale, California, and focuses primarily on the hospitality, education and government verticals. It became a unit of CommScope, a telecom networking equipment vendor, in April 2019 via CommScope's acquisition of Ruckus' parent company, ARRIS. Ruckus provides a full network ecosystem of wired and wireless products with a focus on enterprisewide central management via Ruckus SmartZoneOS. SmartZone Network Controllers can be deployed on-premises or in a public cloud and enable converged network management, multitenant capabilities, analytics, guess access, zero-touch provisioning and reporting. Ruckus access points are available in both controller and controllerless architectures with both on-premises and off-premises management capabilities. The Ruckus R730 access point is prestandards-based 802.11ax (Wi-Fi 6)-compliant and includes Bluetooth low energy (BLE) and Zigbee functionality for IoT endpoints. Ruckus ICX switches offer access, distribution and core switches with multigigabit access and up to 100G uplink and stack capabilities. The Cloudpath solution available as SaaS or on-premises provides centralized policy enforcement, including network access for guest or bring your own device (BYOD) devices.

Ruckus garnered the No. 5 and No. 6 global market shares for WLAN unit shipments and revenue respectively in 2018, while finishing at No. 8 in campus switch revenue, according to Gartner figures. Enterprises located in North America, EMEA and APAC should include Ruckus in consideration for all standard use cases.

Strengths

- Ruckus provides a converged wired and wireless network controller-based architecture that integrates management though a unified control and management plane. Ruckus offers three controllers: ZoneDirector, SmartZone and Ruckus Cloud. ZoneDirector is aimed at smaller, less-complex deployments, while Ruckus Cloud is aimed at multisite deployments with little IT presence. SmartZone is positioned for larger enterprise deployments.
- The Cloudpath Enrollment System, a centralized policy and enrollment system, enables device onboarding for user and IoT devices across both the wired and wireless network.
- SmartZoneOS includes a full set of open REST/JSON and streaming telemetry for network management integration of deployments in a typical hybrid environment.

Cautions

- During the evaluation period, Ruckus was missing capabilities its competitors have already brought to market, including Layer 2 network overlay technologies such as analytics or AI-/ML-integrated automation.
- CommScope is Ruckus' third corporate owner since 2017. Clients should validate that the vendor's global sales and support resources, which can be affected by repeated corporate transitions, are able to support the entire access layer.
- Because Ruckus has historically not seen much traction in the carpeted enterprise vertical, its experience and performance in large and complex environments is still

relatively unknown. Clients with access network requirements for large carpeted enterprise environments should ask for customer references specific to those needs.

Dell EMC

Dell EMC is a division of Dell Technologies, a publicly traded company headquartered in Round Rock, Texas. Dell's wired and wireless infrastructure business focuses on enterprise, education, public sector and healthcare/life sciences verticals, on a global scale. Dell EMC offers a mix of its own PowerSwitch N Series campus switches in addition to wireless network products from both CommScope/Ruckus and Aerohive, which now is owned by Extreme Networks. Additionally, Dell EMC has invested heavily in Open Network Install Environment (ONIE)-enabled open switch platforms that can support multiple third-party network operating systems such as Cumulus and Pica8, in addition to its in-house OS6 campus network operating system. All PowerSwitches are either stand-alone or stackable and focused for varying requirements of the access layer.

Dell EMC offers Aerohive's HiveManager NG as its on-premises/cloud-based management platform and utilizes ZoneDirector or SmartZone for wireless management of Ruckus wireless infrastructures. Both HiveManager and Ruckus SmartCell Insight provide network analytics. Dell offers RSA NetWitness, which is used for security behavioral analytics. Additionally, SonicWall can also be used for advanced threat protection. The vendor provides fabricwide policy enforcement through its partner solutions, including Aerohive's A3 NAC and Ruckus' Cloudpath. Dell's Pulse IoT solution identifies, onboards and monitors IoT endpoints, securing their traffic via an HTTPS tunnel. Enterprises located globally should consider evaluating Dell EMC in its targeted vertical markets.

Strengths

- Dell EMC has one of the largest ecosystems at the network access layer. By combining its wired switches and wireless OEM equipment with management, analytics and security, it provides a high degree of deployment flexibility.
- Dell EMC's support for ONIE provides a credible "brite box" solution at the access layer for enterprises that want to embrace open networking.
- Dell EMC offers a global footprint for sales and support and augments the capabilities of many of its OEM partners that could not support global customers otherwise.

Additionally, Dell EMC offers enterprise credibility and experience at deploying in complex environments at scale.

Cautions

- The acquisitions of OEMs on which Dell is totally reliant for WLAN infrastructure — that is, Ruckus and Aerohive — make the future of those relationships unclear. Dell EMC is totally reliant on its OEMs for security, analytics and other services, which means that clients must be aware of potential support issues because Dell EMC cannot control OEM product roadmaps or guarantee compatibility across a unified fabric.
- Dell's reliance on Aerohive for wireless LAN hardware and the HiveManager management solution makes it dependent on continuation of its current integration agreements with that vendor. Future changes to the relationship raise the risk that it will have to engage a different strategic partner to maintain the unified access layer capabilities it has now.
- Dell EMC lacks many advanced enterprise capabilities in this segment of the market, such as automation, central policy enforcement, intent-based networking analytics, AI/ML and overlay architectures. Because Dell EMC relies on its various OEM partnerships to supply much of its technology components, it makes delivering such technologies more difficult.

D-Link

D-Link, based in Taipei, Taiwan, provides switching and APs manageable as a unified wired and wireless access network, with an enterprise focus on small and midsize organizations. The company competes with larger-enterprise-oriented vendors largely as a low-cost provider supporting basic connectivity and network management capabilities; it also offers on-premises or cloud-based management options. The vendor's primary network management solutions are the Nuclias Cloud NMS and D-View 7, a web-based, on-premises option that utilizes local network probes to collect data from SNMP devices for local and remote network monitoring, management and troubleshooting. This also is D-Link's solution for identifying and securing traffic from IoT devices attached to the access network.

D-Link ranked fourth globally in enterprise campus switch port shipments during 2018, but outside of the top 10 in enterprise AP shipments. The vendor had the No. 5 global share of campus switch port shipments in 2018 but was below the top 10 in enterprise

WLAN equipment, according to Gartner figures. Midsize and large enterprises in emerging markets, EMEA and Asia/Pacific, where D-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 and low support needs.

Strengths

- D-Link is a low-priced solution offering a broad range of indoor and outdoor wireless APs, plus managed and unmanaged stackable Ethernet campus switches suitable for basic networking use cases.
- The Nuclias Cloud subscription includes guest network access features such as customizable captive portal and social media login.
- The D-View web-based management solution can support multivendor device deployments via customization of the third-party hardware's simple ontology for intrusion detection (SOID) and use of CLI commands for standard management and monitoring.

Cautions

- D-Link declined to provide customer references for this research, and Gartner rarely receives client inquiries regarding the vendor. While customer feedback to Gartner Peer Insights is generally positive, some customers report difficulty getting enough tech support in their region. Clients considering this vendor should verify that needed postsale support will be available in their locations and should request customer references from their value-added reseller (VAR) or other D-Link channel partner.
- During the evaluation period for this research, D-Link's Nuclias Cloud-managed infrastructure supported only its DBA AP and DBS-2000 switch models, with on-premises management requiring different product lines. This may limit the appeal to clients with hybrid deployments that require on-premises and cloud management.
- Beyond basic network management and service applications, D-Link does not provide capabilities for more complex deployments such as location-based service applications or security behavioral analytics. It also does not yet support machine learning features for automating access layer connectivity, limiting its utility to enterprise networking requirements.

Extreme Networks

Extreme Networks is a wired/wireless LAN access layer vendor based in San Jose, California, that continues to expand globally. After the start of this research, Extreme Networks acquired Aerohive Networks and completed the deal in 3Q19, adding to its portfolio Aerohive technology that includes SD-WAN and cloud-based management solutions. (Note: Extreme Networks closed its acquisition of Aerohive on 9 August 2019 during the production of this Magic Quadrant.) In 2018, 75% of Extreme’s edge portfolio was refreshed and includes the introduction of 802.3bz switches as well as prestandards-based 802.11ax (Wi-Fi 6) access points and a suite of network applications. The growth-by-acquisition strategy has worked well for Extreme in its wired and WLAN business, which has excelled at provided technical migration strategies for clients, including new access point platforms that can be loaded with differing software personalities. The introduction of Extreme’s “Elements” marketing campaign provides an excellent example of the modularity of the portfolio and the differing requirements of targeted vertical markets. Extreme Fabric Attach modules address the growing need for IoT segmentation that are not able to natively use the virtual segmentation and encryption functionality of Extreme’s access layer fabric.

Aided by acquisitions and organic growth, Extreme campus switch revenue and ports increased by more than 50%, according to Gartner forecasting data, while also increasing market share in 2018. Combined, Extreme and Aerohive had a 4.7% share of the global WLAN equipment market in 2018.

Gartner expects that Aerohive clients will continue to receive sales and other support through existing channels at least through year-end 2020. Clients should consider Extreme Networks, along with its legacy Aerohive products, globally for all wired/wireless LAN access layer opportunities.

Strengths

- The Extreme Defender for IoT provides the access layer fabric connectivity and security for devices that are not natively able to use the fabric for virtual segmentation.
- The release of a single platform access point that can be loaded with different software personalities not only leverages economies of scale, but also provides migration strategies for customers that are part of Extreme acquisitions.

- Extreme Fabric addresses client needs for IoT segmentation through role-based policy enforcement and tunnels that can be encrypted for any enterprise devices across its wired and wireless LAN product portfolio.

Cautions

- Clients have reported Extreme sales channel execution issues that will require additional training to articulate breadth of product and differentiation. Integration of the Aerohive sales channel, technologies and product portfolio could present additional, similar challenges that may affect Extreme's growth capabilities.
- Extreme's cloud strategy is in flux, especially for MNS capabilities. Clients should define on-premises and cloud-based requirements to assure that the vendor can meet them.
- Extreme continues to lag behind on location capabilities that lack the granularity of competitive offerings. Organizations using location solutions from ExtremeWireless or ExtremeWireless WiNG need to document and test to assure that the technology addresses the use case.

Fortinet

Fortinet is a public company headquartered in Sunnyvale, California, that is focused on enterprise, retail, healthcare and education verticals largely in North America and EMEA. Fortinet provides a wired and wireless access ecosystem anchored by the FortiGate firewall product that includes an integrated WLAN controller and switch capability. Fortinet's FortiGate, FortiCloud and FortiOS are core to its portfolio and offer automation for functions such as component provisioning as well as expanded integration capabilities for users, user devices and IoT endpoints. Fortinet acquired ZoneFox late in 2018 and introduced FortiInsight, which provides security-based user and entity behavior analytics (UEBA) in addition to service assurance management. Network analytics are provided by FortiGate, but also by FortiWLM, which can be deployed either on-premises or in the cloud. In 2018, Fortinet acquired Bradford Networks and integrated the technology into its ecosystem as FortiNAC. FortiNAC provides centralized user and device profiling.

During 2018, the vendor's market share for campus switches and enterprise WLAN equipment was outside the global top 10, according to Gartner figures. Enterprises globally should consider Fortinet specially when prior investments in Fortinet have been made, or when a simplified and unified access network and security ecosystem is required.

Strengths

- The unified wired and wireless network architecture is built around a strong security architecture and offers simplified configuration, management and operational capabilities.
- The FortiNAC appliance provides centralized and simple device and user profiling as well as simplified IoT device onboarding throughout a Fortinet fabric.
- Fortinet effectively has acquired and integrated complementary products into its unified ecosystem to increase the functionality of the overall security, simplicity and application visibility functionality. The acquired products do not feel “bolted on,” but rather, they are organically integrated into the existing unified fabric.

Cautions

- Current lack of multigigabit ports on switches places the portfolio at a disadvantage versus competitors’ products.
- Fortinet continues to increase its ecosystem footprint with multiple separate appliances and servers instead of consolidating them. This causes confusion and duplication of many functions across its security, analytics and management platforms.
- Fortinet products have many features that are attractive to large enterprises. However, the underlying hardware portfolio often lacks models with the performance at scale to match the software capabilities. This disjointed product approach confuses many companies regarding the actual fit and value of the Fortinet ecosystem in large and complex enterprise network environments.

H3C

H3C Group, headquartered in Beijing and Hangzhou, China, provides a full portfolio of access layer networking solutions primarily to customers in its home market of China. The company was formed by the 2016 acquisition of a 51% stake in HPE’s former H3C subsidiary by Unisplendour, a subsidiary of Tsinghua Holdings.

H3C provides unified wired/wireless management with the intelligent Management Center (iMC). iMC is a large on-premises-based management platform with a series of modules for applications such as user and device profiling, policy enforcement, network traffic analysis, and management of quality of service (QoS) configurations. For the cloud, H3C offers the Oasis platform, with more granular analytics introduced in 2018, that is aimed at reducing operations and maintenance costs, predominantly for wireless. Oasis can also be deployed in a private cloud or through the Wireless Beneath Cloud (WBC) controller, which also supports location-based services, analytics and network assurance services.

H3C's Seer Network Architecture (SNA) provides AI-driven capabilities for network assurance and automation. SNA Center acts as the unified management platform, while the SeerAnalyzer component provides analysis and health information for network, user and application elements.

The vendor had the No. 4 and No. 5 market shares for campus switch and WLAN AP revenue, respectively, in 2018, according to Gartner figures. Although its target customer base includes service providers and smart city deployments, H3C corporate vertical markets include education, healthcare and government sectors. Clients with Asia/Pacific access layer opportunities can consider H3C for enterprise campus and branch office deployments.

Strengths

- The operations and management functionality of Oasis provides analytics that look at the health of network devices and users; analyze connection, authentication and interference issues; and provide suggestions for network optimization.
- The Oasis IoT platform can be deployed on-premises and in the cloud. It provides management and automatic onboarding of IoT devices, certificate authentication and secure encrypted traffic.
- SNA provides wired/wireless policy-driven automation and troubleshooting capabilities through Layer 2 to Layer 7 correlation analysis, resulting in more granular analytics of network issues.

Cautions

- H3C offers 24/7 support in only a few countries. Organizations outside of that market should require detailed documentation regarding the level of vendor or partner support for implementation and postsale service and support available at their locations.

- The Oasis cloud-managed network platform is deployed in China and abroad. However, for public cloud versions, organizations outside of China must use the Microsoft Azure public cloud in Singapore, limiting its flexibility for clients seeking more geographic diversity.
- The network assurance capabilities of the Oasis operations and maintenance (O&M) platform are predominantly centered on wireless connectivity only.

HPE (Aruba)

Aruba operates as a subsidiary of HPE and is based in San Jose, California. Aruba is the second-largest vendor in the wired/wireless LAN access layer worldwide market and includes an extensive portfolio of wired switching, access points, networking applications and services. Aruba's Mobile First Architecture provides indoor and outdoor access layer solutions, including 802.3bz switching and pre-standards-based 802.11ax (Wi-Fi 6) access points that address the business requirements for a broad set of verticals, including carpeted enterprise, retail and healthcare. Its marketing message, "The Experience Edge," explains the needs of enterprises with a software-driven architecture that extends from the campus and is well-received by traditional audiences. In 2019, Gartner found that Aruba's messaging also addressed the diverse management and security needs of organizations with IoT devices. End users should be aware that HPE Pointnext offers Aruba on a "networking as a service" consumption model. This model allows organizations to use wired and WLAN infrastructure on a differentiated operating expenditure (opex)-based subscription, rather than spending capital expenditure (capex) to own the access layer solution.

Aruba had the No. 3 share of global campus switch and the No. 2 share of WLAN equipment revenue during 2018, according to Gartner figures. Evaluate Aruba globally for all wired/wireless LAN access layer opportunities.

Strengths

- Aruba's approach to dynamic segmentation allows switches and access points to use Generic Routing Encapsulation (GRE) tunnels to encrypt any device traffic, including IoT, to its policy enforcement engine. The tunnel can be extended across third-party components that may exist in the network, or network architects can use VXLAN for unencrypted overlay traffic communication.

- Aruba's automation and AI/ML portfolio includes solutions such as its sensor-based, cloud-hosted User Experience Insight, which provides Layer 1 to Layer 7 data that is used to monitor end-user physical communications and applications. It also includes a closed-loop setting in its NetInsight solution that allows the network to take recommended actions that range from optimization to remediation.
- Aruba's AirWave management application can address multivendor management, which allows a single pane of glass for clients that are migrating from previously installed vendor solutions.

Cautions

- Automation tools such as NetEdit are only available on AOS-CX switches, one of multiple switching OSs the vendor supports. If configuration and verification are needed for all network components, clients will need to make sure additional management applications are deployed to meet their needs.
- Aruba Central, Aruba's cloud offering, currently lacks the ability to fully address requirements of clients who are looking for "hybrid" usage of both cloud and on-premises applications. In these scenarios, remote offices prefer cloud-based applications while the campus environment prefers on-premises capabilities.
- Aruba's Meridian location service product family does not address all differing asset- and people-tracking use cases. Clients that need to address more than Wi-Fi and BLE will need to consider other vendors.

Huawei

Huawei, headquartered in Shenzhen, China, provides a large portfolio of access layer networking solutions. While predominantly serving its home market of China, the company has expanded its market share in EMEA, Latin America and other countries in Asia. As part of its broader "Intent-Driven Network" architecture, the CloudCampus Solution represents Huawei's end-to-end flagship offering for campus networking, and the Agile Controller-Campus (AC-Campus) broadly serves as the foundation of its network service applications. These include onboarding services, access control, policy enforcement, traffic monitoring, application visibility, WLAN configuration and deployment, location services, and guest access. Agile Controller authenticates IoT endpoints using MAC addresses or PKI certificates and can deliver endpoint security policies to the edge network device, such as a wireless AP. Huawei supports IoT network segmentation using VXLAN. The AC-Campus can be deployed both on-premises and in a private cloud implementation, leveraging eSight for integrated management of wired and wireless networks.

Early in 2018, Huawei introduced CampusInsight, a software suite that provides analytical reporting and automation for network service assurance.

Huawei is the third-largest vendor in the wired/wireless LAN access layer worldwide market based on its global share for campus switch and WLAN equipment, growing well above market rates. Clients should evaluate Huawei for all wired/wireless LAN access layer opportunities, especially for locations in China and EMEA, where it has a sizable installed base.

Strengths

- Huawei’s product strategy, vision and roadmap on intent-based networking align with customers’ growing needs. CampusInsight provides network assurance through quality assessment, root cause analysis and automatic identification of network issues.
- Huawei switches can identify features of encrypted traffic and report potentially suspicious activity to the CIS (Cybersecurity Intelligent System) for detection of advanced threats through behavioral analytics.
- Agile Controller 3.0 is highly scalable (up to 200,000 network devices). Software licensing options deliver functionality encompassing authentication, authorization and accounting (AAA) security, onboarding, guest access management and security orchestration.

Cautions

- China and the EMEA regions generated more than 87% of the access networking revenue in 2018 for Huawei, which also reported stable growth in Latin America and Asia/Pacific regions. Organizations in other regions should evaluate the sufficiency of support for implementation and service of Huawei solutions in their specific locations.
- Huawei’s end-to-end location services rely on partnerships that complement its broader customer value proposition. Organizations should ask for proof points and review Huawei’s ecosystem of partners for additional capabilities.

- Given client concerns regarding political and trade issues between the U.S. and China, risk-averse organizations outside China should conduct due diligence to ensure long-term continuous supply of Huawei access networking solutions.

Juniper Networks (Mist Systems)

Juniper Networks is a public vendor based in Sunnyvale, California. In April 2019, Juniper acquired Mist Systems, which is based in Cupertino, California. The combined organization has a broad access layer portfolio that includes multigigabit EX switching (from Juniper Networks) and prestandards-based 802.11ax (Wi-Fi 6) with a third radio for spectrum monitoring and security threat detection (from Mist). The vendor also offers a patented 16-element BLE antenna array access points. The acquisition addresses Juniper's lack of in-house Wi-Fi domain expertise and provides Mist with an established access layer switching portfolio.

The new organization is expanding on Mist's historical market message of the "AI-driven enterprise" that has been gaining significant traction for the last two years in major enterprise access layer decisions. Mist's cloud-native, microservices-based architecture provides guest access, network management and policy applications, as well as analytics, IoT segmentation, hybrid cloud and AI-driven behavioral analysis at scale. Organizations will need to assure that Juniper-Mist can effectively add the Juniper switching portfolio into the Mist architecture at the level needed to achieve the differentiation that Mist has been able to provide to the wireless community. This will include integration in terms of proactive operations and predictive recommendations to provide network assurance and automation.

Juniper was the No. 6 global campus switch vendor in 2018 but ranked below the top 10 in market share for enterprise WLAN equipment, according to Gartner figures. Juniper-Mist should be evaluated globally for all wired and wireless access layer opportunities.

Strengths

- Juniper-Mist continues to improve the customer support experience by putting every support ticket through its Marvis AI platform for continuous learning capability through a feedback loop that predicts customer issues, proactively notifies IT admins and provides a high-reliability network.

- Juniper’s Mist Edge provides the ability to extend the cloud microservices application environment to on-premises environments, enabling a single management environment that addresses both remote and local campus network service application requirements.
- Juniper-Mist offers service-level assurance that provides continuous service-level monitoring and proactive action, as well as automated notification. A 24/7 network operations center (NOC) service preemptively addresses hardware and software customer issues, thereby eliminating downtime and false alarms.

Cautions

- The acquisition of Mist by Juniper is recent and will require time for employee integration. Clients should validate that their global sales and support resources are able to support the entire access layer.
- The integration of the two product portfolios will take time, even though both vendors began working together before the acquisition and launched some integrated features after the evaluation period of this research. Clients need to verify and test that the functionality and differentiation needed for business decisions and automation can be delivered.
- Wi-Fi and BLE location services do not address all of the location requirements in targeted vertical markets. Clients must document the cross-functional requirements for the entire enterprise and, if needed, deploy platform-based location service vendors to prevent having to implement multiple vendors or overlay solutions.

Mojo Networks (Arista Networks subsidiary)

Mojo Networks is a subsidiary of Arista Networks, based in Santa Clara, California. Arista acquired Mojo in August 2018. Arista expected to fully complete the merger with regulatory approval of its Mojo Indian subsidiary with Arista India in the company's fourth fiscal quarter of 2019. Through the acquisition, Arista added WLAN products from Mojo Networks’ cloud-managed Cognitive Wi-Fi portfolio of access points and applications. Its planned campus switching portfolio includes the Arista 7300X3 and 7050X3, as well as the 720XP Series announced in 2Q19. The Mojo portfolio offers prestandards-based 802.11ax and 802.3bz capabilities in its C-250 access point, as well as other access points to address target vertical market requirements. Although the C-250 and 720XP have been announced and were in field trials during the evaluation period for this research, clients should validate general product availability and support in their specific geography. The ability to deploy the solution in the cloud or on-premises provides the flexibility needed by many organizations.

Many of the Cognitive WiFi network service applications work with the WLAN components. However, it is unclear how well the data from the legacy and planned Arista switches (which were in development before the acquisition) work in conjunction with the Wi-Fi data in the root cause analysis engine or CloudVision Device Analyzer. Arista uses a Virtual Extensible LAN (VXLAN) fabric for group-based segmentation across the wired and wireless LAN portfolio to address issues such as campus IoT issues.

Mojo did not rank in the top 10 for campus switches or WLAN equipment, according to Gartner market share figures. Evaluate Mojo Networks in North America and Europe for all cloud-based access layer connectivity projects and globally through partners that provide the required ability to support installations.

Strengths

- Mojo's CloudVision WiFi collects data from a third radio on the access points to profile and test the network. It uses machine learning algorithms to create a network baseline that automatically detects and highlights potential issues.
- Mojo's CloudVision WiFi tracks when and why clients fail to connect to the network, reporting issues that can be used by network administrators for troubleshooting.
- Network analytics is provided within Cognitive WiFi, with machine learning and a big data platform tracking more than 300 KPIs.

Cautions

- Mojo did not provide company and product profile information or client references for this research. Organizations need to verify that the vendor can address all campus business, product and support requirements, including sales support in required global regions, before selecting the vendor.
- Mojo uses presence, zone and engagement analytics to provide limited location-based services. Clients with expanded requirements will need to consider overlay vendors to address the additional location needs of many vertical markets.

- As of publication, it is unclear how deep the integration of switches is with the Wi-Fi portfolio because all the datasheets continue to reference Wi-Fi only. Clients looking for a complete access layer solution should test to assure that all functionality, including the root cause analysis engine and analytics, apply to wired switches as well as the WLAN components.

Rohde & Schwarz (LANCOM Systems)

LANCOM Systems is a wholly owned, independently operating subsidiary of Rohde & Schwarz, an international electronics company based in Munich, Germany. Although some 70% of sales are with companies of less than 1,000 employees, the vendor provides a broad enterprise-grade portfolio of wired campus switches, wireless indoor and outdoor APs, and network management applications. The primary management solution is LANCOM Management Cloud (LMC), which orchestrates automated configuration of the vendor’s wireless APs and supports centralized configuration of wired campus switches. The E series of LANCOM’s wireless APs include a separate radio module for controlling the vendor’s primary IoT solution, its ePaper digital displays used for applications in retail, logistics and office environments. The LN-1700 B series APs integrate a Bluetooth low energy module to support location-based applications such as iBeacons.

Unlike the larger vendors in this research, LANCOM does not provide a dedicated policy enforcement application or security appliance. This requires enterprises to implement policy enforcement using a combination of LANCOM operating system (LCOS) features included with all LANCOM devices, such as dynamic VLAN assignment, LANCOM Enhanced Passphrase Security (LEPS) feature, Remote Authentication Dial-In User Service (RADIUS) client and RADIUS server.

LANCOM’s shares of the global wired campus switch and wireless LAN equipment markets were below the top 10 in 2018, according to Gartner figures. Organizations in LANCOM’s primary vertical markets of midsize organizations in retailing, education and the public sector, and those located in its core EMEA region, can consider the vendor for basic unified access layer requirements.

Strengths

- The Rohde & Schwarz acquisition provides a broader global organization for marketing and deployment of LANCOM access network products, beyond the vendor’s current Germany-focused base.

- LANCOM offers its Management Cloud solution as either private-cloud-based or multitenant, public-cloud-based in a GDPR-compliant environment.
- LANCOM's wired and wireless LAN portfolio is competitively priced with larger competitors for comparable hardware or network application capabilities.

Cautions

- The vendor generated nearly all of its 2018 revenue from sales to clients in Europe. Enterprises considering LANCOM infrastructure must make sure the vendor and its channel partners can provide sufficient local support in regions outside of Europe.
- LANCOM during the evaluation period had not yet released campus switches or APs with 802.3bz multigigabit support, despite earlier plans for releases beginning in 2018. This limits the portfolio's appeal to organizations seeking to utilize the full performance capabilities of 802.1ac Wave 2 access points.
- The vendor offers limited location-based service capabilities beyond BLE support access to an API for forwarding the location data of WLAN and BLE clients to the LMC solution, limiting its versatility for deployments with more complex location-based service (LBS) requirements.

Ruijie Networks

Ruijie Networks, headquartered in Beijing, provides a full portfolio of access layer networking hardware and software primarily to customers in its home market of China, with a focus on vertical markets that include education, transportation, hospitality, healthcare and finance. Ruijie has a WLAN controller-based and controllerless solution. This includes a “free” cloud-managed offering for small and midsize businesses (SMBs) and the RG-MACC (Managed @ Cloud Center) solution, which can scale to more than 10,000 APs. The free, cloud-based WIS (Wireless Intelligent Solution) monitors WLAN performance and utilizes Ruijie's AI technology to automate optimization of the wireless network. Ruijie's Data Analyzer and IBN Center provide network performance baselining to ease troubleshooting. Ruijie has a rather focused verticalized strategy. For hospitality, for instance, the i-Share+ solution is based on a distributed architecture, whereby an AP supports 24 “mini APs,” virtually acting as RF cards, hence lowering the AP footprint. For the education vertical market, Ruijie's iData suite of licenses evolves around the use of big data analysis — for instance, course attendance rates or students' location tracking.

Ruijie had the No. 8 and No. 7 global market shares for large enterprise campus switch and WLAN AP shipments in 2018, according to Gartner figures. Clients should evaluate Ruijie Networks for all wired/wireless LAN access layer opportunities, especially for locations in China, where it has a sizable installed base.

Strengths

- Ruijie has an aggressive pricing strategy, with a strong focus on the small and midsize business space. The free Wi-Fi Cloud solution excludes licensing costs, regardless of the number of devices, and supports management of switches and routers/gateways as well.
- SAM+ provides authentication, unified access control and policy management, with the ability to scale up to 100,000 terminals, through integration of the N18000 core switch/authentication gateway.
- Ruijie's Open Networking Controller (ONC) provides onboarding and containment of IoT devices through a fingerprint database for automatic service isolation.

Cautions

- Over 75% of Ruijie's s revenue came from China in 2018, according to Gartner figures. Organizations considering Ruijie in other geographies should request partner references for implementation and support/servicing.
- Although Ruijie's Wi-Fi Cloud solution comes with no licensing costs, organizations for which scalability is important should request documentation and references that demonstrate its ability to scale up.
- Ruijie generates little inquiry from Gartner clients for wired and wireless access network infrastructure, which indicates low marketing execution outside of its core China market.

TP-Link

TP-Link, based in Shenzhen, China, provides basic access network connectivity through a low-cost portfolio of wired access switches and wireless access points. The vendor bundles with its products, at no added cost, a public cloud-based network management solution, Omada. Omada supports basic centralized AP management functions such as traffic and performance monitoring, synchronization of AP settings, access control and rogue AP detection using a software controller or cloud controller appliance. The TP-Link TUMS platform, primarily deployed in China, enables centralized, cloud-based management and configuration of enterprise routers, switches, access controllers and APs. Managed switch functionality includes basic access and management features such as Layer 2 to Layer 4 QoS, 802.1X and RADIUS authentication, dynamic and static routing, and integrated access controller functionality in chassis switches.

TP-Link sells a large volume of switches and APs globally, ranking No. 3 in campus switch port shipments and No. 8 in enterprise AP shipments in 2018, but it ranked only No. 8 in enterprise switch revenue and below the top 10 in enterprise AP revenue, according to Gartner figures. Midsize and large enterprises can consider TP-Link as a low-cost option in all regions for wired and wireless LAN implementations with simple connectivity and management requirements.

Strengths

- TP-Link's products offer basic connectivity and management capabilities for cost-focused customers that do not have complex networking requirements.
- Network managers may access the Omada management functions as a cloud-based application via a small, on-premises wireless LAN controller or through a smartphone app.
- The guest network application bundled with the Omada management solution includes customizable splash page and login options such as social media (for example, Facebook) or SMS.

Cautions

- Gartner gets virtually no client inquiry regarding TP-Link's enterprise access network infrastructure and has received no Peer Insights client reviews of its products. Large-enterprise clients should ask for customer referrals from TP-Link channel partners or limit the use of its products to low-risk or low-priority deployments or usage scenarios.
- Management functionality does not include IoT-specific support such as discovery or monitoring of IoT endpoints or segmentation/containment of data traffic from those devices.
- Machine learning/AI features for automating access layer connectivity were limited to automatic collection of network topology and proactive reporting of network anomalies

via the TUMS platform. AI-driven intelligent network analysis is not expected until release of the Omada SDN platform in 1Q20.

Ubiquiti Networks

Ubiquiti Networks, based in New York, provides basic access network connectivity through a low-cost portfolio of wired access switches and wireless access points. The vendor's UniFi management suite, bundled at no additional cost with the hardware, provides basic management functionality either on-premises, through a small (50-AP) controller, or as a license-free SaaS application that clients must install and maintain themselves. Although it has substantial service provider and consumer networking businesses, Ubiquiti now generates more than 60% of its overall revenue from its UniFi enterprise line. The company ranked in the top 10 for global enterprise campus switch and access point shipments in 2018. It handles direct sales only via the online commerce section of its website. It has a negligible direct sales effort, relying instead on VARs, system integrators and other partners for sales and product distribution.

Ubiquiti did not respond to Gartner's vendor questionnaire, nor did it provide customer references for this research. Its inclusion and evaluation are based on information (including the company's publicly available information), Gartner client inquiries and Peer Insights customer feedback. Ubiquiti garnered the No. 10 global share of campus switch port shipments and No. 9 share of enterprise WLAN APs in 2018, according to Gartner figures. Midsize and large enterprises can consider this vendor as a low-cost option for wired and wireless LAN implementations with simple connectivity and management requirements and low support needs.

Strengths

- In inquiries and Peer Insights comments to Gartner, Ubiquiti clients generally report ease of deployment, use and management of Ubiquiti equipment using UniFi cloud controller software.
- Ubiquiti enables "hybrid cloud" management both for remote management of branch sites via the UniFi Cloud solution and for on-premises wireless controller functionality utilizing the Cloud Key network device plugged into a campus switch.
- The UniFi network management suite allows management of VoIP, WLAN, networking and surveillance devices from one central management dashboard, with the UniFi Switch integrating with the UniFi Controller software for centralized management of

UniFi devices. Customers can test the Network Management System for free in a demo/presentation mode, and it is free software download.

Cautions

- For enterprises whose networking requirements will become increasingly complex in order to support advanced features such as dynamic segmentation of IoT endpoints or automated network assurance, UniFi offers no expandability of features beyond its basic, included capabilities.
- Customers report mixed experiences with Ubiquiti support. Corporate product support relies heavily on channel partners and the “Ubiquiti Community” of consumer and corporate IT users, who respond to customer troubleshooting or technical questions via the Ubiquiti website. Enterprise customers should be aware that Ubiquiti has a standard disclaimer regarding potential inaccuracies in information provided by its support community.
- Direct purchase of UniFi products via the company website is limited to customers in the U.S. and Canada. Client feedback indicates little or no negotiability on price for products acquired via channel partners.

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

- Cambium
- CommScope (acquired ARRIS/Ruckus)
- Ruijie Networks
- TP-Link
- Ubiquiti Networks

Dropped

- Aerohive (acquired by Extreme Networks)
- ARRIS/Ruckus Networks (acquired by CommScope)
- Mist Systems (acquired by Juniper Networks)
- Riverbed

Inclusion and Exclusion Criteria

To qualify for inclusion in this research, vendors needed to:

- Demonstrate relevance to Gartner clients in the enterprise access layer market by offering switching and WLAN hardware to address enterprise access layer networking requirements outlined in the Market Definition section.
- Demonstrate relevance to Gartner clients in the enterprise access layer market by providing one or more network service applications, as outlined in the Market Definitions section, with an annual network service application revenue exceeding $10 million USD.
- Produce and release enterprise access layer networking products for general availability as of 15 April 2019. All components must be publicly available, shipping and included on the vendors' published price list. Products shipping after this date will only have an influence on the Completeness of Vision axis.
- Have at least 50 enterprise customers that use its access layer networking products in production environments as of 15 April 2019.
- Demonstrate production enterprise customers with at least five reference customers supporting access layer networks of more than 100 access points.
- Provide production enterprise reference customers for at least three of the five geographic regions.
- Have no more than 80% of revenue generated in any one country in a single region.

Additional Vendors

There are several additional vendors that garner interest from Gartner clients or that could impact this market over time. These vendors do not currently meet our inclusion criteria, but they can address enterprise access layer connectivity in certain usage scenarios. In some cases, these vendors sell to customers outside the traditional IT organization. Specific players we track include:

- ADTRAN
- Cloud4Wi
- NETGEAR
- Pica8
- Samsung
- Sundray Technology
- Zyxel Communications

Evaluation Criteria

Ability to Execute

Product/Service: Gartner evaluates the ability to offer access layer infrastructure products and services consisting of switches, access points and related components. We also evaluate network service applications such as management, monitoring, guest access, policy enforcement and security applications as well as new services. We consider product differentiation and architectural migration strategies from legacy implementations, whether there is an incumbent vendor or a new solution provider. We also look at maintenance and deployment service capabilities across the global landscape.

Overall Viability: Viability includes an assessment of the organization’s overall financial health, and the financial and practical success of the business. We also evaluate whether the organization continues to invest in access-layer-related business, including technology and product development, as well as solution delivery to the market, including sales channels, marketing communication and service delivery.

Sales Execution/Pricing: We evaluate the organization’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/Track Record: We look at the vendor’s 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 to changing market demands.

Marketing Execution: We evaluate the clarity, quality, creativity and efficacy of programs designed to deliver the organization’s message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This “mind share” can be driven by a combination of publicity, promotional, thought leadership, social media, referral and sales activities.

Customer Experience: How do customers view this vendor? This evaluation includes significant input from Gartner clients in the form of inquiries, face-to-face meetings and customer reference written responses about the vendors. A key component in this category is the vendor’s ability to provide strong presales and postsales support.

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

•

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

Evaluation Criteria	Weighting
Operations	Not Rated

Source: Gartner (September 2019)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements regarding their vision of how they will succeed in this market. This includes current and future market direction, innovation, customer needs and competitive forces, as well as how well they map to Gartner’s view of the market.

Market Understanding: Does the vendor have the ability to look into the future and drive/influence the direction of the market through product roadmaps and offerings? We also evaluate the vendor’s ability to address current hardware requirements to meet the needs of current network service applications and to address market trends. Are vendors focusing on building their core competencies, or are they investing in random technologies?

Market Strategy: We are specifically looking for messaging and marketing campaigns and the vendor’s ability to communicate differentiating functionality and value proposition. Are the issues that are being communicated and addressed meeting the trends in the market and the needs of end users?

Sales Strategy: Does the vendor have a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication? Does the vendor have partners that extend the scope and depth of market reach, expertise, technologies, services and its customer base?

Offering (Product) Strategy: Does the current and planned future product line meet the needs of buyers now with differentiable functionality, and how will it do so in the future? Is the vendor simply building products that the buyer is asking for, or is it anticipating the issues that those buyers will face and allocating resources to address them?

Business Model: We evaluate the design, logic and execution of the organization’s business proposition to achieve continued success. Does the business model meet the needs of the target market and enable the vendor to grow?

Vertical/Industry Strategy: Does the vendor’s strategy, direct resources, skills and offerings meet the needs of market segments, including vertical industries? In this market, can the vendor differentiate itself with solutions that are specifically developed for the unique requirements of targeted verticals, such as healthcare, logistics, manufacturing, retail, hospitality and others?

Innovation: What has the vendor done to address the future requirements of access layer infrastructure, including the need for tighter integration with wired networking products, requirements of IoT, and use of machine learning/AI to solve client business problems? Is there innovation in the access layer applications that address client needs for any of the equipment management, monitoring or life cycle? Has the vendor successfully differentiated the current and future product lines to better address customer requirements, both now and two years to five years out?

Geographic Strategy: We evaluate 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. Can the vendor meet the needs of global enterprises for product and support?

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

•

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Low

Evaluation Criteria	Weighting
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (September 2019)

Quadrant Descriptions

Leaders

A vendor in the Leaders quadrant will have demonstrated an ability to fulfill a broad variety of customer requirements through the breadth of its access layer product family. Leaders will have the ability to shape the market and provide complete and differentiating access layer 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 no obvious gaps in their portfolios.

Challengers

A vendor in the Challengers quadrant will have demonstrated sustained execution in the marketplace and will have clear and long-term viability in the market, but it may not have a complete access layer product portfolio for either products or network applications. Additionally, Challengers may not have shown the ability to shape and transform the market with differentiating functionality or 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 access layer technologies within the enterprise (for example, security, management or operational efficiency). The ability to apply differentiating functionality across the entire access layer 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 solution, 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

The WLAN continues to grow as a prevalent access network in larger enterprises. Given its greater deployment flexibility than the wired LAN, enterprises increasingly plan the WLAN as the first or only connection to the enterprise network for employee client devices and connected office equipment such as video displays, printers or projectors. The prevalence of employee smart devices also continues to generate interest in retirement of wired IP desk phones where possible, using the WLAN to support voice from cellular phones, laptops or tablets using a corporate unified communications solution or native Wi-Fi calling features (see “Cost Optimization: The Mobile Phone Is the Only Phone the Digital Workplace Employee Needs”).

As a result, enterprise customers increasingly focus on WLAN service quality, such as effectiveness supporting latency-sensitive applications such as voice. They also differentiate vendors based on capabilities that go beyond basic campus or branch connectivity and the “check the box” management and security features that now are common to all major vendor equipment. Connectivity for traditionally non-IT applications continues to be an emerging use case, as organizations address the need to network formerly OT domains such as HVAC, lighting and access security with the IT-governed LAN that now may be the primary network for IoT.

Gartner observes that most changes in wired and WLAN capabilities have been incremental since the previous version of this Magic Quadrant. In 1H19, 802.11ax access points accounted for less than 2% of global enterprise shipments (see “Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2Q19”). Vendors began rolling out 802.11.ax APs relatively slowly because customer demand had yet to gain significant momentum given that there were few available client devices or endpoints with 802.11ax radios.

As it was in 2017 and 2018, 802.11ac Wave 2 currently remains the default purchase choice given its capabilities to handle typical enterprise requirements for data throughput and effective management of the growing number of Wi-Fi-enabled devices per user.

Gartner has recommended that organizations best optimize their wired campus switching infrastructure financially and functionally by aiming for “good enough” solutions rather than opting for high-end premium infrastructure. This means preferring vendors that provide a management fabric that enables groups of devices to be managed as a single construct rather than as a collection of individual devices, and that support central configuration of switches and embedded automation of common operational network tasks such as switch installation and common adds, moves or changes.

Likewise, clients express a preference for unified management of wired and WLAN infrastructure from a primary console, for network management in addition to network service applications such as guest access, authentication and location-based services. Most wired/wireless LAN vendors offer multivendor management capabilities of varying degrees in their software suites, addressing the many organizations that use different vendors for wired and WLAN infrastructure. In fact, 54% of customers surveyed for this research indicated that multivendor applications were a highly important factor in their vendor selection criteria.

Most vendors can provide their LAN management tools as either on-premises or cloud-based solutions, although supporting hybrid deployments that require on-premises for some locations and cloud for others remains a challenge.

Vendors are still in the early stages of leveraging artificial intelligence capabilities to incorporate more intelligence and automation in the management and security of the access layer, including proactive assurance and troubleshooting. Gartner recommends that organizations invest in solutions that will support these capabilities, but only after requiring verification of them in a real environment. Given the benefits vendors are ascribing to these features, ask them to back up the performance claims with SLAs you can apply to their infrastructure’s actual performance in your own deployment.

Market Overview

Extended Market Definition

Gartner’s view of the wired and wireless access network infrastructure market is focused not only on the market as it is today, but also on transformational technologies or approaches that deliver on the future needs of end users. Gartner research shows that global enterprise wired and wireless campus networking revenue growth YoY was 9.8% in 2018, vs. 10.3% in 2017. This was driven largely by 11.1% growth in campus switches (see “Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q18 and 2018”), due to strong demand plus an increasing contribution from software subscriptions encompassing functions such as policy enforcement, troubleshooting and network automation.

Longer-term WLAN will continue to drive the market’s revenue growth, at a forecast 6.4% compound annual rate through 2023, compared with an expected 0.5% annual rate for campus switch revenue (see “Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2016-2023, 3Q19 Update”). Growth will be driven partly by increasing availability of prestandards-based products supporting Wi-Fi 6/802.11ax as organizations address device proliferation in which the average number of users/devices supported per deployed WLAN AP will increase by approximately 20% to 30% from 2018 through 2023 (see “Forecast Analysis: Enterprise Network Equipment, Worldwide”). Wi-Fi 6 increases throughput speeds in densely device-populated areas by improving the efficiency of existing 2.4 GHz and 5 GHz spectrums compared with 802.11ac, which accounted for 97% of global enterprise access point revenue in 2018.

Consolidation of vendors covered by this Magic Quadrant reflected demand for WLAN, creating more mature providers that can provide unified wired/wireless LAN infrastructure without having to rely on strategic partners for WLAN product development. This occurred with the acquisitions by Juniper Networks of Mist Systems and by Arista Networks of Mojo Networks. CommScope’s acquisition of ARRIS/Ruckus Networks marked CommScope’s entry into enterprise wired and WLAN infrastructure. In contrast, Extreme Networks’ acquisition of Aerohive combined companies with full WLAN portfolios but enabled Extreme to obtain SD-WAN-oriented products and cloud management capabilities it did not already have. Similarly, Cambium’s acquisition of Riverbed’s Xirrus WLAN portfolio significantly expanded an enterprise WLAN business that accounted for less than 10% of Cambium’s total 2018 revenue.

Typical Business Outcomes

The primary business outcome is wired and wireless LAN connectivity within carpeted enterprise environments, in campus buildings and in remote or branch offices, between client devices and applications or other assets residing in corporate data centers, the cloud or the internet.

Market

This market includes these typical vendor types:

- *The vendor provides its own wired and wireless infrastructure components, network applications and services.*
- *The vendor primarily provides a specific connectivity option, such as either wired or wireless components.* These vendors often focus on solutions addressing a unique set of market requirements, such as cloud-based management of a predominantly wireless LAN or a vertical market such as retail or healthcare.
- *The vendor uses a strategic partner to provide some or all the hardware or software components of an end-to-end access solution, including network service applications.* These vendors should provide differentiating functionality for the combined solution that will be considered a better option for enterprises that might otherwise buy solution components directly from the strategic partner.

This market includes vendors providing and supporting enterprise wired and wireless LAN infrastructure globally, in at least three of the main geographies Gartner identifies:

- Asia/Pacific
- Latin America
- Middle East and North Africa
- Europe
- North America

Typical Buyers

Within the enterprise, CIOs, CTOs, VPs of infrastructure and operations (I&O), directors of networking, and network managers typically make the buying decisions for wired and WLAN infrastructure. Line-of-business executives may be involved if the infrastructure is intended to enable specialized vertical market applications. Examples include indoor location services for tracking drugs, medical devices and people inside a healthcare facility, or retail analytic software that consumes location data gathered by the WLAN or associated beacons to generate sales lead, marketing or customer engagement actions.

How Buyers Shape Their Buying Decisions

Wired and wireless LANs in many organizations are business-critical infrastructure, with medium-term life cycles of about five years to seven years for WLAN equipment and seven years to 10 years or longer for campus switches. Strong influences on buyers include historical vendor relationships (including technical familiarity with previously installed products), their experiences with the effectiveness and quality of their existing solutions (including support), ease of network management (including for onboarding and management of guest access and BYOD clients), network segmentation to segregate IoT devices and their data traffic, and the perceived competitiveness of the net pricing (that is, list price minus discount) they receive from the vendor or its channel partner, such as a VAR or reseller.

Important buyer considerations include:

- Multivendor Management: Buyers also commonly are interested in how well a vendor's wired and WLAN equipment will work with existing infrastructure from other vendors. This includes a new vendor's ability not only to monitor, configure or control existing vendor switches, controllers or APs through a single pane of glass, but also how effectively its equipment will work with existing systems such as a unified communications platform.
- IoT Containment: The proliferation of IoT endpoints requiring connectivity via the enterprise network has increased buyer attention to access infrastructure vendor capabilities to identify, provision and dynamically segment traffic to and from those devices. In addition to IT-controlled devices, "headless" endpoints such a sensors, lighting controls or security devices, formerly managed as OT, pose potential attack vectors that can be mitigated with network access control features such as device fingerprinting and generation of unique device credentials, along with encryption and containment of their data traffic to isolate it from the rest of the access network from endpoints to the data center.

- Automation. Gartner expects that, in the next two years, vendors will deliver “self-healing” capabilities that enable the network to automatically detect specific failures and dynamically recover from them through automated troubleshooting for network assurance or by addressing security threats. This may include hardware, software, cabling or configuration problems, a capacity issue, or even an application performance issue. Automation also will enable component provisioning through automation or establishment and maintenance of baseline performance for each device based on policy. This capability will be driven by advances in machine learning and AI that vendors are embedding into products. These products consume data generated at the network edge and extract knowledge from that data by utilizing advanced network or behavioral analytics, such as UEBA, to identify and address unusual or problematic patterns. Vendors have begun executing this long-term vision to support:
  - More rapid service delivery (such as deployment or expansion of branch office Wi-Fi)
  - Location-based applications with improved location granularity
  - Proactive, potentially automated management of the network fabric to meet enterprise user requirements for high performance and availability

- Automation enabled by machine learning and network configurations based on network and business policies eventually will drive intent-based solutions that will be self-monitoring to ensure that the network actually meets the intent of the policies set at configuration time. Vendors that can successfully develop and integrate automation of such functions will be able to differentiate themselves by providing service-level agreements (SLAs) that guarantee the performance of their networks when configured and managed to the customer’s network performance, availability and management-related key initiatives (KIs).

Gartner also has observed a growing vendor focus on integrating SD-WAN functionality with management of the wired/wireless LAN, but has seen little client interest or adoption of this among large enterprises as of yet. Vendor offerings of “SD LAN” or “SD campus” should align with an enterprise’s technology roadmap and whether consolidating WAN and access layer management will improve the cost-efficiency of its infrastructure.

How Providers Package, Market and Deliver

Buyers typically source their wired/wireless LAN infrastructure through a vendor channel partner — such as a VAR, system integrator or network service provider — with relatively few purchases coming directly from the vendor. Hardware is typically a one-time cost, with hardware licensing required to maintain firmware or software such as operating system updates, feature upgrades or security patches. Vendors charge for hardware and software licenses either as a perpetual license or as a subscription license. Vendors also may bundle basic network services, such as simple management and guest access, in the price of the hardware.

Architectures with cloud-managed networking capabilities have become a standard element of vendor infrastructure portfolios to meet client preferences for the ability to deploy network service applications on-premises or in a public or private cloud. However, specifications for many client access network "greenfield" deployments and network refreshes do not necessarily mandate a cloud-managed solution; clients still widely require on-premises options.

There is also inconsistency in how closely vendor cloud architectures map to the features and functionality of their on-premises options. Further, Gartner continues to see client preference for cloud-managed architectures to serve branch office deployments rather than campus deployments. When cloud-managed is the choice, many clients want to look beyond proprietary products that create vendor lock-in and integration challenges. Vendor differentiation is also apparent in whether the cloud versions of network service applications share all the features and functionality of the on-premises versions.

Elements of Wired and Wireless Access Networking Solutions

Enterprise wired and wireless local-area networking components include:

Hardware — Physical network elements, including:

- Wireless access points
- Wired switches
- Controllers (physical or virtual), if needed

Software — Network service applications that are cloud-based, appliance or virtual appliance, including but not limited to:

- Network management
- Network monitoring
- Guest access, including captive portal
- Onboarding services
- AAA security/authentication
- Policy enforcement
- Intrusion detection systems/wireless intrusion detection systems
- Location services
- Performance management
- Network assurance
- Application visibility
- Network and vertical market analytics
- Security, including behavioral analysis

Evidence

[1] Gartner analysts conducted more than 800 inquiries on the topic of wired and wireless access networking from 31 March 2018 through 15 April 2019.

[2] Revenue and port share for campus switches and WLAN is derived from "Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q18 and 2018."

[3] Except where noted otherwise, vendors in this research responded to a questionnaire regarding their current/future wired/wireless LAN access network infrastructure solutions.

[4] We surveyed reference customers (n = 137) provided by vendors in this research.

[5] Analysts reviewed Gartner's Peer Insights customer reviews for this market.

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 subcriteria.

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 organizational 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 organization 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.

By Bill Menezes, Christian Canales, Tim Zimmerman, Mike Toussaint

- About
- Careers
- Newsroom
- Policies
- Site Index
- IT Glossary
- Gartner Blog Network
- Contact
- Send Feedback

Gartner®