

Magic Quadrant for the Wired and Wireless LAN Access Infrastructure

Published: 17 October 2017 **ID:** G00316060

Analyst(s):

Tim Zimmerman, Christian Canales, Bill Menezes

Summary

Enterprise LAN vendors providing access layer connectivity must respond to changing demands. Infrastructure and operations leaders should evaluate vendors based on their ability to provide an intelligent access layer capable of network automation that addresses all of the business requirements.

Strategic Planning Assumption

By 2022, more than 60% of IT organizations will use access layer network automation, up from less than 5% today.

Market Definition/Description

Gartner's view of the market is focused on the vendor's ability to anticipate and integrate transformational technologies or approaches delivering on the future needs of end users. Gartner defines the wired and wireless LAN access infrastructure market as a market that consists of vendors supplying wired and wireless networking hardware and software that enables devices to connect to the enterprise wired LAN or Wi-Fi network. These devices may include laptops; smartphones, tablets and other mobile smart devices; networked office equipment; sensors and other Internet of Things (IoT) endpoints; and other fixed or mobile endpoints communicating to a wired switch port or a wireless access point at the edge of the enterprise infrastructure. This research does not cover wired and wireless access networking infrastructure for adjacent markets, such as public venues, small office/home office, commercial and industrial settings, or point-to-point solutions.

Enterprise wired and wireless local-area networking components include:

- Software — Network service applications that are cloud-based or deployed on an appliance or virtual appliance, including but not limited to:
 - Network management
 - Network monitoring
 - Guest access
 - Onboarding services
 - Authentication, authorization and accounting (AAA) security
 - 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
- Hardware — Physical network elements including:
 - Wireless access points
 - Wired switches
 - Controllers, if needed

Vendors serve enterprises with three distinct go-to-market approaches:

- The vendor provides its own wired and wireless infrastructure components, network applications and services. Examples include Cisco, Hewlett Packard Enterprise (HPE) Aruba, Extreme Networks and Huawei.
- 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 (WLAN) or a vertical market, such as retail or healthcare. Examples include Aerohive, Mist Systems and Mojo Networks.
- The vendor uses a strategic partner to provide some or all of the hardware or software components of an end-to-end access solution. These vendors provide differentiating functionality in the network applications for the combined solution. Examples include Dell and Juniper Networks.

Magic Quadrant

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



Source: Gartner (October 2017)

Vendor Strengths and Cautions

Aerohive

Aerohive provides public and private cloud management, as well as on-premises management for access points, switches and routers. For unified access networks using Aerohive wireless access points and HiveManager NG software, the enterprise can employ the vendor's own stand-alone and stackable switches or manage any Fastpath-based switch, including N-Series switches from strategic partner Dell. HiveManager NG comprises a full suite of access applications, including

network configuration and management, policy management, onboarding and provisioning guest access. Aerohive provides network analytics for reporting and forensics, as well as presence location service applications.

With 87% of sales generated in North America and EMEA, Aerohive grew faster than the overall WLAN market with 16.8% revenue growth in 2016. Aerohive continues to focus on serving clients in the educational and retail industries, and other enterprises with distributed locations. Small and midmarket organizations in North America and Western Europe should include Aerohive when evaluating on-premises or cloud-managed WLANs. Aerohive should also be included for a global enterprise opportunity that uses Dell wired switching based on the product integration and uses Dell's global support capabilities.

STRENGTHS

- Aerohive addresses small and midsize businesses or larger enterprises with remote offices where the Connect configuration of HiveManager NG provides basic functionality for network configuration, autoprovisioning tools, device and client monitoring, and guest access. Organizations can add more functionality from an advanced configuration menu when it is needed with seamless scalability.
- Aerohive can deploy HiveManager NG as an on-premises solution or in either a public or private cloud where competitors often require two separate offerings depending on whether the deployment is on-premises or in the cloud.
- Aerohive gives clients the ability to monitor all end users through a client health score, which also enables automatic corrective actions to meet preset service-level agreements (SLAs) for end-user connectivity.

CAUTIONS

- HiveManager NG's multivendor network management capabilities are limited to Dell's N-Series switch line, likely deterring prospective customers that must maintain substantial deployments of legacy hardware from other vendors.
- Aerohive continues to be a growing vendor that is geographically limited without its channel and strategic partnerships. Enterprises with global deployments must ensure that Aerohive is able to provide the necessary support capabilities.
- Aerohive has limited machine learning and artificial intelligence capabilities that will affect its near-term ability to deliver on advanced enterprise requirements.

ALE

ALE, marketed under the brand Alcatel-Lucent Enterprise, is a private company owned by China Huaxin, which attained 100% ownership of the company in June 2017. The vendor provides a unified access network portfolio comprising its Alcatel-Lucent OmniSwitch wired switches combined with either its own Alcatel-Lucent OmniAccess Stellar wireless access points or those from OEM partner HPE Aruba. For larger and more complex campus deployments, access points from HPE Aruba or its Stellar products can be managed with the Alcatel-Lucent OmniVista 2500 management application. For Stellar access points, the OmniVista application also provides simplified guest access functionality, including automated onboarding of guest or employee "bring your own device" (BYOD), social media login capability and device fingerprinting.

ALE's unified wired and wireless access network capabilities primarily serve the hospitality, healthcare, transportation, education and government verticals, as well as general enterprise campus deployments. Clients in North America, EMEA and Asia/Pacific within their target markets should evaluate ALE.

STRENGTHS

- Launch of the OmniAccess Stellar access points allows ALE to guide its own product roadmap and speed to address market requirements.
- ALE continues expanding its OmniSwitch product line, including new models: its OmniSwitch 6560 fixed-format switches aimed at remote office deployments; the OmniSwitch 6865 hardened access switch intended for industrial or outdoor IoT deployments; and new modules for the 9900 48-port chassis switch aimed at core, aggregation or access network functions.
- ALE's Intelligent Fabric technology enables automated configuration or reconfiguration of devices or applications, helping to reduce deployment time and related overhead costs for adds, moves or changes.

CAUTIONS

- ALE offers two WLAN solutions, including an in-house option and an OEM option. There is currently overlap in capability, which can confuse prospects and lead to suboptimal selection.
- Enterprises must be aware that ALE has multiple pricing methods — consumption and direct purchase — which may cause difficulty in determining the total solution price.
- ALE has limited machine learning and network automation, as well as a limited indoor location strategy that will affect its ability to deliver on advanced enterprise access layer requirements.

Allied Telesis

Allied Telesis offers an end-to-end wired and wireless LAN portfolio, even though the Extricom product line that was acquired in 2015 has been retired. Organizations can manage the switching and WLAN product portfolio on-premises with Vista Manager EX or in the private or public cloud using AMF Cloud. Allied Telesis also has a new controller, the Unified Wireless Controller (UWC), which is suitable for small and midsize deployments and can be deployed as hardware or a virtual appliance. The Allied Telesis Autonomous Management Framework (AMF) delivers a suite of features to optimize reporting and network management. Allied Telesis sells predominantly through channels. The company does not appear in Gartner inquiries, although it has a global footprint and more than 50% of its revenue comes from Japan. Allied Telesis mainly targets the public-sector, education, healthcare and hospitality vertical markets. Predominantly small and midsize businesses should consider Allied Telesis for their wired and wireless LAN infrastructure needs.

STRENGTHS

- All products operate via the same operating system (AlliedWare Plus) for uniform functionality, better support, migration and upgradability.
- Vista Manager/AMF can be deployed on-premises or in the cloud and offers integration, which provides deployment flexibility while simplifying network management and automation.
- Vista Manager/AMF can also be integrated with Allied Telesis Secure Enterprise Software Defined Networking (SES) which offers an additional layer of protection to organizations.

CAUTIONS

- Allied Telesis has limited functionality for basic applications, such as guest access. It does not have a captive portal that is capable of automatically issuing guest access through SMS or email.

- Allied Telesis has limited real-time traffic analysis or security behavioral analytics that will affect its near-term ability to deliver on advanced enterprise requirements.
- Allied Telesis operates globally but has less than 2% global market share and has 60% of its revenue from a single geography. Clients should validate that the reselling partner has the ability to provide sufficient local support capabilities.

Brocade (Ruckus)

Brocade provides unified access networks integrating its ICX wired switch line with WLAN infrastructure from Ruckus, a division of Brocade, which it acquired in May 2016. Currently, there is a pending acquisition of Brocade by Broadcom and another acquisition of the Brocade access layer switching assets and the Ruckus WLAN organization by Arris that may occur and should be considered in enterprise evaluations. Both switches and wireless hardware in larger implementations can be managed and monitored by the Brocade Network Advisor solution. For wireless-centric deployments, the Ruckus Cloud Wi-Fi or SmartZone WLAN controller provide management and monitoring functionality at no additional licensing cost. Brocade offers both controller-based and cloud-managed WLAN architectures plus a complete suite of network service applications for indoor location services, guest access and policy management.

Enterprises in North America and EMEA with access layer opportunities in education, hospitality and government should evaluate Brocade (Ruckus) but should exercise caution until the details of the acquisition are known.

STRENGTHS

- The CloudPath network service application provides device onboarding, self-service guest access, security and policy management across the ICX switch, and Ruckus WLAN infrastructure.
- The Brocade ICX 7000 switches support a campus fabric that allows the network to look like a single logical switch, which simplifies deployment and management.
- Ruckus SmartCell Insight (SCI) provides predictive analytics and reporting that alerts IT organization of anomalies in the WLAN solution.

CAUTIONS

- Acquisitions create uncertainty in long-term strategies and roadmaps. Enterprises must be aware of current pending and proposed acquisitions as part of their evaluation process.
- The Brocade switch fabric does not include the Ruckus controllers and access points, limiting the fabric benefits, as well as requiring a separate management application.
- A Brocade (Ruckus) solution has many management and network service application options, including CloudPath, Brocade Network Advisor, Cloud Wi-Fi, ZoneDirector, Unleashed and SmartZone. This can confuse customers and lead them to purchase the wrong application and/or overpay for multiple applications.

Cisco

Cisco has the broadest portfolio of access wired switching and WLAN products. DNA Center, announced in July 2017, allows Cisco to provide network assurance to the access layer through contextual insights from network monitoring, security, analytics and policy enforcement. Cisco continues to be the market share leader for access layer connectivity, but it continues to lose market share. From 2015 to 2016, Cisco's revenue grew by 1.3% for WLAN and declined by 10.6% for campus switching, while the rest of the market grew 16.7% and 11.8%, respectively.

The vendor continues to offer two access layer solutions: Aironet/Catalyst and Meraki. Cisco's on-premises solutions include the new Catalyst 9000 switching family as part of its Catalyst line of fixed-format and modular switches. Cisco's controller-based and controllerless Aironet access points provide on-premises WLAN connectivity that is supported by Identity Services Engine (ISE) for policy-based access and Prime for management. Cisco's Meraki solution has its own separate fixed-format switches and access points and a separate cloud-based policy and management console solution.

Clients should consider Cisco globally for all enterprise on-premises and cloud-based access layer opportunities.

STRENGTHS

- Cisco's Software-Defined Access is a programmable network architecture that provides software-based policy and segmentation from the edge of the network to the application. The fabric architecture provides investment protection to address the requirements of IoT and new markets.
- Cisco expanded its switching product line with the introduction of Catalyst 9000 Series. It is a high-end purpose-built campus platform with expandable storage designed for high-performance requirements.
- Cisco has a robust set of network services, including Software-Defined Access and Network as a Sensor (NaaS) with Cisco ISE for IoT segmentation and encrypted traffic analytics with Cisco Stealthwatch to address end-user security concerns.

CAUTIONS

- Meraki is not part of Cisco's DNA Center and cannot provide network assurance or directly manage the Catalyst 9000.
- The Aironet/Catalyst and Meraki engineering and marketing teams continue to operate separately, and functionality is implemented differently between two teams.
- End users looking to deploy both Catalyst/Aironet and Meraki solutions will need to purchase and implement ISE/Prime and the Meraki components, because consolidation to a single dashboard through DNA Center is not yet available.

Dell EMC

Dell EMC supports the unified access network market through its Dell EMC N-Series fixed-port, stackable Ethernet switches with Aerohive wireless access points. This architecture is administered via an integrated, Dell EMC-branded version of HiveManager NG that provides control and network service applications for the unified network. Dell EMC also provides its own OpenManage solution for management of either Dell EMC or multivendor wired switches. Dell EMC supports customers in over 200 countries and focuses on higher education, public institutions and government vertical markets, as well as healthcare and life sciences.

Enterprise organizations needing a global access layer vendor in Dell EMC's target markets should evaluate the solution, especially incumbent organizations that have existing Dell EMC switching infrastructure.

STRENGTHS

- Dell EMC has an end-to-end wired/wireless LAN access infrastructure solution that can be deployed on-premises, as well as cloud-based network service applications.

- Dell EMC continues developing and expanding its N-model wired switches with the addition of 802.3bz 2.5 Gbps and 5 Gbps ports, available for the N2100 and N3100 lines.
- Dell EMC provides ProDeploy, an enterprise suite of services to help customers in all phases of installation and deployment and to test/validate the results.

CAUTIONS

- Dell EMC offers multiple access layer solutions, which may cause confusion or redundant licensing. It continues to support the embedded base of its legacy, controller-based W-Series WLAN architecture, while offering a migration path to its Aerohive-based portfolio.
- Dell relies on Aerohive for new wireless technology development, which means it has less control over its ability to respond to changing enterprise requirements.
- Dell EMC does not deliver advanced enterprise access requirements, such as machine learning and network automation.

D-Link

D-Link provides wired and wireless solutions for the unified access layer, as well as other network and security devices. Government, education and communications service providers are the most important markets for D-Link, which generates 85% of its revenue through channels. In 2016, D-Link released an 802.11ac access point, a new WLAN controller platform for larger configurations and a 10 Gigabit Ethernet switch. D-Link has also made some investments in IoT solutions and introduced Auto Surveillance VLAN. Supported on some of its switches, this is a technology that allows the support of a hybrid network that can handle data and Internet Protocol (IP) surveillance traffic separately. D-Link focuses on delivering a basic wired and wireless solution that is scalable and easy to use. However, the solution is limited in the network application functionality that is needed to automate processes such as guest access or policy enforcement.

Prospects in EMEA, Asia and North America with basic access layer requirements looking for a practical and cost-effective solution for small branch offices or remote locations or in the education market should engage D-Link.

STRENGTHS

- D-Link provides its Central WiFiManager software at no cost to the overall solution, which addresses network management and guest access that makes D-Link solutions very cost-effective for organizations with basic requirements.
- D-Link remains a low-price leader for a broad range of wired switch and wireless network hardware for enterprises with a limited number of use cases.
- D-Link provides a better hardware warranty than its competitors, and there are no annual software maintenance costs for its network applications for solutions where the business requirements can be addressed.

CAUTIONS

- D-View 7 provides basic wired and wireless network management that is behind on advanced services, such as device location insight, user roles, radio frequency performance and detailed monitoring capabilities.
- D-Link's Central WiFiManager software supports only the vendor's access points and cannot be deployed in a cloud-based model.

- D-Link is not keeping pace with enterprise requirements, such as limited indoor location services, policy enforcement, network assurance, analytics and IoT containment/separate strategies.

Extreme Networks

Extreme Networks is a global vendor with a broad portfolio of wired and wireless products that can meet a wide range of enterprise needs. In 2017, Extreme acquired Avaya's access layer business to further grow its customer base and strengthen its presence in its target markets. Government and education remain the top vertical market, but retail, manufacturing and healthcare growth was bolstered through the Zebra acquisition, which included the WiNG technology. Extreme provides enterprise flexibility by delivering edge-to-core infrastructure solutions that can be managed from on-premises, cloud or hybrid network service applications. ExtremeManagement, ExtremeControl and ExtremeAnalytics provide network management, guest access, policy enforcement and application analytics for Extreme network components, as well as multivendor networks for Cisco, Aruba and others. Extreme continues to provide strong customer service through a 100% insourced service and support team.

Prospects in North America, South America or EMEA should consider Extreme for access layer opportunities in education, government, retail, hospitality, manufacturing and healthcare.

STRENGTHS

- Extreme has an experienced management team that is developing and executing its access layer strategy.
- ExtremeManagement is a single console that provides multivendor, centralized management applications for wired and wireless environments that can be deployed on-premises or virtually in a public or private cloud environment.
- ExtremeWireless semiautonomous access points offer management for on-premises or the cloud using the same hardware (switches and access points), offering investment protection for either mode of deployment.

CAUTIONS

- Extreme now has three separate access layer architectures that will need to be rationalized. Strategic investment in multiple platforms may wane with time and not keep pace with enterprise requirements.
- Extreme's indoor location services 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.
- Extreme's implementation of network assurance is implemented using two applications (Extreme Management Center and ExtremeAnalytics) requiring organizations to review their requirements to assure the combination of Extreme Management Center and ExtremeAnalytics addresses the business needs.

Fortinet

Fortinet delivers a unified-access wired/wireless network capability with strong security applications that simplify management, troubleshooting and policy enforcement. Fortinet serves midsize and distributed enterprises, including education and retailers. The Secure Access Architecture integrates Fortinet's core firewall and other security capabilities into a unified access network. Version 5.6 of FortiOS (Fortinet's network security operating system) has extended network visibility and management under a common framework that includes switches, WLAN

access points, sandboxing and security products (Fortinet's previous operating system included only firewall and endpoint products). Fortinet's wireless solution has two distinctive architectures. One is based on the FortiGate firewall appliances with integrated WLAN controller functionality, and the other is a more traditional infrastructure — based on its acquisition of Meru Networks — that can be managed on-premises via a WLAN controller or from the cloud. The FortiAP-S series is Wave 1 and Wave 2 802.11ac access points that also include an integrated firewall and are able to perform real-time security processing. The company generates about 80% of its revenue in the North America and EMEA regions and focuses on education, retail and distributed enterprise markets.

Prospects, globally, should include Fortinet when considering vendors for a unified-access network deployment or refresh in education or retail, and when considering options for consolidating access network security infrastructure.

STRENGTHS

- Fortinet pushes real-time security patches and malware or virus definition updates out to network customers, rather than providing them as periodic batch updates, reducing the time that network elements may be vulnerable to newly created or identified threats.
- Fortinet does not charge a licensing fee for its infrastructure wireless access points, leading to lower cost.
- The combination of FortiOS running on every Fortinet device with FortiSIEM delivers a strong security framework for managing IoT devices at the access layer, including the ability to implement IoT containment through policy-driven segmentation.

CAUTIONS

- Fortinet's unified network management solution enables management of only Fortinet switches, access points and security appliances. This narrows its appeal to enterprises with multivendor infrastructure deployments.
- Fortinet has several different lines of wireless access points that are usable to different degrees across the vendor's different access networking architectures. This potentially causes customer confusion about the interoperability and migration of the overall product line, as well as suboptimal choices.
- Fortinet does not directly control the roadmap direction of FortiPresence, its indoor location service and application platform, since the functionality exists through an ecosystem partnership. This may limit Fortinet's ability to keep pace with changing enterprise requirements.

HPE (Aruba)

Aruba operates as a subsidiary of HPE and retains its brand for campus networking and security solutions. HPE (Aruba) is the second-largest vendor in the wired/wireless LAN access layer worldwide market, with revenue share of 19% for wireless and 10% for campus switching in 2016. HPE has rationalized what was a complex and overlapping portfolio of WLAN and wired access switching products. The company has a wide portfolio that includes WLAN controllers, a controllerless architecture through the Aruba Instant access points, and a cloud-managed offering with Aruba Central. Recent additions to Aruba Central include guest access management that leverages *some* functionality derived from ClearPass, the addition of Clarity (a feature that enables real-time testing of the quality of network connectivity services) and the ability to manage Aruba switches. Aruba Meridian, a cloud-only solution, provides end-to-end location-based services with remote beacon management tools, offering analytics, wayfinding and asset tracking capabilities.

The Mobile First Platform is a software platform that allows organizations and third-party developers to access network, security and location insights. Aruba has expanded its security portfolio beyond ClearPass to include user and entity behavioral analytics (UEBA) with the acquisition of Niara (rebranded as IntroSpect). The combination of the AirWave management solution and Aruba's AppRF technology performs deep packet inspection for application visibility and control, and enables organizations to monitor latency of voice and video sessions, both over wireless and wired.

Evaluate HPE (Aruba) globally for all wired/WLAN access layer opportunities.

STRENGTHS

- Gartner clients report a high degree of satisfaction with Aruba's ClearPass, which provides guest access, device profiling, posture assessment and onboarding.
- Aruba's management and service applications (ClearPass, IMC, Meridian and AirWave) support non-HPE devices such as Cisco, ALE and others, which simplifies orchestration within multivendor environments.
- The acquisition of Niara and Rasa Networks strengthen Aruba network traffic and security monitoring capabilities.

CAUTIONS

- HPE FlexNetwork legacy switches do not offer the same level of functionality from AirWave and ClearPass compared with Aruba switches, which increases the likelihood of a suboptimal deployment. Enterprises should evaluate the difference in relation to their requirements.
- Aruba Central, Aruba's cloud offering, currently lacks the same functionality as its on-premises ClearPass and AirWave offerings, limiting its capabilities.
- Aruba has made changes to HPE's broadly available lifetime warranty for campus switches, which may be confusing and increase the total cost for the Aruba solution.

Huawei

Huawei's Enterprise Business Group (EBG) is a global solution provider that has strong presence in its local Chinese market, which generated more than 55% of its switching and WLAN revenue in 2016. In the last three years, Huawei has grown at above-average market rates, although primarily in the Asia/Pacific and EMEA regions. Huawei's Agile Network Solution offers end-to-end campus networking that is predominantly focused on education, government and the public sector, hospitality, and retail. Many Huawei switches have integrated WLAN controller functionality, eliminating the need for a physical appliance and providing a more cost-effective solution. The Agile Controller platform offers programmability for tighter wired and wireless management and monitoring of network application services in branch offices. The Agile Controller also acts as the gateway for Huawei's CloudCampus solution, which allows management of switches and WLAN access points from the cloud.

Clients should evaluate Huawei for all wired/WLAN access layer opportunities, especially where it has a sizable installation base, mainly in China and EMEA.

STRENGTHS

- Huawei's campus Agile Controller architecture can scale to up to 6,000 access points and over 1,000 access switches.
- Huawei has a strong foundation in switching, which provides a broad range of fixed-form and modular switches, generally at lower prices than competitors.

- eSight is a flexible network management application that supports infrastructure and devices from third-party providers, as well as the broad range of Huawei wired and wireless access layer components.

CAUTIONS

- Organizations should request references for implementation and service of applicable Huawei solutions when installations are outside of China and EMEA.
- Huawei's location services lag behind competitive offerings. Organizations should ask for proof points and review Huawei's ecosystem of partners for additional capabilities.
- Huawei has a limited machine learning, network automation strategy that will affect its ability to deliver on advanced enterprise access layer requirements, such as SLAs that will need to act on the data instead of collecting and alerting IT.

Juniper Networks

Juniper Networks provides access networking via its EX Series wired switching and NFX Series service platform, but largely relies on ecosystem partnerships for wireless and expanded network applications through its Open Convergence Framework strategy. This ecosystem includes HPE (Aruba), Aerohive, Brocade (Ruckus), Lancom Systems and Samsung. The Juniper Unite Cloud-Enabled Enterprise is an integrated framework that provides automation, analytics and security from the cloud to the campus to branch networks. Juniper continues to expand its focus on security with its Software-Defined Secure Networks (SDSN) strategy, which delivers automated security policy enforcement to network device throughout the network via the Juniper Policy Enforcer engine. Junos Space Network Director delivers on-premises, single-pane-of-glass network management for wired, wireless, security and policy network elements.

Juniper maintains a well-thought-out campus switching architecture but lacks control over a wireless connectivity roadmap that is an enterprise connectivity requirement. Juniper should be considered for wired switching opportunities in midsize and large enterprises.

STRENGTHS

- Juniper's Unite Branch solution extends SDSN to the branch, applying security policies for organizations that have a central campus (headquarters) as well as remote offices.
- Juniper Unite and its Open Convergence Framework ecosystem deliver choice for hardware and software components. The interoperable options have been expanded to the global ecosystem of partners.
- Junos Fusion Enterprise creates a campus network fabric which behaves as a single logical device for simplified management and provides virtual segmentation to isolate IoT devices from the access layer to the data center.

CAUTIONS

- The Open Convergence Framework strategy limits Juniper's ability to control WLAN roadmaps, including indoor location, traffic analytics and security behavioral analysis, which may cause the company to lag competitors in keeping pace with enterprise needs.
- Juniper's wireless relationships are "meet in the channel," which means sales, support and maintenance are separate from the relationship with Juniper.
- Juniper has a limited unified wired and wireless LAN access strategy, since it must collect information from partners that are part of the Open Convergence Framework, but none are integrated into Juniper's network fabric.

Mist Systems

As one of the smallest but fastest-growing vendors, Mist Systems has over 200% growth year over year. Mist offers a portfolio of wired and wireless components, which are typically delivered in the cloud. Mist dual radio access points have 16 integrated antenna elements for Bluetooth low energy (BLE) and collect over 100 different user states, which are processed through a machine learning engine. In addition to guest access, network management and policy applications, Mist provides indoor location capabilities and virtual BLE beacon functionality for wayfaring applications and asset management. The Mist architecture also allows it to leverage artificial intelligence technology for proactive operations, predictive recommendations and rapid troubleshooting required to provide network assurance and automation.

Mist focuses on midsize and large enterprises and should be evaluated in education and retail opportunities in North America or globally through partners, such as NTT, that have a global footprint.

STRENGTHS

- Mist has an indoor location solution that provides 1- to 3-meter granularity and virtualizes BLE beacons, eliminating the need for physical-battery-powered beacons.
- The Mist solution has over 100 pre- and postconnection user states in its access points, which are integrated into a machine learning engine to deliver network automation and lower the cost of management by automating operations and making predictive troubleshooting.
- The Mist solution provides a complete view of metrics for the users of Wi-Fi and BLE data on the cloud console, which can also be deployed on-premises. Organizations that have custom reporting or analytic requirements should review all the information available via APIs.

CAUTIONS

- Mist has a small direct and indirect sales organization that focuses mainly in North America. Organizations need to assure that sales and support, either directly from Mist or through partners, are available for all geographical areas where the Mist solution will be deployed.
- Lack of control of wired connectivity, which is provided through partners, limits Mist's ability to directly control development in areas such as traffic analytics, security behavioral analysis and IoT containment. Organizations must understand the functionality and support of Mist's ecosystem partners.
- Mist has higher-priced access points in a market that has continually declined in price. Organizations must assure that any access point premium yields the appropriate return on investment.

Mojo Networks

Mojo Networks is a wired and wireless access layer infrastructure provider with a portfolio of switches, access points and access layer applications. While focused in North America, Mojo has a global customer base. The cloud-managed Cognitive WiFi solution has been optimized for large-enterprise networks, as well as higher education and K-12 markets. Mojo is a proponent of open standards and is a member of the Open Compute Project Foundation (OCP), which helps drive the vendor community to open-source access layer connectivity. It recently demonstrated several Open Network Install Environment (ONIE)-compliant "white box" access points, working in tandem with several ecosystem partners, and released a three-radio access point. The third radio is to be used for many applications, including full-time wireless intrusion prevention systems (WIPSs), spectrum analysis and client simulation. Evaluate Mojo Networks in North America for all wireless

cloud-based access layer connectivity projects and globally through partners that provide the required ability to support installations.

STRENGTHS

- In line with enterprise clients' adoption of network automation, Mojo intelligent cognitive architecture automates network monitoring and troubleshooting, allowing the network to detect, diagnose and resolve autonomously. Organizations seeking high reliability and having limited IT staff or remote offices could benefit from the ability to rapidly troubleshoot and resolve issues.
- Mojo AirTight is a WIPS that provides comprehensive protection from wireless vulnerabilities and threats. This is particularly suitable for enterprises with strong rogue or intrusion detection requirements.
- Mojo's licensing model and hardware purchasing model make it very competitive in its target markets while providing ease of ordering and deployment.

CAUTIONS

- Mojo has a direct sales organization that focuses in North America and EMEA with a global presence through partners. Organizations need to assure that sales and support are available for all geographical areas where the Mojo Networks solution will be deployed.
- Mojo lacks roadmap control and development resources of wired connectivity, indoor location and IoT containment. Organizations must evaluate those portions of the solution provided by Mojo's ecosystem partners.
- The lack of multivendor network management support in Mojo's cloud means organizations need to be aware that multiple vendor-specific network applications may be needed.

New H3C

In May 2016, HPE announced that it had closed the sale transaction of H3C with Tsinghua Holdings. New H3C is a strong infrastructure vendor in China with a large portfolio of hardware and applications, including switches, WLAN, security and cloud computing products. For wired/wireless LAN access layer opportunities, New H3C's key vertical markets are the education, healthcare and government sectors. The intelligent Management Center (iMC) provides unified wired/wireless management and guest access, and the more recent Oasis platform provides wireless management from the cloud, including data analytics and basic device/user behavior analysis in a multitenant environment.

Clients with Asia/Pacific access layer opportunities should consider New H3C.

STRENGTHS

- Organizations can deploy iMC modules that provide capabilities ranging from user behavior analysis to security policy management and automation.
- New H3C has a strong foundation in switching, with a broad portfolio of fixed-form and modular switches at competitive pricing.
- New H3C's Oasis platform provides cloud-based management that supports network health inspection, user experience, wireless network analysis, troubleshooting and indoor location application services in conjunction with its Cupid indoor location services.

CAUTIONS

- Over 90% of New H3C's revenue is in Asia/Pacific; organizations considering New H3C in other geographies should request partner references for implementation and support/servicing.
- iMC is a large network service application with many modules that is confusing to organizations and requires additional training for network administrators.
- New H3C lags behind other vendors in the breadth of controllerless products, such as access points with embedded controller functionality, which are more resilient and cost-effective.

Riverbed (Xirrus)

Riverbed acquired Xirrus in April 2017 as part of expanding its SteelConnect software-defined wide-area network (SD-WAN) offering with an enterprise-grade cloud-managed WLAN solution. The addition of Xirrus' wireless-focused portfolio provides a larger range of access points; the cloud-based or on-premises Xirrus Management System (XMS); and service applications such as its EasyPass access solution suite. As with any acquisition, execution within the first 12 months is critical to success, and Riverbed (Xirrus) is faced with the task of integrating and rationalizing multiple hardware, software and management product lines, and merging corporate cultures.

Prospects in North America and EMEA should evaluate Riverbed (Xirrus) for opportunities in education and distributed enterprises.

STRENGTHS

- Riverbed (Xirrus) access points support two to eight software-defined radios to provide flexibility to address increasing density requirements as clients carry more devices.
- EasyPass is a suite of network applications that provides Wi-Fi device onboarding and guest access services and policy control, including single sign-on for users with Microsoft Office 365 or Google Cloud credentials.
- The acquisition of Xirrus by Riverbed adds additional sales and support resources to expand the ability to deliver an access layer solution.

CAUTIONS

- Customers that have recently purchased Xirrus wireless access points or prospects should request detailed sales, support and migration plans from Riverbed (Xirrus).
- Riverbed (Xirrus) has a limited machine learning and network automation strategy that will affect its ability to deliver on advanced enterprise access layer requirements.
- Riverbed (Xirrus) has limited traffic and security monitoring capabilities beyond network management and device profiling functionality.

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

The following vendors were added to this year's Magic Quadrant:

- New H3C
- Mist Systems
- Mojo Networks
- Riverbed (Xirrus)

Dropped

The following vendors were dropped from this year's Magic Quadrant:

- Avaya's switching and WLAN organization was acquired by Extreme Networks. It will be assessed as Extreme Networks.
- Xirrus was acquired by Riverbed. The combination will be assessed as Riverbed (Xirrus).
- Zebra Technologies' WLAN organization was acquired by Extreme Networks.
- ZTE did not meet the inclusion criteria.

Other 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
- Lancom Systems
- Netgear
- Ruijie Networks
- Ubiquiti Networks
- Zyxel Communications

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, vendors need 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/Description section.
- Demonstrate relevance to Gartner clients in the enterprise access layer market by providing one or more network applications as outlined in the Market Definition/Description section with an annual network service revenue exceeding \$5 million.
- Produce and release enterprise access layer networking products for general availability as of 15 April 2017. 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 2017.
- Demonstrate production enterprise customers with at least five reference customers supporting access layer networks of more than 100 access points.

Evaluation Criteria

Ability to Execute

Gartner evaluates technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to have a positive effect on revenue, retention and reputation. Technology providers are ultimately judged on their ability and success in capitalizing on their vision.

Product/Service: We evaluate vendors for completeness of their access layer infrastructure products and services consisting of switches, access points and related components such as external antennas and outdoor enclosures needed for the end-to-end solutions in various vertical markets. This year, we have placed greater emphasis on network applications such as management, monitoring, guest access, policy enforcement, location, network analytics and security applications. 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 (Business Unit, Financial, Strategy and Organization): 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: This involves the vendor's capabilities to understand client needs and communicate differentiation, as well as the direct and indirect channel sales structure to support client opportunities. This criterion includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel, both direct and indirect.

Marketing Responsiveness and Track Record: This includes the quality and effectiveness of the organization's marketing messages in communicating to the market the advantages and differentiating capabilities of the vendor's product lines, company and supporting partners/services. This evaluation also includes the history of the vendor's marketing messages and its ability to react to changes in market requirements in its target markets.

Marketing Execution: This criterion focuses on how the vendor is perceived in the market, and how well its marketing programs are recognized. For access layer infrastructure, the evaluation focused on how well the vendor was able to influence the market around key messages and attributes. An additional indicator for this criterion is how often Gartner clients consider a vendor as a possible supplier in a shortlist evaluation. The change in momentum in this indicator is particularly important.

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 written responses about the vendors. A key component in this category is the vendor's ability to provide strong presales and postsales support, especially aligned with vertical requirements.

Operations: This criterion was not ranked.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	High
Customer Experience	High
Operations	Not Rated

Source: Gartner (October 2017)

Completeness of Vision

Gartner evaluates technology providers on their ability to convincingly articulate logical statements about current and future market directions, innovation, customer needs and competitive forces, as well as how they map onto the Gartner position. Technology providers are ultimately rated on their understanding of how to exploit market forces to create opportunities for themselves.

Marketing Understanding: Does this vendor's marketing message articulate a clear, understandable message that answers the market requirements for technologies and services? Do the vendor's message and supporting products lead the access layer market requirements or merely fulfill them?

Market Strategy: We evaluate the ability of the vendor to look into the future and drive/influence the direction of the market through product roadmaps and offerings. We also look at its ability to communicate differentiating functionality and value proposition. Are the issues that are being addressed meeting the trends in the market and the needs of end users? Are vendors focusing on building their core competencies, or are they investing in random technologies?

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 it have partners that extend the scope and depth of market reach, expertise, technologies, services and the customer base?

Offering (Product) Strategy: Does the current and future planned 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. Specifically, we look for whether the business model meets the needs of the target market and provides growth for the vendor.

Vertical/Industry Strategy: Do 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 and hospitality?

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, voice, video and application visibility support? Is there innovation in the access layer applications that address client needs for easier installation or onboarding, as well as better management? Has the vendor successfully differentiated the current and future product lines to better address customer requirements, both now and two to five years out?

Geographic Strategy: Can the vendor meet the needs of global enterprises for products and support?

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner (October 2017)

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 shape the

market, 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 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.

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, convergence, 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, but may not be able to control development or provide differentiating functionality because part of the solution is being offered through a strategic partnership, 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 market has evolved beyond the speeds and feeds of technology, whether it is high-performing radios or the access point platforms that integrate them. While the processing power and functionality of access points at the edge of the campus network have grown, they have consumed the requirement for controller hardware in access layer architectures. Additionally, we are seeing the implementation of fabric architectures in the access layer that we often see in data center architectures. The value is now in the network applications that consume the data that is generated at the edge. The baseline of functionality is clearly drawn with network management, guest access, policy enforcement and wireless intrusion detection system (WIDS) capabilities that once differentiated the vendors. Today, the data is consumed by machine learning engines that provide the necessary granularity for indoor location services or proactively manage the devices and adjust the network fabric so that it provides the performance and the high availability that is now expected by end users in every market segment. These next-generation applications are the differentiation of today's access layer vendors.

Market Overview

Prospects' decisions historically have been made based on the speeds and feeds of the hardware, but this has changed as access layer switches and access points are more of a commodity. Access layer applications at the edge of the campus network are the mainstay of the access layer and use information provided by connected network equipment and mobile devices to help organizations make business decisions. These decisions can include the location of devices and whether guests and any device or user should be able to connect to the network. The complexity

of the access layer has risen because there are fewer IT resources to manage the increasing requirement for wireless connectivity. Instead of just collecting information at the edge of the network, vendors are using machine learning algorithms to automate discover, management, troubleshooting and resolution to automate the access layer.

Clients Seek Stability, Flexibility

While many clients seek solutions enabling unified management of multiple vendors across wired and wireless infrastructure as they migrate from one vendor to another, the reality remains that over 70% of clients tell Gartner they prefer using a single vendor for their access layer network. Gartner clients indicate during surveys and inquiries and in RFP or network refresh requirements that they prefer a unified wired and wireless access network, with a common set of security, policy enforcement and management solutions that are available from a single pane of glass.

Enterprise feedback and market figures also reflect an increasing preference for architectures that have the flexibility to deploy network service applications on-premises, or in a public or private cloud. Clients also show increased interest in outsourced managed LAN services, often from service providers depending on the geography, which assume management and operation of wired and wireless network infrastructure. Finally, in the midst of ongoing changes to the market's corporate landscape, where we saw three acquisitions and another one in process, vendor viability and the capability to integrate key technologies from merged or acquired companies remain key client concerns.

What's Changed in the Market

During the past 12 months, we have seen the market, through client inquiry and surveys, increasingly focused on network service applications versus hardware components because of lack of differentiation. There is an emergence of basic or standard check-the-box applications that are required for enterprise deployments, such as guest access, network management, WIDSs and policy enforcement, where all vendors provide solutions that exceed the basic functionality needed by enterprises. In 2016, several new applications emerged, including location-based services, traffic analytics, behavioral analytics and network automation capabilities.

Enterprise Requirements Focus on Network Application Services

Access layer hardware has increasingly become commoditized, making software — the end-user-facing applications needed to configure, secure, manage and automate the infrastructure — a greater vendor differentiator than switch or wireless access point features. This is further supported by the access layer WLAN market growing at 9.5% while the hardware components such as switching revenue in 2016 declined 2.5% and access point prices also declined. Enterprises also want greater insight into network performance, security and monitoring due to the diversity of client devices using the network, a trend that started with BYOD and guest access scenarios but has since expanded to IoT devices.

The focus on network service applications is becoming especially true in outsourced managed LAN scenarios, where the customer may focus more on the network assurance capabilities that the provider offers — and the SLAs for supporting a specific user experience — than on the listed throughput, capacity or antenna specs for the deployed infrastructure. Some vendors have begun characterizing their ability to automate network configuration, provisioning, onboarding, monitoring and other services as software-defined networking (SDN) or virtualization of the network, although the applications are not yet capable of dynamic reconfiguration of the network resources based on application needs.

End-user discussions based on inquiry and have primarily been about:

- Understanding the end-user experience
- Refresh of the existing network or migrating from one technology/vendor to another
- Understanding that cloud is a "how" to implement, not a "what" or a requirement
- Understanding the performance and security issues associated with IoT
- Understanding whether SDN is relevant to the access layer

Other emerging trends include:

- New pricing models, including per use connectivity
- The need for network assurances and SLAs in the access layer

IoT Requirements Drive Software Innovation

Clients continue to tell Gartner through inquiry, customer interactions and surveys that new business strategies with IoT implementations are attaching large numbers of new endpoints to an enterprise's access network. These new devices require new discovery and location capabilities, new security, and provisioning functionality to attach to the network (since many IoT devices do not have keyboards or displays), as well as new management capabilities. This new functionality must be part of any new access layer RFP, or the organization risks increasing the security attack surface with unknown and unmanaged devices, as well as being unable to meet the service-level requirements for authorized end users.

Consolidation Continues, New Providers Emerge

Just as in the previous two years, established vendors in 2017 continued to acquire companies to enhance their unified access capabilities. Extreme Networks acquired Zebra Technologies' access networking business in 2016 and has also acquired Avaya's networking business in 2017. Riverbed acquired Xirrus. HPE completed the divestment of the majority of its interest in its China-based networking business into New H3C. Enterprises need to be aware of the acquisitions, because they will affect service, support, migration strategies and new solution deployment strategies.

Evidence

Vendor Survey

Customer Reference Survey

Inquiry

Vendor Briefings

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.

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](#) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."

