Fonctionnalités critiques pour l'infrastructure LAN filaire et sans fil de l'entreprise

4 janvier 2023 - Pièce d'identité G00762497 - Temps de lecture : 36 min

Par **et 1 de plus**Christian Canales, Tim Zimmerman,

Les fournisseurs notés dans cette étude fournissent des fonctionnalités pour les besoins de connectivité de base. Cependant, les responsables de l'infrastructure et des opérations ont également besoin de capacités en matière d'assurance réseau, d'automatisation, d'application des politiques et de confinement de l'Internet des objets basés sur l'IA/ML, pour lesquels il existe une plus grande différenciation.

Aperçu

Principales constatations

- Les scores de Gartner pour les cinq cas d'utilisation définis indiquent peu de différenciation entre les quatre principaux fournisseurs, ce qui indique que leurs portefeuilles peuvent répondre à une grande variété de cas d'utilisation d'entreprise, indépendamment de la taille de l'entreprise et du marché vertical.
- Les capacités matérielles sont de plus en plus banalisées, avec une différenciation de moins en moins importante entre les fournisseurs de réseau.
- De nombreuses entreprises connectent un nombre croissant d'appareils de l'Internet des objets (IoT) convergeant vers le réseau de l'entreprise, ce qui renforce l'importance de la visibilité et de la sécurité des appareils IoT.
- Les plates-formes de gestion de réseau et les feuilles de route de produits mettent de plus en plus l'accent sur l'analyse basée sur l'intelligence artificielle et l'apprentissage automatique (IA/ML), visant à établir une base, à surveiller et à résoudre de manière proactive les problèmes de performance du réseau.

Recommandations

Les responsables de l'infrastructure et des opérations (I&O) du cloud et de la périphérie responsables de la planification, de l'approvisionnement et de la gestion des réseaux filaires et sans fil doivent :

- Hiérarchisez leurs exigences en matière de gestion, d'automatisation, d'application des politiques et de fonctionnalités de localisation intérieure, le cas échéant, afin de répondre à leurs cas d'utilisation.

- Limitez les fonctionnalités de sécurité pour les cas d'utilisation de l'IoT, car les points de terminaison IoT sont sujets à une authentification faible ou inexistante. Les fonctionnalités clés doivent inclure la découverte et la classification des appareils IoT, la segmentation virtuelle et la surveillance continue.

- Appliquez les meilleures pratiques pour la mise en œuvre d'un réseau local sans fil (WLAN), telles que l'identification des besoins en bande passante, en latence et en mobilité pour les utilisateurs finaux. Bien que l'utilisation de l'analytique tirant parti de l'IA pour les opérations informatiques puisse simplifier le dépannage et améliorer l'assurance des services, des WLAN mal conçus et mal mis en œuvre entraîneront une mauvaise expérience utilisateur.

Hypothèses de planification stratégique

Les coûts d'exploitation du réseau augmenteront d'au moins 15 % chaque année au cours des cinq prochaines années, pour 70 % des entreprises, faute d'un plan visant à atténuer les problèmes de chaîne d'approvisionnement du matériel réseau.

Plus de 90 % des entreprises qui achètent des points d'accès Wi-Fi 6E ne réaliseront aucun retour sur investissement calculable avant au moins 2024 en raison d'un manque d'appareils prenant en charge la nouvelle norme.

Ce que vous devez savoir

Cette étude sur les capacités critiques est le complément du **Magic Quadrant de Gartner pour les infrastructures LAN filaires et sans fil d'entreprise**. Il évalue 12 offres dans cinq cas d'utilisation conçus pour refléter les principaux critères d'évaluation recommandés par Gartner pour les responsables I&O responsables de la planification, de l'approvisionnement et de la gestion des réseaux d'accès filaires et sans fil d'entreprise.

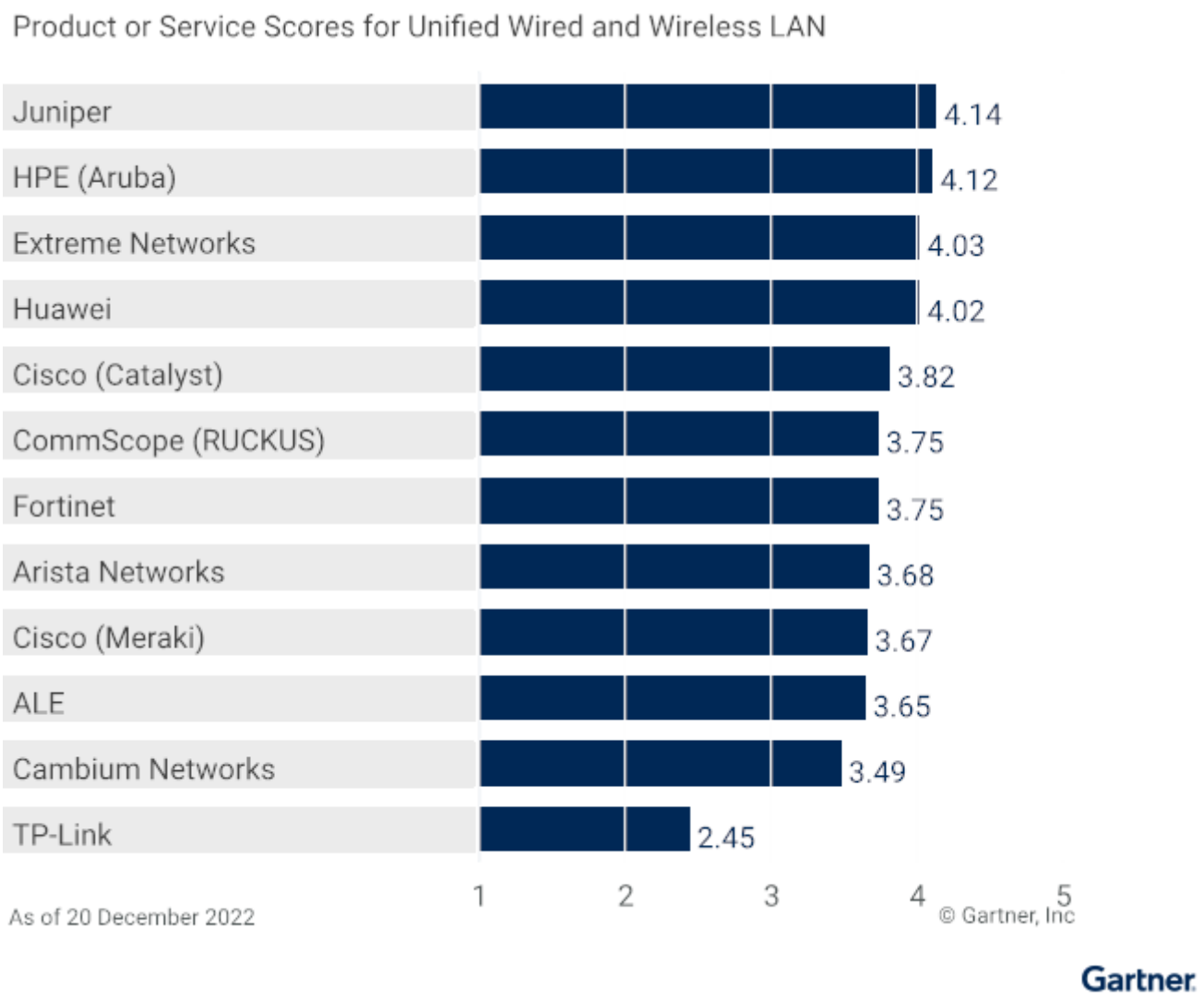
Les responsables I&O responsables de la mise en réseau peuvent utiliser les capacités critiques évaluées dans cette étude pour éclairer leur recherche de solutions appropriées qui répondent mieux à leurs cas d'utilisation spécifiques.

Avec l'évolution du marché, le matériel de réseau basé sur des normes offre aujourd'hui peu de différenciation. Les capacités de surveillance et la possibilité de gérer les produits sur site et dans le cloud ont également atteint leur maturité. Les capacités de sécurité tirant parti de la technologie de contrôle d'accès au réseau ou de la segmentation virtuelle pour l'intégration de l'IoT sont également de moins en moins différenciées, bien que la fonctionnalité de détection et de réponse au réseau (NDR) sépare un certain nombre de fournisseurs. Ensuite, il y a les domaines où l'innovation et le développement de produits sont plus nombreux, tels que l'automatisation et les fonctionnalités d'IA « auto-réparatrice » pour les opérations informatiques (AIOps) qui vont au-delà de la fourniture de recommandations de dépannage.

Analyse

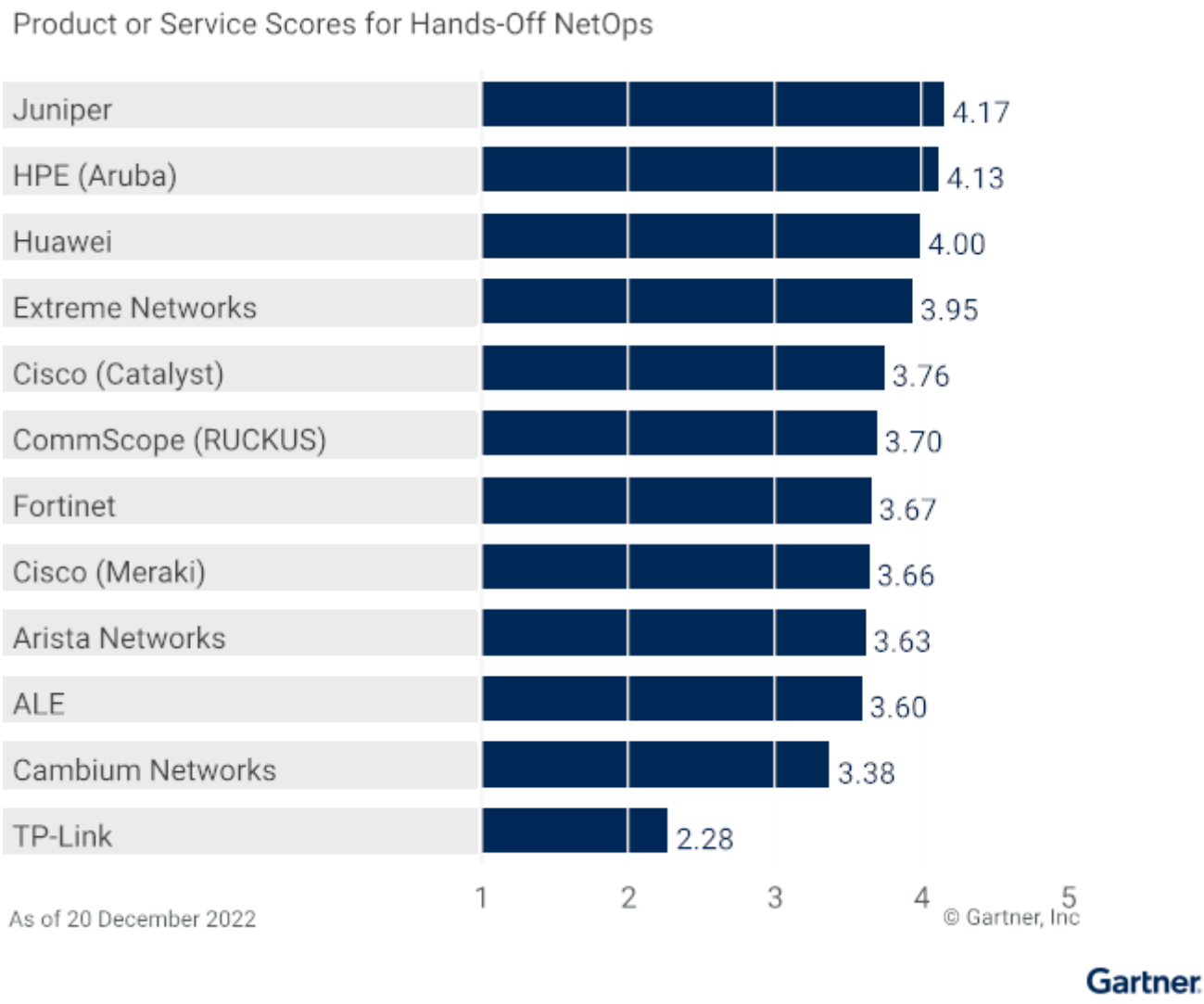
Graphiques de cas d'utilisation des fonctionnalités critiques

Scores des fournisseurs pour le cas d'utilisation d'un réseau local câblé et sans fil unifié



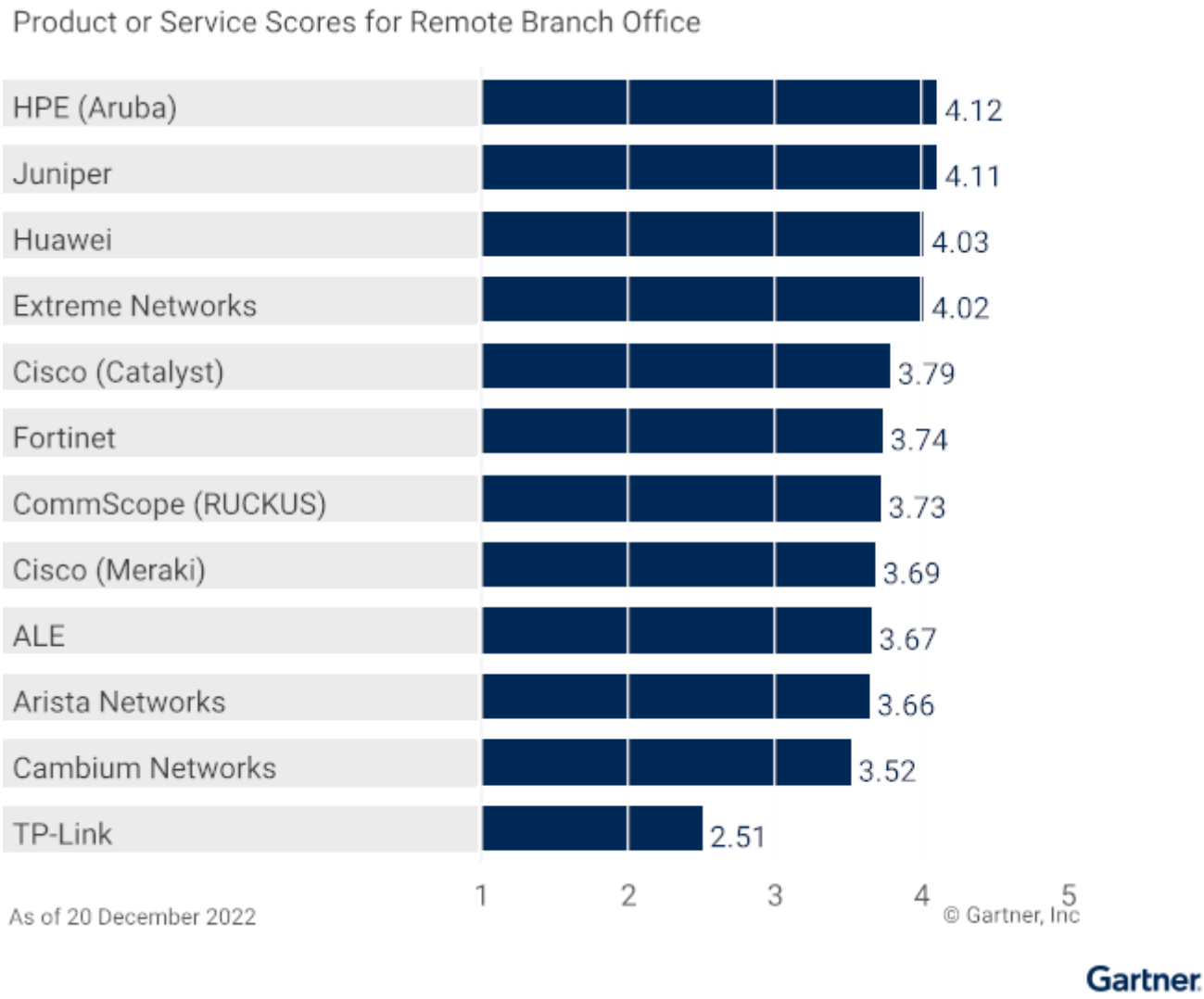
Source : Gartner (janvier 2023)

Scores des fournisseurs pour le cas d'utilisation NetOps sans intervention



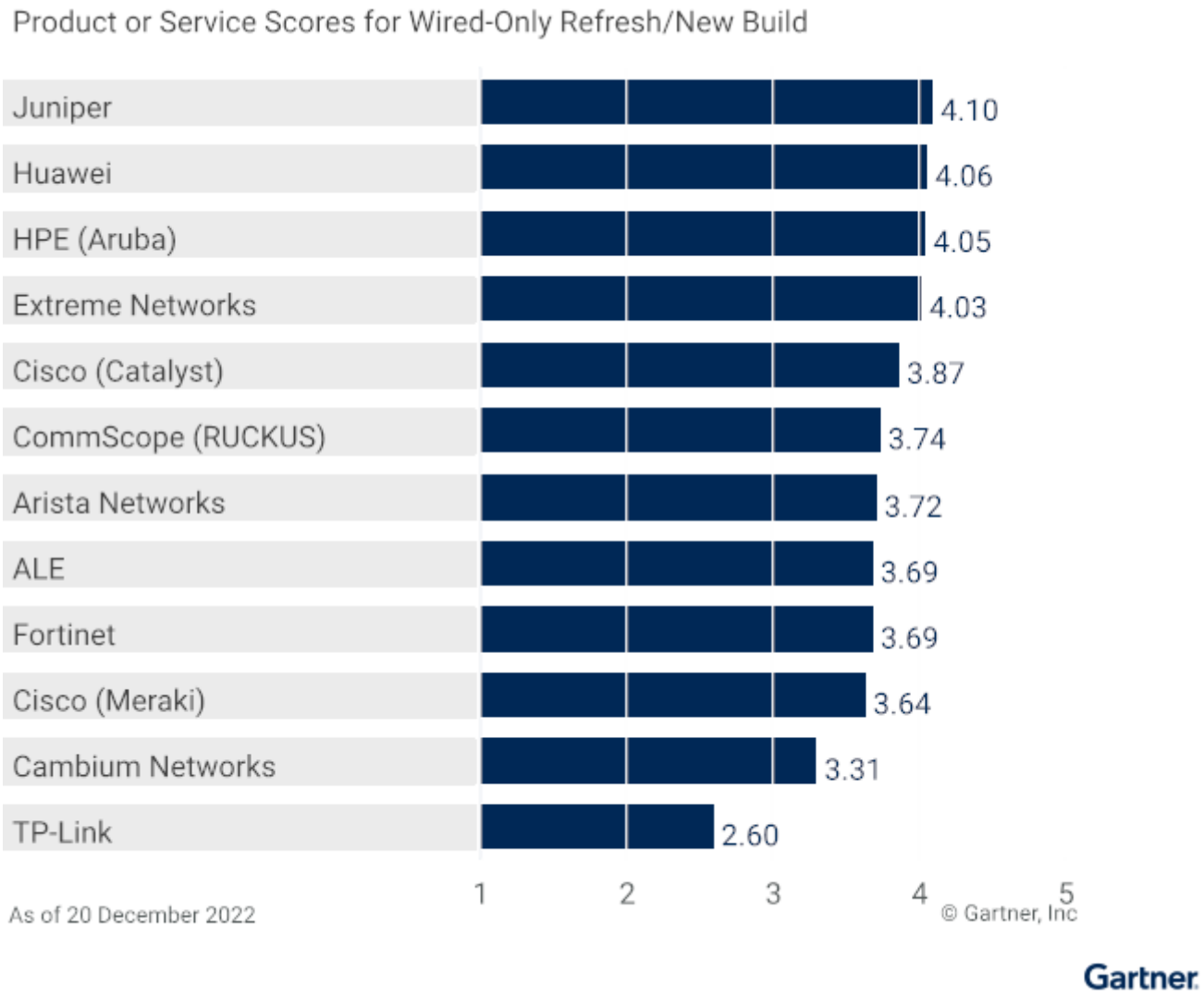
Source : Gartner (janvier 2023)

Scores des fournisseurs sur les produits pour le cas d'utilisation des succursales distantes



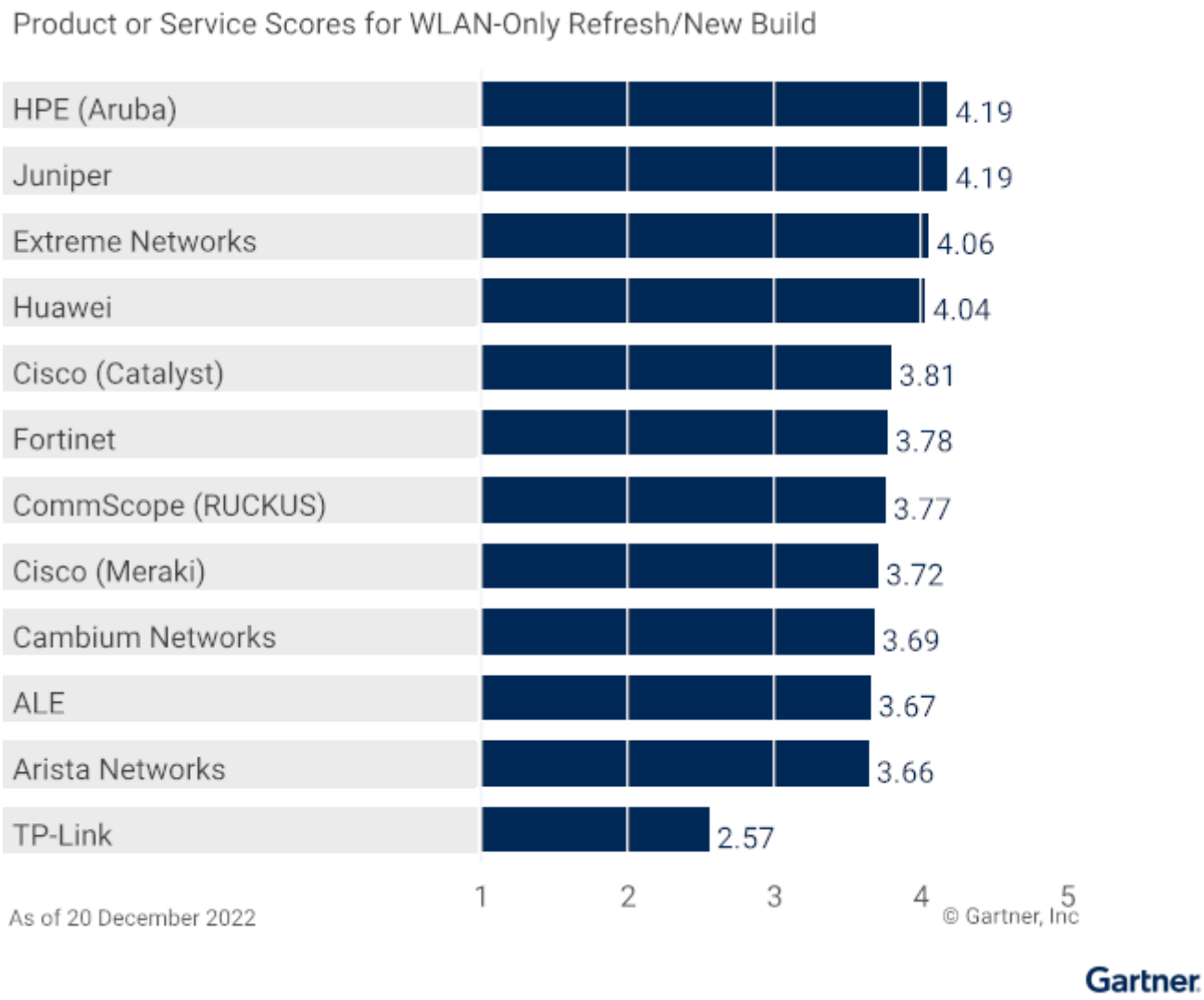
Source : Gartner (janvier 2023)

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



Source: Gartner (January 2023)

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



Source : Gartner (janvier 2023)

Fournisseurs

ALE

Alcatel-Lucent Enterprise (ALE) est basée à Colombes, en France. Ses points d'accès sans fil OmniSwitch, ses points d'accès sans fil OmniAccess Stellar et ses logiciels réseau associés répondent à tous les besoins des entreprises. La gestion est proposée en mode SaaS avec OmniVista Cirrus et sur site avec le système de gestion réseau OmniVista 2500.

Au cours de l'année écoulée, ALE a continué d'investir dans ses capacités de connectivité et de gestion du réseau. L'entreprise a amélioré ses analyses LAN et Wi-Fi pour des performances plus prédictives et un dépannage plus simple, et a augmenté les fonctionnalités de configuration automatisée pour les entreprises et les succursales à l'aide de sa technologie Intelligent Fabric. La technologie de fabric d'ALE automatise le déploiement de grandes installations réseau, ce qui permet de simplifier le cadre, y compris l'application des politiques et l'intégration de l'IoT. La fonctionnalité AIOps d'ALE pour l'assurance réseau s'appuie sur son moteur de règles Rainbow Workflow. La plate-forme de gestion OmniVista comprend des analyses de localisation LAN et Wi-Fi de base, ainsi qu'une fonctionnalité gratuite de contrôle d'accès au réseau (NAC) avec Unified Policy Access Manager (UPAM). En 2021, ALE a également lancé son offre de réseau en tant que service (NaaS), basée sur une offre d'abonnement hybride regroupant ses commutateurs, ses

points d'accès et ses micrologiciels, ainsi que des services de support, moyennant un tarif forfaitaire, mensuel, trimestriel ou annuel, ainsi qu'une petite dépense d'investissement.

Les scores de l'ALE sont inférieurs à la moyenne. Les scores pour les réseaux locaux filaires et sans fil et pour les capacités de gestion et d'administration ont été relativement élevés, en raison d'un portefeuille complet et d'une solide fonctionnalité de gestion du réseau. Les scores pour les capacités de sécurité étaient inférieurs à la moyenne, car ALE est à la traîne en matière de capacités avancées de détection des anomalies NAC et filaires.

Remarque : Les scores de capacités critiques d'ALE reflètent une évaluation des propres produits d'ALE et excluent ceux issus de son partenariat entre le fabricant d'équipement d'origine (OEM) et Hewlett Packard Enterprise (HPE) (Aruba).

Réseaux Arista

Arista Networks est basée à Santa Clara, en Californie. Son portefeuille de réseaux locaux filaires et sans fil se compose de commutateurs Leaf de la série 700, de commutateurs dorsaux d'entreprise de la série 7000 et des points d'accès Cognitive Wi-Fi des séries 200 et 300 . La gestion du réseau est assurée par CloudVision, sa plateforme de gestion du réseau.

Au cours de l'année écoulée, Arista a lancé son EOS Network Data Lake (NetDL), qui accumule des données pour les traiter et les utiliser dans le moteur d'IA/ML intégré à CloudVision. L'assistance virtuelle autonome

(AVA) étend NetDL grâce à une architecture basée sur des capteurs pour permettre l'analyse et l'analyse des cas d'utilisation de la NDR, y compris la détection et la chasse aux menaces avancées. Les commutateurs des gammes CCS 722 et 750 fournissent un chiffrement MACsec sur tous les ports pour une sécurité renforcée avec les points d'accès et les commutateurs d'agrégation. CloudVision AIOps prend en charge le traitement du langage naturel, la classification de la gravité des incidents et l'analyse de la résolution des problèmes, fournissant aux administrateurs des recommandations de correction exploitables. Arista ne fait pas de différence significative entre le fonctionnement et les fonctionnalités de ses commutateurs de centre de données et de réseau d'entreprise. Les organisations qui ont déployé Arista dans le centre de données utiliseront les mêmes outils EOS et CloudVision pour déployer et gérer la topologie du réseau d'entreprise.

Arista obtient des résultats inférieurs à la moyenne, sauf dans le cas d'utilisation de l'actualisation câblée/nouvelle version. Il est à la traîne dans la sélection des points d'accès WLAN, et son portefeuille de commutation de campus découle en grande partie de son architecture de centre de données leaf-spine, ce qui en fait un meilleur choix pour les déploiements de grandes entreprises.

Cambium Networks

Cambium Networks est basée à Rolling Meadows, dans l'Illinois. La société s'adresse au marché des réseaux locaux d'entreprise avec ses points d'accès Wi-Fi 6, cnPilot et Xirrus et ses

commutateurs filaires cnMatrix. cnMaestro fournit une gestion simplifiée des réseaux filaires et sans fil sur site et dans le cloud.

Au cours de l'année écoulée, Cambium Networks a investi dans ses capacités basées sur l'IA et l'apprentissage automatique en termes d'analyse du comportement des clients et des performances, en déterminant les anomalies et les causes profondes des problèmes de réseau. Cependant, les fonctionnalités de l'AIOps restent limitées, se concentrant sur des fonctionnalités de base telles que la sélection automatisée des canaux Wi-Fi, l'identification des applications et des appareils et la détection des intrusions. Cambium offre une sécurité IoT robuste, offrant une évaluation spécifique des menaces pour les appareils IoT, un profilage, une segmentation du réseau virtuel et une automatisation basée sur des règles. En 2021, pour l'intégration de l'IoT et du BYOD (Bring Your Own Device), l'entreprise a étendu l'évolutivité de sa technologie ePSK. Cela permet de définir des politiques par appareil avec des clés prépartagées uniques, une mise à l'échelle jusqu'à 1 000 appareils par point d'accès et à une échelle pratiquement illimitée à l'aide de RADIUS. La plate-forme de gestion cnMaestro minimise l'utilisation de l'interface de ligne de commande, même pour les configurations et les tâches les plus complexes. Il comprend également un assistant de langage naturel basé sur la voix et le texte pour le dépannage.

Cambium obtient des résultats inférieurs à la moyenne. Il obtient un score faible pour les capacités LAN câblées, se concentrant principalement sur les entreprises de taille moyenne et manquant de véritables capacités d'empilage et de haute capacité. En revanche, ses capacités WLAN sont très élevées, en partie grâce à la capacité de Cambium à prendre en charge une couverture haute densité grâce à sa technologie flexible de radio définie par logiciel.

Cisco (Catalyseur)

Cisco est basé à San Jose, en Californie. Cisco dispose d'un large portefeuille de réseaux locaux filaires et sans fil et de la plus grande portée géographique par l'intermédiaire de ses partenaires de distribution. Tous les commutateurs et points d'accès nécessitent une licence obligatoire à durée déterminée (le logiciel DNA de Cisco), à partir d'un abonnement minimum de trois ans.

Au cours de l'année écoulée, Cisco a continué d'investir dans les capacités de DNA Center. Le serveur DNA Center agit comme une plate-forme de gestion de réseau basée sur l'IA/ML qui peut réduire la complexité de la configuration, du dépannage et de l'exploitation pour les déploiements Catalyst 9000 filaires et sans fil. DNA Center sert également de plan de contrôle pour l'accès et la segmentation basés sur des règles avec Software-Defined Access (SD-Access).Cependant, en ce qui concerne la vaste base de clients de Cisco, l'adoption de Cisco DNA Center continue d'être limitée en raison de la complexité et des coûts perçus. La plupart des entreprises déploient plutôt Cisco Prime Infrastructure ou d'autres applications de gestion pour une gestion unifiée du réseau. Dans le cadre de la licence Cisco DNA, Essentials fournit une automatisation de base, tandis que des fonctionnalités plus avancées (par exemple, les services de localisation en intérieur, l'analyse avancée, le NAC et la détection des menaces de sécurité) nécessitent la licence Advantage supérieure. Pour les déploiements WLAN de petite et moyenne taille (jusqu'à 100 points d'accès), Cisco propose une solution sans contrôleur sans licence.

Cisco Catalyst se classe parmi les cinq premiers dans tous les cas d'utilisation. Son score le plus faible se situe dans les NetOps non interventionnistes, où SD-Access peut identifier et corréler statistiquement les problèmes en mettant l'accent sur les recommandations au lieu d'offrir une résolution automatique. Cisco a obtenu des résultats supérieurs à la moyenne en matière de capacités de sécurité, bien que TrustSec reste propriétaire pour le confinement des appareils IoT.

Remarque : Historiquement, Cisco n'utilisait la marque Catalyst que pour son portefeuille de commutateurs d'entreprise. Aujourd'hui, la marque Catalyst comprend également ses produits WLAN.

Cisco (Meraki)

Cisco est basé à San Jose, en Californie. Son portefeuille de produits filaires et sans fil Meraki est commercialisé auprès des clients à la recherche de réseaux gérés dans le cloud. Tous les produits sont configurés uniquement via le tableau de bord Meraki basé sur le cloud, qui unifie la gestion sous une seule interface utilisateur graphique (GUI).

Malgré de nouveaux produits dans le domaine de la sécurité, du WAN et de l'IoT, Cisco Meraki n'a pas introduit d'innovations ou de différenciateurs significatifs en matière de produits LAN filaires et sans fil en 2021. Il y a toujours eu un manque d'intégration entre Meraki et Catalyst, bien qu'en juin 2022, Cisco ait annoncé la disponibilité de la surveillance et de certaines capacités de configuration de son portefeuille Catalyst via le tableau de bord Meraki. Les points d'accès Catalyst 9100 récemment introduits prennent en charge les modèles de gestion de l'ADN Meraki et Cisco. L'empreinte digitale Network Based Application Recognition (NBAR) de Meraki fournit un pare-feu et une mise en forme du trafic pour assurer le contrôle des appareils, des applications et des utilisateurs accédant au réseau. L'intégration du tableau de bord Meraki avec Umbrella améliore encore le filtrage du contenu et la gestion des politiques de sécurité. L'intégration avec le moteur de services d'identité de Cisco prend en charge des exigences NAC plus avancées.

Meraki obtient des résultats inférieurs à la moyenne et dans le tiers inférieur en matière de rafraîchissement câblé uniquement/nouvelle construction. Bien que le choix de commutateurs d'accès soit large, Meraki dispose d'une sélection limitée de commutateurs d'agrégation, bien que, dans certains scénarios, ceux-ci puissent remplir à la fois des fonctions de distribution et des fonctions de base. Meraki se classe dans la moitié supérieure pour ses capacités de gestion et d'administration, et l'une des principales valeurs perçues du tableau de bord Meraki est sa facilité d'utilisation, son intuitivité et sa capacité à prendre en charge des changements fréquents.

CommScope (RUCKUS)

CommScope (RUCKUS) est basé à Sunnyvale, en Californie. Son portefeuille de réseaux d'entreprise se compose des commutateurs ICX de la marque RUCKUS, des points d'accès des séries R et H et de son AIOps basé sur le cloud, ainsi que de sa solution d'analyse et d'assurance réseau, RUCKUS Analytics.

Au cours de l'année écoulée, CommScope a amélioré ses capacités basées sur l'IA et l'apprentissage automatique avec la plateforme RUCKUS Analytics. Il offre une visibilité détaillée sur l'identification des problèmes et les décisions de résolution des problèmes, en plus d'un

assistant de réseau virtuel (VNA) en langage naturel, Melissa. CommScope a également ajouté la possibilité de remédier aux problèmes identifiés directement via l'interface RUCKUS Analytics, à partir de la version 6.1, qui a été publiée en décembre 2021. CommScope propose une suite complète d'outils d'automatisation du réseau, tels que des playbooks Ansible, des scripts et des bibliothèques d'API REST. Les points d'accès 802.11ac ont été abandonnés et, actuellement, seuls les produits Wi-Fi 6 (802.11ax) et Wi-Fi 6E sont disponibles à l'achat. Dans l'ensemble, CommScope dispose d'un solide portefeuille filaire et sans fil, avec une plate-forme d'orchestration intégrée pour faciliter la configuration, mais il manque des commutateurs de châssis modulaires.

CommScope obtient des résultats supérieurs à la moyenne dans trois cas d'utilisation (et inférieurs à la moyenne dans deux d'entre eux), avec son score le plus élevé dans le domaine de l'actualisation/nouvelle construction WLAN uniquement. Il a également obtenu des résultats supérieurs à la moyenne dans le cas d'utilisation NetOps non interventionniste, en raison de son VNA, de ses capacités de gestion intégrée des services informatiques (ITSM) et de ses technologies de validation des services réseau sans capteur. RUCKUS Analytics dispose de solides capacités pour identifier et corréler statistiquement les problèmes. Cependant, la capacité de correction est relativement nouvelle au moment de la rédaction de cet article, et les adoptants doivent s'attendre à des mises à jour substantielles à court terme.

Réseaux extrêmes

Extreme Networks est basé à Morrisville, en Caroline du Nord. Elle dispose d'une large gamme de commutateurs et de points d'accès qui tirent parti de la portabilité de ses licences, ainsi que d'un portefeuille d'applications et de services de réseau gérés dans le cloud et sur site. Les commutateurs 5720, 5520, 5420 et 5320 prennent en charge une structure de campus (SPB ou VXLAN EVPN).

Au cours de l'année écoulée, Extreme Networks a étendu ses capacités AIOps dans le cadre de la plate-forme de gestion ExtremeCloud IQ. CoPilot offre une détection proactive des anomalies et des recommandations basées sur l'AL/ML qui peuvent être immédiatement mises en œuvre, en fonction des écarts par rapport à l'environnement de référence d'un appareil ou d'une organisation (cela inclut les anomalies sans fil et filaires). Le jumeau numérique est également inclus. ExtremeCloud IQ fournit non seulement la gestion du portefeuille d'Extreme, mais également une stratégie de migration transparente pour les entreprises ayant des appareils multifournisseurs sous gestion. L'automatisation de la structure réseau reste un atout, car elle permet aux entreprises qui ont besoin de topologies de structure réseau de réduire la charge de configuration manuelle et le temps de déploiement. La technologie Fabric Connect prend également en charge la segmentation granulaire des utilisateurs, des applications et des services, y compris les appareils IoT.

Extreme Networks se classe parmi les quatre premiers dans tous les cas d'utilisation, dépassant les capacités de confinement des appareils IoT, en raison d'une forte segmentation sécurisée de bout en bout de l'IoT, indépendante des limites de la couche 3. Les problèmes de migration restent néanmoins une mise en garde pour une entreprise qui s'est développée grâce à un certain

nombre d’acquisitions au cours des six dernières années, certains clients exprimant des inquiétudes quant à une stratégie de migration peu claire et limitée des caractéristiques et des fonctionnalités.

Fortinet

Fortinet is based in Sunnyvale, California. Its FortiAP and FortiSwitch products are broadly focused on tight integration with network security capabilities leveraging its FortiGate security appliances and FortiCloud, and FortiLAN for cloud-based management. FortiManager provides on-premises management.

During the past year, Fortinet has expanded its network assurance capabilities with the introduction of FortiMonitor and FortiAIOps, with FortiMonitor also providing visibility into multivendor environments.

The FortiAIOps AI engine provides event correlation and network remediation suggestions, although it lags in the ability to automatically fix issues. For IoT onboarding, FortiOS has NAC functionality, and the licensed FortiNAC offering provides anomaly detection capabilities for advanced threat security. For customers that do not deploy FortiGate appliances (hardware or virtual), Fortinet offers cloud-based management of its switches and APs with FortiLAN Cloud. However, the FortiAIOps AI engine relies on leveraging data feeds from the FortiGate portfolio. FortiPresence provides indoor location services, with optimal accuracy of approximately one meter.

Fortinet scores mostly average across all use cases, although lower in wired-only refresh/new build.

There are some hardware product gaps, such as no modular chassis switches (required for high-density switching and currently in development) and no multigigabit support for its Wave 2 802.11ac APs. Fortinet scores the highest for security capabilities.

HPE (Aruba)

Hewlett Packard Enterprise (HPE) (Aruba) is based in Spring, Texas. Its switching portfolio includes the Aruba CX product lines, complemented by a broad range of WLAN APs. While the Aruba AirWave management platform is still offered, the bulk of new features and investment has shifted to its cloud-based Aruba Central solution.

During the past year, HPE (Aruba) has continued to develop its AIOps features in Aruba Central. Aruba’s AIOps tools reduce troubleshooting time by identifying hard-to-find network configuration issues. HPE (Aruba) provides prescriptive recommendations and automated remediation to continuously optimize network operations (NetOps). Aruba Central NetConductor (launched in 1Q22) simplifies policy provisioning in complex and distributed networks. Aruba EdgeConnect, a cloud-managed SD-Branch platform, focuses on branch-scale deployments, offering a subset of the features found in HPE (Aruba)’s full enterprise-scale solution. With GreenLake for Aruba, HPE (Aruba) has placed delivering NaaS at the core of its enterprise networking go-to-market strategy.

HPE (Aruba) scores in the top three in all use cases, with high marks in WLAN and security capabilities, the latter in part due to its strong NAC solution, Aruba ClearPass. Overall, the company has a strong and scalable portfolio. Organizations looking for an on-premises management platform will find growing technical disparities between Aruba AirWave and Aruba Central, and should consider the Aruba Central on-premises offering. While HPE (Aruba)'s NaaS allows consumption of network gear as a subscription basis, it lacks the ability to add, remove and scale most required network features through a dashboard interface as the business need arises.

Huawei

Huawei is based in Shenzhen, China. It has a broad wired and wireless LAN offering, with its CloudEngine S series switches and AirEngine wireless APs. Huawei's iMaster NCE is the controller platform for its AI/ML-driven CloudCampus solution, which provides management across the LAN and WAN.

During the past year, Huawei has continued to invest in the capabilities of iMaster NCE, including automated network provisioning across sites and network assurance. Its digital twin technology provides the ability to simulate and verify network planning for higher predictability in the move to production networks. Huawei's low-carbon campus architecture is based on a central switch with 4/8-port extension remote units (RUs) that can be desktop- and wall-mounted. Based on hybrid cabling supporting 10 Gbps and Power over Ethernet (PoE) over 300 meters, these RUs provide network access and power supply to terminals, reducing cabling costs and energy consumption. By interacting with a security controller, CloudCampus provides advanced security such as threat detection in encrypted traffic and blocking of lateral movements. However, access to many of these capabilities requires iMaster NCE-Campus, which can be complex or costly for some organizations in on-premises deployment mode.

Huawei scores in the top four across all use cases. IoT device containment capabilities scored slightly lower as Huawei's HLink IoT protocol entails integration with its IoT module or the use of Huawei's open API and software development kit (SDK). This can limit its relevance to organizations standardizing on other endpoint platforms.

Juniper

Juniper Networks is based in Sunnyvale, California. It has a broad wired and wireless LAN offering, consisting of APs, the EX switching line and various QFX switches. The Juniper Mist Cloud platform is a NetOps management suite with integrated automation, AI and ML that can also be deployed as Juniper Mist Edge.

During the past year, Juniper has continued to invest on the AIOps differentiation of its Mist Cloud platform by providing additional AI algorithm support and conversational interface enhancements. The Marvis VNA and its natural language interaction enable automated resolution of network issues. A key differentiation of Marvis VNA, as a self-learning tool, is that it ingests data based on trouble ticket resolution, enabling troubleshooting capabilities without human intervention. Juniper's various Assurance licensed services enable network optimization, application

performance, end-user experience metrics and real-time measurement of targeted SLA compliance metrics. For on-premises LAN management, in addition to the legacy Junos Space Network Management Platform, the Mist Edge offering handles some network functions on-premises. However, to get the most value (e.g., access to real-time statistics and device updates), it requires synchronizing (a connection) to the Mist Cloud.

Juniper scores in the top two across all use cases, with slightly lower scoring in security capabilities. While the acquired NAC assets from WiteSand provide a stronger framework, this was a 2022 acquisition. IoT device containment was rated high, with Mist IoT Assurance supporting simplified IoT onboarding and strong policy enforcement.

TP-Link

TP-Link is based in Hong Kong, China. Its Omada WLAN, T series wired switches and associated network software products mainly focus on addressing the needs of the small and midsize businesses (SMBs). The Omada SDN controller provides network management for TP-Link's switches, wireless APs and routers.

During the past year, TP-Link expanded its Wi-Fi 6 (802.11ax) portfolio. The company also invested in its AI/ML-based technology by adding anomaly detection capabilities that give suggestions to tune up network parameters and some RF functionality to improve roaming and Wi-Fi user experience. However, TP-Link lags in network assurance capabilities, given these are basic features and rely on human interference. For network management and administration, Omada SDN is delivered as an appliance, a virtual machine and as SaaS. The Omada Cloud-Based Controller is hosted on Amazon Web Services (AWS) and offers unlimited scalability, while the Omada Software Controller can manage up to 1,500 network devices and is free of charge. TP-Link provides basic IoT onboarding and indoor location services, given Bluetooth low energy (BLE) integration into its WLAN APs is on the roadmap, and these capabilities either rely on partnerships or are not available.

TP-Link scores below average in all use cases. Among its scores, those for wired and wireless LAN capabilities were more positive, mostly due to the maturity of hardware components in the market. Its highly competitive pricing remains a strength, aligning with the needs of SMBs or, more broadly, with those of organizations with basic connectivity needs looking for a cost-effective solution.

Context

WLAN hardware has become largely commoditized, with all vendors assessed in this research offering Wi-Fi 6 (802.11ax) APs. Many have also introduced Wi-Fi 6E products, starting in the second half of 2021 (Aruba's AP-635 — marketed as the industry's first enterprise Wi-Fi 6E AP — was announced for availability in 3Q21). Wi-Fi 6E extends the radio spectrum to 6GHz, hence utilizing additional, unlicensed radio spectrum beyond that which is available to Wi-Fi products. This potentially triples the spectrum available to Wi-Fi 6, while enabling the Wi-Fi 6 protocol to operate at its best efficiency by removing the need to work around legacy products.

As highlighted in **Quick Answer: Should I Deploy Wi-Fi 5, Wi-Fi 6, Wi-Fi 6E, or Wait for Wi-Fi 7?** Gartner does not recommend moving to Wi-Fi 6E yet. The 6GHz spectrum can make sense for deployments in dense urban areas and high-occupancy buildings, where high levels of contention for traditional radio frequencies adversely affect the Wi-Fi network. However, adopting this prestandard means vendor lock-in so is difficult to financially justify. Finally, realizing the promise of Wi-Fi 6E and its increased performance in the uncrowded 6GHz spectrum is problematic. First, in addition to a lack of standardization, most devices do not yet support 6GHz and will continue to operate in the 5GHz spectrum. So if the goal is to mitigate poor performance due to challenging RF environments, there will be no immediate relief. Second, if the goal is to realize multigigabit throughput for bandwidth-intensive applications, then the supporting wired switch infrastructure must also be upgraded.

Having noted this, vendor push will lead to growing adoption of Wi-Fi 6E, as we have historically seen with each new generation of Wi-Fi products. While Wi-Fi 6E sales are just beginning to ramp up, Gartner has forecast that, as a percentage of overall AP units, Wi-Fi 6E will grow from approximately 10% in 2024 to over 30% by 2026 (see **Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2020-2026, 3Q22 Update**).

A key trend we are seeing in this market is that of AIOps (AI/ML-driven products) feeding growing automation needs, or end-user aspirations. AI and ML technology is increasingly used to interpret events, support and automate decisions, and deliver actionable insights. This improves operational effectiveness, building trust in a solution that finds the optimal data correlations, and fostering growing use of automation.

More and more enterprises are embracing automation, even though a culture of risk aversion remains an important market inhibitor. We see increasing interest in network automation tools as organizations want to reduce cycle times for network activities to align with digital and cloud strategies. At a higher level, this embraces NetOps as an approach that incorporates the use of DevOps practices to networking activities. This results in heavily automating operational network tasks, including troubleshooting and provisioning, enabling a more nimble and easier-to-manage network. Digital twins are part of this push for network automation, where operational teams can test and validate network changes in a simulated environment before moving to production networks.

At the access layer, NetOps applies predominantly to Wi-Fi, although it has begun to extend to wired networking. For too long, Wi-Fi has been one of the “pain points” for organizations, because it comes with inherent challenges associated with interference and distance, and it’s a shared medium. Although these challenges can be addressed, improperly implemented Wi-Fi installations continue to result in a poor end-user experience.

Market maturity in WLAN and switching hardware means that vendor differentiation continues to predominantly rely on software capabilities used to configure, secure, manage and operate the network. This is a source for the different “software-defined” marketing terms that have evolved in the past few years, such as “SD-LAN” or “SD-campus” (or SD-Access in the case of Cisco). These terms largely define an architecture that separates hardware and software layers to form an

application-driven fabric. Here, policy enforcement and management can be operated at scale and with greater flexibility, from the cloud or via a central orchestration platform.

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

Product/Service Class Definition

Gartner defines the enterprise wired and wireless LAN infrastructure market as that of vendors supplying, at a minimum, wired and wireless networking hardware and the related network software. Products in this market enable devices and end users to connect to the enterprise wired LAN or Wi-Fi network in support of the required organizational mission. Supported network devices include end-user-operated devices such as laptops, smartphones and networked office equipment; and non-user-operated devices such as Internet of Things (IoT) devices.

The rated vendors provide some or all of these elements:

Hardware — The core capabilities of physical network elements include:

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

Software — Network service applications that are cloud-, appliance- or virtual-appliance-based. The core capabilities include, but are not limited to:

- Network management
- Network monitoring
- Guest access portals
- Self-service device onboarding services
- Network security integration (for example, IPS, IDS, 802.1X, DNS security and anomaly detection)
- Network policy enforcement/integration
- WLAN location services

- Application visibility and/or performance management
- AI- and ML-enabled network assurance tools
- Network automation tools
- Dedicated non-user device (IoT) management and security mitigation
- Natural language troubleshooting interface

However, the enterprise wired and wireless LAN infrastructure market has evolved beyond its traditional role of merely providing network connectivity for devices. The market now comprises vendors delivering not only wired and wireless networking hardware, but also the inter-related network management, analytics and security applications. This tight integration of network hardware and software delivers the mission agility, pervasive security and increased levels of experience required by end users across all types of connected applications and devices.

Additionally, core integration of artificial intelligence (AI) and machine learning (ML) are integral to correlating the flood of resultant data. They present the data points necessary to optimize the network in support of digital business requirements while also becoming a source of business-relevant data useful to I&O and business leadership.

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

Critical Capabilities Definition

Wired LAN

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

Key capabilities include:

- Different form factors and port densities that meet specific wired switching requirements. These include fixed-form-factor, port-extension and chassis-based switches.
- Capabilities for separating data and control planes (on-premises and/or cloud based).
- Support for virtual segmentation and other integrated security mechanisms.
- Support for fabric management technologies such as VXLAN, EVPN and SPB in the campus.
- Support for end-user and application visibility.
- Product capabilities at the core, distribution and access network layers.

- 802.3bz capabilities that enable 2.5/5 Gbps links to wireless APs for supporting high-density Wave 2 802.11ac and 802.11ax deployments.

Wireless LAN

The vendor's enterprise WLAN solution is inclusive of wireless APs, WLAN controllers and integrated WLAN software/firmware. Point-to-point (fixed wireless access/WAN) solutions are excluded.

Key capabilities include:

- A range of wireless AP form factors to support different indoor and outdoor enterprise and campus environments.
- Ability to scale from hundreds to several thousand APs. The network retains active ability to connect to the controller, whether on-premises, virtualized or cloud-based.
- WLAN controller-based (hardware) and controllerless management options (cloud managed or controller application integrated in an AP-based solution).
- WLAN location services (supporting varying location accuracy).
- Support for end-user and application visibility.
- Ability to measure latency for voice and data applications and to provide sufficient data for mean opinion score (MOS) calculations to support toll-quality voice over WLAN (VoWLAN).
- AP hardware that can support OSs from different acquired vendors (e.g., as part of an integration roadmap for acquired WLAN assets), including end-user security and policies.

Network Security

These are solutions that protect LAN network resources and attached devices governed by policy, including defining roles to control access levels/rights to network resources.

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

Key capabilities include:

- NAC capabilities that enable policy enforcement for user-oriented devices and IoT devices. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity.
- Anomaly detection (increasingly based on AI/ML capabilities) to detect suspicious activities on the network.
- Support of captive portals for employee and guest onboarding and device profiling.

- Network application innovation to support security, policy enforcement and other capabilities at the network core, distribution and access layers.
- Role-based access control.

Management and Administration

This includes the unified deployment (wired and wireless), configuration and ongoing management/administration capability of the vendor's products.

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

Key capabilities include:

- Unified graphic configuration interface for network management, including mechanisms that reduce reliance on a legacy command line interface (CLI): API, scripting, templates, etc.
- Policy-based management, configuration and troubleshooting capabilities
- Application and end-user experience visibility
- Zero-touch and automation features
- Cloud and/or on-premises management capabilities
- Digital twins as a management model to improve situational awareness and reduce network downtime
- Multivendor network monitoring (commonly through SNMP, although also by ingesting third-party data sources via APIs)
- Third-party device visibility and health monitoring

Network AIOps Features

These are solutions that feed data into a data lake and — combined with the use of AI/ML algorithms — can train, baseline, monitor, react, proactively resolve, and report LAN network performance issues.

AIOps features range from solutions that require considerable or full human intervention (e.g., configuration that must be manually applied) to solutions that require little or no human intervention (e.g., self-diagnose and automated remediation capabilities).

Key capabilities include:

- Root cause analysis (leading, for example, to suggestions for network administrators to tune up WLAN settings based on inferences)
- Proactive recommendation engine and predictive analytics for future events
- Detection of wired issues, such as misconfiguration of virtual LANs and overloaded switches
- Automation, such as provisioning and orchestration of network resources, automated network configuration with validation for consistency and compliance, autoremediation based on identified anomalies, etc.
- Identification and diagnosis of bugs in software code
- Incident recognition in connectivity services (e.g., response times with the AAA server)

IoT Device Containment

This is the specific treatment of IoT endpoints and the ability to effectively contain IoT devices and applications. It ensures security of the network using virtual segmentation, access control and IoT device containment.

This includes “fabric” technology approaches that securely handle IoT traffic across the various layers of the network, from the access network connection (ingress point) to the final destination at the edge, data center or cloud.

Key capabilities include:

- Ability to discover an IoT endpoint once connected to the network, whether they are IP-based or non-IP-based
- Ability to secure, profile and monitor IoT endpoints
- Ability to identify the application and how it secures the device through virtual segmentation
- Ability to identify the application and how it assigns a role, if applicable
- Support of VXLAN encapsulation to handle the Layer 2 limitation of microsegmentation

Use Cases

Unified Wired and Wireless LAN

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

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

Users are typically badged employees, although contractors and guests also require connectivity. Employees are usually issued corporate-owned devices. However, the network may also support

BYOD for mobile devices, such as smartphones, tablets and, possibly, laptops. This buyer is typically technically competent and/or routinely makes granular changes to wired/wireless LAN infrastructure components. This is the most common use case for newly constructed office space, although it's often initiated by a campus refresh.

Hands-Off NetOps

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

In this use case, the primary driver is to reduce the operational burden and costs associated with managing network infrastructure. This is an emerging use case, driven by the advances in analytics, AI and ML. It applies predominantly to WLAN, although it has begun to extend to wired networking as well. This use case applies to SMB and large-enterprise networking environments. The primary driver for buying LAN equipment is limited manual work, with the aspiration to achieve a hands-off operational experience. Users want the vendor's management system to configure itself, monitor itself and self-remediate/optimize, with limited human intervention. Monitoring WLAN performance remains a key sought-after capability, due to the challenges associated with controlling the RF environment.

Remote Branch Office

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

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

Wired-Only Refresh/New Build

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

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

WLAN-Only Refresh/New Build

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

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

Vendors Added and Dropped

Dropped

The following vendors were dropped:

- **H3C:** Gartner was unable to validate inclusion criteria for this year's Magic Quadrant.
- **Allied Telesis:** Gartner was unable to validate inclusion criteria for this year's Magic Quadrant.

Inclusion Criteria

Gartner's clients utilize the Magic Quadrant and Critical Capabilities research to identify and analyze the most relevant network vendors' business strategy, overall vision, products and services within the marketplace. Gartner uses, by default, an upper limit of 15 vendors to support the identification of the most relevant vendors in the global enterprise wired and wireless network market. On some specific occasions, the upper limit may be extended when limiting the number of vendors might diminish the research's value to our clients. As such, the inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, vendors must:

- Demonstrate relevance to Gartner clients in the enterprise wired and wireless networking market by offering a robust Ethernet switching and wireless LAN (Wi-Fi) hardware portfolio that addresses at least two of the three network layer (core, access, and/or distribution) requirements as outlined in the Market Definition section.
- Manufacture and deliver enterprise networking products that provide mechanical and/or virtual stackable wired networking for general availability as of 30 April 2022. All components must be publicly available for purchase, exist in inventory, and be available for shipping and included on the vendor's publicly published price list. Products shipping after this date will only have an influence on the Completeness of Vision axis.
- Have at least 400 customers that have greater than 500 employees and have deployed network products in their production environments as of 30 April 2022.
- Have a cloud and/or on-premises based network discovery, identification, configuration, security, management and monitoring platform that includes integrated network automation

tools, the minimum of which is zero-touch provisioning (ZTP). Such tools must also demonstrate visibility into network connected applications and end-user-specific connection data/issues.
- Provide integrated network security tools that offer, at a minimum, device and user segmentation with specific remediation for guest users/devices, and IoT devices.

- Have no more than 60% of revenue generated in a single region (of the five regions noted in the Market Definition section).

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

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*Unified Wired and Wireless LAN*	*Hands-Off NetOps*	*Remote Branch Office*	*Wired-Only Refresh/New Build*	*WL Ref Bui*
Wired LAN	20%	5%	15%	50%	0%
Wireless LAN	20%	20%	20%	0%	45
Network Security	15%	10%	15%	15%	15
Management and Administration	15%	20%	25%	15%	15
Network AIOps Features	15%	35%	15%	10%	15
IoT Device Containment	15%	10%	10%	10%	10

As of 20 December 2022.

Source: Gartner (January 2023)

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

Critical Capabilities Rating

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

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*ALE*	*Arista Networks*	*Cambium Networks*	*Cisco (Catalyst)*	*Cisco (Meraki*
Wired LAN	3.8	3.8	3.2	4.0	3.6
Wireless LAN	3.8	3.7	4.1	3.9	3.8
Network Security	3.5	3.8	3.5	3.9	3.7
Management and Administration	3.8	3.5	3.7	3.6	3.8
Network AIOps Features	3.4	3.6	2.7	3.7	3.5
IoT Device Containment	3.5	3.6	3.6	3.7	3.6
As of 20 December 2022.					

Source: Gartner (January 2023)

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

critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

Use Cases	*ALE*	*Arista Networks*	*Cambium Networks*	*Cisco (Catalyst)*	*Cisco (Meraki)*
Unified Wired and Wireless LAN	3.65	3.68	3.49	3.82	3.67
Hands-Off NetOps	3.60	3.63	3.38	3.76	3.66
Remote Branch Office	3.67	3.66	3.52	3.79	3.69
Wired-Only Refresh/New Build	3.69	3.72	3.31	3.87	3.64
WLAN-Only Refresh/New Build	3.67	3.66	3.69	3.81	3.72
As of 20 December 2022.					

Source: Gartner (January 2023)

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

Critical Capabilities Methodology

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

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

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

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

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

Ratings and summary scores range from 1.0 to 5.0:

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

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

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

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