Critical Capabilities for WAN Edge Infrastructure

Published 20 September 2021 - ID G00738187 - 38 min read

By Analyst(s): Jonathan Forest, Naresh Singh, Andrew Lerner, Evan Zeng

Initiatives: Cloud and Edge Infrastructure

Infrastructure and operations leaders responsible for networking evaluate WAN edge solutions to connect branches and workers to cloud applications and other enterprise locations. Vendors' capabilities vary widely, so use this research to identify which vendors best address your specific use cases.

This Critical Capabilities is related to other research:

Magic Quadrant for WAN Edge Infrastructure

View All Magic Quadrants and Critical Capabilities

Overview

Key Findings

- SD-WAN vendors adding cloud security to offer native SASE solutions is a major trend in this market, with a focus on tighter integration of networking and cloud-delivered security components as well as simpler consumption and operation.
- In addition to interconnecting their own sites, most enterprises are trying to solve two main challenges in this market: how to connect to the cloud, and how to secure the enterprise network when deploying distributed internet access. Consequently, cloud teams and security teams are increasingly part of SD-WAN procurements.
- As a result of the COVID-19 pandemic, there is increased emphasis on remote worker software solutions integrated into the broader SD-WAN offering.
- Vendor feature gaps are closing, but there still are differences in ease of use, application performance, cloud connectivity and security.

Recommendations

Infrastructure and operations (I&O) leaders responsible for cloud infrastructure should:

- Evaluate vendors by including security teams and comparing native and partnered security functionality, as well as on-premises versus cloud deployment to differentiate capabilities, for security-sensitive organizations.
- Evaluate SD-WAN to the cloud capabilities by including cloud teams and validating orchestration with cloud service providers (such as Microsoft Azure and Amazon Web Services [AWS]), carrier-neutral facilities (such as Equinix) and virtual image compatibility with different cloud platforms, for cloud-first organizations.
- Validate functionality by verifying that work from anywhere (WFA) solutions are integrated with SD-WAN orchestration, when remote worker solutions are required.
- Shortlist based on your desired functionality by focusing on ease of use, application performance, cloud connectivity and security functionality, versus perceived leadership in the market or incumbency.

Strategic Planning Assumptions

By 2025, 50% of SD-WAN purchases will be part of a single vendor SASE offering, up from less than 10% in 2021.

By 2025, 40% of enterprises with SD-WAN deployments will use artificial intelligence (AI) functions to automate Day 2 operations, compared with fewer than 5% in 2021.

By 2024, 35% of enterprises will manage their branch and remote worker network access via the same management console, up from less than 1% in early 2021.

What You Need to Know

The WAN edge market is addressing the shift from traditional hub-and-spoke WAN architectures connecting enterprise locations to cloud workloads, internet-based resources and remote workers. [1] It is driven by SD-WAN, including routing, path selection, orchestration and VPN/firewall capabilities. We see vendors differentiating themselves with advanced security, cloud connectivity/networking, application performance optimization and ease of use. Over time, we do expect that AI functionality will increasingly be a differentiator. [2]

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

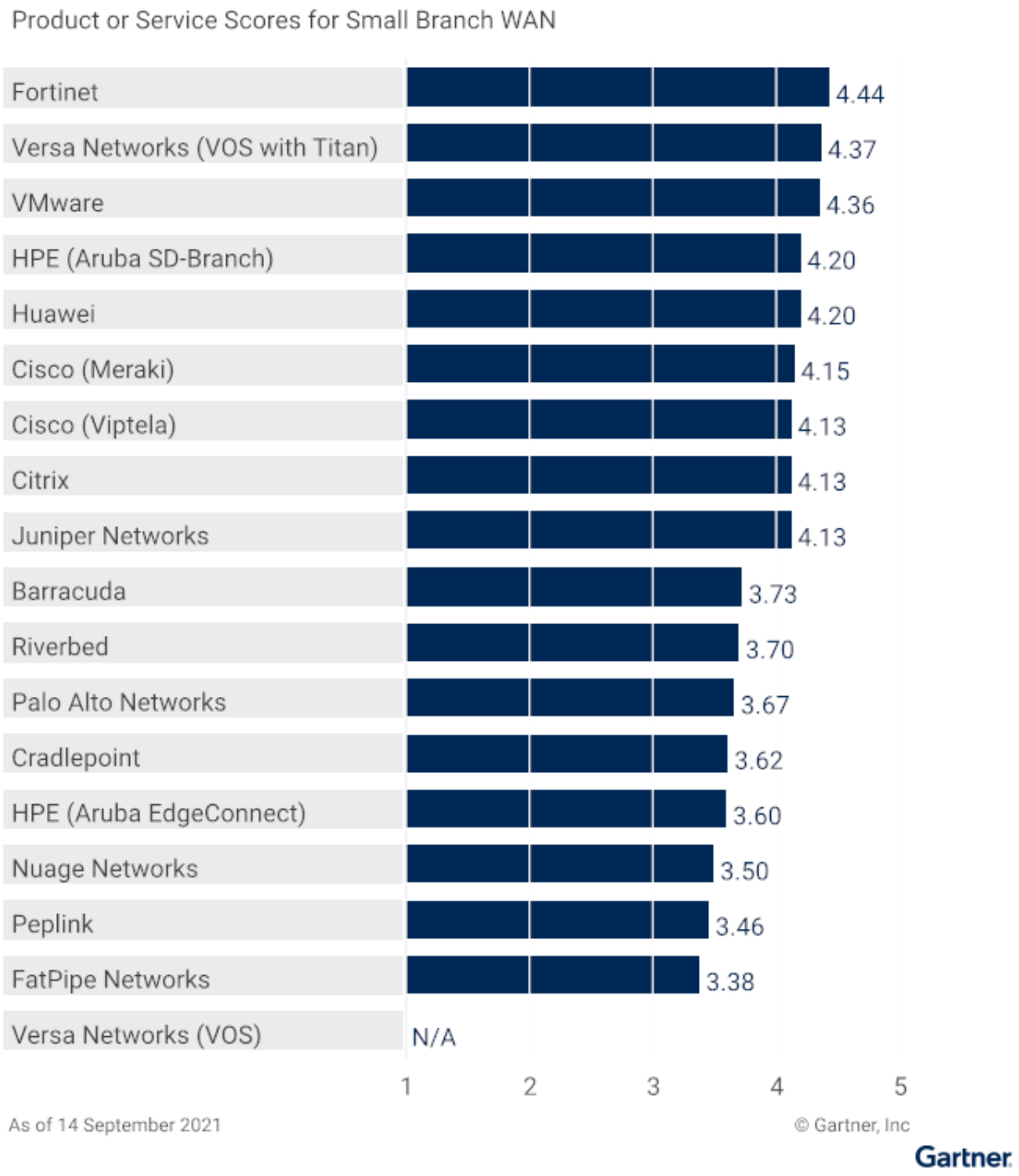
Analysis

In this research, we analyze five popular use cases: [2]

- Small branch WAN that requires simple and secure branch networking solutions with ease of use as a main driver. This use case can be any number of sites with branch locations, typically with fewer than 10 people.
- A large global WAN requirement for larger multinational organizations with over 300 sites that spans at least two continents.
- A security-sensitive WAN typical in some mid- to large-scale organizations focused on securing branch offices as the main priority, where network and security procurements are increasingly converging.
- A cloud-first WAN with varying amounts of sites where customers have workloads mainly in the cloud and, to a lesser extent (if at all), on-premises.
- Remote workers connecting to the enterprise network and cloud resources from remote locations such as their homes, instead of solely connecting from the branch.

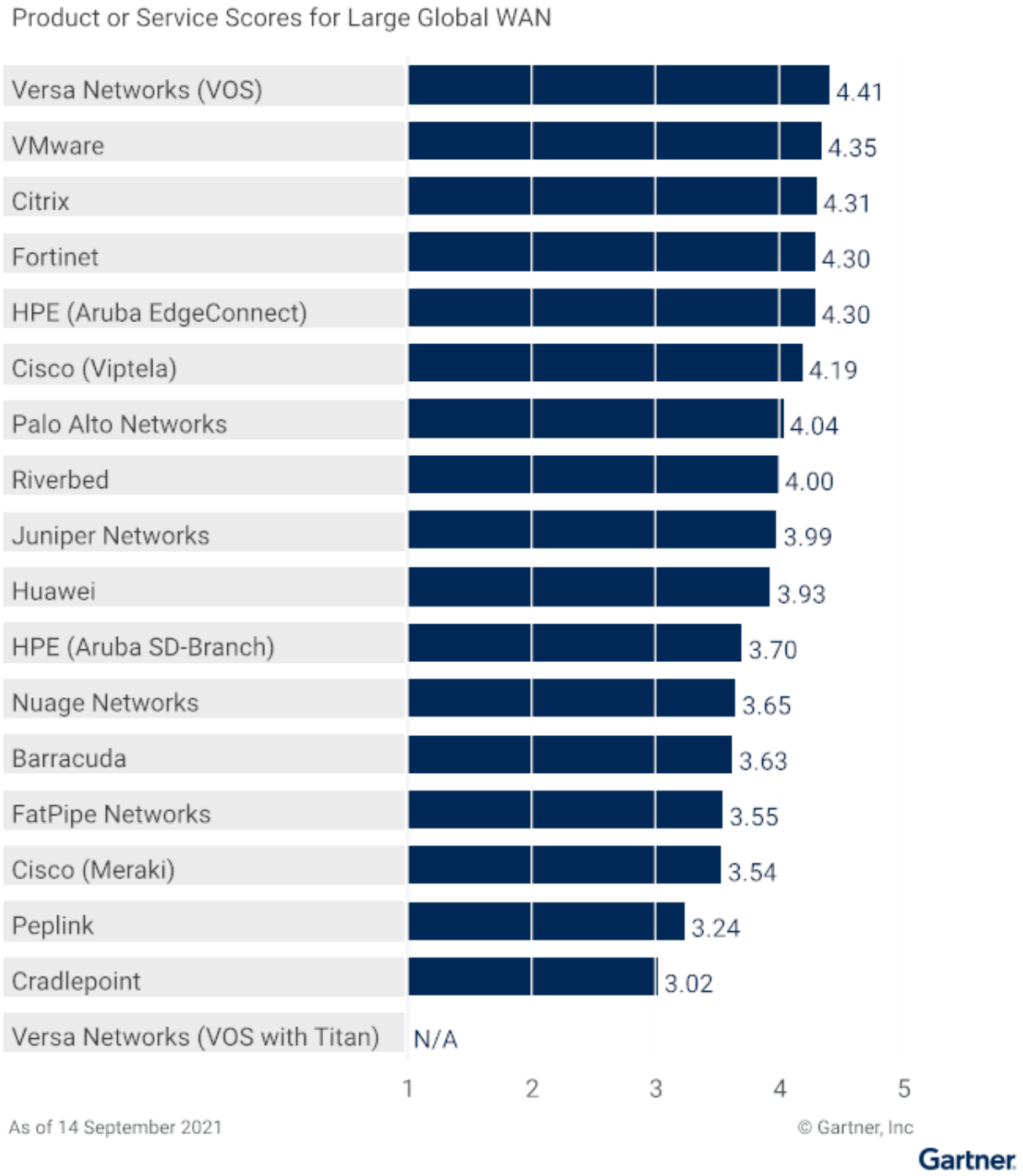
Critical Capabilities Use-Case Graphics

Vendors' Product Scores for Small Branch WAN Use Case



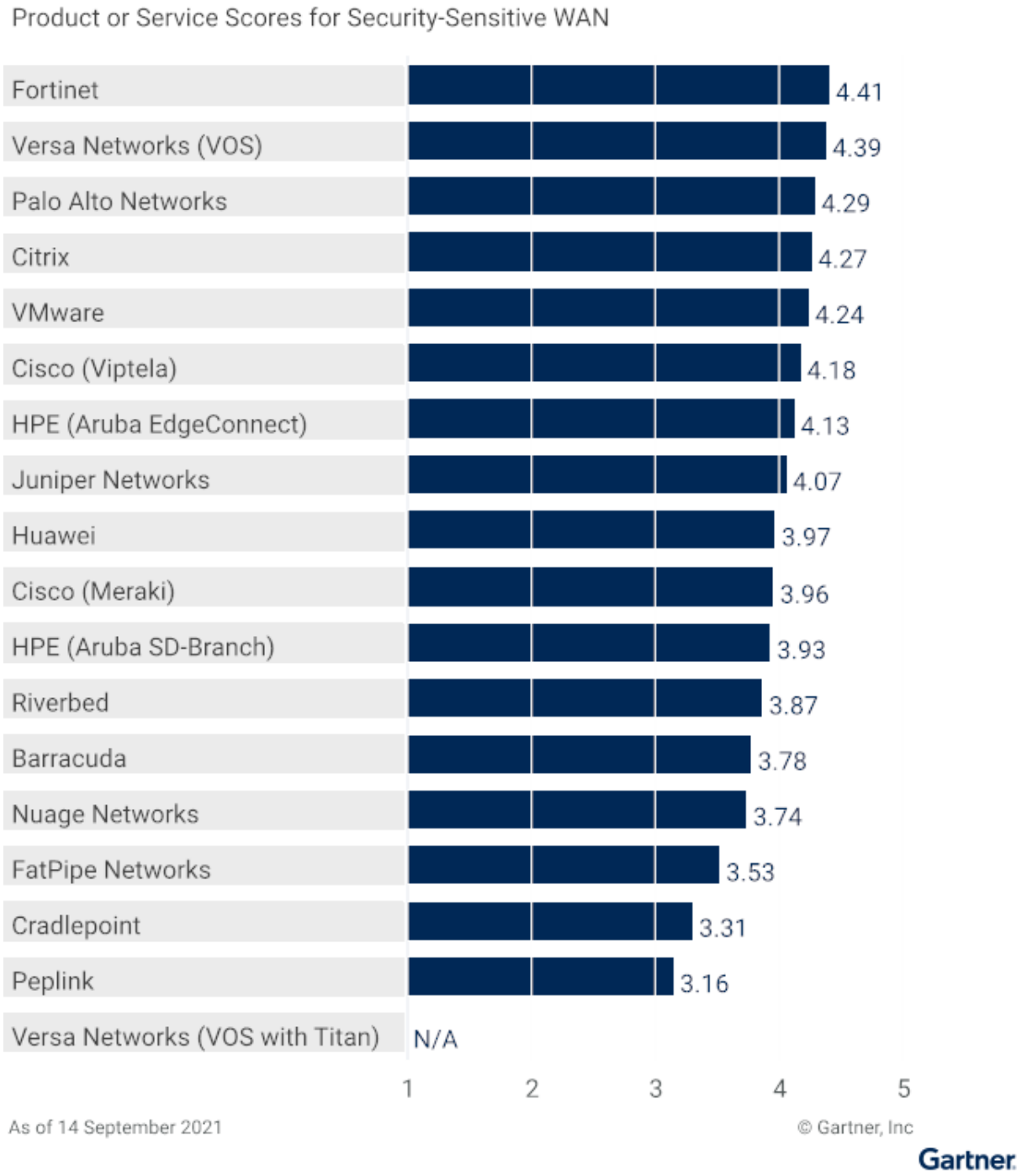
Source: Gartner (September 2021)

Vendors' Product Scores for Large Global WAN Use Case



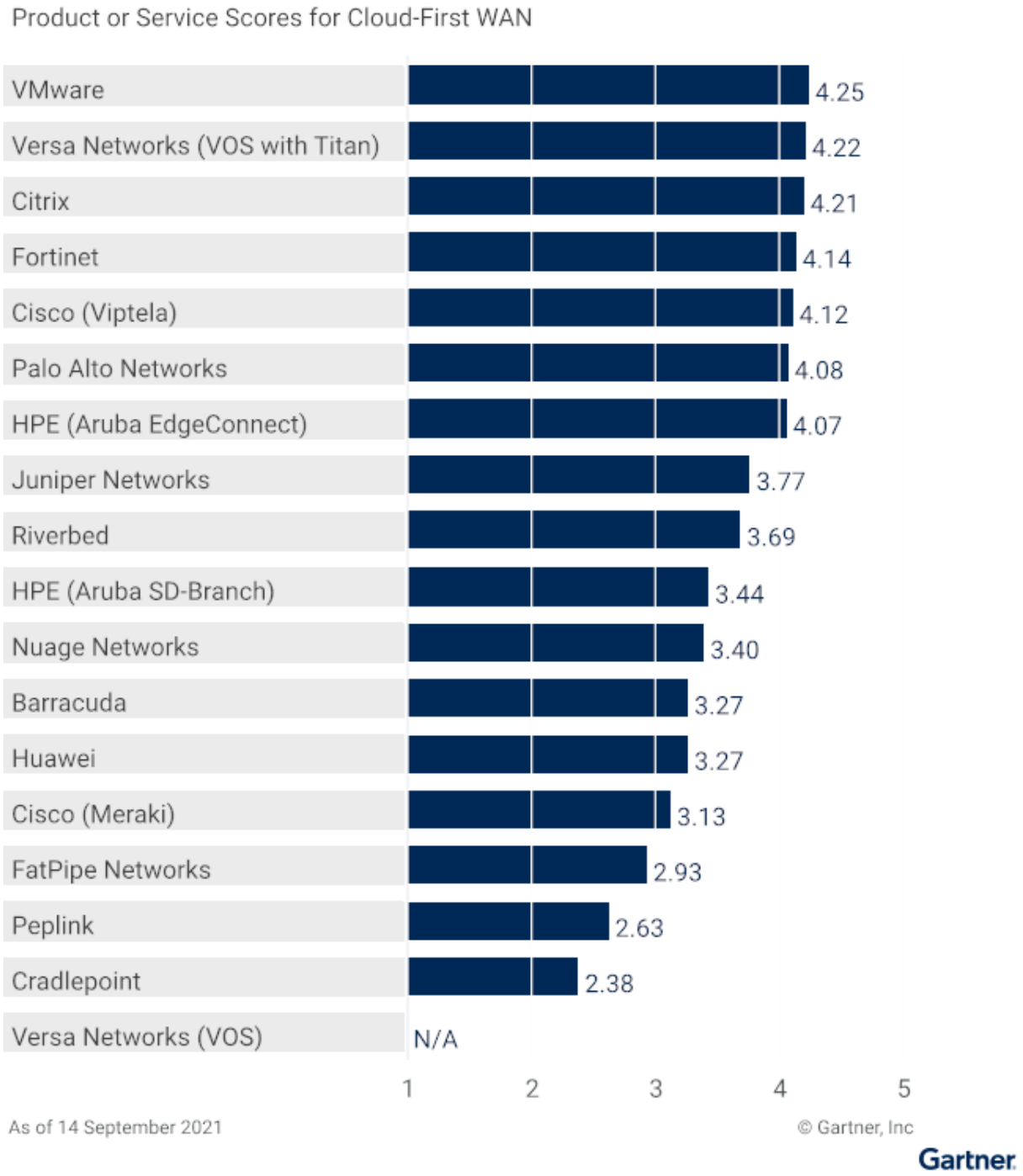
Source: Gartner (September 2021)

Vendors' Product Scores for Security-Sensitive WAN Use Case



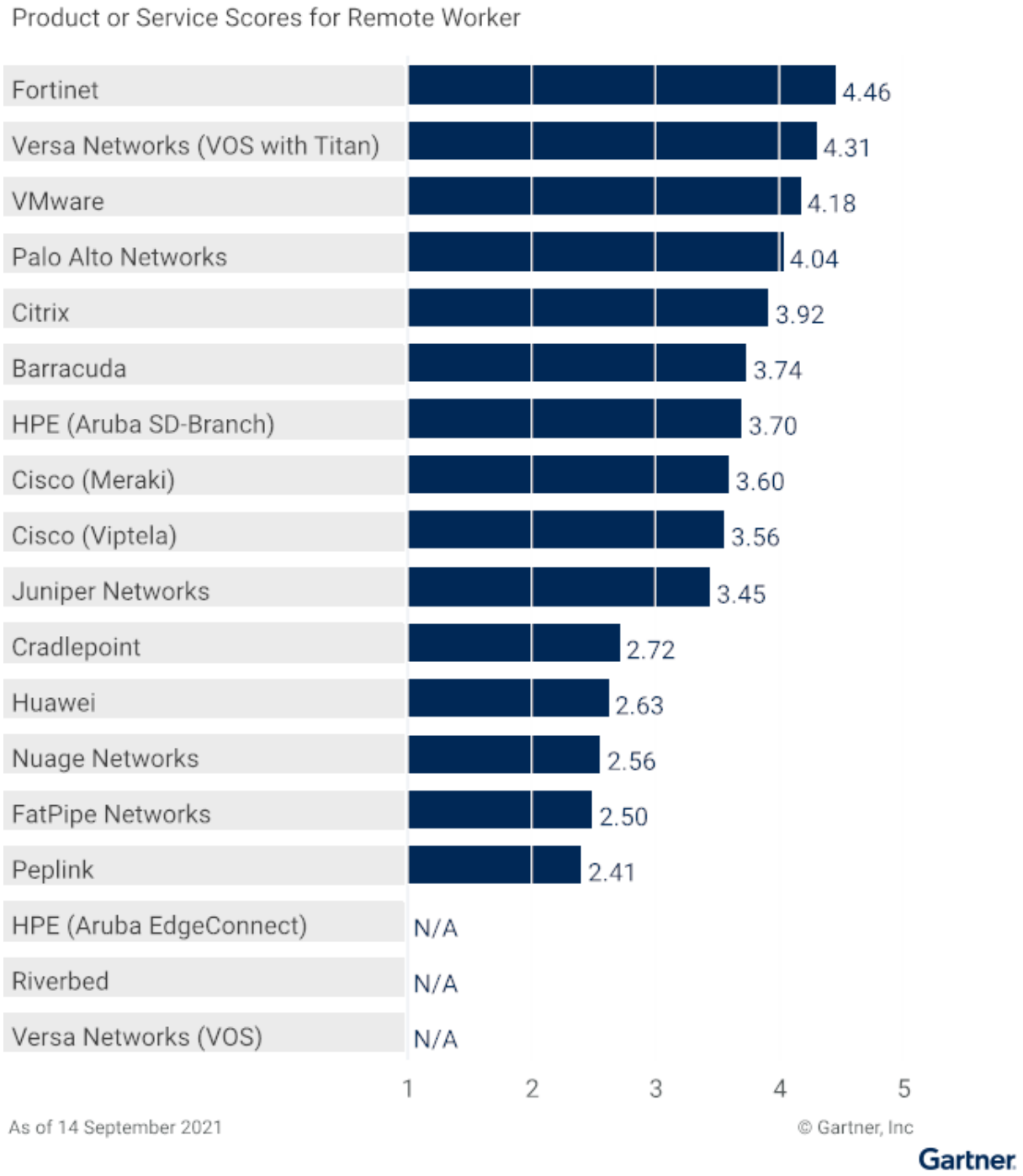
Source: Gartner (September 2021)

Vendors' Product Scores for Cloud-First WAN Use Case



Source: Gartner (September 2021)

Vendors' Product Scores for Remote Worker Use Case



Source: Gartner (September 2021)

Vendors

Barracuda

Barracuda is based in California, U.S., and Gartner estimates that it has over 12,000 WAN edge customers. Its WAN edge flagship product is CloudGen Firewall, and it includes hardware and software appliances, and associated orchestration and management. The vendor also offers CloudGen WAN, a cloud-native service now deployed in Microsoft Azure. Barracuda has been focused on security across its WAN edge solution, but still lacks partnerships to integrate and orchestrate with third-party cloud security vendors.

Barracuda is rated as good across all use cases. In particular, this vendor scored excellent on scalability and security features, fair for operational features and cloud features, and good for the rest of the capabilities.

Cisco (Meraki)

Cisco is based in California, U.S., and Gartner estimates that Meraki accounts for approximately 25,000 of Cisco's estimated 40,000 WAN Edge customers. Its product is branded as Cisco SD-WAN, powered by Meraki. For this research, we assess MX appliances with secure SD-WAN software licenses (managed via the Meraki cloud management console), Cisco Umbrella Security Internet Gateway (SIG) for security and Teleworker gateway (required for the remote worker scenario). Cisco Meraki offers an advanced licensing option for improved analytics and advanced SD-WAN features, but would still benefit from more advanced cloud features and application performance optimization functionality.

Cisco Meraki ranks as good in four use cases and excellent in the small branch WAN use case. In particular, Meraki has excellent scalability, operational features and small platform flexibility capabilities. Meraki's cloud features and application performance optimization capabilities are rated as poor, with the rest rated as good.

Cisco (Viptela)

Cisco is based in California, U.S. and Gartner estimates that Viptela accounts for over 5,000 of Cisco's estimated 40,000 WAN Edge customers. The product is branded as Cisco SD-WAN, powered by Viptela. For this research, we assess ISR 1100 and Catalyst 8000 appliances running IOS XE, with Cisco Umbrella SIG for security. Cisco Viptela has enhanced its connectivity to the cloud options, but would still benefit from tighter integration with Umbrella to simplify SASE implementations.

Cisco Viptela supports all five use cases with excellent scores in each except for remote worker, where it ranks as good. In particular, Viptela has excellent SD-WAN features, operational features, cloud features and security capabilities, enabled by the Umbrella SIG platform. While Cisco has an excellent small platform capability, it lags several competitors in this area.

Citrix

Citrix is based in Florida, U.S., and Gartner estimates that it has more than 1,700 WAN edge customers. Its product is Citrix SD-WAN, which includes physical, virtual appliances and Cloud Direct service managed via the Citrix SD-WAN Orchestrator. It also includes Secure Internet Access (SIA) and Secure Workspace Access (SWA) as part of its broader SASE offering. Citrix has evolved its security portfolio with a stronger focus and positioning on SASE, along with a more cost-effective entry-level appliance and remote worker solution. However, it lacks some automation capabilities, including limited integrations with Ansible or Terraform.

The vendor is rated excellent in all use cases with the exception of remote worker, where it is rated as good. This is due to its excellent ratings with application performance optimization, deployment flexibility, SD-WAN features, security and cloud features capabilities. While Citrix does score as good for operational features, it doesn't score as well as most other products in this research.

Cradlepoint

Cradlepoint is based in Idaho, U.S., and Gartner estimates that it has approximately 9,000 WAN edge customers. Its offering is the Cradlepoint NetCloud service with NetCloud Manager, which can be used with its E, R, W, AER and IBR Series of physical routers and adapters with NetCloud Perimeter and Cloud Virtual Router (CVR). Cradlepoint, which was acquired by Ericsson in November 2020, is very strong in 4G and emerging 5G use cases. However, it does lack broader application performance optimization and cloud features capabilities, such as integration with Azure Virtual WAN (vWAN) and Amazon Web Services (AWS) Transit Gateway to simplify cloud onramp.

The vendor scores as good in the small branch WAN, large global WAN and security-sensitive use cases, and fair in the cloud-first WAN and remote worker use cases. This is driven by excellent scores in small platform flexibility and scalability, good scores in SD-WAN features and security features, and poor scores in cloud features and application performance optimization capabilities.

FatPipe Networks

FatPipe Networks is based in Salt Lake City, Utah, U.S., and Gartner estimates that it has more than 2,000 WAN edge customers. Its SD-WAN product is MPVPN, which consists of physical and virtual appliances configured and managed with the FatPipe Symphony orchestrator, offering an on-premises or cloud-hosted option. Although it has invested in cloud offerings and automation capabilities including AIOps, its product lacks several cloud features, such as integration with Azure vWAN and AWS Transit Gateway to simplify cloud onramp.

The vendor is rated as good in the small branch, large global WAN and security-sensitive WAN use cases, and fair in the cloud-first WAN and remote worker use cases. Its ratings were driven by an excellent score in deployment flexibility, and good scores in application performance optimization and SD-WAN features. The vendor is rated as poor in cloud features and fair in remote worker capabilities.

Fortinet

Fortinet is based in Sunnyvale, California, U.S. Gartner estimates that it has over 34,000 WAN edge customers with over 10,000 SD-WAN customers. Its product is FortiGate Secure SD-WAN, which includes physical and virtual appliances, FortiOS, FortiGuard Security Services, FortiSandbox, FortiCASB and cloud-based services managed with FortiManager orchestrator. Fortinet has a very strong security-focused SD-WAN offering that now has added critical features such as ZTNA and a SASE portfolio. Its FortiSASE offering has recently been launched based on last year's OPAQ Networks acquisition, but it is largely unproven at this point.

Fortinet is rated excellent for all use cases in this research. This is driven by excellent security features, scalability, small platform flexibility, deployment flexibility and SD-WAN features capabilities, although it does lag behind other leaders in that capability. Fortinet also ranks as good in the cloud features capability.

HPE (Aruba EdgeConnect)

Hewlett Packard Enterprise (HPE) is based in San Jose, California, U.S. Gartner estimates that it has more than 2,500 WAN edge customers for its Aruba EdgeConnect SD-WAN platform. This includes physical and virtual appliances along with an optional Aruba Boost WAN Optimization managed through Aruba Orchestrator. Aruba EdgeConnect, from the Silver Peak acquisition, continues to be offered as a separate platform by HPE, although there has been some integration with the rest of the Aruba portfolio such as Aruba ClearPass and Aruba Central. The product delivers a strong application experience for end users. However, it lacks some native security capabilities, especially as a single-vendor SASE solution.

We rate the Aruba EdgeConnect platform in four of the five use cases except for the remote worker, as the only solution the vendor has with this product is for higher-end users, not the typical remote worker. Of these four use cases, Aruba EdgeConnect is rated excellent for all except small branch WAN, where it is rated as good. This is driven by excellent scores in application performance optimization, deployment flexibility and SD-WAN features. The vendor also scores as good in cloud features and operational features capabilities. Although the product is rated as good for small platform flexibility, it ranks on the lower end when compared with other vendors in this research.

HPE (Aruba SD-Branch)

HPE is based in San Jose, California, U.S., and is estimated to have more than 800 WAN edge customers for its Aruba SD-Branch. Aruba SD-Branch is the vendor's platform targeting unified LAN, WLAN and WAN orchestration for customers. The SD-WAN portion includes branch and headend gateways along with Aruba Central orchestration. The vendor has been focused on SD-Branch and AIOps capabilities, but still lacks some native security functionality to deliver a single-vendor SASE offering.

Aruba SD-Branch is rated excellent in the small branch WAN use case and good in all other use cases. This is driven by excellent scores in small platform flexibility and operational features. The vendor scores as fair in cloud features and application performance optimization capabilities.

Huawei

Huawei is based in Shenzhen, China, and Gartner estimates that it has more than 20,000 WAN edge customers. Its product includes Huawei NetEngine AR series routers, iMaster NCE Orchestrator, HiSecEngine USG series gateways and Qiankun cloud security services. The vendor has been focused on 5G/4G, AIOps, SRv6 and a single-vendor SASE offering, but it still lacks cloud features applicable to global customers.

The Huawei WAN edge solution is rated as excellent for the small branch WAN use case, good for the security-sensitive WAN, large global WAN and cloud-first WAN use cases, and fair for the remote worker use case. The vendor scores as excellent in SD-WAN features, security features, small platform flexibility, scalability and deployment flexibility capabilities. The vendor scores as good for application performance optimization and poor for remote worker and cloud features capabilities.

Juniper Networks

Juniper Networks is based in California, U.S., and Gartner estimates that it has over 18,000 WAN edge customers. Its product is branded as Juniper AI-driven SD-WAN. For this research, we assess Juniper's primary SD-WAN offering, which includes Session Smart Routers and associated Conductor, Mist WAN Assurance and the ATP Cloud service (for the security use case). We estimate that Juniper has 500 customers deployed on this solution, which is based heavily on technology acquired via 128 Technology in December 2020. The vendor also has the Juniper SRX platform that we didn't evaluate, since the Session Smart Router is considered the flagship product going forward. Juniper has invested in integrating 128 Technology with its Mist WAN Assurance platform. Still, the vendor has limitations with its application performance optimization capabilities.

Juniper Network scores excellent for the small branch WAN and security-sensitive WAN use cases. It scores as good in the remaining use cases. In particular, Juniper scores excellent in SD-WAN features, security features, operational features and small platform flexibility. It also scores as good in cloud features and remote worker capabilities.

Nuage Networks

Nuage Networks is based in California, U.S., and is a division of publicly traded Nokia, based in Espoo, Finland. Gartner estimates that Nuage Networks has over 2,500 enterprise WAN edge customers. Its offering is Nuage's Virtualized Network Services (VNS), which includes Network Services Gateways (NSG) managed by the Nuage Networks Virtualized Services Platform (VSP) controller. The vendor has been enhancing its software-defined cloud interconnect (SDCI) capabilities and expanding its branch platform form factors. But, they do lack a native SASE solution and rely on partners.

Nuage Networks scores as good in the small branch WAN, large global WAN, security-sensitive WAN and cloud-first WAN use cases. The vendor also scores fair for the remote worker use case. This is driven by its excellent scalability scores and good scores in all remaining categories, except in remote worker and application performance optimization capabilities where it is rated as fair.

Palo Alto Networks

Palo Alto Networks is based in California, U.S., and Gartner estimates that it has more than 2,000 WAN edge customers. We assessed Prisma SD-WAN with Instant-On Network (ION) appliances and corresponding orchestration, which is integrated with Prisma Access to deliver a SASE solution. The vendor also offers the PAN-OS SD-WAN solution, but it is outside the scope of this evaluation since it is not the main solution and is only sold in limited scenarios. The vendor has been focused on a single-vendor-integrated SASE solution and AIOps for SD-WAN, but still lacks fundamental WAN optimization and voice optimization features such as FEC and packet duplication.

Palo Alto Networks is rated as good for the small branch WAN use case, and as excellent for the rest of use cases. The vendor scores excellent for SD-WAN features, security features, scalability and cloud features capabilities. It scores as fair for the application performance optimization capability.

Peplink

Peplink is headquartered in Hong Kong, China, and Gartner estimates that it has approximately 14,000 WAN edge customers. The vendor has two product families in this market, Balance for enterprise branch SD-WAN and MAX for industry and mobility SD-WAN. Both have branch appliances with SpeedFusion technology and InControl 2 orchestration. Peplink has been focused on 5G/4G and wireless-focused SD-WAN offerings, but has limited cloud features that are desired by many enterprises.

Peplink's WAN edge solution is rated as good for the small branch WAN, large global WAN and security-first use cases, and as fair for the cloud-first WAN and remote worker use cases. In particular, the vendor scores excellent in scalability, fair in operational features and application performance optimization features, poor in cloud features and remote worker, and good in the rest of the capabilities.

Riverbed

Riverbed did not respond to requests for supplemental information or to review the draft contents of this document. Therefore, Gartner's analysis is based on other credible sources, including client inquiries, past information shared by the vendor, reviews of public statements, its website and other publicly available data sources.

Riverbed is headquartered in California, U.S., and Gartner estimates that it has approximately 30,000 WAN edge customers, with over 3,000 SD-WAN customers. For this analysis, we evaluate the SteelConnect EX, which is based on software from Versa Networks. The solution includes the EX edge appliance and the SteelConnect EX orchestrator. Riverbed is enhancing its AI/ML and analytics capabilities, but the SD-WAN solution it leads with relies on the Versa OEM partnership.

The vendor supports four out of five use cases. For remote workers, we don't assess Riverbed as addressing this use case because, in our assessment, it doesn't support ZTNA or remote VPN consistent with the use case description. However, Riverbed can supplement other remote worker offerings with its client-based acceleration technologies. Riverbed is rated good for all the use cases that it supports. The vendor's scores are driven by its excellent application performance optimization and strong SD-WAN feature ratings. Riverbed scored as good in cloud features and scalability capabilities, but lower when compared with some other vendors in this research.

Versa Networks (VOS)

Versa Networks is based in California, U.S., and Gartner estimates that it has more than 12,000 WAN edge customers. Versa Networks has two offerings and, for this analysis, we evaluate the full-featured Versa Operating System (VOS), which can be delivered on the Versa branch Cloud Services Gateways (CSG) or third-party hardware, along with the Versa Director and Versa Analytics managed by the Concerto orchestration platform. We estimate that Versa has over 10,000 customers using this solution. Versa has developed its native SASE solution and it has overall comprehensive capabilities, yet remains complicated to operate for some DIY users.

We evaluate Versa's VOS solution for the large global WAN and security-sensitive WAN use cases. In both use cases, Versa is rated as excellent primarily due to its excellent scores in SD-WAN features, security features, scalability and deployment flexibility capabilities.

Versa Networks (VOS with Titan)

Versa Networks is based in California, U.S., and Gartner estimates that it has more than 12,000 WAN edge customers. Versa Networks has two offerings and, for this analysis, we evaluate VOS with Titan, which tends to be for smaller organizations, so the functionality is more limited compared with the full-featured VOS solution (although it is the same platform). VOS with Titan is a simpler, cloud-based solution using the same CSGs as with VOS, and Gartner estimates that Versa Networks has over 2,000 customers with this solution. The vendor has developed its native SASE solution and remote worker solution, and VOS with Titan tends to be for lean IT customers so the functionality and deployment flexibility is more limited when compared to the full-featured VOS solution.

We evaluate Versa's VOS with Titan solution for the small branch WAN, cloud-first WAN and remote worker use cases. In all three use cases, Versa VOS with Titan is rated excellent primarily due to its excellent scores in SD-WAN features, cloud features, operational features, remote worker and small platform flexibility capabilities.

VMware

VMware is based in California, U.S., and Gartner estimates that it has over 14,000 SD-WAN customers. Its product is branded as VMware SD-WAN, which is part of VMware SASE. The VMware offering includes SD-WAN gateways, SD-WAN Edge appliances, Orchestrator, Edge Network Intelligence along with VMware Cloud Web Security and VMware Secure Access. VMware has been focused on building out its SASE solution, but it still has limited traditional WAN optimization capabilities.

VMware scores as excellent in all five use cases associated with this research. In particular, they score excellent in cloud features, SD-WAN features, remote worker, scalability and deployment flexibility capabilities. It does rank as good with the application performance optimization capability.

Context

WAN edge products deliver the required features for a modern WAN to connect branches and users to each other and to workloads on- or off-premises. The WAN edge infrastructure market is a combination of existing capabilities, such as routing, WAN optimization and edge security, and is now driven by mainstream SD-WAN products, which includes all those functions plus path selection and orchestration.

WAN edge solutions can be combined with cloud-resident functionality for overarching policy and operational control, as well as with cloud gateways and cloud security in a SASE architecture (see 2021 Strategic Roadmap for SASE Convergence). The result is a simpler, more streamlined remote office footprint (especially for lean IT organizations) that enables organizations to better deal with more dynamic and distributed traffic flows resulting from greater use of cloud and internet resources.

Product/Service Class Definition

WAN edge solutions cover a broad spectrum of deployment and procurement options and, given the market adoption and trends, we focus on SD-WAN. The branch office footprint can be delivered as a fully integrated appliance from a single vendor, an open VNF-ready hardware and software solution with software from multiple vendors, or as virtualized software on a dedicated third-party hardware device. Since the start of the pandemic, we have also seen the need to support remote workers in mainly a software-driven solution for the majority of situations.

In some cases, solutions are deployed as hardware or software in all enterprise locations, with possible deployments in cloud service provider locations (often available in the cloud marketplace). Meanwhile, other solutions also offer cloud resident gateways, which are deployed in selective locations to enhance the delivery of internet/cloud-destined traffic. A variety of capabilities run between these cloud PoPs — from basic VPN tunneling and route determination to more complete WAN optimization, security and cloud optimization features. Business models also cover a range of options, including traditional capital expenditure (capex)-heavy, operating expenditure (opex)-capex hybrid models and full opex-based subscription service offerings. Both DIY and managed options can be delivered in each model.

Common attributes with SD-WAN solutions are:

Core Functionality

- Licensed software
  - Routing (such as BGP)
  - Path Selection (such as Layer 7 traffic steering)
  - VPN
  - Basic firewall

- Form factors
  - Software and/or physical
  - Remote worker, edge, headend and cloud
- Orchestrator (on-premises or in cloud)
  - Configuration (zero touch configuration)
  - Management
  - Visibility
  - Reporting
  - API support

Optional Functionality

- Advanced security (such as NGFW, SWG, CASB and DLP)
- Service chaining capabilities
- Cloud gateways for service insertion and simplified cloud connectivity
- Application performance capabilities (such as WAN optimization and SaaS optimization)

Critical Capabilities Definition

SD-WAN Features

SD-WAN features include different application-aware and routing (protocols and topology) capabilities, and the ability to support various overlay and underlay functionality.

SD-WAN represents a simplified way of deploying and managing the WAN edge. SD-WAN provides a replacement for WAN routers with an ability to terminate multiple diverse carrier transport options. This includes autorecognition of applications, dynamic path selection functionality (algorithm for failover and time for failover) across diverse WAN connections (e.g., internet or MPLS) with application performance awareness and broad routing/architecture support.

Security Features

Security includes a broad feature set related to ensuring secure networking across the WAN. It can be delivered directly from the network edge equipment or via a cloud service. This includes both native vendor-provided capabilities and integrations with third-party security providers.

Security has been a stand-alone functionality as part of the overarching WAN edge infrastructure. Specifically, this consists of basic functionality such as ACLs, VPN, segmentation and firewalls. Examples of advanced functionality are IPS, application layer firewall, antivirus/malware, URL/content filtering, DLP, SWG, CASB, ZTNA and sandboxing. These advanced security capabilities are increasingly being integrated into broader SD-WAN solutions either at the network edge or in the cloud. In this category, we assess the vendor's feature breadth as far as having certain native capabilities and ability to deliver turnkey orchestration with specific third parties.

App Performance Optimization

Application performance optimization is driven by broad WAN optimization features, but also includes SaaS optimization, quality of service (QoS) techniques and optimization for real-time traffic to improve the quality of experience (QOE) across the WAN.

While a mature stand-alone technology, WAN optimization includes TCP protocol optimizations, HTTP and SSL optimizations, in-line compression and deduplication, and caching and latency mitigation. SaaS optimization involves methods to optimize various network metrics (such as packet loss, latency and jitter) usually across the internet for applications hosted in the cloud. QoS includes techniques from prioritization to end-to-end enforcement of class of service (CoS). Real-time voice optimization includes techniques such as FEC, packet duplication and protocol optimization techniques.

Operational Features

WAN edge solutions should enable significantly simplified operational environments compared to traditional branch office routing solutions. GUIs are used for business policy configuration management from a centralized management system and offer application analytics/visibility.

Networkwide configuration must be supported for all required configurations via a central controller that can automatically push/pull out all individual device configuration data. The central controller acts as a repository for all configuration data, as well as all device, application visibility and network reporting. The solution must also support zero-touch configuration for new branches, which entails on-site branch personnel having to make physical (i.e., cabling) changes only and administrators not having to make configuration changes to bring new branches online.

We also evaluate analytics, workflow, automation and ease of use in network setup as well as ongoing management. Solutions should also have API integrations with external systems, orchestrate third-party solutions and have the ability to support automation tools such as Ansible. Finally, we analyze the vendor's support capabilities.

Deployment Flexibility

New WAN edge solutions need to deliver a variety of form factors (both software and physical), WAN interfaces and deployment options. Hardware, software, cloud options and service chaining are important for many architectures.

The fundamental purpose is to enable connectivity between distributed locations with varying form factors, including headquarters, branches, remote workers, corporate data centers, colocation/hosting facilities and cloud providers. This means that WAN edge infrastructure must be able to support a diverse set of deployment options, including hardware appliances, software or a cloud-based service. Virtual form factors should be available on several hypervisors, support remote workers and enable connectivity to hybrid cloud services. Form factors will have different scaling requirements from low-throughput scenarios to very high throughput, as well as small networks to very large networks. It must be possible to create redundant solutions for high availability in an integrated turnkey manner. Appliances should offer multiple choices for WAN connectivity, such as Ethernet, broadband, and 4G/LTE and 5G.

Small Platform Flexibility

Solutions have the ability to scale downward to meet a specific use case that meets the necessary form factor and features capabilities. Also, the product needs to be able to offer solutions in a highly automated and easy-to-use way that can also scale.

Scalability

Solutions demonstrate the ability to deploy and manage thousands of branch locations with SD-WAN solutions. This also includes the level of network complexity, speed of deployment and manageability. We evaluate both the theoretical scale and real-world customer environments.

Cloud Features

Solutions demonstrate the ability to offer broad, automated, high-performing and flexible architectures to access cloud workloads (SaaS and IaaS). This can be done with native solutions or through partnerships with tight integration and orchestration.

This includes demonstrated capabilities to automate and orchestrate connectivity to cloud providers such as Azure and AWS. It also includes the ability to deploy and support SD-WAN virtual images in cloud providers. It also may include native cloud gateways that offer enhanced steering, service insertion, improved application performance and/or direct connectivity to various cloud service providers. Lastly, it includes partnerships with vendors where technical integrations have occurred that enable simplified cloud connectivity (e.g., software-defined cloud interconnect vendors and carrier-neutral vendors), such as turnkey support for AWS Transit Gateway.

Remote Worker

This refers to the capability to support remote workers in either software-only or lightweight hardware form factors. We look at security capabilities such as ZTNA and other SASE capabilities. We also look at how this is managed and orchestrated as part of a broader SD-WAN offering..

Use Cases

Small Branch WAN

This use case requires simple and secure branch networking solutions with ease of use as a main driver. Typical branch offices have less than 10 people.

This use case is representative of small site needs that are common in distributed enterprise (convenience stores, gas stations, bank branches, fast food restaurants, etc.) and midmarket WANs. There is a strong expense focus — that is, minimum capital and WAN expenditures — with a heavy reliance on the internet where possible, often using xDSL, Ethernet, cable, LTE/5G or VSAT for either primary or secondary connections as part of an active/active configuration. This use case often requires advanced handling of LTE connections to ensure service continuity, as well as support for integrated Wi-Fi in a single orchestration platform. Increasingly, we see the demand for integrated orchestration of LAN, WLAN, WAN and security to simplify management.

These enterprises rely on a variety of business applications, with an increasing reliance on SaaS applications. It can be any number of branch locations ranging from a few to thousands. They need visibility and, at times, voice optimization (e.g., FEC), but not the full suite of application performance, as well as some level of security that is trending to more cloud delivered. Additionally, ease of use and automation are major drivers due to generally smaller IT staff. Managed network services are typically more prevalent in this use case over DIY.

Large Global WAN

Requirements include the ability to scale to hundreds or thousands of sites, typically across multiple geographic regions.

Many global enterprises with large WANs span more than 300 sites across several countries in several regions. Additionally, with geographically dispersed sites, the need for some level of WAN optimization or SaaS optimization to improve performance is desired. Many solutions will require some type of overlay or intelligent routing to avoid congestion, latency and packet loss in order to provide a higher-quality experience than what the internet can offer natively.

These enterprises need flexible and robust security as well as ways to optimize access to various types of XaaS. The solution needs to be simple, yet robust enough to overcome the effects of latency and packet loss due to the unpredictability of the internet. Architecturally, most sites will have an MPLS circuit and some type of internet access circuit, and some less critical sites may only have redundant active/active internet circuits. Much of the traffic is still destined for workloads hosted in the on-premises data center, with increasing needs to access workloads hosted in the cloud. Network teams are generally more technical and hands-on, and are looking for specific features/functionality and complex architectures.

Security-Sensitive WAN

The main focus of the enterprise is to provide an advanced security solution combined with the networking solution, often preferring to work with a single vendor.

Enterprises in this use case are looking for some type of network firewall along with SD-WAN. This can be delivered as a third-party cloud security service integrated with SD-WAN, via an SD-WAN vendor with native cloud security, or via an SD-WAN appliance with integrated native security or the ability to host a third-party security solution on the branch device. Examples of advanced security required in this use case include IPS, A/V, SWG, CASB, sandboxing, ZTNA and DLP. Preferably, the solution incorporates SD-WAN and security in the same solution or service chained without the need for a separate physical appliance.

Example verticals of this use case are financial services, some retail, some healthcare, some regulated industries, some government and broadly across midmarket enterprises. Security teams are active participants with network teams and sometimes are the driving force in the procurement of solutions in this use case to ensure that the security parameters are met regardless of the technology/architecture used. Different implementations may be desired by different types of customers, depending on if they want security at the edge versus in the cloud or a combined networking/security solution from the same vendor or service chained between two or more vendors. There are several architectural approaches in this use case including SASE, which is increasingly an option, especially for remote workers.

Cloud-First WAN

The main focus of the enterprise is to provide support for easy, automated and flexible cloud access since there is a preferred use of cloud services to deliver applications.

What drives the use case is no or limited workloads in on-premises data centers and more reliance on cloud workloads. This can be SaaS or IaaS in a centralized or distributed way with few or many cloud providers involved. WAN transport is typically internet only, but can be enhanced internet or private connectivity as well. Clients that often describe themselves as having a cloud-first and/or cloud-only application strategy generally have plans to close corporate data centers and eliminate corporate private WANs, but not cloud onramp WANs. Flexibility in network architectures and network setup is key to this use case, as is delivering application performance to the workloads. Consequently, cloud onramp (a connectivity solution that enterprises use to access cloud service providers) automation and orchestration capabilities and SaaS optimization are very important for this use case. This solution may leverage cloud provider security rather than security at the edge, although it isn't a requirement. The solution may be delivered by a single provider/vendor or via multiple providers/vendors through partnerships.

Remote Worker

In this use case, we focus on individual workers connecting to the enterprise network from remote locations such as their homes, instead of connecting from the branch.

Enterprises typically choose a software-driven product (preferably ZTNA or, as an alternative, VPN-oriented) for most remote workers or a lightweight hardware solution for power users. Both are meant for single-user environments. Security with ZTNA (which includes VPN) is a main focus with other cloud security functionality (SWG, firewall, etc.) based on worker identity and split tunneling in order to securely connect to cloud workloads. Lightweight networking to direct traffic to multiple locations, path conditioning and path selection functionality is also desired in some cases, but not required in most cases. Integrated management, visibility and orchestration with branch network solutions is key.

Vendors Added and Dropped

Added

No vendors were added to this Critical Capabilities research.

Dropped

- Teldat was dropped because it failed to meet the inclusion criteria, based on our assessment and data provided by the vendor.
- Silver Peak was dropped because it was acquired by HPE.

Inclusion Criteria

To qualify for inclusion, vendors need to show relevance to Gartner clients by:

- Providing hardware and/or software that addresses the enterprise WAN edge requirements outlined in the Market Definition/Description section of Magic Quadrant for WAN Edge Infrastructure. Alternatively, they may address this need by using in-house-developed hardware/software to deliver as a managed service.
- Producing and releasing enterprise WAN edge networking products for general availability as of 11 June 2021. All components must be publicly available, shipping and included on the vendors' published price list as of this date. Products shipping after this date, and any related publicly available marketing information, may only have an influence on the Completeness of Vision axis.
- Providing commercial support and maintenance for their enterprise WAN edge products (24/7) to support deployments on multiple continents. This includes hardware/software support, access to software upgrades, security patches, and troubleshooting and technical assistance.

Product Capabilities

Vendors must have generally available products that support all of the following capabilities:

- Ability to operate as the branch office router (including BGP, OSPF, support hub and spoke, mesh and partial mesh topologies with automation for a minimum of a 250-site network) with traffic shaping and/or QoS
- Centralized management for devices (with GUI), including reporting and configuration changes, and software upgrades
- Zero-touch configuration
- VPN (Advanced Encryption Standard [AES] 256-bit encryption) with basic firewall
- Ability to deliver network firewalls either natively or through a partner
- Native cloud security functionality or the ability to redirect and orchestrate with at least two cloud security vendors

- Dynamic traffic steering based on business or application policy (not limited to only DiffServ Code Point [DSCP]/ports, IPs/circuits or 5tuple) that responds to network conditions (e.g., changes in packet loss, latency, jitter, etc.) in an active/active configuration
- At least 200 well-known application profiles included (auto discovered)
- Visibility of application performance data of traffic delivered across the WAN
- Software (ability to operate as a VNF at the branch or in the network, and deployable in at least two cloud providers, such as AWS and Azure)
- Remote worker solution

Business/Financial Performance

Vendors must show relevance to Gartner's enterprise clients by meeting the following with their WAN edge infrastructure solution that also meet the product capabilities inclusion criteria listed above:

- Demonstrate baseline scalability and customer adoption by servicing at least 10 customers with active support contracts that have at least 100 sites each.
- Show relevance to Gartner's enterprise clients on a global basis with at least one of the two following criteria with product or products that also fulfill the product inclusion criteria:
    - At least 100 WAN edge infrastructure customers with 10 or more production sites each, headquartered in two or more geographic regions (North America, South America, EMEA or the Asia/Pacific region) under active support contracts. This means 100 customers with headquarters in one region and another 100 customers with headquarters in a different region, for a total of at least 200 customers between the two regions.
    - At least 50 WAN edge infrastructure customers with 10 or more production sites each, headquartered in three or more geographic regions (North America, South America, EMEA or the Asia/Pacific region) under active support contracts. This means 50 customers each with headquarters in three different regions, for a total of at least 150 customers between the three regions.

- Meet at least two of the three following criteria with WAN edge infrastructure products that also fulfill the product inclusion criteria:
  - Top 10 SD-WAN market share vendor published by Gartner in Table 16-2 (SD-WAN Equipment, Vendor Revenue, Worldwide, 2019-2020 [Millions of U.S. Dollars]) from the Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q20 and 2020
  - At least 40,000 WAN edge sites deployed and under active support contracts
  - At least 1,000 WAN edge customers under active support contracts or at least 500 WAN edge customers under active support contracts with 250 or more sites deployed each

Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

Critical Capabilities	*Small Branch WAN*	*Large Global WAN*	*Security-Sensitive WAN*	*Cloud-First WAN*	*Remote Worker*
SD-WAN Features	10%	25%	15%	20%	5%
Security Features	10%	10%	45%	10%	5%
App Performance Optimization	0%	15%	5%	5%	0%
Operational Features	10%	10%	15%	10%	5%
Deployment Flexibility	5%	10%	0%	5%	0%
Small Platform Flexibility	50%	0%	5%	5%	5%
Scalability	10%	20%	10%	5%	5%
Cloud Features	5%	10%	5%	40%	5%
Remote Worker	0%	0%	0%	0%	70%
As of 14 September 2021					

Source: Gartner (September 2021)

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

Critical Capabilities Rating

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

Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

Critical Capabilities	Barracuda	Cisco (Meraki)	Cisco (Viptela)	Citrix	Cradlepoint	FatPipe Networks	Fortinet	HPE (Aruba SD-Branch)	Huawei	Juniper Networks	Nuage Networks	Palo Alto Networks	Peplink	Riverbed	HPE (Aruba EdgeConnect)	Versa Networks (VOS with Titan)	Versa Networks (VOS)	VMware
SD-WAN Features	3.8	3.4	4.1	4.5	3.6	3.9	4.1	3.7	4.2	4.6	3.6	4.1	3.2	4.5	4.5	4.5	4.7	4.6
Security Features	4.2	4.4	4.2	4.4	3.5	3.8	4.6	4.0	4.0	4.1	3.9	4.7	3.2	3.8	4.1	4.5	4.5	4.1
App Performance Optimization	3.1	1.9	3.9	4.2	1.5	3.8	3.9	2.9	3.3	2.9	2.9	2.4	2.9	4.2	4.5	3.8	3.8	3.5
Operational Features	2.6	3.7	4.3	3.7	2.8	2.9	4.1	4.1	3.8	4.2	3.7	4.0	2.5	3.8	3.9	4.2	3.9	4.1
Deployment Flexibility	3.6	3.9	4.7	4.5	2.6	4.5	4.5	3.5	4.4	4.6	3.9	4.0	3.6	4.3	4.1	4.4	4.6	4.6
Small Platform Flexibility	3.8	4.4	4.0	4.0	4.0	3.3	4.5	4.5	4.4	4.1	3.2	3.0	3.7	3.5	3.0	4.4	4.0	4.3
Scalability	4.5	4.9	4.3	4.4	4.5	3.5	4.9	4.5	4.8	4.0	4.3	4.8	4.5	3.7	4.5	4.3	4.8	4.9
Cloud Features	2.7	2.2	4.0	4.1	1.0	1.8	3.9	2.8	2.0	3.1	3.0	4.2	1.7	3.1	3.9	4.0	4.0	4.1
Remote Worker	3.8	3.5	3.3	3.8	2.5	2.2	4.5	3.6	2.1	3.2	2.1	4.0	2.1	2.1	1.3	4.3	4.6	4.1

As of 14 September 2021

Source: Gartner (September 2021)

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

(Enlarged table in Appendix)

Use Cases	Barracuda	Cisco (Meraki)	Cisco (Viptela)	Citrix	Cradlepoint	FatPipe Networks	Fortinet	HPE (Aruba SD-Branch)	Huawei	Juniper Networks	Nuage Networks	Palo Alto Networks	Peplink	Riverbed	HPE (Aruba EdgeConnect)	Versa Networks (VOS with Titan)	Versa Networks (VOS)	VMware
Small Branch WAN	3.73	4.15	4.13	4.13	3.62	3.38	4.44	4.20	4.20	4.13	3.50	3.67	3.46	3.70	3.60	4.37	-1.00	4.36
Large Global WAN	3.63	3.54	4.19	4.31	3.02	3.55	4.30	3.70	3.93	3.99	3.65	4.04	3.24	4.00	4.30	-1.00	4.41	4.35
Security-Sensitive WAN	3.78	3.96	4.18	4.27	3.31	3.53	4.41	3.93	3.97	4.07	3.74	4.29	3.16	3.87	4.13	-1.00	4.39	4.24
Cloud-First WAN	3.27	3.13	4.12	4.21	2.38	2.93	4.14	3.44	3.27	3.77	3.40	4.08	2.63	3.69	4.07	4.22	-1.00	4.25
Remote Worker	3.74	3.60	3.56	3.92	2.72	2.50	4.46	3.70	2.63	3.45	2.56	4.04	2.41	-1.00	-1.00	4.31	-1.00	4.18
As of 14 September 2021																		

Source: Gartner (September 2021)

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

Evidence

[1] Gartner analysts conducted more than 3,500 Gartner client inquiries on the topic of WAN between 11 June 2020 and 11 June 2021.

[2] Gartner analysts conducted more than 2,000 Gartner client inquiries on the topic of SD-WAN between 11 June 2020 and 11 June 2021.

[3] All vendors in this research except Riverbed responded to an extensive questionnaire regarding their current/future data center networking solutions.

[4] Analysts reviewed Gartner Peer Insights data for this market.

[5] Gartner analysts reviewed publicly available information.

Critical Capabilities Methodology

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

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

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

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

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

Ratings and summary scores range from 1.0 to 5.0:

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

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

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

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

Document Revision History

Critical Capabilities for WAN Edge Infrastructure - 30 September 2020

Critical Capabilities for WAN Edge Infrastructure - 26 November 2019

Critical Capabilities for WAN Edge Infrastructure - 3 December 2018

Recommended by the Authors

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

How Products and Services Are Evaluated in Gartner Critical Capabilities

Magic Quadrant for WAN Edge Infrastructure

Don’t Expect 5G to Replace Wired Access WANs Anytime Soon

Innovation Insight for Software-Defined Cloud Interconnection

How to Optimize Network Connectivity Into Public Cloud Providers

Best Security Practices for SD-WAN

Toolkit: RFP Template for Managed and DIY SD-WAN Products and Services

Infographic: How to Best Connect to Public Cloud Services

Cool Vendors in Enhanced Internet Services and Cloud Connectivity

Hype Cycle for Enterprise Networking, 2021

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*Small Branch WAN*	*Large Global WAN*	*Security-Sensitive WAN*	*Cloud-First WAN*	*Remote Worker*
SD-WAN Features	10%	25%	15%	20%	5%
Security Features	10%	10%	45%	10%	5%
App Performance Optimization	0%	15%	5%	5%	0%
Operational Features	10%	10%	15%	10%	5%
Deployment Flexibility	5%	10%	0%	5%	0%
Small Platform Flexibility	50%	0%	5%	5%	5%
Scalability	10%	20%	10%	5%	5%
Cloud Features	5%	10%	5%	40%	5%
Remote Worker	0%	0%	0%	0%	70%
As of 14 September 2021					

Source: Gartner (September 2021)

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*Barracuda*	*Cisco (Meraki)*	*Cisco (Viptela)*	*Citrix*	*Cradlepoint*	*FatPipe Networks*	*Fortinet*	*HPE (Aruba SD-Branch)*	*Huawei*	*Juniper Networks*	*Nuage Networks*	*Palo Alto Networks*	*Peplink*	*Riverbed*	*HPE (Aruba EdgeConnect)*	*Versa Networks (VOS with Titan)*	*Versa Networks (VOS)*	*VMware*
SD-WAN Features	3.8	3.4	4.1	4.5	3.6	3.9	4.1	3.7	4.2	4.6	3.6	4.1	3.2	4.5	4.5	4.5	4.7	4.6
Security Features	4.2	4.4	4.2	4.4	3.5	3.8	4.6	4.0	4.0	4.1	3.9	4.7	3.2	3.8	4.1	4.5	4.5	4.1
App Performance Optimization	3.1	1.9	3.9	4.2	1.5	3.8	3.9	2.9	3.3	2.9	2.9	2.4	2.9	4.2	4.5	3.8	3.8	3.5
Operational Features	2.6	3.7	4.3	3.7	2.8	2.9	4.1	4.1	3.8	4.2	3.7	4.0	2.5	3.8	3.9	4.2	3.9	4.1

Deployment Flexibility	3.6	3.9	4.7	4.5	2.6	4.5	4.5	3.5	4.4	4.6	3.9	4.0	3.6	4.3	4.1	4.4	4.6	4.6
Small Platform Flexibility	3.8	4.4	4.0	4.0	4.0	3.3	4.5	4.5	4.4	4.1	3.2	3.0	3.7	3.5	3.0	4.4	4.0	4.3
Scalability	4.5	4.9	4.3	4.4	4.5	3.5	4.9	4.5	4.8	4.0	4.3	4.8	4.5	3.7	4.5	4.3	4.8	4.9
Cloud Features	2.7	2.2	4.0	4.1	1.0	1.8	3.9	2.8	2.0	3.1	3.0	4.2	1.7	3.1	3.9	4.0	4.0	4.1
Remote Worker	3.8	3.5	3.3	3.8	2.5	2.2	4.5	3.6	2.1	3.2	2.1	4.0	2.1	2.1	1.3	4.3	4.6	4.1
As of 14 September 2021																		

Source: Gartner (September 2021)

Table 3: Product Score in Use Cases

Use Cases	*Barracuda*	*Cisco (Meraki)*	*Cisco (Viptela)*	*Citrix*	*Cradlepoint*	*FatPipe Networks*	*Fortinet*	*HPE (Aruba SD-Branch)*	*Huawei*	*Juniper Networks*	*Nuage Networks*	*Palo Alto Networks*	*Peplink*	*Riverbed*	*HPE (Aruba EdgeConnect)*	*Versa Networks (VOS with Titan)*	*Versa Networks (VOS)*	*VMware*
Small Branch WAN	3.73	4.15	4.13	4.13	3.62	3.38	4.44	4.20	4.20	4.13	3.50	3.67	3.46	3.70	3.60	4.37	-1.00	4.36
Large Global WAN	3.63	3.54	4.19	4.31	3.02	3.55	4.30	3.70	3.93	3.99	3.65	4.04	3.24	4.00	4.30	-1.00	4.41	4.35
Security-Sensitive WAN	3.78	3.96	4.18	4.27	3.31	3.53	4.41	3.93	3.97	4.07	3.74	4.29	3.16	3.87	4.13	-1.00	4.39	4.24
Cloud-First WAN	3.27	3.13	4.12	4.21	2.38	2.93	4.14	3.44	3.27	3.77	3.40	4.08	2.63	3.69	4.07	4.22	-1.00	4.25

Remote Worker	3.74	3.60	3.56	3.92	2.72	2.50	4.46	3.70	2.63	3.45	2.56	4.04	2.41	-1.00	-1.00	4.31	-1.00	4.18
As of 14 September 2021																		

Source: Gartner (September 2021)