

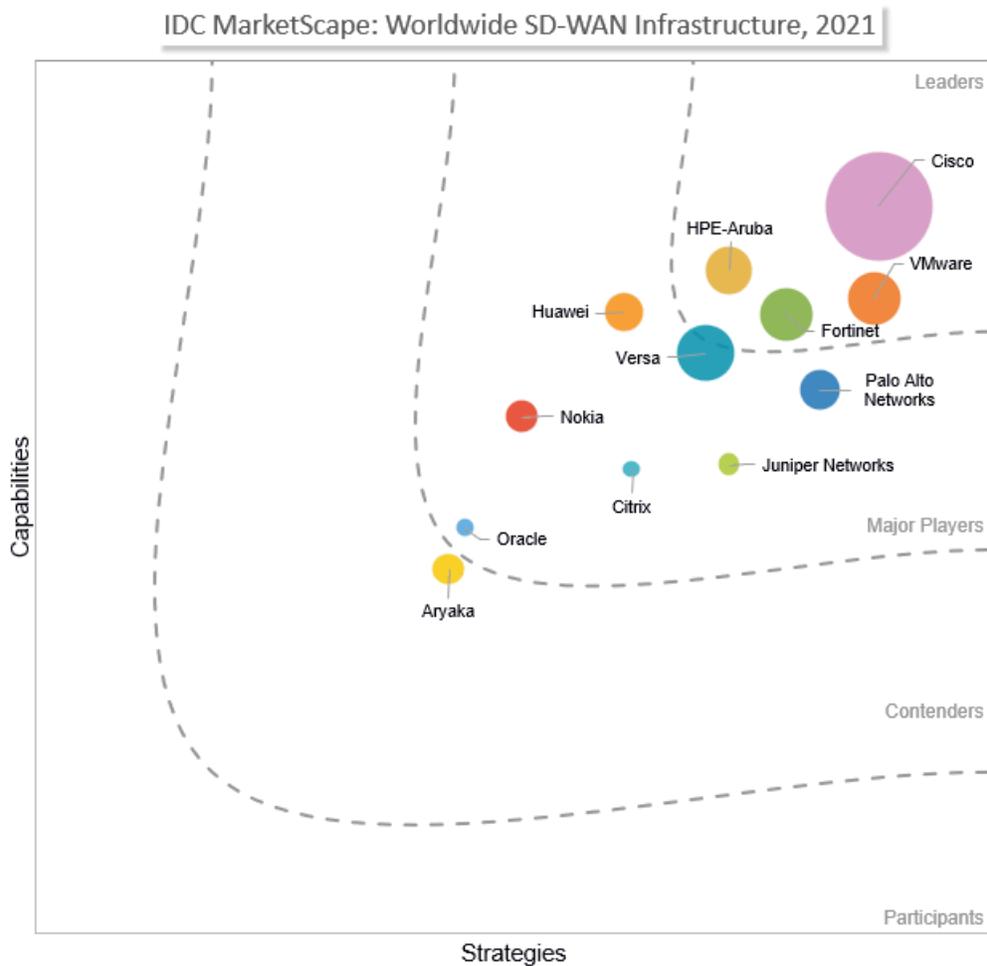
IDC MarketScape: Worldwide SD-WAN Infrastructure 2021 Vendor Assessment

Brandon Butler

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide SD-WAN Infrastructure Vendor Assessment



Source: IDC, 2021

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

This IDC study represents a vendor assessment model called the IDC MarketScape, which is a quantitative and qualitative research assessment of vendors' present and future offerings in the software-defined wide area networking (SD-WAN) infrastructure market. This study assesses the capability and business strategy of 12 SD-WAN infrastructure vendors. The evaluation is based on a comprehensive framework and a set of parameters expected to be most conducive to success in providing SD-WAN infrastructure solutions.

The SD-WAN infrastructure market is highly competitive and undergoing important strategic shifts. Key findings include:

- SD-WAN remains one of the fastest-growing segments of the network infrastructure market due to this technology's ability to improve user and application experiences, provide integrated connectivity and security, enable seamless connectivity to the cloud and hosted applications, and provide an opportunity for organizations to save money.
- Key components of SD-WAN infrastructure include a centralized policy controller, automatic management of hybrid WAN connections, dynamic path selection of application traffic, and optional programmability, security, and analytics of wide area network (WAN) traffic.
- SD-WAN enables myriad benefits for organizations including, but not limited to, improving reliability by augmenting existing WAN connectivity with redundant failover across dual links; setting application traffic steering via automated software management tools, ensuring that sensitive traffic is prioritized over noncritical traffic; and the ability to provide more direct connections between users and devices and the distributed applications they're accessing.
- In 2020, the SD-WAN infrastructure market grew 18.5%. Through 2025, IDC estimates that the market will grow at a compound annual growth rate of 18.9%.
- IDC's Digital Infrastructure research has identified the critical role of cloud-centric, consumption-based, and highly automated cloud and datacenter digital infrastructure architectures as enablers of digital business transformation and agility. IDC expects enterprise adoption of as a service and subscriptions for cloud and dedicated compute, storage, network, and edge systems and software – including SD-WAN offerings – will increase faster than traditional capex-centric infrastructure in the years to come.
- The need for intelligent, adaptable, and always-on (pervasive) connectivity has become a mandatory requirement for businesses to operate and for people, processes, and things to connect with one another. IDC's Future of Connectedness research shows the strategic importance of a wireless-led and cloud-enabled connectivity strategy that removes network and IT silos, automates critical business processes, empowers employees to become more productive, and ensures a continuous digital experience for employees, customers, and partners.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This research includes the analysis of 12 SD-WAN infrastructure vendors spanning IDC's research coverage. This assessment is designed to evaluate the characteristics of each firm across a set of criteria broken into two major buckets: current and future capabilities of the SD-WAN infrastructure and current and future strategy of the SD-WAN infrastructure offering.

IDC used a variety of primary research methods to produce this document including interviews with vendors and customers, a detailed questionnaire all vendors completed and detailed product briefings from each vendor. This evaluation should not be considered a final judgment of firms to consider for a project, however. An enterprise's specific objectives and requirements will play a significant role in determining which firms should be considered as potential candidates for an engagement.

For inclusion in this IDC MarketScape, vendors had to:

- Demonstrate two years of general worldwide availability of an SD-WAN infrastructure offering.
- Derive at least \$20 million per year in SD-WAN infrastructure revenue.

This document also includes a profile of Extreme Networks in the Vendor to Watch section. This company did not meet our criteria for full inclusion in the study but is likely to be an important SD-WAN infrastructure vendor in the future.

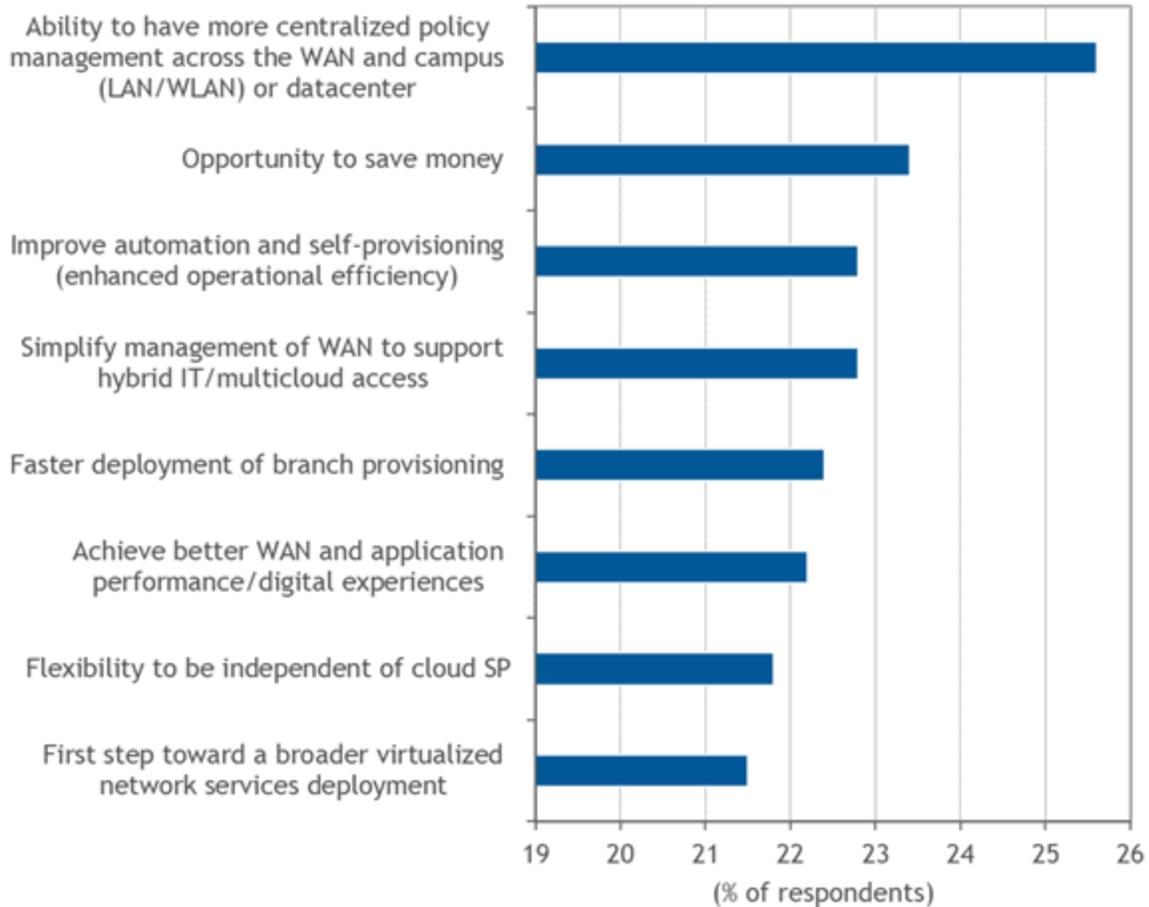
ADVICE FOR TECHNOLOGY BUYERS

SD-WAN infrastructure is a compelling technology for any organization looking to improve WAN reliability, optimize network performance and user experiences for applications accessed via the WAN, or reduce costs or avoid future cost increases on WAN connectivity. Figure 2 shows data from a global survey which asked respondents what their top motivations were for deploying SD-WAN. Centralized management of WAN and local area network (LAN), operational efficiencies, and simplified WAN for multicloud access were among the top-rated responses.

FIGURE 2

Top Motivations for SD-WAN Deployments

Q. *What are the top motivations for considering an SD-WAN deployment (percentage of respondents selecting)?*



n = 375

Note: Multiple responses were allowed.

Source: IDC's *Global SD-WAN Survey*, June 2021

All SD-WAN products featured in this IDC MarketScope have a core set of features. These include WAN routing, management of multiple WAN links (e.g., broadband, MPLS, and 4G/LTE), dynamic WAN path selection, application-based policy controls, and application steering and prioritization. Beyond these features, most SD-WAN offers on the market today include additional features such as optimized connections to public clouds (IaaS and SaaS), WAN link visibility and analytics, end-user experience monitoring, zero-touch provisioning, and forward error correction.

Other considerations perspective SD-WAN buyers should take into account are discussed in the sections that follow.

SD-WAN + Security

One of the most significant developments in the market in recent years has been the advancement of integrated security functionality with SD-WAN products. This provides an opportunity for SD-WAN customers to use natively integrated security features from their SD-WAN vendor or integrate the SD-WAN with a third-party security toolset. IDC refers to the comanagement of network and security functions as the software-defined branch (SD-Branch). When vendors offer cloud-managed networking and security capabilities, it is referred to as the secure access service edge (SASE). Common security features in SD-WAN products include intrusion detection and prevention (IDS/IPS), next-generation firewall (NGFW), and content/web/URL filtering. Similarly, almost all SD-WAN vendors have integrations with third-party security tools, most commonly with cloud access security brokers (CASBs) or secure web gateway (SWG) providers such as Zscaler and Check Point.

SD-WAN Deployment Options

Most SD-WAN vendors offer customers various deployment options, including offering integrated hardware – typically a router or firewall, or both – along with virtualized versions of the SD-WAN software that can be deployed on existing infrastructure or hosted in a public IaaS cloud. Organizations also have a choice related to architectural designs of their wide area network. For example, from a multicloud access perspective, many SD-WAN vendors offer integrations with IaaS provider gateways, such as AWS Transit Gateway or Azure virtual WAN. Many SD-WAN vendors also offer integrations with colocation vendors such as Equinix and Megaport, which provide direct connections from the colocation vendor into IaaS and SaaS clouds. Alternatively, many SD-WAN vendors are building software-defined cloud interconnect (SDCI) services that utilize a series of points of presence (POPs), usually hosted in colocation facilities, that provide access to IaaS and SaaS clouds.

Customers have a choice for the SD-WAN management platform being hosted on-premises or from the cloud. Most SD-WAN vendors offer a cloud-hosted management plane, but some offer on-premises management too. Enterprises may also consider existing relationships they have with SD-WAN vendors across other product areas and what sorts of licensing discounts they may be able to receive as part of a longer-term subscription package.

Another consideration is what type of partner organizations would like to purchase SD-WAN infrastructure from. Some SD-WAN vendors have value-added resellers (VARs), others rely on communications service providers (SPs) that bundle WAN connectivity (e.g., MPLS, broadband, or cellular) with an SD-WAN service. Many managed service providers bundle and integrate the requisite underlays (transports) with an SD-WAN overlay.

SD-WAN + LAN

Increasingly, some SD-WAN vendors are building integrated network management offerings that include the ability for centralized visibility, and some management features, of enterprise campus and remote/branch office sites, usually via a cloud-based platform. While LAN/WLAN and WAN networks are still largely managed separately, IDC expects networking vendors with strong access technology solutions to explore ways of building integrated management features across the LAN, WLAN, and SD-WAN, which IDC also refers to as SD-Branch. One benefit of this approach is it provides an opportunity for enterprises to have centralized visibility and analytics into their enterprise network, across the LAN and WAN, and some policies related to user, application, or network prioritization that are applied across both networking domains.

Visibility and Analytics

Other factors enterprises should consider are what sort of visibility and analytics platforms they require from their SD-WAN vendor. Some vendors have robust platforms that monitor not just WAN link health, but application and user experiences too; others offer visibility platforms that extend into the local area network.

These are among the considerations enterprises should research when purchasing SD-WAN infrastructure, but some features and functions will be more important than others for individual customers. Organizations should always think about what business need they have and then consider what solution will best meet those needs.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Aryaka

Aryaka is positioned in the Contenders category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Aryaka was founded in 2009 and is headquartered in San Mateo, California. The company has an integrated offering of WAN technology and life-cycle services, which include managed SD-WAN and SASE. A key architectural feature of Aryaka's offering is more than 40 services POPs located around the world – mostly in tier 1 colocation facilities. Aryaka customers use an Aryaka Network Access Point (ANAP) – an appliance available in multiple sizes with zero-touch provisioning capabilities – to connect into the POPs. Customers can use SD-WAN capabilities (e.g., multi-WAN link connectivity and dynamic application steering) to connect from the ANAPs to the POPs. Aryaka can optionally manage customers' last-mile WAN connectivity between ANAPs and the POPs. The POPs are interconnected via dedicated L2 fiber links for end-to-end performance SLAs. In an additional 40+ metro areas where Aryaka does not have a POP, the company leverages the Equinix Fabric, which then provides connectivity into Aryaka's network.

ANAPs have a series of integrated security features, including an access firewall and a zones function for segmenting traffic across the middle mile. In May 2021, the company acquired Secucloud, a German security company. Aryaka has begun deploying Secucloud functionality at the company's POP locations to provide cloud-managed SASE security capabilities such as a firewall as a service, SWG, and threat prevention. Customers can also deploy third-party virtual security functions on ANAP appliances; Aryaka has partnerships with Check Point and Palo Alto Networks for this functionality. Aryaka has integrations with other security tools such as Zscaler too.

For multicloud connectivity, Aryaka offers customers secure hand-offs from its POPs to multicloud IaaS and SaaS platforms. Customers pay for Aryaka as a subscription offering, which includes the ANAP as well as WAN traffic management. Customers can control traffic policies through a cloud-based portal that provides mapping and reporting capabilities. Aryaka also offers Private Access, a solution for remote workers to use a client that connects directly into Aryaka's global POP footprint.

Strengths

- Aryaka offers a single subscription price that includes the ANAP appliance, life-cycle services management, on-ramps into IaaS and SaaS clouds, and optional security tools and last-mile connectivity management.
- Aryaka has a footprint of Services POPs around the globe that provide managed SD-WAN and SASE as well as create a SDCI for customers.
- Aryaka offers a range of security services from its POPs, as well as integrations with on-premises security services from partners; Aryaka's cloud-based SASE capabilities will increase in the future as the company continues to integrate the Secucloud capabilities into its product offering.

Challenges

- While Aryaka has strong technology and services integrations, the company's platform may not be a fit for customers that want to customize or manage an SD-WAN deployment themselves or those that are not looking for a managed SD-WAN.
- Aryaka's range of ANAP appliances has less user-configurable options compared with vendors with a routing heritage.
- Aryaka does not offer native management of local area networks (e.g., WLAN or Ethernet switching) in the enterprise campus or branch.
- Aryaka sells mostly through a channel of VARs, for the company may be challenged in building out its channel with traditional managed SPs that see Aryaka as a competitor, given its integrated managed services offering.

Consider Aryaka When

IDC recommends that customers that are looking for a cloud-based SD-WAN-managed service consider Aryaka. Aryaka has a mix of customers across vertical industries, but some target verticals for the company are manufacturing and business services/technology, as well as healthcare, retail/e-commerce, and financial services.

Cisco

Cisco is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Cisco has two primary products in its SD-WAN portfolio: Cisco SD-WAN powered by Viptela and Cisco SD-WAN powered by Meraki. The Cisco SD-WAN powered by Viptela platform stems from the company's 2017 acquisition of Viptela, one of the initial start-ups that helped develop the SD-WAN market.

The primary management platform for Cisco SD-WAN powered by Viptela is vManage, and recent innovations have focused on three areas: multicloud connectivity, security, and analytics. From a multicloud connectivity standpoint, Cisco SD-WAN has direct integrations with the major IaaS and SaaS vendors, including Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and AliCloud. The company has built-in optimizations to support popular SaaS offerings, such as Microsoft 365 and Cisco WebEx unified communication platform. Cisco has also recently built a partnership with Equinix to provide SD-WAN Cloud Interconnect, which leverages Equinix for access to a variety of cloud applications and destinations; Cisco also has a partnership with Megaport for similar SDCI capabilities. The company has also recently announced a strategic partnership to use Google's IaaS

cloud backbone for site-to-site interconnect via Cisco CloudHub. The company has recently delivered innovations for DevOps teams to automatically apply specific network policies to internally created cloud-native apps. Beyond network transport features, Cisco SD-WAN also integrates application optimization features such as data redundancy elimination (DRE), TCP optimization, and data compression as well as an integrated application telemetry for Microsoft Office 365.

On the security front, the company's Umbrella and Duo platforms are key tools that integrate natively with both vManage and Meraki. Umbrella provides a Secure Internet Gateway (SIG), along with firewall, DNS security, and a cloud access security broker, while Duo provides a zero trust network access (ZTNA) framework; the security platforms also leverage Cisco Talos for threat intelligence. As part of the new Cisco+ offering, the company has a road map to offer an integrated subscription-based license for vManage, Umbrella, Duo, and ThousandEyes (for visibility).

On-premises Cisco SD-WAN security includes SSL decryption, intrusion prevention, URL filtering, and malware sandboxing. Cisco SD-WAN has an integrated application-aware zone-based firewall with logging, inspection, and access control. Cisco SD-WAN integrates user identity-aware security-based on Cisco Trustsec and Security Group Tags, and the platform is SGT aware and can enforce access control at the network layer based on user identity, allowing for policy enforcement across sites and clouds.

In analytics, Cisco is leveraging its acquisition of ThousandEyes to provide detailed visibility and analytics and, in the future, to provide closed-loop telemetry capabilities to automatically resolve issues. For deployment options, the company uses its platform of ISR and Catalyst 8000 series routers, along with having a range of software-based virtualized routers. Cisco SD-WAN powered by Viptela also offers integrated unified communications management through vManage for centrally configuring, deploying, and maintaining branch telephony functions.

Cisco SD-WAN powered by Meraki provides a simplified, cloud-managed platform that includes zero-touch provisioning and an intuitive web interface. Native security features include a next-generation firewall, content filtering, IDS/IPS, antimalware, a GeolP firewall, and HTTPS inspection. Other recent advancements in the Cisco SD-WAN portfolio include performance-based underlay routing and VPN exclusion for optimized SaaS experience and mixed wired and cellular SD-WAN via either an integrated LTE device or dedicated cellular gateway.

Cisco SD-WAN by Meraki also has increased analytics capabilities through Meraki Health, a suite of capabilities that leverages advanced analytics and ML capabilities to determine root cause analysis of problems that arise across the WAN and LAN. Meraki Insights for web application, WAN health, and VoIP health also includes Smart Thresholds for intelligently setting thresholds for application performance. Cisco SD-WAN by Meraki runs on the company's MX physical or virtual unified threat management (UTM) infrastructure, and the company offers an ability to deploy the Meraki MX, MG, and Z Series appliances for remote workers.

Strengths

- Cisco has been able to leverage its strong heritage in enterprise routing to build its SD-WAN market share, particularly the ISR customer base.
- Cisco has a strong go-to-market channel with a large network of resellers, managed service providers, and value-added resellers, along with partnerships with many prominent communications service providers.

- Cisco's acquisition of ThousandEyes gives its Viptela and Meraki platforms a strong visibility and analytics platform.
- Cisco Viptela has built strong integrations for multicloud connectivity, particularly through recent enhancements with Google Cloud Platform and Equinix to create direct cloud on-ramps to interconnection sites.
- Cisco Meraki offers a range of integrated network and security solutions, from WLAN and ethernet switching to SD-WAN and integrated security, along with remote worker tools, all delivered from a cloud-managed platform.

Challenges

- Cisco's dual products – Viptela and Meraki – can cause some confusion in the market and for customers about which platform is best for which use cases.
- Cisco has strong natively integrated security capabilities, primarily through Umbrella and Duo, but the company's integrations are not as strong with third-party security tools.
- Cisco has an opportunity to further build integrations across its WAN and LAN portfolios, including across its SD-WAN portfolio and its line of popular Catalyst switches, WLAN equipment, and DNA Center software.
- Cisco is often considered a "premium" option and may not be ideal for price-conscious SD-WAN buyers.

Consider Cisco When

Cisco has a broad range of networking solutions for organizations of multiples sizes and structures and provides an easy migration path for existing Cisco routing customers to transition to SD-WAN. Top verticals for the Cisco SD-WAN by Viptela portfolio include government, manufacturing, financial and professional services, retail, education, and healthcare. For Cisco SD-WAN by Meraki, the cloud-managed platform is known for its simplicity in deployment and ongoing management, which makes it a good fit for distributed enterprise and "lean IT" organizations. Top verticals for Meraki include retail, healthcare, professional services, manufacturing, and financial services.

Citrix

Citrix is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Citrix is an enterprise software company that offers solutions across digital workspaces – including virtual applications and virtual desktops – and application delivery infrastructure and security. The company's SD-WAN business fits within its application delivery and security business unit that also includes its application delivery controller (Citrix ADC, formerly NetScaler ADC), along with the company's API security and web application firewall.

Citrix SD-WAN focuses on application-centric capabilities including quality of service, fast failover, packet-level prioritization, and visibility into traffic. Other key components of the product include ease of deployment and zero-touch provisioning. The company's cloud-based platform for managing the SD-WAN is named Citrix SD-WAN Orchestrator, which is a microservices-based platform with multitenant capabilities that support templates and role-based access controls with a REST API kit.

In February 2021, the company launched Citrix Secure Internet Access (SIA) as part of the company's SASE strategy, a platform of more than 100 POPs around the world where it hosts cloud-based security tools including a SWG, CASB, data loss prevention (DLP), firewall, sandboxing, and malware

protection. SIA also allows customers to take advantage of private peering with dedicated links from the POPs to IaaS and SaaS providers, as well as the company's desktop as a service; customers can also use SIA as a backbone for connectivity to private datacenters.

For customers that want an on-premises security stack, Citrix SD-WAN includes a native ICSA-certified firewall and an optional, integrated, advanced edge security stack, which includes web filtering, antimalware, intrusion prevention, and SSL inspection. Customers can alternatively choose to integrate the Citrix SD-WAN with existing security tools; the company has partnerships with Palo Alto Networks Prisma, Zscaler, Check Point, and Symantec. Customers can also host next-generation firewalls as a virtual network function (VNF) on the Citrix SD-WAN appliances. AES 128- or 256-encryption methodology and FIPS mode for compliance plus segregation of traffic into zones with zone-based policies are standard.

Citrix offers a range of standard and premium edition SD-WAN appliances. Citrix SD-WAN is also available as a virtual appliance that can be deployed on IaaS clouds and is offered in the AWS, Azure, and Google Cloud marketplaces. Customers also have the option of putting a Citrix SD-WAN appliance in Equinix's interconnection-oriented datacenters. About half of the company's SD-WAN customers overlap as Citrix Workspace customers; for those customers, Citrix SD-WAN offers granular visibility into HDX user sessions, and it uses proprietary Citrix ICA protocol to ensure quality of service. In the future, the company is building up SD-WAN-as-a-service capabilities, including flexible licenses and pooled capacity, a feature from its ADC. The company has an analytics engine that provides visibility and analytics across the networks it manages.

Strengths

- Citrix has a large customer base across its virtualized workspace products and ADCs; the company will be able to leverage this customer base to grow in the SD-WAN infrastructure market.
- Citrix has a strong portfolio of offerings for remote and hybrid workers, including its SD-WAN capabilities with its Workspace solutions, which can be leveraged via a small gateway appliance (e.g., Citrix SD-WAN 110) or as a soft client that connects into the SIA POPs.
- The company's SIA cloud-based security and peering platform represents an advanced architecture for SASE and multicloud connectivity, but the platform was recently launched in 2021, so it is new, and the company must continue to develop it.
- Citrix has a road map to provide flexible consumption and "as a service" licenses for its SD-WAN offering, similar to what the company has done for many of its other products.

Challenges

- Citrix's heritage is in workspace solutions and application delivery but not enterprise routing, which could be limiting its market awareness among customers evaluating SD-WAN solutions.
- Citrix SD-WAN appliances support Wi-Fi, but the company does not have strong integrations or offerings with existing enterprise campus and branch (Ethernet Switch and WLAN technologies), which could be limiting for customers that prioritize such an offering.
- The company is building up its channel for selling the SD-WAN solution but will face a competitive market among communications service providers that are increasingly offering multivendor solutions.

Consider Citrix When

Citrix's SD-WAN platform is a good fit for customers of the Citrix Workspace products and organizations that embrace a cloud-delivered security model. The company's top vertical markets for its SD-WAN infrastructure are financial services, business services, manufacturing, retail, and government.

Fortinet

Fortinet is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Fortinet is a security company founded in 2000, headquartered in Sunnyvale, California. The company is known in the SD-WAN market for having a strongly integrated network and security offering. Fortinet's Secure SD-WAN consolidates SD-WAN, NGFW, advanced routing, and ZTNA proxy functions in its popular FortiGate appliance.

FortiGate runs FortiOS, which is a layer 7 firewall with SD-WAN capabilities, along with malware protection, web/URL filtering, IPS, cloud-hosted sandbox, deep SSL inspection, application control, and ZTNA access proxy. Customers can use the SD-WAN functionality atop a FortiGate next-generation firewall appliance or a virtualized software-based FortiGate. FortiGate includes a custom application-specific integrated circuit (ASIC) that performs near-real-time/inline SSL inspection.

Customers manage the Fortinet SD-WAN from the Fabric Management Center, which includes FortiManager and FortiAnalyzer. FortiManager provides management capabilities for deploying, configuring, and managing FortiGate appliances; FortiManager can be deployed in hardware, software, or hosted form factors. FortiManager can scale to 10,000+ sites and allows for the segregation of large deployments by grouping devices and agents into geographic or functional administrative domains (ADOMs) and provides device and agent provisioning, detailed revision tracking, and auditing capabilities. FortiAnalyzer provides in-depth discovery, analysis, prioritization, and reporting of network security events. It features scripts and automates device provisioning and policy pushing with JSON APIs or allows customers to build custom web portals with the XML API. Within FortiManager, management responsibilities can be strictly controlled by implementing role-based administration. Also, FortiManager can centrally control firmware upgrades and content security updates.

In addition to the SD-WAN portfolio, Fortinet also offers a range of WLAN (Wi-Fi) and LAN (Ethernet switch) products along with recently announced wireless WAN (LTE/5G functionality via FortiExtender), giving customers an opportunity to manage LAN + WAN functionality from FortiManager. For cloud and multicloud connectivity, Fortinet offers cloud on-ramp and a virtualized version of its custom ASIC instantiated in a VM form factor that can be deployed at IaaS cloud provider sites; Fortinet also has integrations with Equinix Network Edge, Megaport Virtual Edge, and Teridion for SaaS optimization.

FortiCASB provides policy-based insights into users, behaviors, and data stored in major SaaS applications, as well as comprehensive reporting tools. Fortinet sells 100% through the channel and has built up strong partnerships with communications service providers while also continuing to build a channel of managed service providers and value-added resellers.

Strengths

- Fortinet offers a highly integrated security and networking SD-WAN capability. Most Fortinet SD-WAN customers deploy the product on the company's FortiGate physical or virtual security appliance, which has integrated next-generation firewall capabilities, along with SSL inspection.
- Fortinet also offers LAN and WLAN products, giving customers an opportunity to work with an existing vendor across LAN + WAN.
- Fortinet has successfully built up a channel partner strategy that includes strong relationships with communications SPs, as well as managed SPs and VARs.
- Fortinet's FortiGate infrastructure uses custom ASICs that improve performance and allow the company to do inline SSL inspection.
- Fortinet still has room to expand its SD-WAN portfolio into its existing customer install base.

Challenges

- Fortinet is primarily a security vendor and may need to work harder with some customers that are looking to work with a vendor with a stronger heritage in routing and networking.
- While Fortinet offers integration with third-party security tools, its primary security solutions are offered by Fortinet itself; this may be a limitation to customers that want to use Fortinet for SD-WAN but integrate it with third-party security tools.
- Fortinet in the past year has introduced cloud-based security services delivered via a network of POPs, whereas some other vendors have more advanced cloud-based security capabilities.

Consider Fortinet When

Fortinet SD-WAN is a good platform for existing Fortinet customers or organizations looking for a highly integrated SD-WAN and security offering, particularly for on-premises managed security. Customers that are looking for integrations across the WAN + LAN and wireless WAN could also consider Fortinet. The top vertical markets for Fortinet's SD-WAN include government, retail, financial, manufacturing, and healthcare.

HPE-Aruba

Hewlett Packard Enterprise (HPE)-Aruba is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

The SD-WAN portfolio from Aruba, an HPE company, is part of the company's Edge Services Platform (Aruba ESP), the company's "edge to cloud" vision for unified infrastructure, security, and AIOps across wired, wireless, and SD-WAN. Aruba has two SD-WAN offerings: Aruba EdgeConnect and Aruba SD-Branch.

Aruba EdgeConnect SD-WAN is based on technology from Silver Peak, which HPE acquired in 2020. Silver Peak was founded in 2004 and has a strong history in the WAN optimization market, and then successfully pivoted to the SD-WAN market in 2015. Aruba EdgeConnect is managed by Aruba Orchestrator, a centralized software platform providing real-time visibility into SD-WAN health and application performance. A key feature of Aruba EdgeConnect is Business Intent Overlays (BIOs), which provide an automated way for customers to prioritize application traffic based on business intent. BIOs allow network teams to select routing and WAN link policies, apply granular security policies, and implement WAN optimization techniques for ensuring quality of experience. Aruba Boost WAN Optimization is an optional software performance pack for EdgeConnect systems.

Native security capabilities for Aruba EdgeConnect include a zone-based L7 stateful firewall, segmentation, and intrusion detection and prevention. Aruba also offers integrations with a variety of cloud-based security services from vendors such as Zscaler, NetSkope, Check Point, and Palo Alto Networks.

In 2021, the company announced stronger integrations for the EdgeConnect products with Aruba security tools, namely the Aruba Threat Defense portfolio, including Aruba ClearPass, the network access control (NAC) platform. These integrations allow network teams to set up and enforce policies that segment and microsegment users and devices based on user identities and role-based access controls. EdgeConnect offers a series of purpose-built hardware appliances and software-based virtual appliances.

Aruba's other SD-WAN offering is Aruba SD-Branch, which offers integrations across Aruba's broader portfolio of enterprise networking products (e.g., wireless LAN, wired LAN, VPN, and security), managed by the Aruba Central cloud-based management platform. Security for Aruba SD-Branch includes native support for L3 through L7 applications, as well as a user-aware policy enforcement firewall, web content filtering, and inline IDS and IPS functionality with multiple prepackaged rulesets and listing capabilities.

Multicloud connectivity options for Aruba EdgeConnect and SD-Branch include:

- Direct connections for AWS, Azure, Google, and Oracle
- Virtual appliances within IaaS marketplaces using IPsec tunnels to major cloud providers
- Automated connectivity to AWS Transit Gateway, Azure virtualWAN, and Google Network Connectivity Center (NCC) for branch-to-cloud connectivity or for using an IaaS backbone for branch-to-branch connectivity
- Certification for Microsoft 365 applications
- Support for cloud on-ramp via Equinix, Teridion, CloudFlare, and Megaport

Aruba offers both SD-WAN offerings through the company's global sales and channel partner teams, as well as through HPE Greenlake, for flexible consumption and subscription-based models.

Strengths

- Aruba's EdgeConnect SD-WAN offering is based on technology from Silver Peak, which pioneered several innovative features in the WAN optimization market and successfully pivoted to the SD-WAN market.
- Aruba is continuing to build integrations across Aruba EdgeConnect and its broader Aruba Edge Services Platform (ESP) platform. Customers can launch and do basic management across Aruba Central and the EdgeConnect Orchestrator, and the company has developed a road map to increase integrations across the management platforms.
- Post Silver Peak acquisition, Aruba has an opportunity to leverage the company's strong global channel presence for selling EdgeConnect into its existing customer base, particularly for customers that use Aruba for wired and wireless networking.
- The Aruba SD-Branch platform provides integrations across campus (LAN and WLAN) and branch (SD-WAN), along with remote worker tools (such as microbranch and VIA for secure remote connectivity), managed by Aruba Central.
- Both Aruba EdgeConnect and Aruba SD-Branch systems are offered as an HPE Greenlake as-a-service solution for flexible acquisition, deployment, and management options.

Challenges

- Aruba has two offerings for SD-WAN across Aruba EdgeConnect and Aruba SD-Branch, which, in some instances, could create questions for customers about which platform is best for their specific use cases.
- Unlike some other SD-WAN vendors, Aruba EdgeConnect has not built out a series of POPs for cloud connectivity or software-defined interconnect; however, the company does offer integrations with popular IaaS, SaaS, and colocation providers.
- From a go-to-market perspective, Aruba relies heavily on its enterprise channel partners for selling its SD-WAN and, compared with some other SD-WAN vendors, has fewer communications service providers as channel partners, with plans to add more in 2022.
- Aruba has well-established network access control and identity-based security tools (e.g., Aruba ClearPass), but the company does not have in-house developed or acquired cloud-based security systems, which is why the company offers integrations with third-party security tools.

Consider HPE-Aruba When

Aruba EdgeConnect is a strong SD-WAN platform, particularly for customers that are looking for WAN optimization capabilities natively integrated into the overall solution. Top vertical markets for Aruba EdgeConnect include manufacturing, finance and insurance, professional services, healthcare, and government. Aruba SD-Branch is ideal for customers looking for a simple branch solution that includes wired, wireless, WAN, and security. Target vertical segments for Aruba SD-Branch include retail, healthcare, and hospitality.

Huawei

Huawei is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Huawei is a multinational information and communication technology vendor headquartered in Shenzhen, China, with a heritage as a producer of telecommunications equipment. The company formed an Enterprise Business group in 2011 and has since offered a broad portfolio of networking, optical, storage, and compute infrastructure products, including its SD-WAN product. Huawei's SD-WAN infrastructure is managed by a platform named iMaster NCE, which provides centralized management across both campus (LAN and WLAN) and branch (routing and SD-WAN).

Huawei offers a variety of deployment options for its SD-WAN product including its portfolio of NetEngine routers, which range from SOHO to small, medium-sized, and large enterprise sizes and have an optional 5G SIC card. Huawei also offers a virtualized version of the router, named the AR1000V, which can run on a virtual machine or in a hosted cloud. Customers can also use the company's HiSec Engine, a firewall appliance and a virtualized version of the firewall named the USG6000V, as a deployment option for the SD-WAN product. Innovative features of the SD-WAN offering include iMaster NCE's ability to generate recommended policies based on WAN traffic simulations, adaptive and dynamic TCP acceleration, and per-packet load balancing across multiple WAN links.

Huawei offers the Qiankun CloudService, which provides cloud-based security services including zero trust, cloud access security, advanced threat protection, and cloud application security. The company has partnerships with Zscaler, Forcepoint, Leagsoft, and NSFocus for third-party cloud-based security services. For visibility and analytics, the company offers Campus Insight, which can provide unified

visibility across the LAN and WAN. The company has a network of more than 100 POPs that provide customers the ability to create direct connections into public IaaS and SaaS clouds, including the company's own Huawei Cloud, Alibaba Cloud, China Telecom e-Cloud, AWS, Microsoft Azure, and Tencent Cloud.

Huawei offers a feature named SRv6+SD-WAN, which allows end-to-end programmable path selection with guaranteed SLAs, allowing customers to program path selection across WAN edge routers. Huawei has a strong presence in Asia, particularly China, and across Europe, but does not compete in North America. Huawei develops almost all of its own technology in-house, with a strong research and development team. The company sells mostly through a network of partners, and it has good relationships with communications SPs, particularly in Asia, Europe, and Latin America including China Telecom, Italy Telecom, and Vodafone.

Strengths

- Huawei is one of the market share leaders in enterprise and service provider routing in Asia and Europe. The company has been able to leverage its strength in WAN routing to successfully pivot into the SD-WAN market.
- Huawei offers an extensive portfolio of routers and firewalls that customers can use in their SD-WAN deployments.
- Huawei offers a single management platform across the WAN and LAN named iMaster NCE, including an integrated visibility and analytics platform named Campus Insight. The company has a number of other advanced features of its SD-WAN platform, such as SRv6.
- Huawei has a strong go-to-market channel for its SD-WAN product, particularly in Asia and Europe, but it's still building a channel in Latin America and the Middle East; meanwhile, the communications SP channel is becoming increasingly competitive.

Challenges

- Huawei's products are not sold in North America, in part due to geopolitical tensions that have constrained the company from competing in certain markets.
- The company offers a range of security products natively integrated into the SD-WAN along with its cloud-based Qiankun CloudService platform, but its SD-WAN could be limiting for customers that want an SD-WAN that integrates with third-party security tools.
- Huawei has a broad portfolio of offerings across multiple product lines, which can make for a complex offering; Huawei works with managed service providers and offers support for helping customers implement SD-WAN and other technologies it offers.

Consider Huawei When

Non-United States-based organizations should consider Huawei's SD-WAN, particularly those in China, Asia, or Europe and customers that already use or would consider using Huawei for other enterprise networking needs such as in the campus (LAN/WLAN). Key vertical markets for Huawei's SD-WAN include finance, government, retail, energy, and carrier resale.

Juniper Networks

Juniper Networks is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

In December 2020, Juniper Networks acquired 128 Technology (128T), a company founded in 2014 with a focus on tunnel-free routing and SD-WAN infrastructure. Juniper has integrated 128T into its AI-

Driven Enterprise (AIDE) business unit and supports its cloud-based Mist management platform. The company's AI-driven SD-WAN product is part of a broader portfolio of campus and branch networking and security offerings. Other components include WLAN, Ethernet switches, and management tools; assurance software for visibility and analytics; and its Marvis tool, which the company calls a virtual network assistant that provides automated troubleshooting and incident resolution.

A key to Juniper's SD-WAN offering is what the company calls Session Smart Routing (SSR), which is a tunnel-free, vector routing architecture that creates stateful sessions for WAN traffic, centrally managed by the Session Smart Conductor platform. The Session Smart Conductor uses templates to simplify deployments and can construct multirouter packet captures that describe packet transmissions between two or more network nodes, creating real-time telemetry data. The Session Smart Conductor is a cloud-based platform, although customers can deploy it on premises if they wish. A road map item for Juniper is to offer deeper integrations between the Session Smart Conductor and the Juniper Mist cloud-based management platform. Juniper is also integrating the 128T-based technology portfolio with Juniper's SRX and vSRX (virtualized) firewall and the NFX universal CPE. The company is releasing a series of Juniper-branded hardware appliances as an integrated hardware/software offering for SD-WAN infrastructure. Initial points of integration across 128T and Mist have been for the WAN Assurance visibility and analytics platform, which complements the existing Juniper Mist Wi-Fi and Wired Assurance products, along with the natural language processing capabilities of Marvis.

For security, the SSR technology is a zero trust secure routing architecture with stateful, session-aware routing capabilities. Juniper's SD-WAN also includes native NGFW, content security, and IDS/IPS capabilities. Juniper's SD-WAN also offers integrations with Juniper Security Director Cloud, the company's SASE portal for real-time threat awareness. The company also offers integrations with cloud-based security platforms such as Zscaler. Juniper has seen some success with managed SPs that offer a full suite of Mist products.

Strengths

- Juniper has a significant market presence in enterprise and service provider routing, along with existing customers across networking and security; the company will be able to leverage its existing customers to grow in the SD-WAN infrastructure market.
- Juniper has a strong road map to build integrations between the company's Mist cloud-managed LAN/WLAN components and the SD-WAN product.
- Juniper's Session Smart Routing utilizes a unique Secure Vector Routing (SVR) capability for tunnel-free, stateful WAN routing.

Challenges

- Juniper is still building out its integrations of the 128T platform with its broader AIDE, Mist, and SRX portfolios. Initial areas of integration include a WAN Assurance capability (visibility and analytics on WAN health, etc.), but the company is still building out broader integrations for the 128T platform with the SRX and the Mist platforms.
- Juniper is building out its cloud-based security capabilities. There are some integrations across the 128T portfolio and the Juniper SRX firewall and the company's recently launched Juniper Security Director Cloud, but those are expected to increase in the future. Juniper's SD-WAN solution will benefit from the development of broader cloud-based security solutions from Juniper in the future to create a more fully featured SASE architecture.
- In late 2021, Juniper launched a series of 128T-based hardware appliances, prior to that, customers typically deployed 128T on a certified hardware device from a 128T partner.

Consider Juniper Networks When

IDC recommends Juniper's AI-driven SD-WAN for customers that may already use its switching, routing, WLAN, or security products or for those customers that find value in the 128T Session Smart Routing capabilities. The company's top vertical markets include retail, healthcare, federal government, and manufacturing.

Nokia

Nokia is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Nokia is a Finnish multinational provider of telecommunications equipment. In 2016, the company acquired Alcatel-Lucent, which had an internal spin-in named Nuage Networks. Nuage specialized in software-defined networking in the datacenter and WAN and was one of the early entrants in the SD-WAN market. Today, the Nuage Networks from Nokia SD-WAN platform is primarily deployed by communications SPs and managed SPs that then offer their own branded managed SD-WAN service to enterprise customers. The company's largest target markets are in Europe and North America. Within Nokia, Nuage sits in the company's IP Routing business unit, which includes solutions for IP/MPLS, optical networking, and the company's SDN technologies, including SD-WAN.

The Nuage SD-WAN solution set, named Virtualized Network Services, is part of the company's Virtualized Services Platform (VSP), which provides SDN capabilities in the datacenter and WAN by abstracting the management, control, and data planes. In the WAN, this allows for large-scale, multitenant deployments by service providers with isolation for each enterprise service instance. The Nuage SD-WAN solution includes L2/L3 routing, WAN optimization, IPSec, and a firewall among its base features. The company also offers separately licensed security suite called Virtualized Security Services (VSS), which provide automated detection, prevention, and response. The solution includes a centralized management and policy engine called Virtualized Services Directory, which provides the management and control of security, host, application, and zone policies.

Nuage Networks SD-WAN can be deployed on purpose-built x86 hardware appliances named Network Service Gateways (e.g., 7850 NSG Series), with larger models supporting third-party virtual network functions. Nuage also offers a pure software image of the NSG that can run on customer provided x86 hardware (vNSG) with options for the major cloud provider images (AWS, Azure, etc.).

The company offers a range of security services through VSS, including a L3-L7 firewall, web/URL filtering, L7 application ACLs, IP threat intelligence, and IDS/IPS. Nokia also offers integrations with security services from vendors such as Check Point and Zscaler for a suite of cloud-based/SASE security services. Many of Nuage's communications SP customers offer integrations with Palo Alto Networks, Fortinet, and others as value-added firewall-as-a-service offerings of their managed SD-WAN service.

Nuage Networks SD-WAN has two consumption options: one is an on-premises managed, which is used by most large communications SPs and managed SPs, and the other is a Nokia-hosted and -operated cloud-managed offering, which is used for smaller communications SPs and managed SPs and those that wish to buy SD-WAN as a service. With the later offering, Nuage has a multicloud access feature (AppWAN), which uses a set of global POPs to provide connections into the major IaaS providers including AWS, Microsoft Azure, and GCP.

Strengths

- Nuage Networks is one of the pioneers of the SDN market in the datacenter launching in 2013 and one of the early entrants in the SD-WAN market having launched VNS in 2014, giving the company a strong heritage in SDN and SD-WAN.
- Nuage's SD-WAN platform has strong multitenant capabilities for service providers, which are a major go-to-market channel for the company.
- Nuage Networks ownership by Nokia gives the company an opportunity to sell its SD-WAN platform into Nokia communications SP and managed SP customers of the broader Nokia routing and network management portfolio.
- Nuage has strong partnerships with a broad set of communications SPs and managed SPs, most of whom offer their managed SD-WAN under their own branding.

Challenges

- Nuage's primary go to market is through communications SPs and managed SPs, which is becoming an increasingly competitive channel for SD-WAN. Communications SPs and managed SPs are increasingly offering multivendor SD-WAN platforms, meaning Nuage will face increased competition in its primary route to market.
- Nuage could face branding and market awareness challenges among enterprises considering an SD-WAN as communications SPs and managed SPs offer its SD-WAN as a white-label service. Nokia also continues to work to build up its enterprise sales resources.
- Nuage has some natively integrated security services, including a firewall, URL filtering, and IDS/IPS and partnerships with security vendors such as Check Point, but it does not have a heritage as a security company, if that is a priority for customers.
- Nuage does not offer native integrations with the enterprise campus or branch networking technologies in the LAN/WLAN. Some communications SPs and managed SPs offer bundled offerings for customers across the Nuage SD-WAN and other LAN/WLAN offerings.

Consider Nokia When

Customers should consider Nokia's SD-WAN offering when they're looking for managed SD-WAN deployment from a communications SP or managed SP that will be able to offer bundled connectivity with the SD-WAN service. Key verticals markets for the company's SD-WAN platform include financial services, banking, retail, and manufacturing.

Oracle

Oracle is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Oracle, one of the largest enterprise software and database companies in the world, entered the SD-WAN market with the 2018 purchase of Talari Networks. When Talari was founded in 2008, the company focused on intelligent WAN path selection, which made for a natural pivot into SD-WAN. The SD-WAN product is part of the Oracle Communications strategy, which has solutions for enterprise network communications and mission-critical carrier networks such as a Session Border Controller, 5G core network solutions for telecom operators' 5G deployments and signaling, and policy solutions for carrier-grade 3G/4G networks.

Oracle SD-WAN runs on a family of appliances, including models for small branch office to large datacenters. A key component of Oracle SD-WAN is edge software, which customers can run on

premises, from IaaS public clouds (e.g., Oracle Cloud Infrastructure [OCI], Amazon Web Services, or Microsoft Azure) or as a virtual deployment (e.g., on KVM, ESX, or Hyper-V). For on-premises management, customers can select an edge device to be a controller, typically in a central location. Alternatively, customers can use a cloud-managed service named Oracle SD-WAN Orchestration Cloud Service (OSOC), which is hosted in OCI and can manage all devices running SD-WAN Edge software.

Oracle Edge nodes track detailed WAN information, which enables fast recovery from network impediments such as packet loss, delay, and jitter by measuring – on a per-packet basis – the status of each path and dynamically adjusting traffic if poor link quality is detected. Oracle SD-WAN Aware is a centralized analytics system for monitoring SD-WAN Edge devices; it natively aggregates per-appliance statistics covering critical operational aspects of the SD-WAN.

Oracle SD-WAN supports zero-touch provisioning, dynamic routing protocols, integrated WAN optimization, and service chaining of third-party software on the company's E100 network appliance, among other features. The service chaining allows KVM virtual appliances including the Oracle SBC and Check Point's Quantum Edge NGFW to be deployed on a single physical E100 appliance.

Oracle SD-WAN includes a stateful zone-based firewall that conducts policy-based filtering between services and security zones along with dynamic network address translation. Security zones can extend across multiple branch locations for ease of managing global and site-specific templating. Additional security features of Oracle SD-WAN include 128- or 256-bit AES encryption, per-session rotating keys, IPsec termination, and virtual routing and forwarding. Oracle also has pretested interoperability with Zscaler and Check Point's Quantum Edge.

Strengths

- Oracle SD-WAN's per-packet monitoring enables business-critical applications to be delivered in environments with challenging connectivity.
- Oracle has built – and is growing – its integrations of the SD-WAN platform with Oracle Cloud Infrastructure, which makes Oracle SD-WAN a good fit for customers of OCI. Similarly, customers can expect Oracle to build stronger integrations across Oracle SD-WAN with the company's SaaS-based applications.
- Oracle offers natively integrated visibility and analytics capabilities that are consolidated via SD-WAN Aware

Challenges

- Oracle SD-WAN thus far has relied on a combination of managed service providers and direct sales as its go-to-market channel; unlike other vendors in the SD-WAN market, the company has not developed relationships with communications service providers as a channel.
- For security, Oracle's SD-WAN offers a stateful zone-based firewall and offers partnerships and integrations with a range of third-party security tools, but unlike many other SD-WAN vendors, the company does not offer capabilities such as intrusion detection or prevention or deep packet inspection.
- Oracle has a vision to build a next-generation version of its platform that will enable ZTNA and VPN capabilities, but it is likely more than a year away from being released.

Consider Oracle When

Oracle SD-WAN provides high-quality WAN management, particularly for business-critical applications. Small and medium-sized businesses are a core segment for Oracle SD-WAN. Key vertical markets for the company's SD-WAN platform are contact centers, including business and emergency services; legal firms; financial services, such as banking/credit unions; shipping; logistics and transportation; manufacturing; and utilities.

Palo Alto Networks

Palo Alto Networks is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Palo Alto Networks entered the SD-WAN infrastructure market in 2020 with the acquisition of CloudGenix, a company that was founded in 2013 and rose to become one of the largest remaining start-ups in the SD-WAN market prior to its purchase by Palo Alto Networks. The Palo Alto Networks SD-WAN offering is now branded as Prisma SD-WAN.

The company focuses on providing a cloud-managed SASE platform that combines Prisma SD-WAN with a series of cloud-based security tools named Prisma Access. Palo Alto Networks also has a user and application experience management platform named Autonomous Digital Experience Manager (ADEM). Combined, these components form the company's Prisma SASE offering, which the company now sells as an integrated offering.

Prisma SD-WAN is controlled via a multitenant, cloud-native management platform. Each function within the management platform is available through a secure REST API, including reporting, configuration, and deployment capabilities. A unique aspect of Prisma SD-WAN is the company's CloudBlades, an API abstraction platform that provides more than a dozen native third-party service integrations, including for IaaS and SaaS cloud providers, such as AWS Transit Gateway and Azure virtualWAN; UCaaS providers; and providers of workflow operations and incident management platforms.

Prisma SD-WAN has deep integrations with Prisma Access, the cloud-based security platform that offers firewall as a service, SWG, ZTNA and CASB, and ML-powered threat prevention, including IPS/IDS, URL filtering, malware analysis, and DNS security, among other cloud-based security offerings.

Prisma SD-WAN runs on the company's ION (Instant-On Network) SD-WAN appliances, which are available in both physical and virtual versions. Virtual IONs (vION) can be deployed in public clouds (e.g., AWS, Azure, GCP, and colocation facilities like Equinix). Two appliances – the ION 1000 and ION 1200 – can be used for remote and hybrid workers as a gateway for connecting into Prisma Access and Prisma SD-WAN management platform. The ION 1200 has integrated 5G backup LTE for wired and wireless connectivity. Another unique feature of Prisma SD-WAN allows SD-WAN appliances at customer locations to not be upgraded at the same time as the centralized platform, allowing customers to plan staggered upgrades while still being able to take advantage of many feature enhancements of the centralized cloud-based controller.

Strengths

- Palo Alto Networks is known for being an enterprise security company and has integrated the CloudGenix SD-WAN technology into its broader family of products to create a SASE offering.

- Palo Alto Networks sells a single SASE offering that combines Prisma SD-WAN with Prisma Access, along with optionally including ADEM. This single offering will allow enterprise customers, and service providers, to consume SD-WAN and security tools more easily.
- Palo Alto Networks has an opportunity to grow by selling its Prisma SD-WAN offering into its existing Palo Alto Networks customer base.
- The company has an intuitive and feature-rich management platform and strong API support and an integrated visibility and analytics tool.

Challenges

- Palo Alto Networks takes a cloud-first approach to SASE, which combines cloud-managed Prisma SD-WAN with cloud-managed security in Prisma Access. While the company offers options for customers to manage their SD-WAN and security services on premises, the company's strength is in cloud-managed SASE, which could be a limitation for some customers that do not want to embrace a cloud-based security offering.
- Palo Alto Networks is primarily a security company and entered the SD-WAN market in 2020 through an acquisition, so it could have challenges appealing to organizations looking for a strong routing heritage in their SD-WAN.
- Palo Alto Networks does not have strong integrations or an offering for campus local area networking technology such as WLAN and LAN.
- Palo Alto Networks continues to build up its go-to-market channel, particularly with communications service providers. While communications SPs could be a significant go-to-market opportunity for the company in the future, it will also face competition from other SD-WAN and security vendors in leveraging the communications SPs as a channel.

Consider Palo Alto Networks When

Customers that are interested in a tightly integrated SD-WAN and security offering should consider Palo Alto Networks Prisma SASE solution, which combines Prisma SD-WAN with Prisma Access. Prisma SD-WAN is also a good fit for customers that use Palo Alto Networks' existing security tools or customers that prefer a cloud-managed approach to SD-WAN or security. Top vertical markets for Prisma SD-WAN include financial services, retail, healthcare, manufacturing, and technology companies.

Versa

Versa is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

Versa was founded in 2012 by a team of network and security industry veterans who built a cloud-delivered SD-WAN platform and now have pivoted to SASE. The company provides a series of SD-WAN and security products via the cloud, on premises, or as a blended combination of both. A key to Versa's offering is a cloud-native, multitenant platform that provides centralized policy management of security and networking services. Customers can also manage their Versa SASE and Secure SD-WAN on premises, too.

Versa has built security tools atop the cloud-based platform, including a next-generation firewall, UTM, malware protection, zero trust network access, secure web gateway, data loss prevention, and cloud access security broker. Versa SASE and Secure SD-WAN are made up of multiple components, including the Versa Operating System (VOS), Versa Director for provisioning and management of VOS, and Versa Concerto for configuration. The company also offers Versa Cloud Gateways, which

are located in 90 POPs around the world and provide optimized connectivity to IaaS and SaaS platforms. Versa Cloud Gateways are also interconnected over the Versa Fabric, which Versa offers as a low-latency middle-mile connectivity offering. Versa Analytics provides historical and near-real-time reporting for network usage and monitoring, performance, and fault monitoring and other insights. SASE and Secure SD-WAN-specific analytics include a location map with real-time connectivity, live monitoring of path selection, and application usage per user and WAN link.

For deployment options, Versa offers a fully cloud-delivered solution, entirely on premises, or a blended combination of on premises and cloud delivered. The company offers a family of Versa CSG appliances, along with virtualized and containerized versions, and has a partnership with Dell to run the Versa SD-WAN on Dell VEP appliances. Customers can also run Versa SASE and Versa Secure SD-WAN on certified white-box appliances. The company has partnerships with a variety of third-party providers, including Azure API integration via vWAN, AWS Transit Gateway, and Google Cloud; third-party security service integrations with Zscaler, Netskope, Symantec, and Palo Alto Networks Prisma; and colocation providers Megaport, Mode, and Equinix.

As managed SPs and communications SPs are a key go-to-market channel for Versa, the company also offers Versa Titan, which is a simplified, cloud-delivered offering for partners with predefined settings for controlling multiple enterprise customer SASE and SD-WAN deployments. Versa supports customer integrations with existing on-premises or cloud-based security services too. Versa is the largest remaining start-up in the SD-WAN infrastructure market and has raised close to \$200 million with backing from a range of investors.

Strengths

- Versa's platform leverages what it calls single-pass parallel processing, which enables the company to provide a range of services via a multitenant cloud-based platform. It enables customers and partners to choose which components of the Versa SASE offering are deployed.
- Versa SASE and Secure SD-WAN are multitenant, which is popular with managed SPs and communications SPs that are able to centrally manage multiple enterprise customer deployments.
- Versa SASE and Secure SD-WAN run VOS in both the cloud and on premises, giving customers a consistent functionality whether it is managed on premises or via the cloud.
- Versa has a partnership with Dell to deliver SASE and Secure SD-WAN on Dell VEP appliances.

Challenges

- Versa has a wide range of optional features within its platform, which can make for a complex offering.
- Versa remains the largest of the original SD-WAN infrastructure start-up companies. The company's investors will likely look for an exit through an acquisition or initial public offering in the coming years.
- Versa does not have an Ethernet switch or WLAN access point (AP) offering.
- Versa, from its inception, has provided a range of natively integrated security tools, but the company's heritage is in networking more so than security, even though it has pivoted heavily toward SASE as a major value proposition. Versa also offers integrations with popular third-party security tools such as Zscaler and Palo Alto Networks.

Consider Versa When

Versa's configurable SD-WAN offering makes it applicable for a range of enterprise and SME customers. The company's multitenant capabilities make it a good fit for managed SPs and communications SPs. The company's cloud-native platform is also good for large enterprises that have an IT team that can act as an managed SP for their organization. The company's top vertical markets include finance, retail, healthcare, manufacturing, and government.

VMware

VMware is positioned in the Leaders category in the 2021 IDC MarketScape for worldwide SD-WAN infrastructure.

VMware's SD-WAN is built on technologies acquired in December 2017 from VeloCloud, one of the original start-ups in the SD-WAN market. VMware's SD-WAN portfolio sits within the company's Service Provider and Edge Business Unit, which packages SD-WAN and SASE cloud-based security products with a range of offerings for telecommunications SPs, including edge compute, telco core, and telco RAN solutions.

Core to the company's SD-WAN platform is the VMware Cloud Orchestrator, which is a cloud-delivered, multitenant, and multitiered platform for managing the company's network, security, and what it calls AIOps. The company's SD-WAN platform includes a series of distributed VMware SD-WAN Gateways, which are a network of POPs the company has built and will continue to increase in number. The gateways allow customers, if they wish, to connect any site to the nearest POP where the company hosts a security stack of zero trust network access solutions that enforce conditional access policies. Security services include a SWG, which is delivered in partnership with Menlo security, as well as an inline CASB; on the road map is to include the NSX-distributed firewall and DLP services at the gateway sites too.

The company offers a range of VMware SD-WAN Edge appliances, which can host third-party virtual network functions. Atop the VMware SD-WAN solution, the company offers Edge Network Intelligence (ENI), which is built on technology acquired by Nyansa. ENI offers visibility into the experience of users connecting to business applications. The solution also provides operational assurance for critical IoT devices if these devices deviate from performance or security baselines.

The company has six strategic pillars for its SD-WAN offering:

- Zero trust security via the company's cloud-web security services delivered via the Gateways
- Support for work from home/work from anywhere, specifically through integrations with VMware Workspace ONE and VMware Horizon and the VDI platform
- Multicloud integrations: The company has strong partnerships with Microsoft Azure, AWS, Zscaler, and other IaaS and SaaS vendors.
- Network visibility and analytics, including "self-healing" capabilities that build off the Nyansa technology and include a range of ML and AI-enhanced network automation tools for identifying and, as a road map item, providing automatic remediation of network issues in the WAN and some LAN components too
- Telco and 5G buildouts: Telcos are a significant route to market for VMware SD-WAN; in addition to enabling SPs to offer an SD-WAN, it offers a range of additional public and private 5G management tools for telcos.
- Edge computing, specifically running containerized applications on SD-WAN edge devices

Strengths

- VMware's SD-WAN platform has a strong heritage in the SD-WAN market because it is based off technology the company acquired from VeloCloud, which before the acquisition was one of the companies credited with initially developing SD-WAN technology.
- VMware is building a portfolio of cloud-based security tools that it will deliver from its SD-WAN Gateways, giving customers optimized connections into IaaS and SaaS, and a platform for hosting distributed security services including a CASB, URL filtering, and DLP.
- VMware has successfully leveraged communications service providers as an effective go-to-market channel, and VMware's broader efforts to build management offers for communications SPs beyond SD-WAN, including security and integrated core and RAN services, will make VMware's SD-WAN even more appealing for communications SPs in the future. The communications SP channel is becoming increasingly important for SD-WAN vendors, however.
- VMware has a portfolio of network visibility and analytics solutions from its Nyansa acquisition.
- VMware's SD-WAN has integrations with a variety of other management tools from VMware that make VMware's SD-WAN a strong choice for VMware customers and give the company significant opportunity to expand its SD-WAN customer base.
- VMware's work-from-home solutions, namely Anywhere Workspace, are well rounded to support remote workers, including using SD-WAN capabilities in the solution.

Challenges

- VMware has some integrations with campus LAN technologies, particularly around visibility, analytics, and management, but the company does not offer its own WLAN or LAN solutions, which could be a challenge for organizations that would prefer to use a single vendor across the WAN and LAN.
- VMware does not have a strong heritage in the routing, WAN optimization, or security market compared with other SD-WAN vendors, although it's been able to build up capabilities across all of these areas.
- VMware is still building out its network of POPs for its cloud-based security tools, some of which VMware rely on third parties.

Consider VMware When

VMware SD-WAN is a strong offering in the market and is also a good fit for customers that already use any number of VMware's popular IT management tools. Furthermore, many communications SPs already work with VMware, so customers that are looking for integrated connectivity and SD-WAN could look to VMware SD-WAN. Top vertical markets for VMware SD-WAN include retail, financial services, healthcare, industrial, and hospitality.

Vendor to Watch

Extreme Networks is worth considering for SD-WAN infrastructure, but the company did not meet our annualized revenue criteria for full analysis due to the acquisition of its SD-WAN technology closing in late 2021.

Extreme Networks

In September 2021, Extreme Networks closed its acquisition of the SD-WAN business unit from InfoVista named Ipanema. Extreme Networks has a portfolio of offerings for enterprise campus and

branch technologies including wireless and wired LAN solutions, along with a cloud-managed platform, among other products. The Ipanema SD-WAN could become a key part of the company's "Infinite Enterprise" vision, which focuses on distributed connectivity and consumer-centric experiences delivered at cloud scale. By purchasing Ipanema, Extreme Networks has an opportunity to build out a stronger LAN/WLAN + SD-WAN offering, which IDC refers to as the software-defined branch.

Ipanema's SD-WAN provides application visibility and control, allowing users to define end-user quality of experiences for applications on the WAN. Ipanema's SD-WAN dynamically controls each user session across multiple underlying network transports, allowing customers to tie business objectives to WAN routing policies. Ipanema is available in physical form factors or a virtual appliance. It includes native WAN optimization, encrypted IPsec VPNs, a cloud orchestrator, and integrations with secure web gateway providers.

Key to Extreme Networks' success in the SD-WAN market will be building out a channel for selling the SD-WAN solution, particularly with communications service providers, and selling the Ipanema SD-WAN into its existing customer base. Extreme Networks will also look to build stronger integrations across its cloud-managed campus and branch portfolio (ExtremeCloud), as well as build up security capabilities natively within the SD-WAN platform. With a variety of products across campus and branch networking technology, and by now adding an SD-WAN technology to its portfolio, Extreme Networks is a key vendor to watch in the SD-WAN infrastructure market in the years to come.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

This document pertains to SD-WAN infrastructure, which encompasses the infrastructure/products that constitute SD-WAN hardware and software offerings from vendors. SD-WAN infrastructure has the following capabilities:

- Provides automated management of hybrid WANs, which are defined as at least two WAN connections from each branch office that leverages two or more networks (MPLS, broadband internet, 4G/LTE, etc.)
- Includes a centralized, application-based policy controller with optional analytics for application and network visibility
- Includes a software overlay that abstracts underlying networks and an optional SD-WAN forwarder (routing capability) that together provide intelligent path selection across WAN links based on the application policies defined on the controller

As such, IDC's market sizing for SD-WAN infrastructure excludes all standalone routers and WAN optimization products that are not encompassed by "in use" SD-WAN deployments. IDC also excludes managed services (e.g., setup, operations, and support), connectivity, security, and leased line service costs (e.g., MPLS, broadband, and 4G/5G) when sizing the SD-WAN infrastructure market.

Strategies and Capabilities Criteria

This section includes an overview of the market-specific criteria that were used to assess vendors across two major categories: strategy and capability, as shown in Tables 1 and 2, respectively. IDC has identified these as the primary characteristics that vendors in the SD-WAN infrastructure market must take into consideration when crafting a future strategy and in leveraging existing capabilities to optimize their opportunities. Weightings are factored differently among strategy and capability criteria as determined by enterprise priorities based on IDC customer interviews and market studies of buyer needs along with IDC research on effective business practices required to optimize the value of SD-WAN infrastructure.

TABLE 1**Key Strategy Measures for Success: Worldwide SD-WAN Infrastructure**

Criteria Categories	Definition	Weight (%)
Functionality or offering strategy	<ul style="list-style-type: none"> ▪ SD-WAN portfolio that matches evolving business needs ▪ Product road map that covers key areas of future need ▪ Track record in achieving road map strategic objectives ▪ Specific offering road map ▪ Pricing and licensing model 	26.0
Other strategies	<ul style="list-style-type: none"> ▪ Organizational ▪ Ecosystem ▪ Security 	23.0
Delivery	<ul style="list-style-type: none"> ▪ Channel delivery ▪ Go to market ▪ Cloud-based delivery ▪ Methodologies 	17.0
Growth	<ul style="list-style-type: none"> ▪ Growth via existing customer base ▪ Customer growth ▪ Financial growth ▪ Geographical growth ▪ Adjacent portfolio growth ▪ Industry expertise growth 	23.0
R&D pace/productivity	<ul style="list-style-type: none"> ▪ Overall R&D strategy ▪ Thought leadership development ▪ R&D planning 	6.0
Financial/funding	<ul style="list-style-type: none"> ▪ Financial stability 	5.0
Total		100.0

Source: IDC, 2021

TABLE 2

Key Capability Measures for Success: Worldwide SD-WAN Infrastructure

Criteria Categories	Definition	Weight (%)
Functionality or offering	<ul style="list-style-type: none"> ▪ Essential capabilities ▪ Additional integrated product features ▪ Adjacent networking technologies or features ▪ Product delivery ▪ Native security ▪ Partner-led security ▪ Advanced management capabilities ▪ Product-specific features 	44.0
Partner programs	<ul style="list-style-type: none"> ▪ Integration with colocation, middle-mile, or software-defined cloud interconnection providers 	2.0
Go to market	<ul style="list-style-type: none"> ▪ Partner programs ▪ Strength of channel 	12.0
Customer service delivery	<ul style="list-style-type: none"> ▪ 24-hour coverage ▪ Tiered support service — basic to premium ▪ Geographic footprint of support 	11.0
Range of services	<ul style="list-style-type: none"> ▪ Adjacent services (e.g., implementation and consulting services) 	7.0
Pricing model or structure of product/offering	<ul style="list-style-type: none"> ▪ Pricing models offered ▪ Pricing model of additional features 	6.0
Total cost of ownership (TCO)	<ul style="list-style-type: none"> ▪ Assessment of TCO ▪ Business value of the SD-WAN offer 	8.0
Other capabilities	<ul style="list-style-type: none"> ▪ Marketing and thought leadership 	4.0
Other	<ul style="list-style-type: none"> ▪ Mergers and acquisitions 	6.0
Total		100.0

Source: IDC, 2021

LEARN MORE

Related Research

- *Worldwide vCPE/uCPE Forecast, 2020-2025: Emergence of SD-Branch and NaaS Provides Opportunity for Communications Service Providers* (IDC #US48177321, September 2021)
- *Extreme Sets Sights on SD-WAN with Purchase of Ipanema* (IDC #lcUS48181821, August 2021)
- *Worldwide SD-WAN Infrastructure Market Forecast, 2021-2025* (IDC #US47272921, July 2021)
- *Five Key Trends Driving the Enterprise Networking Market in 2021* (IDC #US47488821, March 2021)
- *Five Major Datacenter and Multicloud Networking Trends in 2021 and Beyond* (IDC #US47498321, March 2021)
- *Five Key Carrier Network Infrastructure Trends to Watch in 2021* (IDC #US47479421, February 2021)
- *Future of Enterprise Networking: Emergence of the New Normal* (IDC #WC20210202, February 2021)
- *Branch of One: Evolution of the Enterprise Network Edge for Remote Workers* (IDC #US47476821, February 2021)

Synopsis

This IDC study provides an assessment of the capabilities and business strategies of 12 vendors in the worldwide SD-WAN Infrastructure market for 2021.

"The SD-WAN infrastructure market continues to be one of the fastest-growing segments of the networking market, driven by the significant value this technology enables for organizations. As enterprises look toward the future state of their networks, they're increasingly looking for technology that helps optimize connectivity to cloud-based applications, while also exploring ways to integrate security functionality directly into their networks," says Brandon Butler, IDC research manager, Enterprise Networks. "Today's SD-WAN products increasingly achieve these goals while also providing detailed visibility and analytics into WAN health, application, and user performance. These advancements will continue to make SD-WAN a key technology for enterprises as they look to build out their digital transformation journeys in 2022 and beyond."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2021 IDC. Reproduction is forbidden unless authorized. All rights reserved.

