

As enterprises continue to rapidly adopt SD-WAN technologies, they are looking for SD-WAN solutions that incorporate three key features: integrated security, multicloud connectivity, and application reliability.

Three Key Requirements of Enterprise SD-WAN: Integrated Security, Multicloud Connectivity, and Application Reliability

April 2021

Written by: Brandon Butler, Senior Research Analyst, Enterprise Networks

Introduction: Enterprise-Grade SD-WAN

The software-defined wide area networking (SD-WAN) market is at an inflection point. This powerful technology has moved beyond initial deployments and proofs of concept and graduated to full-scale, enterprisewide adoption.

The maturation of the SD-WAN market has resulted in enterprises gaining significant value from SD-WAN deployments, and many are now looking to standardize on software-defined principles for managing their WAN. At the same time, three key, interwoven requirements of an SD-WAN platform have crystallized to make this technology enterprise grade. These requirements reflect how enterprises want to architect their networks and the business priorities of organizations. They consist of the following: flexible security consumption models that meet business and compliance requirements; multicloud connectivity as a foundational component of SD-WAN technology; and the ability of an SD-WAN platform to guarantee high levels of application reliability, no matter where the application is hosted.

Meanwhile, COVID-19 changed many dynamics in enterprise networking. The global pandemic forced organizations to reconsider how their WANs support users who access the network from more distributed sites — whether a traditional campus or branch, at home, or from another remote location. SD-WAN platforms must be agile enough to support these various deployment options. In conjunction with more ways to deploy SD-WAN, customers are also exploring new modes of consuming SD-WAN infrastructure via more flexible consumption licensing and procurement models. This trend is giving rise to networking as a service, and SD-WAN is a key component.

AT A GLANCE

WHAT'S IMPORTANT

SD-WAN's rapid rate of enterprise adoption has been driven by a handful of important factors, including:

- » Integrated management of multiple WAN connectivity types, including MPLS, broadband, and LTE
- » A centralized application policy controller that enables dynamic path selection across application links

Next-generation SD-WAN solutions should focus on integrated security, multicloud connectivity, and application reliability.

Nonetheless, enterprises that adopt SD-WAN platforms will reap the greatest benefits from the technology (see Figure 1).

FIGURE 1: **Key Benefits of Cisco SD-WAN Adoption**



45%

Reduced app latency



38%

Lower 5-year cost of operations



33%

More efficient WAN management

n = 8

Source: IDC's Business Value of Cisco SD-WAN Solutions, April 2019

SD-WAN Security: Flexible Consumption Models

Security is a foundational requirement for any enterprise-grade technology. As threats and attack vectors simultaneously continue to increase, staying ahead of security in the WAN and beyond requires a robust set of tools. Customers should have choice in how they deploy security that is integrated closely with the SD-WAN. Security may be delivered on premises in SD-WAN routers/other infrastructure or in a cloud-hosted Secure Access Service Edge (SASE) framework, depending on the business requirements and compliance needs of an enterprise.

Tools such as next-generation firewalls, intrusion prevention systems, role-based access controls, URL filtering, and malware protection have become key for on-premises security. Together, these capabilities provide secure WAN access and help enterprises meet compliance demands onsite while offering constant protection against internal and external threats from a range of sources. Other enterprises may prefer to use a SASE framework with security tools such as a secure web gateway (SWG), firewall as a service (FWaaS), cloud access security broker (CASB), zero trust network access (ZTNA), and DNS layer security. These cloud-based tools provide a flexible way to deliver protection to users anywhere they access the network and cloud applications.

Whether security is managed on premises or in the cloud, enterprises are looking for certain fundamentals in a secure SD-WAN platform. In the control plane, enterprises should be operating on a zero trust model where every user, device, and data traffic flow is authenticated and monitored on the network. The management plane is where role-based access controls and access control lists are established and enforced. Within the data plane, enterprises are looking for security controls such as next-generation firewalls, intrusion prevention systems, and intrusion detection systems that can be managed on premises or from the cloud. In addition, the hardware and firmware at the data plane need to be able to withstand attack as the number of advanced persistent threats (APTs) grows.

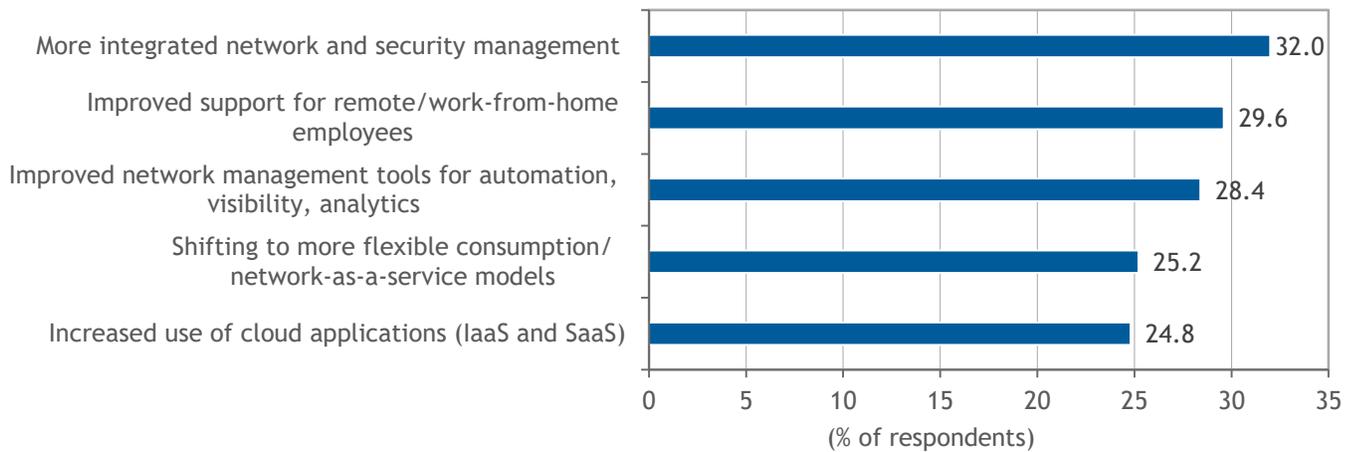
"The fact that we can do end-to-end segmentation with Cisco SD-WAN has allowed us to build out a framework to put devices on the network that maybe we don't fully trust but that the business wants while still securing the network."

Cisco SD-WAN customer from an IDC Business Value study sponsored by Cisco

Combined, these fundamentals of SD-WAN security provide a robust, secure platform. Enterprises are keenly interested in more flexible integrations between network and security tools given the network's unique ability to secure enterprise environments. Figure 2 shows survey data reinforcing this point: When IDC asked enterprises what changes that were put in place during COVID-19 will become permanent, more integrated network and security management topped the list.

FIGURE 2: **More Integrated Network and Security Management Is a Key Enterprise Priority**

Q What are the most important changes to your network operations in 2020 in response to COVID-19 that will become permanent changes to your organization?



n = 250 U.S. respondents

Note: Multiple responses were allowed.

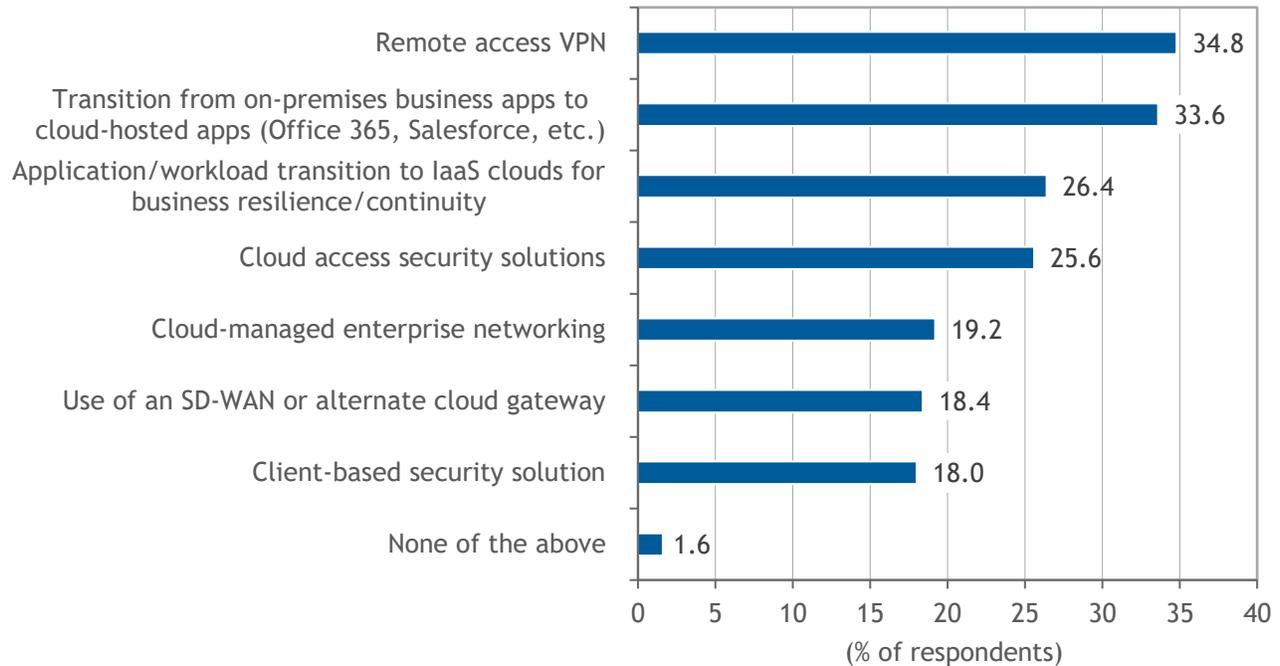
Source: IDC's Enterprise Networking: Emergence of the New Normal Survey, December 2020

Enabling Secure and Efficient Multicloud Connectivity

One of the chief drivers of SD-WAN adoption among enterprises is enabling secure, reliable, and high-performance connections to public cloud platforms. Usage of public cloud platforms has become pervasive among enterprises, which is a trend that was accelerated during the COVID-19 era. Figure 3 shows survey data indicating the most important new technologies enterprises have used since the pandemic. Secure connectivity topped the list, followed by the transitioning of business applications and workloads to the cloud. This data reinforces why connectivity to multiple public clouds is so critical for SD-WAN deployments.

FIGURE 3: **COVID-19 Has Accelerated the Enterprise Journey to the Cloud**

Q Since the COVID-19 pandemic began, what have been the most important new technology solutions your organization has taken advantage of for work-from-home (WFH) users?



n = 250 U.S. respondents

Note: Multiple responses were allowed.

Source: IDC's Enterprise Networking: Emergence of the New Normal Survey, December 2020

Some challenges enterprises face in connecting to these cloud platforms are as follows:

- » A lack of control over how traffic is routed to public cloud platforms
- » Difficulty determining the quality of WAN connection to cloud platforms
- » Complexity in coordinating traffic from multiple geographically disparate sites to cloud platforms

SD-WAN platforms can specifically address these concerns. The key is having a platform that allows enterprises to centrally design, provision, and manage multicloud networks. SD-WAN platforms should offer customers on-ramps to public cloud platforms, allowing a centralized controller to provide real-time, automatic dynamic path selection of traffic across multiple WAN links to find the most efficient route to any destination across public or private clouds.

SD-WAN platforms should also provide enterprises with visibility into the quality of the links via an easily understood link-quality score. Customers should also have the option to deploy SD-WAN platforms at colocation facilities to aggregate traffic from multiple sites before directly connecting it to the cloud. In addition, SD-WAN platforms should give users the ability to create a virtual dedicated interconnect from branches to the cloud via cloud interconnect partners to enhance availability and reliability of connectivity to multiple cloud providers. Combined, these qualities make SD-WAN an essential tool for securely and reliably enabling cloud-based usage.

SD-WAN for Application Optimization and Reliability

Business applications are only as good as the network connection that delivers them to users. Enterprises are increasingly relying on applications delivered via a network connection for mission-critical tasks. It's crucial that these connections have low latencies and high bandwidth.

SD-WAN platforms enable enterprises not only to optimize application traffic but also to increase the reliability of the applications, maintain high quality of service levels, and monitor application performance. The key enabler of this functionality is having visibility into what is happening at the application level as well as on the network. To do this requires a platform that's able to monitor both the underlay components and the overlay components, with the ability to conduct real-time analytics. Next-generation SD-WAN platforms go a step beyond just providing analytics into what is happening across the network — they help proactively solve problems. Machine learning—and artificial intelligence—enhanced automation platforms can instantaneously detect a performance degradation or security incident based on these analytics. They also can provide guided steps to remediate the issue or be programmed to automatically take actions to fix the issue before it impacts any user.

The visibility into what's happening on the network and the functionality to automate responses to problems have become key criteria for SD-WAN because together they enable network agility. When the business needs to onboard a new third-party, cloud-hosted application, the networking team should be an enabler rather than a roadblock. Modern microservices-based applications are increasingly made of components that are hosted across multiple on- and off-premises locations. SD-WAN becomes an integral tool for managing the seamless delivery of these applications to a global set of users.

In addition to visibility and analytics, SD-WAN platforms are also now supporting broadened connectivity methods, such as LTE and, in the future, 5G. As enterprises look toward an increasingly wireless WAN edge, SD-WAN platforms will be a key enabler.

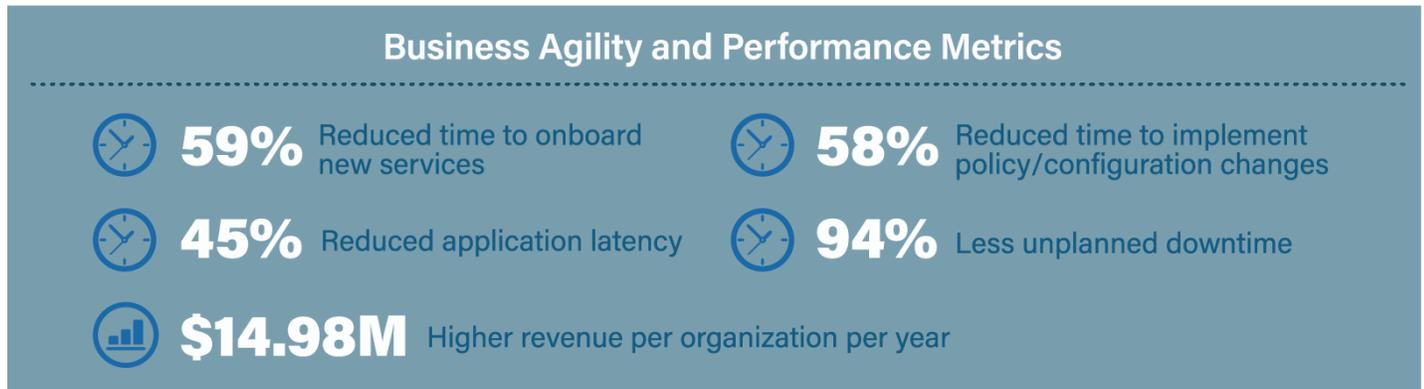
"Making network changes has been a huge change with Cisco SD-WAN. It used to be that implementing network changes to support internet-based services took many months. Now, the network provides agility where services can be deployed in the cloud immediately."

Cisco SD-WAN customer from an IDC Business Value study sponsored by Cisco

Considering Cisco SD-WAN Solutions

An IDC Business Value study found that Cisco SD-WAN solutions enable a range of agility benefits, along with less downtime and reduced application latency, resulting in an overall higher revenue per year for organizations that adopt this technology, as shown in Figure 4.

FIGURE 4: *SD-WAN as an Enabler of Agile Operations: Business Value Benefits of Cisco SD-WAN*



n = 8

Source: IDC's Business Value of Cisco SD-WAN Solutions, April 2019

Cisco SD-WAN is a cloud-delivered overlay WAN architecture that fits in with a multidomain management architecture and enables a multicloud enterprise network. Cisco SD-WAN includes integrated security functions, such as microsegmentation across layers of the stack, a firewall, secure web gateway, and the ability to have common role-based and access control policies across the WAN, datacenter, enterprise campus, and cloud. The platform also delivers powerful analytics and assurance capabilities that provide visibility into what's happening across the entire network and automated remediation capabilities to fix problems before they impact users.

Cisco SD-WAN can be consumed as a virtual, cloud, or physical appliance and managed in-house or by a managed service provider. Cisco SD-WAN based on Viptela and vManage technology allows for advanced routing and flexible deployment options, while Cisco SD-WAN powered by Meraki is an all-in-one SD-WAN and security platform for lean IT shops.

Challenges

SD-WAN is one of the fastest-growing segments of the network infrastructure market, which has led to a crowded playing field for SD-WAN vendors. However, the SD-WAN market will remain competitive, and enterprises will have a multitude of vendors to choose from. Cisco's strong technology platform and large base of customers will help the company differentiate itself from other vendors in this space.

Conclusion

As enterprises continue to adopt SD-WAN solutions, the buying criteria for an enterprise-grade SD-WAN platform are crystallizing. SD-WAN deployments today are about more than just the technology: They're about enabling an agile and dynamic business that can support changing business requirements and the employees, regardless of their location, who drive the business. New ways of procuring SD-WAN technology will be an important enabler of having more cloudlike scalability and management of the network.

Meanwhile, integrated security, multicloud connectivity, and application reliability will continue to be the core driving features of an enterprise-grade SD-WAN platform. When executed correctly, these three pillars combine to provide enterprises with an SD-WAN platform that enables comprehensive connectivity to any endpoint.

About the Analyst



Brandon Butler, Senior Research Analyst, Enterprise Networks

Brandon Butler is a Senior Research Analyst with IDC's Network Infrastructure group covering Enterprise Networks. He is responsible for market and technology trends, forecasts, and competitive analysis in Ethernet switching, routing, and wireless LAN, and he closely follows segments such as SDN and SD-WAN.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2021 IDC. Reproduction without written permission is completely forbidden.