Secure SD-WAN Buyer’s Guide

5 Key Considerations to
Help You Choose

Introduction

Companies across industries rapidly accelerated their digital transformations in response to the global pandemic. Now, enterprises are under immense pressure to adopt next-gen technologies such as software-defined wide area networks (SD-WANs) to meet the needs of distributed networks, applications, and a hybrid workforce.

This guide will help you understand SD-WAN technology's key characteristics and advantages and what to look out for when choosing an SD-WAN solution, including questions to ask vendors. It also provides access to supporting research.

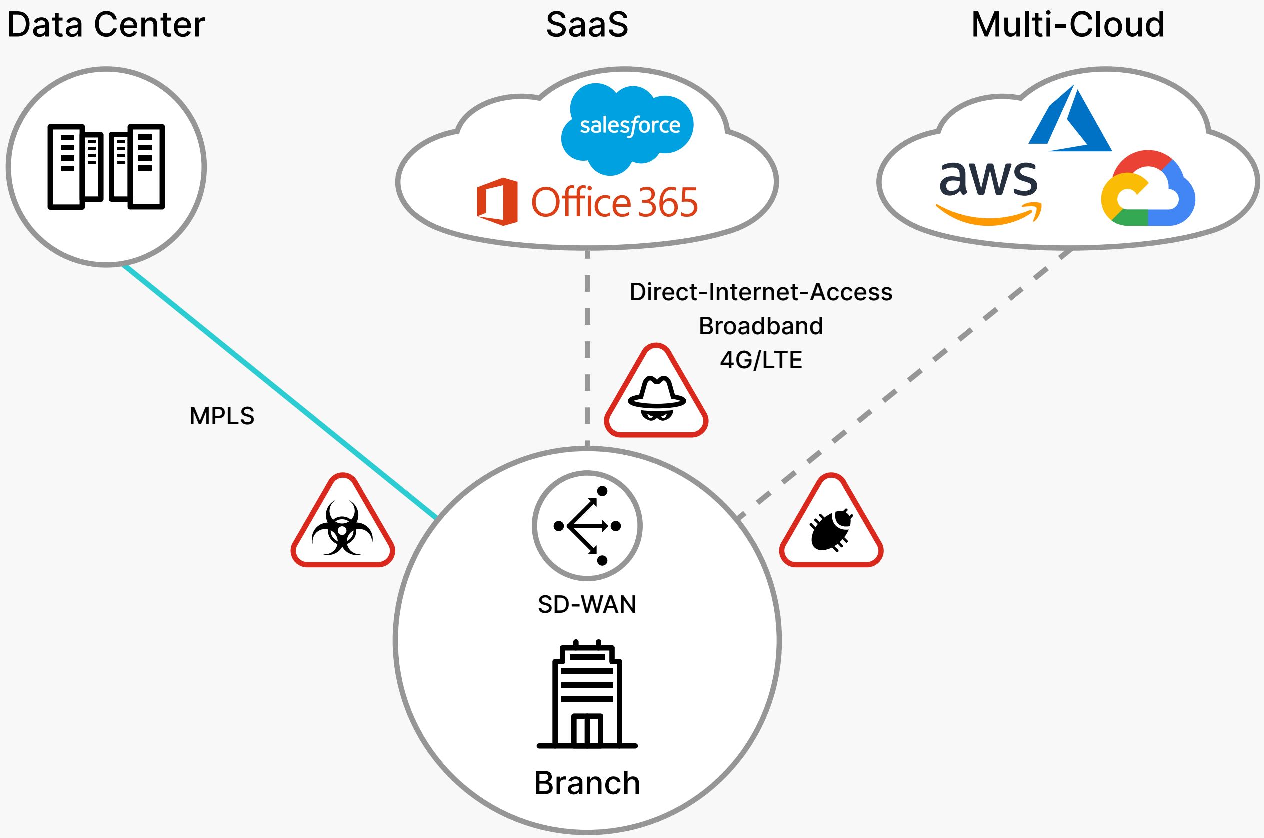
What Is SD-WAN?

SD-WAN is a software-defined approach to transforming the WAN that helps accelerate the adoption of cloud-based applications and other digital transformation initiatives. SD-WAN creates overlay tunnels that can handle a variety of connections and dynamically move traffic over the best transport available. It can provide both redundancy and much more capacity using lower-cost links.

When time-to-installation and time-to-delivery are considered, SD-WAN solutions cost significantly less than MPLS overall. SD-WAN provides end-to-end visibility and centralized management to help organizations manage their networks more efficiently.

SD-WAN products can be managed directly by enterprises or embedded in a managed service offering. The best SD-WAN solutions offer converged networking and security managed by one centralized management system, allowing sites to be brought on quickly without requiring networking or security experts to be on-site for installation.

What Is Software Defined-WAN (SD-WAN)?



5 Key Considerations When Selecting an SD-WAN Solution for Your Enterprise

1 SD-WAN vs. Traditional WAN for Digital Transformation

As a virtualized service that manages enterprise network connectivity, SD-WAN technology has revolutionized how end-users connect to their remote cloud applications. Unlike traditional router-centric WANs, the SD-WAN can intelligently steer traffic based on applications that can be hosted in on-premises virtual data centers (VDCs), private or public clouds, Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS) platforms, such as Microsoft 365, Dropbox, Workday, and Salesforce.com.

As a modern digital transformation technology, SD-WAN offers flexibility, agility, cost savings, and high performance. It addresses the serious challenges posed by traditional WANs that can cause a variance in the time delay, such as jitter, among data packets in the network, such as a disruption of data traffic flow and latency, which slows down the round-trip time it takes for a data packet to be sent and for it to get a response.

SD-WAN addresses these serious challenges by routing network traffic, which improves the performance of network nodes and applications. According to Digital Carbon, from 2018 to 2023, the network market will grow annually by 30.8% due to SD-WAN's crucial role in digital transformation.

2 Does Your Company Need SD-WAN, and Are You Ready for It?

Organizations have relied on WANs for decades to establish connectivity with their branch offices and ensure uninterrupted connectivity to remote locations. However, they have had to invest significantly in WAN infrastructure with heavy maintenance costs to do so. Does this sound familiar?

At the same time, organizations are migrating to cloud solutions. However, network configurations in the cloud are very complex due to the Internet of Things (IoT) and distributed and decentralized environments.

With cloud applications, traffic behavior on the network differs from that of traditional enterprise resource planning (ERP) software. For example, when cloud traffic is forced to backhaul through a data center, users experience slow response times and network congestion.

Furthermore, bandwidth drain due to videoconferencing and cloud applications is another big issue. Site abandonment also presents a significant challenge when customers do not wait for a page to load. Not only that, if you want a network configuration at a new branch location, a traditional WAN requires a technician to travel to that location for router or other network configurations.

SD-WAN can be a perfect solution for your organization if you face similar issues. SD-WAN technology uses virtualization and software services to develop a modern network that delivers cost-effective, simpler, and faster business connectivity to support digital transformation.

3 SD-WAN Solution Options for IT Managers: DIY, Co-Managed or Managed Services

As an IT manager, you need centralized management and zero-touch provisioning to bring your branches online or decommission remotely in just a few hours or days.

Do-it-yourself (DIY) provisioning means companies use their in-house IT staff to deploy the SD-WAN technology. The DIY approach may burden existing resources. The benefit of DIY is that you can build custom solutions according to your specific needs.

Alternatives to DIY include SD-WAN-as-a-Service or co-managed SD-WAN, in which the end-user and managed service provider (MSP) control, maintain, and modify the SD-WAN solution through a cloud-based interface. With these services, end-users can access the most up-to-date features and pay only for what they use.

On the contrary, managed SD-WAN involves outsourcing, whereby an MSP hired by the company deploys and manages the SD-WAN solution. The managed SD-WAN is appropriate for businesses focusing on driving IT value with partners and maintaining a lean IT department.

4 Overcoming Integration Challenges with Existing Network Infrastructure

There are right ways and wrong ways to deploy an SD-WAN. Implemented incorrectly, an SD-WAN solution may pose serious integration challenges within the organization's technology ecosystem. For example, many SD-WAN solutions may not offer seamless integration with cloud providers, such as AWS and Microsoft Azure, or SaaS, such as Microsoft Office 365.

As well, cybersecurity is a prerequisite for organizations considering SD-WAN solutions. Unfortunately, most SD-WAN solutions don't offer robust integration with security tools. Under such circumstances, companies cannot deploy integrated security across distributed networks, including branches and remote office locations.

To overcome security issues due to lack of integration, it's critical to choose a robust and proven SD-WAN solution that can connect with your existing infrastructure and operating system, support all security features, enable a secure networking approach, and weave the SD-WAN into a single management console. Integration can significantly decrease threat remediation time from months to hours or even minutes in case of a cyberattack.

5 Features to Focus on When Choosing an SD-WAN Solution

To enable rapid digital transformation, many enterprises are leveraging SD-WAN solutions to simplify their management and operation of the WAN, increase network visibility, and reduce network complexity and costs. The following sections elaborate on the essential features to consider when evaluating SD-WAN solutions.

Fortinet Secure SD-WAN with NGFW, ZTNA, and Self-Healing Capabilities

Fortinet, named a **Leader in the 2022** Gartner® Magic Quadrant™ for SD-WAN, offers fast, flexible, scalable, and secure SD-WAN, whether on-premises or in the cloud. Additionally, integrating Fortinet's SD-WAN solution within FortiGate Next-Generation Firewalls (NGFWs) offers customers a huge advantage over firewalls that don't offer SD-WAN capabilities.

Transport independence
The SD-WAN must encompass high-speed bandwidth across multiple kinds of transport, such as the internet, MPLS, 3G, 4G, LTE, and 5G.

Path control
The SD-WAN must be able to utilize active paths for bandwidth efficiency, failover, and resiliency.

Security
The SD-WAN must ensure security across each branch location and deploy an integrated, next-gen firewall that offers antivirus, antimalware, data loss prevention, IPS, IDS, sandboxing, and URL and content filtering.

Encryption
SD-WAN creates an end-to-end encrypted tunnel over the broadband between headquarters and branch locations. Companies should use SD-WAN to encrypt WAN traffic and ensure it encrypts WAN traffic effectively.

Application optimization
The SD-WAN solution must optimize applications, including video and voice traffic and SaaS applications. Also, it must be intelligently able to identify thousands of applications and steer them dynamically on the appropriate link.

Automation and orchestration
The SD-WAN must automate mundane and repetitive networking tasks. Moreover, the solution should orchestrate troubleshooting, monitoring, reporting, and other features across the WAN.

Zero-touch deployment
The deployment should be effortless. For example, even a nontechnical person should be able to configure the out-of-the-box product in the branch office.

Microsegmentation
The microsegmentation feature is also essential as it restricts cybercriminals’ activities by limiting their lateral movement.

Scalability
The solution must be able to scale to support any size environment. Organizations with thousands of sites need a solution that can perform at high scalability.

Business continuity
In case of a cyberattack, the SD-WAN solution must help support business continuity by ensuring that your critical systems, networks, and applications are as effective as possible. To accelerate risk mitigation, look for integrated security with AI-powered threat intelligence and a unified view for network operations center (NOC) and security operations center (SOC) teams.

What Are the Pitfalls to Avoid When Deploying SD-WANs?

Like any other modern innovation, SD-WAN solutions may have some limitations. The following are common SD-WAN deployment challenges.

Network efficiency

Although SD-WAN offers secure access to cloud solutions, not every SD-WAN vendor can meet the same criteria. Some SD-WAN solutions cannot ensure end-to-end quality of service (QoS), making it difficult for IT teams to prioritize end-to-end cloud applications.

Inadequate security

If the SD-WAN security is inadequate, it can expose your network to data breaches. For example, when an SD-WAN lacks a built-in NGFW with IPS, DLP, URL, and DNS filtering capabilities, it is vulnerable to attacks. A secure SD-WAN is easily deployed with robust security when integrated with an NGFW.

More importantly, a secure SD-WAN—deployed correctly with a zero-trust network access (ZTNA) application gateway—protects applications from the attack surface and data breaches.

Multivendor devices

After the SD-WAN deployment, a single console will provide a uniform view of your network from a vendor’s management portal. The problem occurs (a lack of transparency) when network analysts assess issues between other vendors’ devices that have to interface with SD-WAN devices.

6 Questions to Ask Your SD-WAN Vendor and Why They Matter

1 How does the SD-WAN support secure access service edge and SD-Branch?

Software-defined branch (SD-Branch), secure access service edge (SASE), and SD-WAN are related to secure edge networking and deal with the challenge of managing an agile, resilient, and secure network of geographically distributed locations. When you choose your SD-WAN solution, you need to ensure that it supports SASE and SD-Branch.

SD-Branch is the next-gen branch networking strategy that ensures a tight integration across the entire infrastructure SD-WAN, LAN, WLAN, and WWAN on all levels of hardware, software, and management.

2 How can SD-WAN help improve my organization's security posture?

SD-WAN can help improve your organization's security posture by providing integrated security with embedded SSL decryption, URL filtering, malware sandboxing, intrusion prevention, IP Security (IPsec), VPN tunnels, microsegmentation, and NGFWs.

3 How does the SD-WAN help in reducing network costs?

SD-WAN can significantly reduce network costs with minimal and less expensive hardware. It also reduces costs through flexibility in the WAN. In addition, it reduces bandwidth costs and dependency on expansive MPLS. Furthermore, SD-WAN technology enhances operational efficiency by simplifying and automating Days 0, 1, and 2.

4 How can the SD-WAN solution simplify network and design complexities?

SD-WAN solutions with integrated security should simplify network infrastructure as a single platform for global services and connectivity. SD-WAN also eliminates design complexities.

5 How scalable is the SD-WAN solution?

Organizations with thousands of distributed sites want a high-performing and scalable SD-WAN solution. Also, as the solution inspects encrypted traffic, it must do so without performance degradation.

6 How does the SD-WAN solution provide visibility at the application and user levels?

SD-WAN allows you to manage your business-critical environment and extends end-to-end visibility. In addition, this solution provides a single pane of glass, enabling complete visibility of SD-WAN’s connectivity status, resource allocation, and QoS.

Determining the ROI and Future-Proofing Your SD-WAN Investments

SD-WAN dramatically increases your return on investment (ROI)—often in double digits within a few months of deployment—by enhancing IT performance, efficiency, and agility. In contrast to WAN, SD-WAN is a modern digital transformation technology that reaps numerous benefits for enterprises, such as:

- Robust security
- Application-driven technology
- Centralized control, simplified management
- Optimized cloud connectivity
- Improved network performance
- Easy to deploy and cost-efficient

SD-WAN technology helps future-proof your environment. For example, 5G and IoT will test the infrastructure by bringing numerous devices, apps, and data volumes to bear on your network and resources. However, knowing what to look for in an SD-WAN solution and asking vendors the right questions is crucial to success.

Forrester Total Economic Impact™ Study on the Value of Fortinet Secure SD-WAN

A case in point, Fortinet commissioned Forrester Consulting to conduct a Total Economic Impact (TEI) study to analyze the value that enterprises can achieve by deploying Fortinet Secure SD-WAN. Forrester Consulting interviewed customers in multiple industries with sites all over the world to examine network and security impacts on businesses.

Forrester TEI Study Covered Enterprises in Multiple Industries and Regions

Interviews

Role	Industry	Region	Revenue	Employees	Sites
CTO solution services	Retail	Asia HQ, global	$13 billion	16.000	8,500
Global connectivity services director	Manufacturing	North America HQ, global	$17 billion	133,000	1,000
Global lead network architect	Financial services	Europe	$18 billion	86,000	2,500
Senior network engineer	Healthcare services	North America	$1.7 billion	3,500	750

To glean the results of the study, watch the webinar or download the full report for the details. The insights can help you:

- Engage with decision-makers
- Explore primary research with peer data and feedback
- See the value Fortinet Secure SD-WAN brings to your organization

Key Findings of the Forrester TEI Study

Forrester has determined the following three-year impact of Fortinet Secure SD-WAN:

ROI

300%

Reduction in the number of network disruptions

65%

Payback

8 months

Increase in productivity of security and network teams

50%

	Retail	Manufacturing	Financial Services	Healthcare Services
Location	Asia HQ, global	North America HQ, global	Europe	North America
Revenue	$13 billion	$17 billion	$18 billion	$1.7 billion
Employees	16,000	133,000	86,000	3,500
Sites	**8,500**	**1,000**	**2,500**	**750**

Fortinet Secure SD-WAN

Following are the unique features and benefits of Fortinet Secure SD-WAN:

Integrated security

- Universal ZTNA Application Gateway (to control access)
- Seamless transition to SASE and SD-Branch architecture
- AI-powered, integrated advanced security
- Self-healing: WAN remediation techniques (FEC and packet duplication)

Centralized management

- User-friendly, centralized management console
- End-to-end visibility, analytics, and reporting
- Centralized network orchestration

Efficient network operations

- Agility, scalability, and high performance
- Advanced routing
- Operational efficiencies via deep analytics and automation

Easy deployment

- Multi-cloud on-ramp
- Zero-touch provisioning
- Advanced RMA and Professional Services

If you are planning to deploy SD-WAN at your organization, contact a Fortinet SD-WAN expert who can help you choose a solution that meets enterprise security and network efficiency improvement demands.

Call toll-free in the U.S.:
+1-866-868-3678
U.S. Federal Government Sales:
+1-833-386-8333
Canada Sales:
+1-833-308-3247

www.fortinet.com

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

August 8, 2023 11:12 AM

2256851-0-0-EN