SD-WAN Toolkit

FORTINET

Table of Contents

Unlocking the Secure WAN Edge:
10 Essential SD-WAN Transformation Capabilities 3

Required Capabilities for Effective and Secure SD-WAN:
The Network Leader's Guide 5

Secure SD-WAN Customer Success Stories:
Transforming and Securing the Networks of Global Enterprises 11

FORTINET

CHECKLIST

Unlocking the Secure WAN Edge: 10 Essential SD-WAN Transformation Capabilities

While software-defined wide area networks (SD-WANs) offer major performance and convenience advantages over the traditional WAN, these benefits come at the expense of centralized security from backhauling traffic through the organization's main data center.

Vulnerabilities associated with an expanding branch network attack surface, increasing infrastructure complexity, and a rapidly evolving threat landscape call for secure networking—namely, deep integration between networking and security capabilities at a platform level. Effective SD-WAN also requires sophisticated management and orchestration capabilities for automatically selecting the best network paths based on contextual factors such as the specific application in use, business priorities, and security risks.

10 Essential SD-WAN Capabilities

Over two dozen vendors currently offer some form of SD-WAN, but only 14 are recognized in the 2023 Gartner Magic Quadrant. But in many cases, comprehensive full-stack security is not integrated into the solution—leaving the network vulnerable to attack or requiring the purchase of additional security devices. When doing initial exploration of SD-WAN, network engineering and operations leaders can use the following checklist of questions to determine which solution is best:

☑ **Risk exposure**
How will my risk posture change if I adopt this SD-WAN solution?

☑ **Threat protection**
Regulatory bodies in some countries require compromise assessments. These authorities understand today's enterprise security challenges and want to ensure businesses are working from a proverbial clean slate, understanding potential risks before any damage can ensue.

☑ **Compliance**
Does the solution support all of the applicable regulatory requirements for industry standards and data privacy obligations, including tracking, auditing, and reporting functions?

☑ **Orchestration**
Does the solution offer automated capabilities for application awareness and path intelligence to select the best network connections based on changing variables?

☑ **Management**
Can the solution provide networkwide management and automation, be easily deployed, and remotely managed (via the cloud)?

☑ **Monitoring**
Can the solution offer comprehensive monitoring of device, link, path, and application performance to optimize user experience and simpify operations?

☑ **Total cost of ownership**
Is there an operational cost to implementing the SD-WAN solution? If so, what is it?

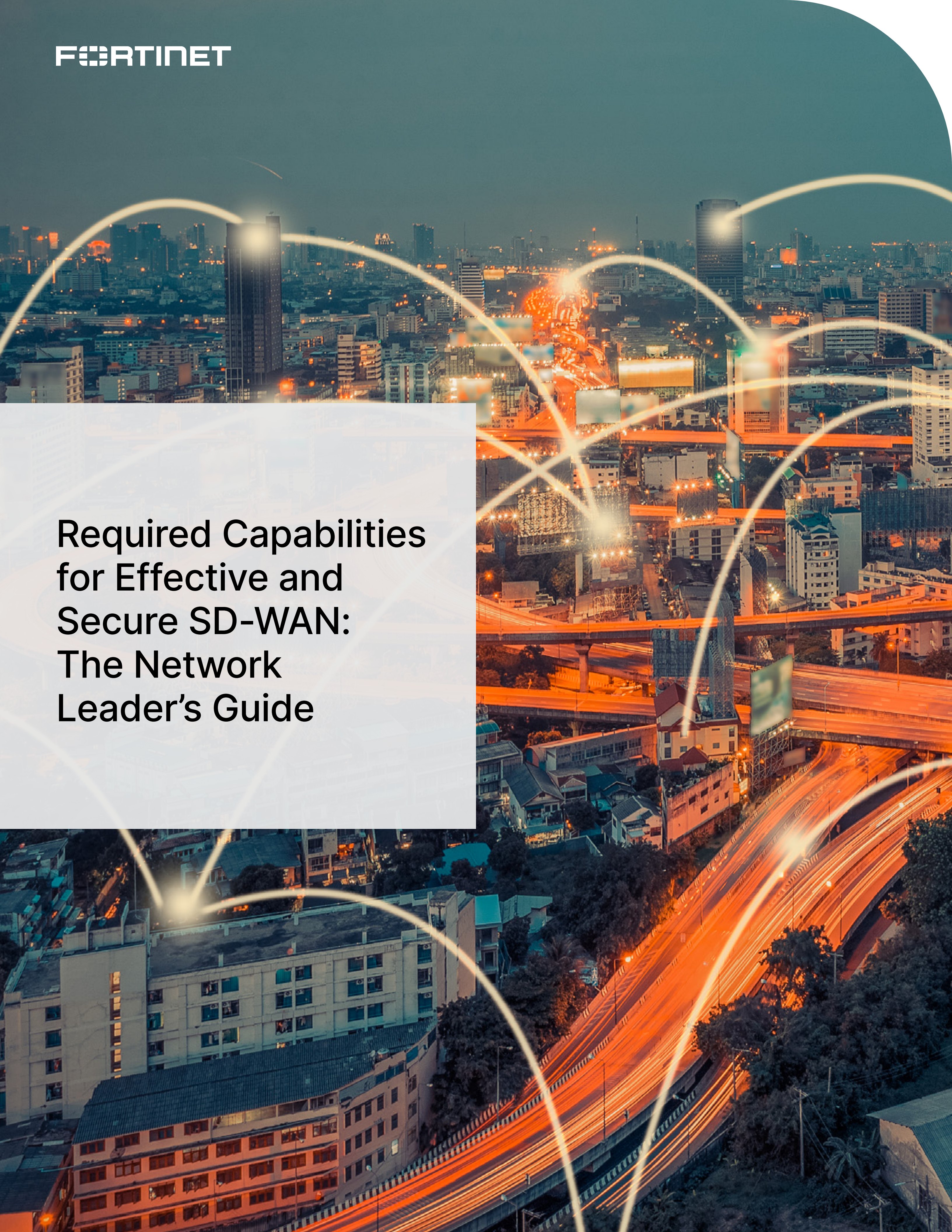
☑ **Third-party validation**
Has the solution been thoroughly tested and recommended by independent industry experts?

☑ **SASE**
Is the SD-WAN solution capable of supporting single-vendor SASE?

☑ **SD-Branch**
Can the SD-WAN solution provide migration to SD-Branch with tight integration on hardware, software, and management levels?

An effective SD-WAN solution offers distributed organizations the chance to solve networking and security problems of traditional WAN at the same. But in order to achieve that, network engineering and operations leaders should carefully compare the comprehensive capabilities of competing products against the full set of their solution needs.

FORTINET



Required Capabilities for Effective and Secure SD-WAN: The Network Leader's Guide

Executive Overview

There are three main trends driving organizations to replace outdated wide area networking (WAN) infrastructures with a secure software-defined WAN (SD-WAN) solution.

- Digital acceleration that leverages Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) increases traffic demands, cost, and performance bottlenecks of multiprotocol label switching (MPLS) connectivity over traditional WAN infrastructures.
- The work-from-anywhere (WFA) model, meant to be a short-term fix at the start of the pandemic, has become the new normal. Organizations need to ensure remote workers have secure, reliable access to all corporate resources.
- Cybercriminals are busier than ever, and innovations in Cybercrime-as-a-Service make it fast and easy for unsophisticated attackers to launch very sophisticated attacks.

When considering SD-WAN solutions, there are three key requirements to look for to address these trends. An effective solution will offer integrated capabilities needed to enable efficient management and operations, excellent quality of experience (QoE) for both end-users and IT staff, and comprehensive security.

Introduction

With digital acceleration, WFA, and increasingly sophisticated cyberattacks placing increased demands on bandwidth requirements to securely deliver the experience users demand, SD-WAN requirements are maturing. However, many solutions on the market today are incomplete. Issues like limited scalability, the lack of automation to simplify operations, and lackluster cloud on-ramp and cloud and SaaS integrations can result in a poor user experience that can undermine the value of an SD-WAN deployment. Further, enabling a direct internet connection via SD-WAN means traffic is no longer backhauled through the data center to apply security controls. Therefore, to be effective, an SD-WAN solution must include a robust set of networking, connectivity, and security tools that can meet and adapt to the dynamic nature of today's networks. The solution must be able to keep up with rapid cloud adoption, transition from regional to global deployments, office or branch expansion, and the remote workforce.

SD-WAN has been evolving from a point product to becoming a platform and foundational for SD-Branch and SASE transition. As a platform, it needs to be able to support this transition in a seamless way and with unified management.

Addressing Business Demands with SD-WAN

SD-WAN offers the ability to use available WAN services more effectively and economically—giving users across distributed organizations the freedom to better engage customers, optimize business processes, and innovate. WAN innovation with additional carrier links can be leveraged to provide redundancy, load balancing, and optimization of application traffic. It also makes WAN management more cost-effective, which is why SD-WAN solutions will continue to be a robust growth market for the foreseeable future.

To answer this demand, there have been many SD-WAN solutions introduced in the last few years. But not all of them include the necessary capabilities.

The optimal SD-WAN for an enterprise depends on the organization's requirements regarding:

- Security
- Application performance
- Cloud on-ramp to multi-cloud deployments
- Simplified operations with centralized management at any scale

To address these business requirements, organizations need a comprehensive SD-WAN offering with built-in security and the performance capabilities to scale across any size enterprise. This solution should also enable centralized visibility and management.

As branch offices are directly exposed to the internet via broadband connections with SD-WAN, an ideal solution integrates SD-WAN and a next-generation firewall in a single appliance or virtual machine (VM).

Instead of separate WAN routers and security devices such as firewalls and secure web gateways (SWGs), a single NGFW should perform all these functions.

Application Awareness for Improved Service Levels

Performance is critical, so an effective SD-WAN solution will deliver fast, dynamic application steering and application identification performance. This includes deep secure sockets layer (SSL)/transport layer security (TLS) inspection with no performance degradation. Encryption inspection capabilities also must include the ability to inspect the packet for the SD-WAN solution to correctly route the traffic.

Technically, SD-WAN works by routing applications over the most efficient WAN connection at any point in time, including LTE/5G wireless WAN options. To ensure optimal application performance, SD-WAN solutions must be able to identify a broad range of applications and apply routing policies at a very granular level. Without these capabilities, SaaS applications, video, and voice can slow and impede end-user productivity.

Advanced SD-WAN solutions can recognize applications by business criticality. Business-critical applications (such as Office 365, Salesforce, SAP), general productivity applications (for example, Dropbox), and social media (Twitter, Instagram) can be given different routing priorities. Unique policies can be applied at a deeper level for sub-applications (such as Word or OneNote within Office 365).

This deep and broad application-level visibility into traffic patterns and utilization offers a better position to allocate WAN resources according to business needs.

When it comes to WAN efficiencies, key capabilities of SD-WAN include:

Automated path intelligence

Application awareness enables prioritized application routing across network bandwidth based on the specific application and user. SD-WAN service-level agreements (SLAs) should be able to be easily defined by dynamically selecting the best WAN connection, including LTE/5G wireless WAN options, for the specific business circumstances. For low- to medium-priority applications, organizations can specify the quality criteria, and the solution will select the corresponding link. For high-priority and business-critical applications, organizations can define strict SLAs based on a combination of jitter, packet loss, and latency metrics.

Automatic failover

Multi-path technology can automatically fail over in a sub-second to the best primary WAN path, including LTE/5G wireless WAN options. This automation should be built into the solution, and occur immediately, which reduces complexity for end-users while improving their experience and productivity.

WAN path remediation

WAN path remediation utilizes forward error correction (FEC) and packet duplication to overcome adverse WAN conditions such as poor or noisy links. This enhances data reliability and delivers a better user experience for applications like voice and video services. FEC adds error correction data to the outbound traffic, allowing the receiving end to recover from packet loss and other errors that occur during transmission. Packet duplication sends copies of packets on alternate available paths, including LTE/5G wireless WAN options. This improves the quality of real-time applications.

Application prioritization

With the ability to define application-specific business policies, the best possible utilization of bandwidth can be ensured by adding precise quality of service (QoS) prioritization for critical applications, while rate-limiting non-critical applications that can impact performance and end-user experience.

Tunnel bandwidth aggregation

For applications that require greater bandwidth, SD-WAN should enable per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity.

Simplified Management and Increased TCO

Network engineering and operations leaders are often in a quandary when it comes to deploying SD-WAN devices in numerous remote sites and branch offices. Truck rolls are expensive, and technical staff is often limited. On the other hand, shipping fully configured devices is not secure. Also, once edge devices are deployed, staff must manage both the WAN and security functions from separate consoles.

Secure SD-WAN solves both deployment and the management problems to reduce total cost of ownership (TCO).

Zero-touch deployment

Simplified deployment capabilities let enterprises ship unconfigured SD-WAN appliances to each remote site. When plugged in, they should automatically connect to a service that authenticates the remote devices and connects them to a centralized management system.

Single-pane-of-glass management

Centralized visibility of all deployed secure SD-WAN devices across the distributed organization is key. A simplified workflow to deploy and update policies with few easy clicks/steps should be included.

An SD-WAN solution should be able to automatically build and manage full mesh overlay links, including LTE/5G wireless WAN options, for secure connectivity between sites.

With guided workflows, automated overlay, and simplified business policies, IT staff hours spent on infrastructure deployment and changes are reduced from months to minutes.

SD-WAN reporting and analytics. Enhanced analytics for WAN link availability, performance SLAs, and application traffic should enable the infrastructure team to troubleshoot and quickly resolve network issues.

These features would include:

- SD-WAN bandwidth monitoring reports and datasets
- SLA logging and history monitoring via datasets, charts, and reports
- Customizable SLA alerting
- Application usage reports and dashboards
- Adaptive response handlers for SD-WAN events as well as event logging and archiving SLAs across applications and interfaces

Application gateway capabilities

The ideal SD-WAN solution will integrate application gateway capabilities, such as zero-trust network access (ZTNA). This allows organizations to host applications anywhere with consistent policy controls to enable and secure hybrid workforce models with seamless and superior user experience.

Controlling Multi-Cloud Complexity

Low-latency access to distributed cloud

An ideal secure SD-WAN solution provides instant multi-cloud access such as Office 365. Plus, built-in security adds another layer of secure access to these applications, while providing a low-latency connection through public internet links so they can become part of the trusted and reliable WAN infrastructure.

This is especially critical as remote workers use advanced, feature-rich, cloud-hosted applications for voice and videoconferencing. While these applications provide enhanced voice and video capabilities, they also demand more bandwidth availability. And in most cases, that traffic can also be encrypted, which adds strain due to traffic inspection. The intelligence to detect sub-applications and provide encrypted applications with SSL inspection capability at line rates ensures these applications are steered to the best-performing WAN link to provide optimal performance.

Public cloud connectivity

SD-WAN technology can play a key role in cloud connectivity. SD-WAN gateways can steer applications over policy-defined links and automatically set up Internet Protocol security (IPsec) tunnels to and across cloud service providers—all from a centralized console.

This means that SD-WAN can be used as a cloud overlay network to connect branch offices to cloud services, virtual networks within a single public cloud, and even across multiple clouds with one another. Its ability to prioritize traffic by application enables the most critical traffic to receive priority, and its ability to steer traffic over multiple routes for the best performance makes it ideal as a multi-cloud overlay. Access and security policies are centralized, and administrators have full visibility into application traffic, performance, and security.

Proven, Comprehensive Security

Secure SD-WAN must have robust threat protection, including Layer 3 through Layer 7 security controls. These include:

- Complete threat protection, including firewall, antivirus, intrusion prevention system (IPS), and application control
- High-throughput decryption and deep packet inspection of SSL/TLS including TLS 1.3 with minimal performance degradation, ensuring that organizations do not sacrifice throughput for complete threat protection
- Web filtering to enforce internet security without requiring a separate SWG device
- High WAN performance for cloud applications, featuring exceptional virtual private network (VPN) overlay performance for superior user experience and low latency

Secure SD-WAN should also monitor firewall rules and policies and highlight best practices to improve the organization's overall security posture. This helps to simplify compliance with security standards as well as privacy laws and industry regulations. Automated auditing and reporting workflows can save staff time while reducing the risk of omissions and errors.

Enabling the SD-Branch

Many enterprise branches are deciding to simultaneously replace both their WAN and local area network (LAN) devices in favor of a solution with deeper integration and simplified branch operations management. Using separate WAN and LAN infrastructures increases branch complexity. There are more devices to deploy and update with multiple management consoles. It also reduces visibility and control of operations while increasing the opportunities for security gaps that hackers can exploit. The right SD-WAN solution will solve these issues and accelerate SD-Branch deployment.

Securing All Users

SASE helps extend secure access and high-performance connectivity to users regardless of their geographic locations. SASE delivers a full set of networking and security capabilities, including secure web gateway (SWG), universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), Firewall-as-a-Service (FWaaS), and secure SD-WAN integration. With a unified solution, you can:

- Overcome security gaps
- Simplify operations and enhance security and networking analytics
- Shift to an OpEx business model with simple user-based tiered licensing

In an Unequal SD-WAN Market, Choose Wisely

As cloud-based applications and tools like voice and video become increasingly critical to distributed businesses, organizations must be able to embrace the benefits of digital innovation without putting security at risk, bottlenecking application performance, or impacting end-user productivity.

To reap the benefits of SD-WAN, organizations should evaluate solutions carefully. Rarely do SD-WAN solutions employ one operating system for SD-WAN and security for true integration. Comprehensive, integrated SD-WAN and security managed by one console, at any scale, is essential, yet few vendors offer it. Further, an effective SD-WAN solution needs to have advanced capabilities to enable expected QoE for end-users and IT staff and improve operational efficiency across WAN and cloud edges.

[1] "Software-Defined Wide Area Network (SD-WAN) Market by Component (Solutions (Software and Appliances) and Services), Deployment Type (On-Premises and Cloud), End User (Service Providers and Verticals), and Region - Global Forecast to 2027," Markets and Markets, accessed April 18, 2023.

[2] Nirav Shah, "Secure SD-WAN: The Foundation for Network Transformation," June 30, 2022.

[3] Nirav Shah, "Using Fortinet Secure SD-WAN to Build Tomorrow's Networks," August 30, 2022.

[4] Nirav Shah, "SD-WAN Works Best as Part of a Platform," January 26, 2022.

[5] Nirav Shah, "Enabling Self-Healing SD-WAN from the WAN Edge to the Cloud Edge," Fortinet, June 22, 2021.

[6] "HTTPS encryption on the web," Google, accessed April 2023.

Secure SD-WAN Customer Success Stories: Transforming and Securing the Networks of Global Enterprises

Executive Summary

Today's networks are constantly increasing in complexity, and attack surfaces are continuously expanding. Inefficient network operations leave IT teams struggling to keep up. When network traffic patterns changed, and applications became more distributed, traditional branch routers began to be replaced by software-defined wide area network (SD-WAN) solutions. But SD-WAN on its own is not enough. Users, branch offices, and traffic without robust, next-generation security are all very vulnerable to ever-evolving cyberthreats. Enter Fortinet Secure SD-WAN.

Since its launch, Fortinet Secure SD-WAN has been highly successful in helping organizations simplify their networks and enable a zero-trust architecture with a smooth convergence of on-premises and cloud-delivered security for users. As organizations want to bring similar network and security experience to their hybrid workforce, Fortinet Secure SD-WAN becomes foundational to seamlessly transition to Fortinet Universal SASE.

According to Forrester, Fortinet Secure SD-WAN is an industry leader, delivering:

- 300% ROI
- Payback in eight months
- 65% reduction in the number of network disruptions
- 50% increase in the productivity of security and network teams

This ebook provides 10 short case studies of organizations across industries that have deployed Fortinet Secure SD-WAN. The details of each company's successful SD-WAN journey can serve as a helpful guide for your own organization's SD-WAN experience.

Introduction

What is Fortinet Secure SD-WAN?

Fortinet Secure SD-WAN is a solution that converges networking and security on a single operating system that is managed by a single management console. It transforms networking and security, consolidating SD-WAN, next-generation firewall (NGFW), advanced routing, and zero-trust network access (ZTNA) application gateway functions into one platform. Secure SD-WAN supports cloud-first, security-sensitive, and global enterprises, as well as the hybrid workforce.

Why is Fortinet Secure SD-WAN needed?

Digital transformation is the process organizations embrace to make improvements in various aspects of their organization or business. The process includes the consumption of applications from the cloud. Unfortunately, the traditional branch router comes up short of meeting the requirements to support digital transformation. Traffic must be intelligently and securely steered from the branch to its destination without backhauling to the data center at headquarters. Furthermore, the high cost of wide area network (WAN) links, along with operational complexity and limited visibility, make it impossible for organizations to become digital-first. This is why deploying Fortinet Secure SD-WAN is necessary.

Fortinet Secure SD-WAN Use Cases

Simplify Secure SD-Branch

With Fortinet Secure SD-WAN, organizations can simplify the entire infrastructure with tight integration across the LAN, WLAN, and WWAN on the hardware, software, and management levels. The solution enhances the application experience, connectivity, and operations, which all lead to an improved user experience and are managed from a single console.

Enhance hybrid, multi-cloud connectivity

Organizations can enable secure, seamless, faster connectivity to, within, and across clouds with a single virtual machine (VM), reducing footprint by using Fortinet Secure SD-WAN.

Optimize the hybrid workforce experience

Organizations can enhance the network and security experience for users working from anywhere with cloud-delivered SD-WAN and security via the FortiSASE points of presence (PoPs) on the Fortinet Universal SASE platform.

10 Customer Success Stories

The Fortinet Secure SD-WAN platform is the cornerstone of a transition to a SASE journey. The following 10 customer success stories provide deep insights into how Fortinet Secure SD-WAN can be successfully deployed in organizations from various industries. We hope you find these real-world success stories inspiring.

1

Global Hospitality Company Improved Network and Security Teams’ Efficiency by 60%

- **4,000+ locations**
- **325,000+ global employees**
- **$19.4 billion gross annual revenue**

Customer Challenges

- High bandwidth cost
- Complex operation
- Unable to meet cloud and mobile requirements
- Lack of visibility
- Difficulty in troubleshooting
- Weak security posture

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer

Results

- Accelerated network and security convergence for hotel enterprises and simplified entire WAN architecture
- Enabled large-scale, faster deployment of digital products and above-property solutions
- Alleviated large scaling of security operations center (SOC) assets, enabling efficient use of security orchestrator and resources
- Centrally managed the ecosystem and enhanced deployments, configurations, and operations with complete visibility, analytics, and reporting
- Increased app availability and performance over WAN transport, enhancing cloud strategy
- Single-pane-of-glass solutions that provided:
  - Complete visibility of the SD-WAN connectivity status and quality of service (QoS)
  - Network metrics of egress from specific properties, QoS of business-critical applications, and real-time performance for each WAN link

Business Outcomes

- Improved network and security teams’ efficiency by 60%
- Improved user experience and satisfaction by 30%
- Reduced cost by 25%
- 15-month deployment due to centralized management

IHG®
HOTELS & RESORTS

Read the Case Study

2

North America’s Largest Trash Collection and Recycling Provider Improved Performance by 38x

- **1200+ locations**
- **43,000+ employees**
- **Fortune 500 large enterprise**

Customer Challenges

- Inefficient and slow legacy solutions
- Wanted to modernize network, improve security, and reduce costs
- Need to make a digital transformation to maintain a competitive edge

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiAP
- FortiSwitch
- FortiExtender
- FortiGuard AI-Powered Security Services
- FortiManager

Results

- Delivered consolidation and best ROI among all vendors
- Provided consistent security posture across WAN and LAN networks
- Increased visibility and simplified management with zero-touch provisioning
- Better user experience
- Easier to troubleshoot across network

Business Outcomes

- Reduced overall cost by 65%
- Improved performance by 38x
- Deployed 1,200+ sites in six months
- Increased visibility and reduced time to remediate user-impacting issues

WM
WASTE MANAGEMENT

Read the Case Study

3

Large Retail Chain in Finland Reduces Calls to the In-House Service Desk By 30%–40%

- **470 locations**
- **4,000+ employees**
- **Finnish retail chain**

Customer Challenges

- Resiliency issues, suffered from frequent outages and lack of redundancy
- High cost of multiprotocol label switching (MPLS)
- Degraded security posture effectiveness

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiAP
- FortiSwitch
- FortiManager
- FortiAnalyzer

Results

- Consolidated and provided consistent security policy enforcement across WAN, WLAN, and LAN networks
- Purpose-built security processors enforced granular security
- Increased visibility and control with centralized monitoring and analytics for the entire infrastructure

Business Outcomes

- 30% to 40% reduction in calls to the in-house service desk
- Increased visibility and control by converging security, LAN, and WAN
- Improved resilience to network failure and attack

R kiosk

Read the Case Study

4

Romanian Bank Reduced Application Response Times by 50%

- **1,000+ locations**
- **2 million clients**
- **7,000+ employees**

Customer Challenges

- Lacked centralized visibility and control
- Slow and unreliable support from the MPLS provider
- Inflexible and manual management to accommodate for rapid growth

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer

Results

- Improved speed and reliability of network
- Enabled cloud and hybrid services
- Provided real-time, automated response to threats
- Provided centralized management, visibility, and analytics

Business Outcomes

- 8x increase in available bandwidth
- 50% reduction in application response times
- Greatly reduced operational complexity
- Increased profitability via the launch of new services and efficiency gains

CEC Bank

Read the Case Study

5

World's Largest Insurance Brokerage and Consulting Firm is Saving $1 Million a Year on WAN Hardware and Support

- **180+ locations**
- **8,000+ employees**

Customer Challenges

- Hypergrowth in the past 30 years overwhelmed IT team
- Too many outages and complex networks to manage
- Difficulty complying with industry regulations

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiSIEM
- FortiGuard AI-Powered Security Services

Results

- Simplified management and architecture
- Enabled company to easily comply with industry regulations
- Provided best-in-class technology
- Reduced network downtime
- Increased IT team productivity

Business Outcomes

- $1 million a year in savings on WAN hardware and support
- Internet connectivity up to 10x faster
- Cut WAN downtime in half

USI®

Read the Case Study

6

One of North America's Largest Dental Services Saw 10x Increase in Performance

- **700+ locations**
- **7,200+ employees**
- **30 states**

Customer Challenges

- High cost of dual MPLS circuits and limited bandwidth
- Slow performance as higher bandwidth was required for applications
- Complex to manage and troubleshoot LAN, security, and WAN

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiAP
- FortiSwitch
- FortiExtender
- FortiGuard AI-Powered Security Services
- FortiManager

Results

- An all-in-one solution that is easier to manage and troubleshoot
- Delivered consolidation (LAN, WLAN, SD-WAN, NGFW, WWAN) and single-pane-of-glass management
- Enabled secure access for users and guests
- Consistent security posture across WAN and LAN networks
- Better visibility, easier to manage, and added new sites with zero-touch provisioning
- Improved user and guest experience
- Easy to troubleshoot across the network

Business Outcomes

- 10x increase in performance
- 60%–70% savings in circuits and equipment
- Ability to support access to new applications

Smile Brands

Listen to the case study podcast

7

Global Oil and Gas Company Decreased Operating Costs by 55%

- **400+ locations**
- **9,000+ employees**
- **Thousands of customers across 60 markets**

Customer Challenges

- Agility problems and inflexibility in IT operations to optimize traffic performance, especially for cloud applications
- Limited visibility into remote sites' traffic
- No centralized control or management
- No security at the edges or security posture effectiveness
- Poor performance and operation hindering business efficiency and user experience
- High cost of MPLS impacting business profitability and performance

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiAP
- FortiExtender

Results

- Reduced operating expenses via centralized management and provisioning of network and security policies
- Improved quality of experience by delivering dynamic application steering based on defined service level agreement (SLA)
- Enhanced user experience via faster transaction
- Improved visibility and accelerated troubleshooting with centralized management

Business Outcomes

- 55% reduction in operating costs from lower MPLS usage and simpler administration
- Increased revenue and enhanced customer experience via 18x reduction in point-of-sale (POS) transaction time
- Increased operational efficiency due to 4x increase in network speed and performance and the elimination of network downtime

اينوك
enoc

Read the Case Study

8

Leading Global Provider of Packaging Solutions Reduced Communications Costs by 40%

- **50 locations worldwide**
- **5,500+ employees**
- **Producers of packaging solutions**

Customer Challenges

- Complex legacy solutions caused frequent outages
- Consolidating IT service infrastructure process left company vulnerable
- Lacked full visibility

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiGuard AI-Powered Security Services

Results

- Simplified network management
- Reduced overhead costs
- Obtained complete visibility
- Extended comprehensive security controls out to the edge of the network
- Can now monitor and control the entire network and security infrastructure from a central location

Business Outcomes

- 40% savings on communications costs
- Enhanced security of complex hybrid services infrastructure
- Increased business continuity via improved application performance and resilience

Sidel

Read the Case Study

9

Global Provider of Consulting and Engineering Services Saves $1 Million in First three Years

- **450 locations**
- **21,000+ employees**
- **$2.8 billion in revenue**

Customer Challenges

- Dynamic multipoint virtual private network (DMVPN) technology and:
  - Frequent lateral breaches
  - Lack of east-west segmentation
  - No traffic inspection close to users and digital assets
- Business profitability and performance due to high costs
- Links not fully utilized [active/standby]
- Disparate networking and security systems
- Limited visibility into offices by IT
- Too much time reacting to lateral breaches
- Four separate management consoles for networking, security, ZTNA, and web filtering hurting business efficiency and hindering user experience

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiGate VM
- FortiManager
- FortiAnalyzer
- FortiClient EPP

Results

- Enabled simplified infrastructure with one unified FortiGate WAN edge for branch offices
- Empowered IT teams to be effective and efficient with networkwide visibility, analytics, reporting, and management
- Lowered total cost of operation (TCO) as one appliance provides all the networking and security functions as well as enables utilization of all available links

Business Outcomes

- $1 million in savings over the first three years
- Reduced FTE management cost and burden with one interface for day-to-day operations
- Reduced vendor sprawl

Anonymous Technology Company

10

Europe’s Second Largest Software Company Reduced Branch Operation Expenses by 25%

- **180+ Locations**
- **140 countries**
- **20,000+ employees**

Customer Challenges

- High cost of WAN communications and operating expenses across branches
- Overall slow performance
- Fragmented point products resulting in vendor finger-pointing and integration challenges

Fortinet Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiAuthenticator

Results

- Single platform for security and SD-WAN
- Reduced operations expenses by decreasing footprint, which had consisted of dual routers, firewalls, and VPN appliances from three different vendors
- Simplified architecture improved staff efficiency and led to less finger-pointing
- Significantly improved performance

Business Outcomes

- 20% reduction in WAN expenses
- 3x improvement in WAN performance
- 25% reduction in branch operations expenses by consolidating network, security, and VPN
- 10% improvement in staff efficiency by consolidating branch network and security hardware footprint from three vendors to just one

Anonymous Technology Company

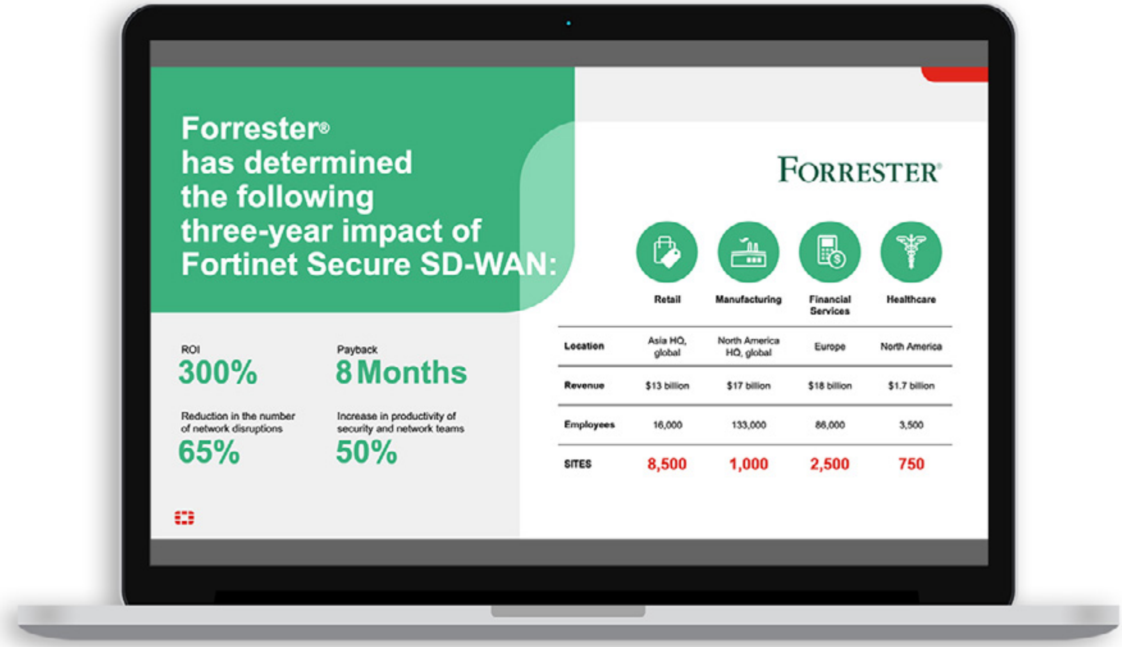
Why Fortinet?

Fortinet is an industry leader in secure networking. We're the first vendor to organically develop and integrate SD-WAN, NGFW, advanced routing, and ZTNA application gateway functions on one platform. Also, Fortinet is the only vendor with purpose-built ASICs to accelerate and offload network and security functions. With tight integrations across the LAN, WLAN, and WWAN on the hardware, software, and management levels, we are unique in offering a seamless transition to SD-Branch managed by a single console. And, as organizations embrace the SASE journey, the Fortinet Secure SD-WAN platform is the cornerstone of that transition.

For 20+ years, Fortinet has been driving the evolution of cybersecurity with networking and security convergence. Our network security solutions are the most deployed, most patented, and among the most validated in the industry. Our broad, complementary portfolio of cybersecurity solutions is built from the ground up with integration and automation in mind. It enables more efficient, self-healing operations, and a rapid response to known and unknown threats.

Why Fortinet Secure SD-WAN?

In addition to real-world customer case studies, Fortinet Secure SD-WAN is also highly rated by industry analysts. Forrester did a Total Economic Impact (TEI) study of the solution across industries.[1] The results were impressive:



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

ROI
300%

Payback
8 Months

Reduction in the number of network disruptions
65%

Increase in productivity of security and network teams
50%

FORRESTER®

	Retail	Manufacturing	Financial Services	Healthcare
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

In the companion report, Gartner® Critical Capabilities report for SD-WAN, Fortinet is the only vendor to rank first in two use cases, on-premises security-sensitive WAN and WAN for small branches, four years in a row.[3]

Furthermore, we're proud to say Fortinet was named the Gartner® Peer Insights™ Customers' Choice five years in a row.[4]

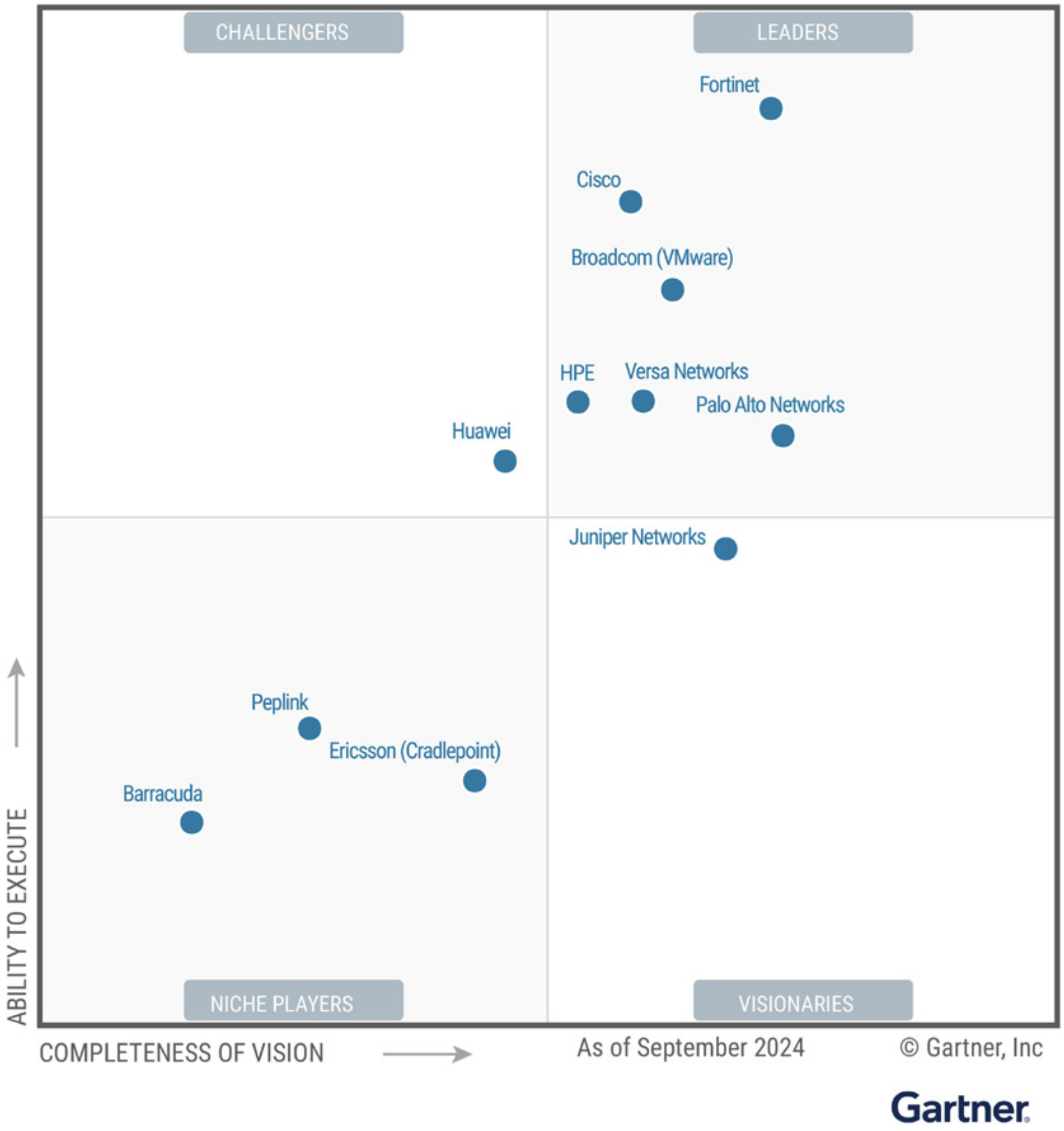
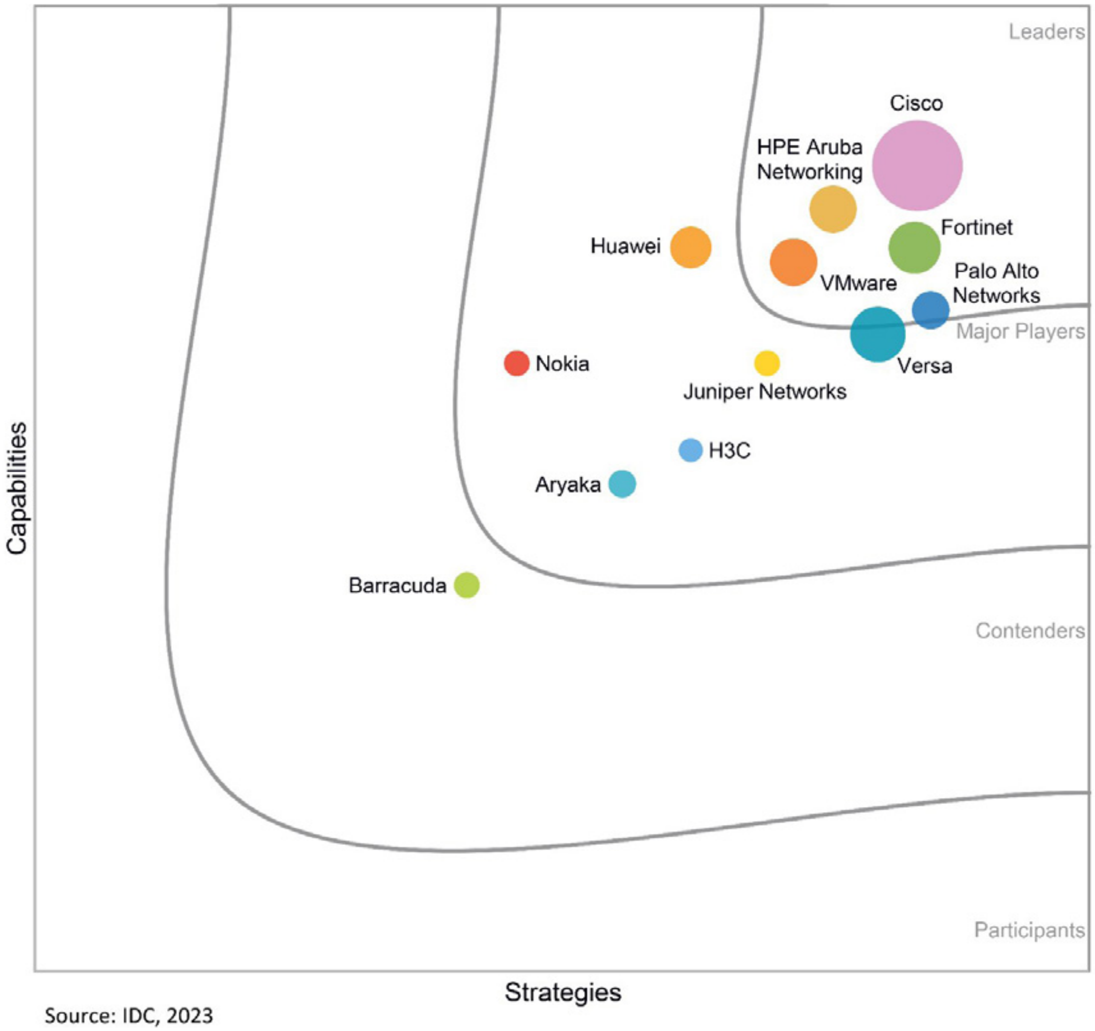


Figure 1: Magic Quadrant for SD-WAN

More Recognition

In the 2023 IDC MarketScape Worldwide SD-WAN Infrastructure Vendor Assessment, Fortinet was recognized as a leader for the second time.[5]

In the recent Q3 2023 testing by independent third-party CyberRatings.org, Fortinet was rated as a "Recommended" solution—the highest rating possible. The report states "The Fortinet SD-WAN handled all use cases with ease and proved to be highly reliable and capable and should be on everyone's short list."



Source: IDC, 2023

Figure 2: IDC MarketScape Worldwide SD-WAN Infrastructure Vendor Assessment, 2023

Conclusion

A highly rated solution by industry analysts, Fortinet Secure SD-WAN is foundational to the seamless transition to Universal SASE. It assists organizations in protecting their users, branch offices, and data with robust, next-generation security.

Fortinet Secure SD-WAN has a solid history of transforming and securing the networks of many global enterprises. The 10 success stories from different organizations in different business arenas featured in this ebook are real-world examples of how successful Fortinet Secure SD-WAN has been and a testament to how it can assist your organization.

Contact the Fortinet team to get started on your own success story.

[1] The Total Economic Impact™ (TEI) of Fortinet Secure SD-WAN, Forrester, December 2022.

[2] Ibid.

[3] Nirva Shah and Rami Rammaha, Fortinet Has Been Recognized for Fifth Straight Year as a Gartner Peer Insights Customers' Choice for SD-WAN, Fortinet, March 18, 2024.

[4] IDC MarketScape: Worldwide SD-WAN Infrastructure 2021 Vendor Assessment (doc #US50471623, September 2023).

www.fortinet.com

October 29, 2024 9:08 AM / 2810500-A-0-EN