FORTINET

# THREE USE CASES FOR TRANSFORMING BRANCHES WITH FORTINET SECURE SD-WAN

WHITE PAPER

## EXECUTIVE SUMMARY

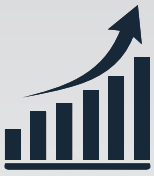
**Digital transformation (DX) of traditional branch networks offers several advantages for distributed enterprises. Many organizations are switching from performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures that offer faster connectivity, cost savings, and other benefits. But SD-WAN has its own challenges. Fortinet FortiGate next-generation firewalls (NGFWs) include Secure SD-WAN capabilities that deliver both networking and security capabilities in a unified solution. It supports application visibility and control, high-quality voice and video delivery, and consolidated management of networking and security for branch networks. It also provides advanced protection against threats. Three common uses cases show how Fortinet enables the full benefits of an SD-WAN architecture without sacrificing security.**

## INTRODUCTION

DX is forcing business leaders to evaluate the costs, capabilities, and risks of their extended network architectures. Traditional WANs utilize private multiprotocol label switching (MPLS) links, which carry a premium price for connectivity. But more important than cost, there is also productivity to consider. Most traditional WANs feature a "hub-and-spoke" architecture that funnels branch network traffic back to the organization's main data center for filtering and security checks.

While this process (known as "backhauling") is secure, it also greatly slows network performance. And the demands of DX only compound branch traffic burdens for distributed enterprise organizations. Companies are expanding their use of Software-as-a-Service (SaaS) applications—as well other cloud-based tools like Voice-over-IP (VoIP) and videoconferencing technologies. Voice and video place a great deal of demand on network resources, especially considering enterprise user expectations for very high-quality performance from these kinds of services.

SD-WAN solves the aforementioned problems of bandwidth costs and traffic latency, allowing organizations to move beyond MPLS to include public broadband connections (e.g., 4G/LTE and 5G). SD-WAN routes network traffic from branches to the cloud, headquarters, or other branches by enabling direct access to cloud applications and services. This makes SD-WAN a very popular choice for transforming enterprises. As Gartner recently notes, "According to our latest forecast, end-user spending on SD-WAN is expected to grow from $475 million in 2017 to $2.32 billion by 2022, at a five-year compound annual growth rate of 37.4%."[1]



**According to our latest forecast, end-user spending on SD-WAN is expected to grow from $475 million in 2017 to $2.32 billion by 2022, at a five-year compound annual growth rate of 37.4%.**

## SD-WAN CHALLENGES

But while SD-WAN offers inherently faster and cheaper connectivity than traditional WANs, it is not a panacea on its own. Despite its transformative capabilities for branch networks, several challenges must be addressed to fully articulate and actualize SD-WAN's potential:

**Lack of visibility.** SD-WAN solutions typically lack visibility into applications at the branch level. This can lead to Shadow IT problems, including SaaS applications (unauthorized applications that may introduce security and/or compliance risks), as well as bandwidth limitations from branch users wasting bandwidth on nonessential applications (e.g., Pandora, YouTube).

**Complexity.** In addition to the other types of complexity that DX technologies introduce, SD-WAN architectures can be difficult to troubleshoot and hard to manage across all the branches. Most solutions do not offer a single management interface for consolidated network oversight and control across all of the enterprise's remote locations. This adds to the burden on limited IT staff and often creates defensive gaps for threats to exploit.

**Security.** Without the centralized protection provided by backhauling traffic through the data center, moving from MPLS to direct internet broadband connections exposes organizations to new risks—especially considering that cyberattacks are growing in both number and sophistication. Effective SD-WAN implementation requires additional security within the enterprise infrastructure to secure those connections and inspect high volumes of traffic—all without inhibiting network performance.

To address these challenges, one approach to effective SD-WAN implementation combines both networking and security functions in a unified solution. The Fortinet **Secure SD-WAN** solution can be enabled on **FortiGate NGFWs**. FortiGate combines NGFW and SD-WAN features into a single solution that improves both WAN efficiency and security. It provides efficient protection across all branch outposts by providing consistent policy enforcement with single-pane-of-glass management. It also allows enterprises to mitigate risks associated with DX. Three common use cases demonstrate how Secure SD-WAN can solve key enterprise challenges while enabling greater business value for organizations.

**"Customers continue to strive for better WAN performance and visibility, but security now tops their priorities when it comes to the challenges with their WAN. In fact, 72% of the respondents said that security was their topmost concern when it comes to their WAN."[2]**

## USE CASE: DIGITAL TRANSFORMATION OF ENTERPRISE BRANCHES

Distributed enterprises with multiple offices are looking for effective adoption of critical SaaS applications (such as Microsoft Office 365) and other multi-cloud services for improved operational efficiency and cost savings across their extended workforce. According to one recent report, 60% of companies have already adopted at least some SaaS applications.[4] And adoption rates are going to increase in velocity: the worldwide SaaS market is projected to continue growing at a compound annual growth rate (CAGR) of 21.2% between 2018 and 2023.[5]

Because of the limits of MPLS connectivity and traffic backhauling, most traditional WAN infrastructures cannot effectively handle the added network strain that cloud-based services introduce. Problems include low bandwidth, limited visibility and control, poor user experience, and increased latency. SD-WAN's ability to perform intelligent load sharing of traffic across multiple broadband connections for greater network efficiency, dynamic operation, and cost savings can alleviate these problems. SD-WAN delivers all the productivity benefits of cloud-based applications to enterprise branches, but only if its connections are secure.

As part of the Fortinet Security Fabric, a FortiGate NGFW with Secure SD-WAN provides advanced security features for protecting direct internet access. This includes comprehensive threat prevention, such as web filtering, anti-malware, and intrusion prevention (IPS). It also encompasses threat detection, such as SSL-encrypted traffic inspection, and sandboxing via FortiSandbox integration.

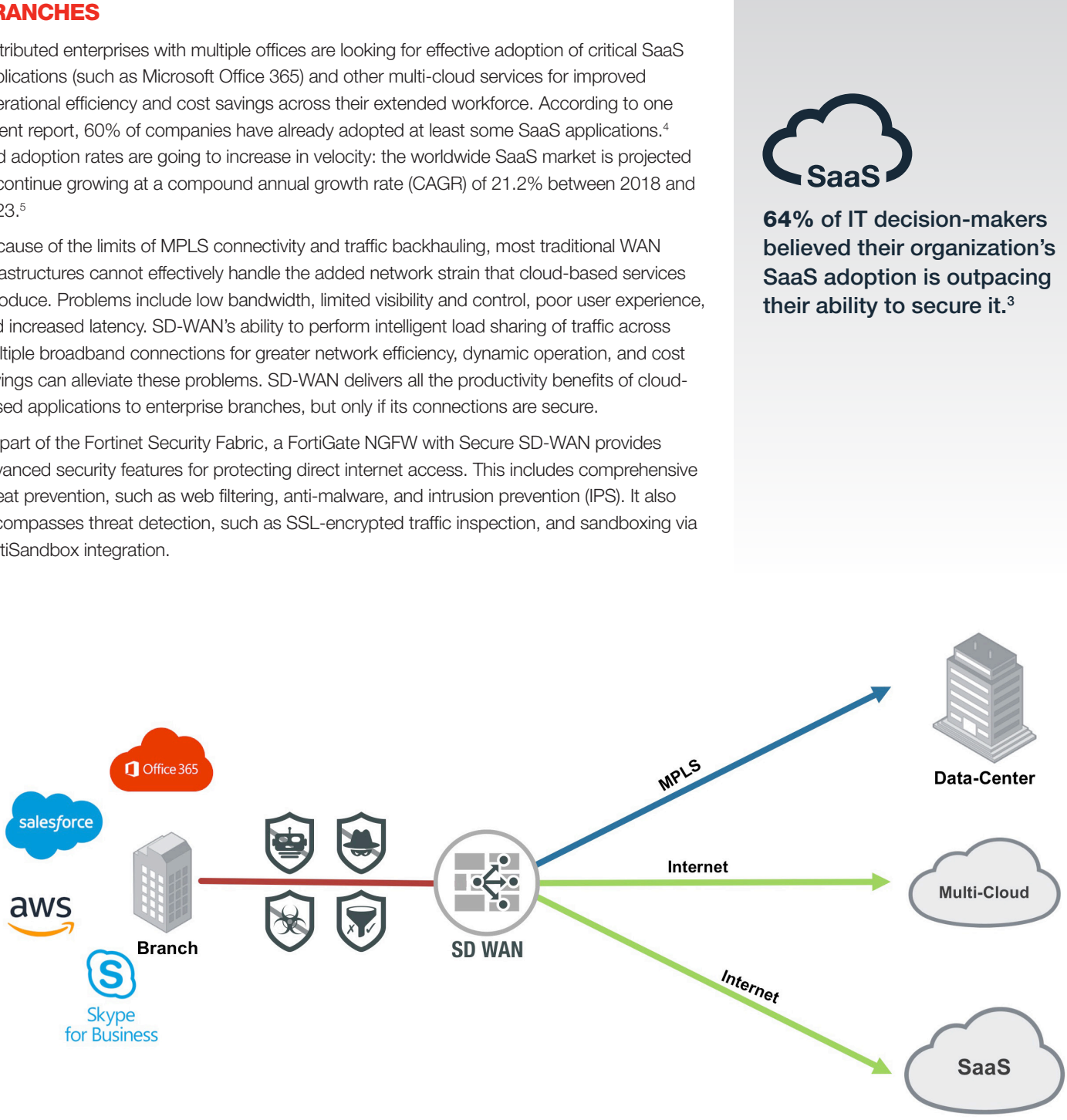



FIGURE 1: A FORTIGATE FEATURING SECURE SD-WAN CAN TRANSFORM ENTERPRISE BRANCH ARCHITECTURES.

Visibility and control are also important considerations for SaaS adoption across an extended branch workforce. Individual employees can easily install cloud-based applications without the involvement or approval of IT management. This form of Shadow IT can directly introduce malicious threats to branch networks, create gaps in security, and even violate compliance with privacy laws and industry regulations if left unchecked. Secure SD-WAN supports full application visibility and control through several key features:

**Broad application awareness.** Fortinet Secure SD-WAN uses "first-packet identification" to intelligently identify applications on the very first packet of data traffic. The solution references an application control database of over 3,000 applications—and this number continues to grow as both the threat landscape and digital network evolve. New applications—including encrypted and cloud application traffic—can be identified and classified via an optional **FortiGuard Security Subscription Service**. FortiGate NGFWs can receive ongoing threat-intelligence updates from FortiGuard Labs researchers for more efficient application routing as well as real-time threat protection.

**Compliance tracking and reporting.** Secure SD-WAN-enabled tracking and reporting helps ensure adherence to privacy laws, security standards, and industry regulations while reducing collateral risks of fines and legal costs in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. They also monitor firewall policies and help automate compliance audits. The Fortinet **Security Rating Service** provides best practices for compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and other regulations. As part of the service, organizations receive their own security posture score and are then able to compare that to the scores of their peers.

**"…the areas of primary differentiation for SD-WAN products are quality of experience (QoE) for VoIP and video performance."[6]**

## USE CASE: REDUCE WAN OPEX SPENDING WITH HIGH APPLICATION PERFORMANCE

Bandwidth requirements are increasing and operating expenses (OpEx) are growing for IT. In response, many organizations are migrating away from traditional WAN (and expensive MPLS connectivity) and turning to SD-WAN to reduce OpEx spending. As organizations adopt low-cost WAN connectivity, they often run into issues with application performance—especially for bandwidth-hungry communications tools like VoIP and videoconferencing. Having the ability to collect granular WAN path data is critical to ensuring optimal business-critical traffic.

**Automated multi-path intelligence.** A key feature of the Fortinet FortiOS operating system, automated multi-path intelligence optimizes application performance by selecting the most efficient route for SaaS, VoIP, and other business-critical traffic through the tracking of granular WAN path information (e.g., latency, jitter, packet loss). With this in mind, the Secure SD-WAN solution makes it easier to define SD-WAN service-level agreements (SLAs), providing them with the optimal link for any given application by leveraging the advanced networking capabilities built into FortiOS.

Maintaining high-quality performance for communications applications is especially important for regional branches and remote offices that rely on collaborative interaction for productive operations. In their 2018 SD-WAN Group Test Results, NSS Labs measured the quality of experience (QoE) of VoIP and video application performance offered by different SD-WAN solutions. Fortinet Secure SD-WAN received top marks for both VoIP (was the highest score) and video QoE and an overall "Recommended" rating.[7]

**Remote VPN overlay connectivity.** Virtual private networks (VPNs) are used to ensure a secure remote network connection by creating a protected "tunnel" over a less secure network transport (e.g., the public internet). One of the reasons for SD-WAN's popularity is connected to the cost-performance benefits of internet-based VPNs with the performance and agility of MPLS VPNs.[8]

Fortinet Secure SD-WAN provides native management of remote VPN connectivity to allow organizations to maintain appropriate levels of security protection and inspection, while ensuring high levels of visibility and control. This applies not only to data and applications passing through the SD-WAN environment but also across the entire distributed network.

For an organization with many remote locations, high-performance scale for virtual VPN overlay is another critical feature of secure and effective SD-WAN. VPN overlays typically feature multiple layers of these network tunnels per branch. When multiplied across an organization with a large number of branches or remote locations, network performance can degrade. FortiGate NGFWs feature powerful, purpose-built security processors (SPUs) that accelerate performance and scalability for high-volume virtual VPN overlay.

## USE CASE: SIMPLIFY WITH "SD-BRANCH"

As Gartner states, "Users also see a need for WAN solutions that effectively integrate with local wireless LANs in the branch and IoT applications being deployed. This means an opportunity of convergence and deeper integration between the WAN and LAN platforms used in the branches."[9]

Many enterprise branches may want to simultaneously replace both their WAN and LAN devices in favor of a solution with deeper integration and simplified branch operations management. Using separate WAN and LAN infrastructures not only increases branch complexity (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.

A **software-defined branch (SD-Branch)** model eliminates these challenges by unifying WAN and LAN operations within a single solution. As an extension of the Fortinet Security Fabric, a FortiGate NGFW featuring Secure SD-WAN integrates with FortiAP and FortiSwitch solutions using a special FortiLink protocol. This enables customers to manage local endpoints (such as IoT devices) connected to LAN and automatically quarantine devices showing indicators of compromise. Fortinet-enabled SD-Branch deployments (Figure 2) provide deep WAN/LAN integration, simplicity, security, and the lowest TCO in the industry.

**Single-pane-of-glass management.** Fortinet provides a single-pane-of-glass view that combines both network and security for centralized SD-WAN management, configuration, and monitoring tools. Fortinet has been been recognized as a leader in both the enterprise firewall and unified threat management (UTM) markets[10] [11] and has a long history of understanding the needs of enterprises from both a security and networking perspective. Fortinet Secure SD-WAN consolidates several point products at the branch—including routing, WAN optimization, SD-WAN, and security elements—into a single device.

**Zero-touch deployment.** Deploying SD-WAN should also be as easy as turning on a feature—and this is exactly what Fortinet Secure SD-WAN zero-touch deployment offers. New branches can be quickly connected and secured with little expertise and no additional overhead. Fortinet simplifies infrastructure and delivers SD-Branch operations with consolidated WAN/LAN functions and advanced security features. No other vendor is able to provide this combination of capabilities.

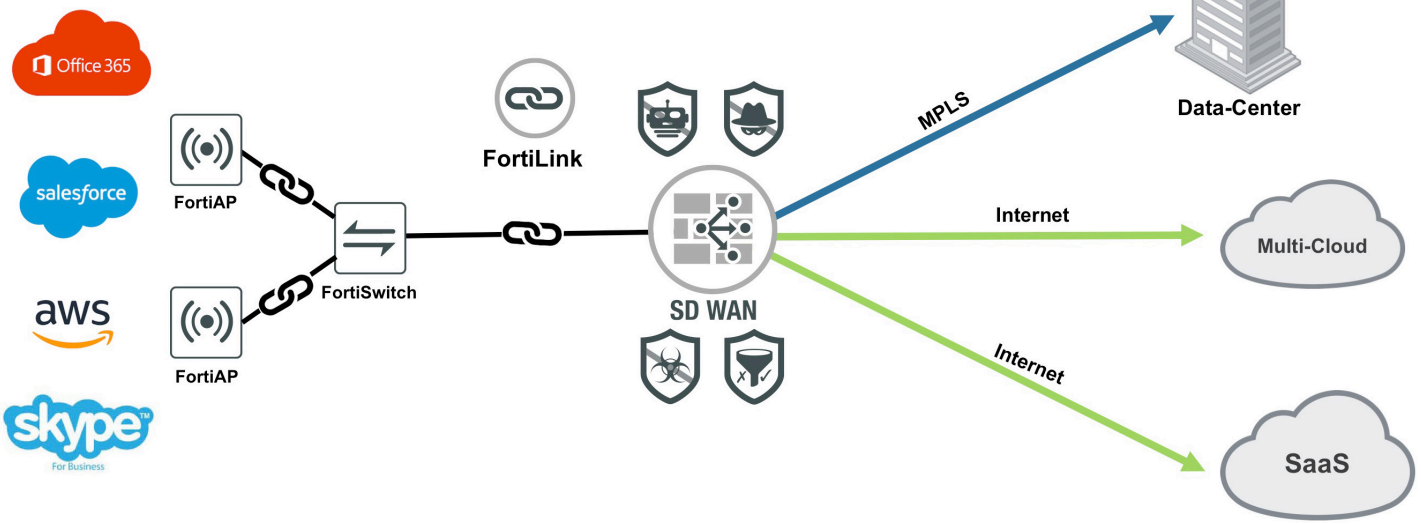
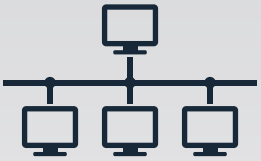



FIGURE 2: THE FORTINET HIGH-LEVEL SD-BRANCH MODEL CONSOLIDATES WAN AND LAN INFRASTRUCTURES.



**"Users also see a need for WAN solutions that effectively integrate with local wireless LANs in the branch and IoT applications being deployed. This means an opportunity of convergence and deeper integration between the WAN and LAN platforms used in the branches."[9]**

## REALIZING THE BENEFITS OF SD-WAN

With continuing growth in SaaS, VoIP, and video applications, SD-WAN can help distributed enterprises embrace the benefits of DX without bottlenecking network performance or impacting the productivity of end users.

The performance and security challenges that often come with SD-WAN are solved by Fortinet Secure SD-WAN—a native component of the Fortinet Security Fabric and the FortiGate NGFW. Secure SD-WAN allows organizations to rapidly adopt cloud applications while keeping security a top priority. It helps reduce OpEx costs while maintaining high-quality performance for VoIP, video, and VPN. It also simplifies the branch network infrastructure by combining networking and advanced security in a single, unified solution.

*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 organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

[1] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[2] Ibid.

[3] Conner Forrest, "Businesses are adopting SaaS too fast to properly secure it," TechRepublic, April 10, 2018.

[4] "SaaS Adoption Rising," Computer Economics, November 2018.

[5] "Global Software-as-a-Service (SaaS) Market Outlook (2018-2023)," Business Wire, November 14, 2018.

[6] Linda Hardesty, "Quality of Experience Is What Distinguishes SD-WAN Products, Says NSS Labs," SDX Central, August 9, 2018.

[7] Nirav Shah, "Fortinet Secure SD-WAN Gives the Performance of a Lifetime, Recommended by NSS Labs," Fortinet, August 9, 2018.

[8] Zeus Kerravala, "Understanding Virtual Private Networks (and why VPNs are important to SD-WAN)," Network World, April 13, 2018.

[9] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[10] Adam Hils, Jeremy D'Hoinne, and Rajpreet Kaur, "Magic Quadrant for Enterprise Network Firewalls," Gartner, October 4, 2018.

[11] Rajpreet Kaur and Claudio Neiva, "Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)," Gartner, September 20, 2018.


GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990





342544-0-0-EN

February 4, 2019 10:59 AM

wp-three-use-cases-for-transforming