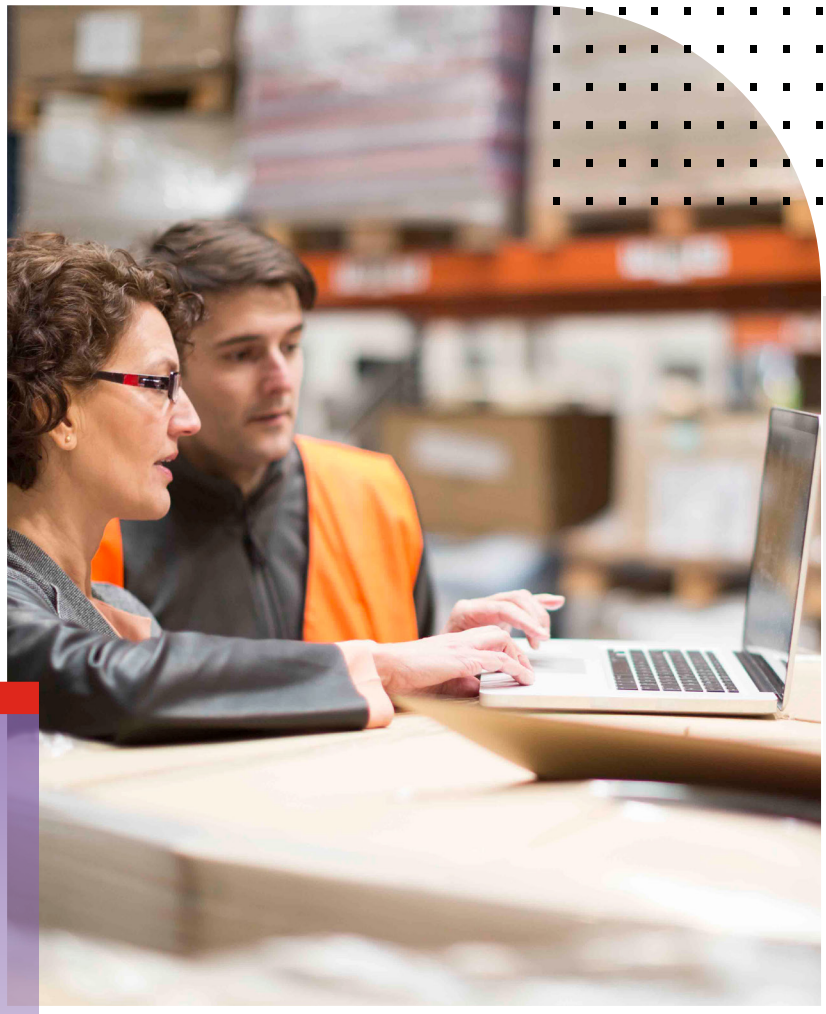
WHITE PAPER

MSPs and MSSPs Boost Revenue While Improving Operational Efficiencies with Fortinet Secure SD-WAN and SD-Branch



Executive Summary

As enterprises and small and midsize businesses (SMBs) adopt digital innovation (DI) throughout their distributed environments, their attack surface expands. Dealing with associated network and security challenges often stretches their overburdened teams to a breaking point. This is where managed service providers (MSPs) and managed security service providers (MSSPs) can help, offering managed software-defined wide-area network (SD-WAN) value-added service (VAS) offerings. Fortinet Secure SD-WAN is a critical linchpin, enabling them to consolidate networking, routing, WAN optimization, and security infrastructure in an integrated, best-in-class solution.

SD-Branch extends SD-WAN capabilities to branch networks, helping to consolidate the network access layer within a secure platform that provides visibility and security to the network and all devices that connect to it. In aggregate, Fortinet SD-WAN and SD-Branch offer an industry-best total cost of ownership (TCO), enabling MSPs and MSSPs to deliver extended VAS while boosting revenue.

More than half (53%) of organizations report that they partner with MSPs or MSSPs for implementation and management support.[1]

Integrated Branch Location Security Supports New Value-added Services

Managed services solutions that replace traditional approaches to WAN edge infrastructure at remote sites and branch offices have great potential for addressing the problems of distributed organizations. SD-WAN can help reduce connectivity costs while improving network support for the latest digital tools—such as Software-as-a-Service (SaaS), Voice over IP (VoIP), and video communications. The SD-WAN solution itself must also secure connections and inspect high volumes of traffic without inhibiting network performance. Choosing the right foundational SD-WAN solution is also critical for establishing an MSP's or MSSP's scope, addressable markets, potential revenue, and size of margins.

SD-Branch technologies can consolidate WAN and LAN capabilities to simplify remote office infrastructure and optimize operations. While a managed SD-Branch offering starts with delivery of SD-WAN-as-a-Service, service MSPs and MSSPs must consider critical factors such as integration (firewall, switches, access points [APs]), ease of deployment, centralized management, TCO, and security.

Fortinet Secure SD-WAN helps MSPs and MSSPs deliver best-of-breed SD-WAN performance and Security-as-a-Service (SECaaS) for their customers. Combined with SD-Branch, it helps them to reduce costs by consolidating multiple point solutions while establishing a secure foundation for new VAS offerings. This, over time, increases annual revenue per user (ARPU) as well as depth of penetration and customer loyalty.

Fortinet Delivers Best-of-Breed Secure SD-WAN for Managed Services

Fortinet Secure SD-WAN improves WAN efficiency without compromising performance, thanks to purpose-built SOC4 integrated circuits (ASICs). At the same time, Fortinet's integrated approach provides consistent policy enforcement and single-pane-of-glass management in a solution that supports managed services with multi-tenancy, interoperability, and automation. This enables MSPs and MSSPs to more easily meet service-level agreements (SLAs) while increasing ARPU.

Some of the ways Fortinet SD-WAN delivers value to MSPs and MSSPs include:

Fortinet Security Fabric integration for centralized visibility and control

Fortinet Secure SD-WAN is part of the Fortinet Security Fabric that offers out-of-the-box integration with third-party vendor products via 12 Fabric connectors and more than 135 Fabric application programming interfaces (APIs). This enables seamless visibility across all connected devices and real-time threat-intelligence sharing.

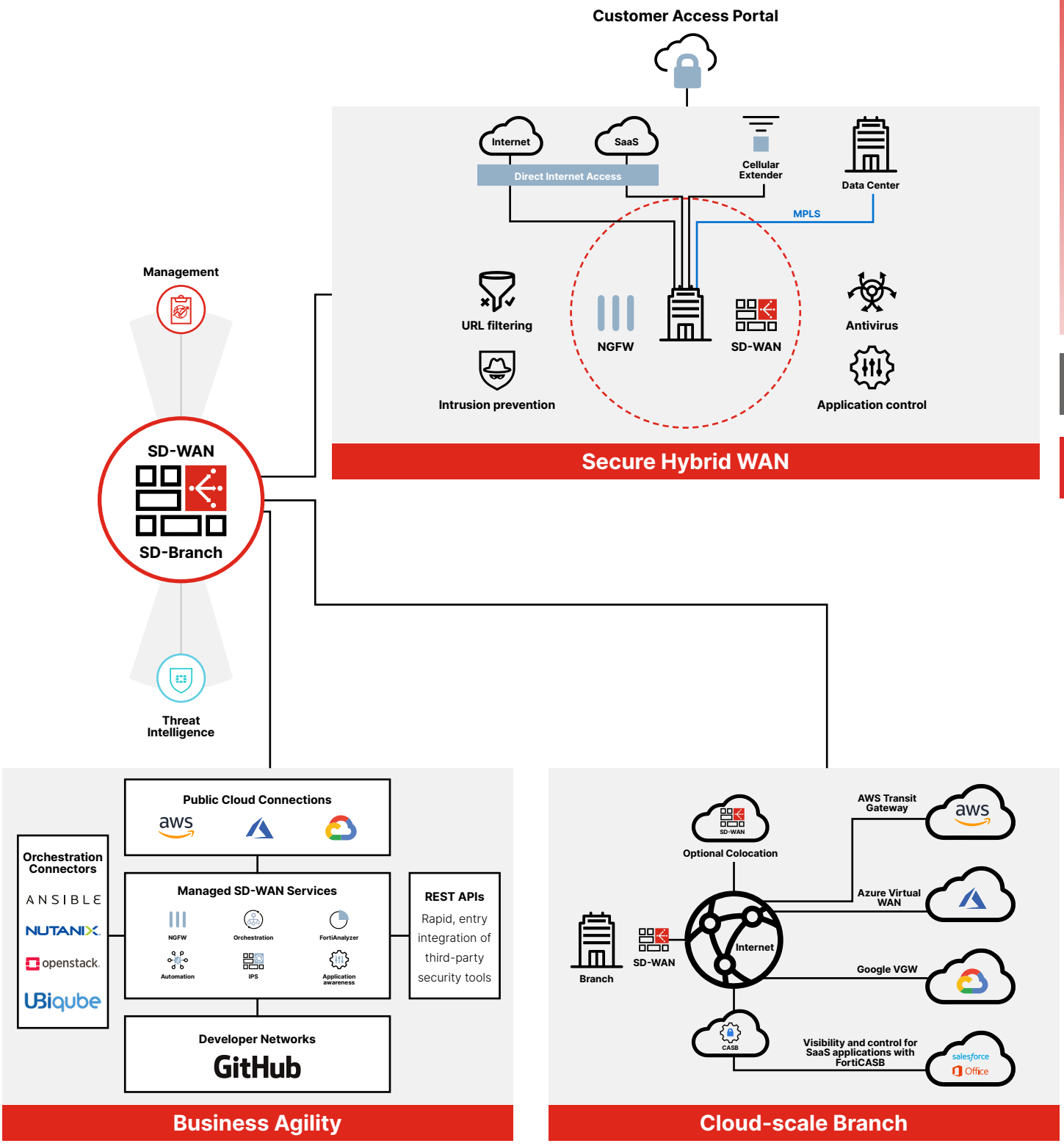


Figure 1: SD-WAN and SD-Branch deployment architecture.

In addition, Security Fabric integration enables MSPs and MSSPs to offer customers limited management control using FortiPortal. This gives them direct control over end-user customizations and access to reporting capabilities built into FortiManager and FortiAnalyzer.

Integration consolidates CapEx and increases service provider ARPU

Fortinet Secure SD-WAN integrates multiple networking and security capabilities into a single-box solution—including network firewalls, intrusion prevention (IPS), anti-malware, and WAN optimizers. This allows MSPs and MSSPs to consolidate the equipment required to deliver a fully featured and secure SD-WAN service that greatly decreases capital expenditure (CapEx) investments and thereby elevates ARPU for service providers.

Simplified orchestration and operations optimize OpEx

Eliminating infrastructure complexity not only lowers CapEx costs but also streamlines deployment and operations for reduced management expenses. Other solutions require multiple tools and devices for comprehensive functionality—which increases management burdens and operational costs for service providers. Fortinet Secure SD-WAN improves efficiency for solution deployment and implementation, which in turn reduces the time, resources, and costs associated with onboarding new customers.

Fortinet Secure SD-WAN also provides automation that simplifies ongoing management workflows for MSP and MSSP staff. Additionally, Fortinet's solution provides historical data and comprehensive analytics to help troubleshoot and quickly address performance issues. These features directly reduce the management time, labor, and costs for customer deployments.

Fortinet Secure SD-WAN-enabled tracking and reporting also helps MSPs and MSSPs to ensure adherence to privacy laws, security standards, and industry regulations, while reducing collateral risks and liability in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. Further, they monitor firewall policies and help automate compliance audits that reduce the operational churn on MSP and MSSP staff.

In NSS Labs testing, Fortinet Secure SD-WAN delivered best user experience with high availability in extreme WAN impairment conditions.[2] The SD-WAN capabilities that were assessed included zero-touch provisioning, WAN performance,application-aware traffic steering, dynamic path selection with service-level agreement (SLA) measurements, and high availability with WAN impairments.

In the latest NSS Labs NGFW group test, FortiGate delivered 99.3% security effectiveness and 100% evasions blocking.[3]

SD-WAN performance helps MSPs and MSSPs meet SLAs

Fortinet Secure SD-WAN is an ideal foundation for managed SD-WAN services, reducing risks along with lowering capital expenditure (CapEx) and operational expenditure (OpEx) costs. It provides enterprise-grade reliability and high IPsec virtual private network (VPN) performance needed for secure direct internet connectivity. This helps MSPs and MSSPs to meet aggressive SLAs without adding more CapEx costs in requisite hardware that often is required in other SD-WAN solution scenarios.

Application awareness and optimized routing improve network performance

Fortinet Secure SD-WAN uses "first-packet identification" to intelligently identify applications on the very first packet of data traffic. As part of this process, it references an application control database of over 5,000 applications—even in encrypted traffic instances. This broad application awareness gives MSPs and MSSPs comprehensive visibility into which applications are being used across the enterprise to help administrators monitor and manage traffic patterns and make well-informed decisions regarding SD-WAN policy implementation.

Being application aware opens the doors to automated path intelligence—namely, the ability to prioritize routing across network bandwidth based on the specific application and user. Here, Fortinet Secure SD-WAN automated path intelligence dynamically selects the best WAN link/connection for the situation. FortiGate next-generation firewalls (NGFWs) that feature the new SOC4 ASIC enable the fastest application steering in the industry, including unrivaled application identification performance. Fortinet offers a per-application-level SLA, which helps service providers better meet client SLAs. This also allows them to avoid higher CapEx and OpEx costs (associated with adding more equipment) as well as SLA penalties.

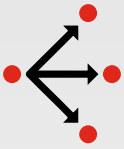
Other related features in Fortinet SD-WAN include:

- **WAN path remediation**, which utilizes forward error correction (FEC) to overcome the most adverse WAN conditions. This delivers a better user experience for business-critical applications like voice and video services.
- **Tunnel bandwidth aggregation**, which provides per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity if an application requires greater bandwidth.
- **Automatic failover capabilities**, which change to the best available link when the primary WAN path degrades. This automation is built into FortiGate NGFWs, reducing complexity for end-users while improving their experience and productivity.

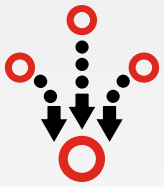
In combination, these features help service providers deliver high application availability to customers based on criticality of applications and users, while also optimizing network costs for lower TCO.

Scalable encryption inspection simplifies malware detection

Organizations need scalable secure sockets layer (SSL)/transport layer security (TLS) inspection to verify the ever-increasing volume of network traffic that is encrypted. Indeed, as much as 60% of encrypted traffic contains hidden malware.[6] To address this issue, Fortinet Secure SD-WAN includes deep SSL/TLS inspection with the lowest possible performance degradation. This provides visibility and prevention against malware while eliminating the need (plus associated CapEx and OpEx costs) for more firewalls and separate encryption inspection appliances. This further improves Fortinet solution TCO while helping service providers elevate their customer revenue streams.



Fortinet Secure SD-WAN delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.[4]



An effective SD-Branch solution should include intelligent, centralized management of SD-WAN, routing, integrated security, network switching (wired), and AP (wireless) functions.[5]

Fortinet Secure SD-Branch Expands Service Provider Opportunities

As an extension of Fortinet Secure SD-WAN, Fortinet purpose-built SD-Branch capabilities allow MSPs and MSSPs to deliver an SDBranch VAS with unparalleled network performance and reliability, while providing centralized control and visibility across the entire network-edge attack surface. It covers all critical branch exposures—from the WAN edge, to the branch access layer, to a full spectrum of endpoint devices. It allows MSPs and MSSPs to extend Fortinet Secure SD-WAN capabilities across wired and wireless networks while simplifying branch infrastructure management—increasing service capabilities and revenue streams without any additional CapEx. By integrating branch location security with Fortinet Secure SD-Branch, MSPs and MSSPs increase ARPU, simplify management, and achieve lower TCO.

Extending security to the access edge boots ARPU

By unifying WAN and LAN environments, the Fortinet SD-Branch solution secures the expanded access edge by combining NGFW, IPS, network access controls (NAC), security of switches and APs, and other critical capabilities in a single device. The

fact that Fortinet offers these advanced security and networking capabilities as part of an existing Fortinet Secure SD-WAN solution allows MSPs and MSSPs to boost ARPU on existing managed services by taking advantage of increased simplicity and lower CapEx and OpEx. Some of the ways in which Fortinet SD-Branch delivers these advantages include:

- **Simplified management and scalability reduce OpEx**

  The Fortinet SD-Branch solution helps MSPs and MSSPs centralize orchestration and management capabilities. It provides single-pane-of-glass management of security, network access, and SD-WAN. This combined interface for security and networking eases management burdens on MSP and MSSP staff while enabling proactive risk management. Fortinet also enables elastic branch scalability through advanced features like multi-tenancy and zero-touch deployment. Further, zero-touch deployment reduces the OpEx associated with initial setup and branch office expansion over time.

- **Visibility, control, and compliance reduces management complexity**

  The Fortinet Security Fabric offers service providers a common management interface via open APIs, providing them with comprehensive branch infrastructure visibility and control. Fortinet SD-Branch automates discovery, classification, and security of all endpoints when they seek network access—including unsecured Internet-of-Things (IoT) devices. To further minimize managed service OpEx, the Fortinet SD-Branch solution also automates anomaly detection and remediation processes based on defined business logic. It supports dynamic and automated NAC based on the type of connection, endpoint device, user, and application. This delivers better edge protection while reducing the management burden for MSPs and MSSPs.

  Without the right tools, compliance reporting processes can be time-consuming and costly (in terms of human resources) for MSPs and MSSPs. Here, the Fortinet SD-Branch solution provides the same automated tracking and reporting capabilities as Fortinet Secure SD-WAN. The SD-Branch solution also monitors firewall policies and facilitates compliance audits—reducing staff time spent on these tasks while eliminating potential human errors and associated operational costs.

- **Simplified security infrastructure drives lower TCO**

  Fortinet dramatically lowers an MSP's and MSSP's CapEx investment and boosts TCO by greatly reducing the number of tools and devices needed to provide secure and functional branch infrastructure to customers. Fortinet's solution integrates switches, firewalls, extenders, and wireless APs into a single, consolidated solution. At the same time, Fortinet's centralized management and automated workflows help reduce OpEx costs. With fewer technology vendors to manage, support, and train, service MSPs and MSSPs increase their margins, improve customer satisfaction, and boost seller confidence. As corroboration, Fortinet delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.[7]

Secure WAN and Network Edge Transformation Begins with Fortinet

Remote branch locations need their own defenses that conform to the unique risks they present. Fortinet solutions for SD-WAN and SDBranch consolidate the network access layer within a secure platform that provides visibility and security to an organization's entire network.

Managed services based on Fortinet Secure SD-WAN provide a seamless migration for extending customers to the benefits of an SDBranch VAS offering. This gives service providers the ability to cultivate new revenue streams with existing customers without additional infrastructure complexity, cost, or deployment churn.

[1] Survey of IT infrastructure leaders conducted by Fortinet. Broader findings of the survey found in "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, August 18, 2019.

[2] Ahmed Basheer, "Software-defined Wide Area Network Test Report: Fortinet FortiGate 61E," NSS Labs, June 19, 2019.

[3] "Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report," Fortinet, June 19, 2019.

[4] Ibid.

[5] Kelly Ahuja, "SD-Branch: The Next Destination On The Digital Transformation Journey," Forbes, November 9, 2018.

[6] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[7] "Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report," Fortinet, June 19, 2019

June 24, 2021 6:55 AM
525600-A-0-EN