

**SOLUTION BRIEF**

# Simplify SD-WAN Operations with Fortinet Secure SD-WAN, FortiManager, and FortiAnalyzer

## Executive Summary

Software-defined wide area networking (SD-WAN) is rapidly replacing traditional WAN for remote office and branch deployments. While SD-WAN offers performance benefits that support new digital innovations, many SD-WAN solutions lack consolidated networking and security features. In response, many network leaders have added a complex assortment of tools and solutions to manage and protect their SD-WAN deployments. A better solution is to take a simplified approach to contain costs, improve efficiency, and reduce risks. Fortinet Secure SD-WAN addresses today's WAN challenges, combining next-generation firewalls (NGFWs) with integrated solutions for management and analytics to centralize and simplify SD-WAN operations.

## Supporting Innovation While Securing Growing Organizations

Distributed enterprises are adopting digital innovations, such as Software-as-a-Service (SaaS) and real-time applications like voice and video to increase productivity, improve communications, and foster rapid business growth. However, traditional WAN architectures at many branch and remote office locations struggle to support the traffic demands of these new technologies. This has led to increasing adoption of SD-WAN architectures that utilize more affordable direct internet connections. The SD-WAN market is expected to grow to over \$42 billion in 2030, from \$4.3 billion in 2023, with a CAGR of 38.9% from 2024 to 2030.<sup>2</sup>

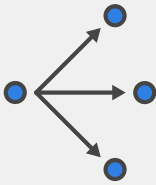
While SD-WAN improves networking bandwidth, it can also increase risk exposure. Therefore, ensuring effective security without adding overhead must be a top priority for IT leaders moving to SD-WAN. This is recognized by the industry, and security-sensitive WAN is one of the five use cases in the 2024 Gartner® Critical Capabilities for SD-WAN report.<sup>3</sup>

In many organizations, the need for SD-WAN security has led network engineering and operations leaders to incorporate many different tools and point products to address individual functions, threat exposures, or compliance requirements. However, this approach leads to infrastructure complexity, which increases management burden while creating security gaps at the network edge.

## Simplifying and Securing SD-WAN Deployments

Consolidating networking and security tools requires a secure SD-WAN solution that eliminates the complexity of disaggregated branch infrastructures. This reduces the organization's attack surface while enabling digital innovation initiatives and simplifies operations for networking teams.

Fortinet enables the convergence of networking and security to simplify network operations, ensuring a secure and optimized user experience across all network edges. SD-WAN capabilities are included in our FortiGate NGFWs. All FortiGate deployments can have unified network management and security policies, whether on-premises appliances in the branch, campus, and data center or virtual machines in cloud and cloud-native environments. Artificial intelligence and machine learning also help provide advanced threat protection.



Fortinet was named a Leader for the fifth year in a row and highest in Ability to Execute for the fourth year in a row in the 2024 Gartner® Magic Quadrant™ for SD-WAN.<sup>1</sup>



FortiManager offers unified, centralized management of all FortiGate deployments. Fortinet Secure SD-WAN can leverage a single-pane-of-glass console with FortiManager, providing enhanced analytics and improved reporting with FortiAnalyzer.

The generative AI (GenAI) capability in FortiManager enables organizations to improve operations efficiency and automate complex tasks. In FortiAnalyzer, the GenAI helps interpret security events, offering insights and advising on remediation actions. Organizations can significantly simplify centralized deployment, enable automation to save time, and offer business-centric policies.

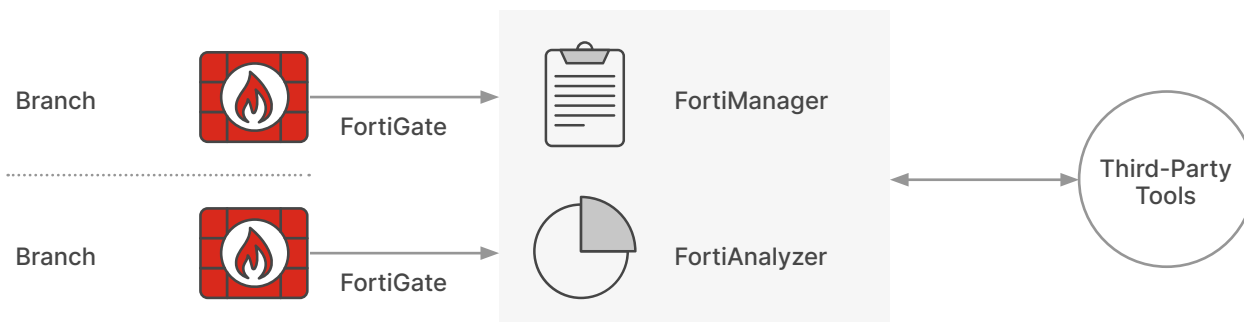


Figure 1: SD-WAN use case featuring network operations center solutions

### Zero-touch deployment

Organizations implementing Fortinet Secure SD-WAN can leverage FortiManager to accelerate deployment, reducing the time from days to minutes. FortiManager zero-touch deployment capabilities enable FortiGate devices to be plugged in at a branch location and then automatically configured by FortiManager at the main office via a broadband connection, thereby avoiding the time and cost of truck rolls. Fortinet's approach can also leverage an existing SD-WAN configuration as a template to accelerate the deployment of new branches and remote sites at scale.

### Centralized management for distributed organizations

Centralized management of all distributed networks across the organization with FortiManager helps network leaders drastically reduce the opportunities for configuration errors that lead to cyber-risk exposures and network outages.

FortiManager allows organizations to significantly simplify centralized deployment, enable automation to save time, and offer business-centric policies. Fortinet management tools can support much larger deployments than competing solutions (up to 100,000 FortiGate devices). Features such as SD-WAN and NGFW templating, enterprise-grade configuration management, and role-based access controls help network engineering and operations leaders quickly mitigate human errors.

### SD-WAN reporting and analytics

Enhanced analytics for WAN link availability, performance service-level agreements (SLAs) and application traffic in runtime, and historical stats allow the infrastructure team to troubleshoot and quickly resolve network issues. FortiManager, integrated with FortiAnalyzer, offers advanced telemetry for application visibility and network performance to achieve faster resolution and reduce the number of IT support tickets. On-demand SD-WAN reports provide further insight into the threat landscape, trust level, and asset access, which are mandated for compliance.

These features include SD-WAN bandwidth monitoring reports and datasets, SLA logging and history monitoring via datasets, charts, and reports, plus customizable SLA alerting and application usage reports and dashboards. It also provides adaptive response handlers for SD-WAN events, event logging, and archiving around SLAs across applications and interfaces.

### Compliance reporting

Organizations need reports and tools for customization to help prove compliance to their auditors. However, compliance management has traditionally been a costly, labor-intensive process for networking teams, often requiring multiple full-time staff and months of work to aggregate and normalize data from multiple point security products.

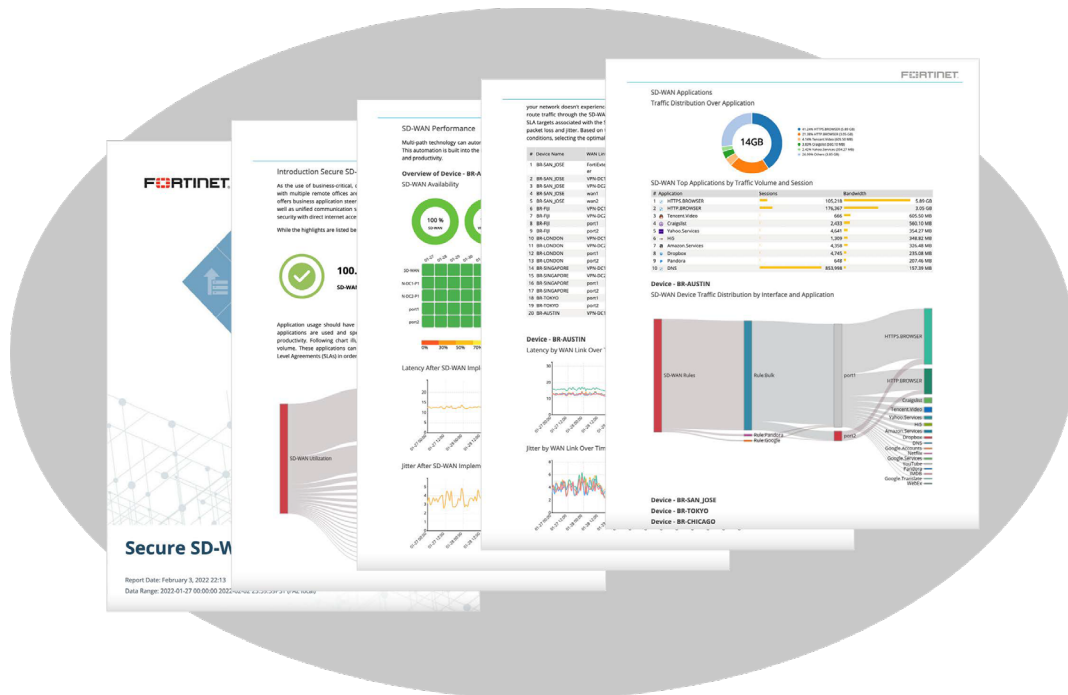


Figure 2: Detailed and highly configurable SD-WAN reports save the IT team valuable time.

Fortinet accelerates compliance reporting by simplifying security infrastructure and eliminating the need for many manual processes. FortiManager and FortiAnalyzer include customizable regulatory templates as well as canned reports for standards such as Payment Card Industry Data Security Standard, Security Activity Report, Center for Internet Security, and National Institute of Standards and Technology. They also provide audit logging and role-based access control to ensure that employees can only access the information they need to perform their jobs.

### Integration and automation

To be effective, security must integrate seamlessly across every part of the distributed organization, including every branch and remote office location. Network engineering and operations leaders need full visibility across the entire attack surface from a single location. They then need automated responses to reduce the time window from threat detection to remediation and alleviate the burdens of manual tasks from their staff.

FortiManager and FortiAnalyzer help decrease threat remediation time from months to minutes by coordinating policy-based automated response actions across the Fortinet Security Fabric, an integrated security architecture that enables security workflows and threat intelligence automation. A detected incident alert sent with contextual awareness data from one branch location allows a network administrator to quickly determine a course of action to protect the entire enterprise against a potential coordinated attack. Certain events can also trigger automatic changes to device configurations to instantly close the loop on attack mitigation.

FortiAnalyzer and FortiManager also automate many required SD-WAN tasks to help network leaders reduce the burden on their staff resources. Both products integrate with third-party tools, such as security information and event management, IT service management, and DevOps (for example, Ansible and Terraform) to preserve existing workflows and previous investments in other security and networking tools.

## Realizing Value, Simplicity, and Security

FortiManager and FortiAnalyzer help bolster security and deliver branch networking capabilities with industry-leading benefits:

**Increases return on investment:** Fortinet's integrated approach to secure SD-WAN improves return on investment by consolidating the number of networking and security tools required via capital expenditure while also reducing operating expenses through simplified management and workflow automation. The move to public broadband means expensive multiprotocol label switching connections can be replaced with more cost-effective options.

**Improves efficiency:** Simultaneously, Fortinet institutes a simplified infrastructure for SD-WAN that reduces operational complexity at the branch and across the entire distributed organization. Fortinet Secure SD-WAN can be administered through a single, intuitive management console. With FortiManager, FortiGate devices are truly plug-and-play. Centralized policies and device information can be configured with FortiManager, and the FortiGate devices are automatically updated to the latest policy configuration. The flexibility of single-pane-of-glass management includes scalable remote security and network control via the cloud for all branches and locations. The GenAI included in FortiManager helps IT teams complete complex tasks faster and more efficiently.

**Contains risks:** Fortinet's tracking and reporting features help organizations ensure compliance with privacy laws, security standards, and industry regulations while reducing risks associated with fines and legal costs in the event of a breach.

FortiAnalyzer tracks real-time threat activity, facilitates risk assessment, detects potential issues, and helps mitigate problems. Its close integration with Fortinet Secure SD-WAN allows it to monitor firewall policies and help automate compliance audits across distributed business infrastructures. With the GenAI included in FortiAnalyzer, security events, remediation, and threat responses are quickly interpreted and identified.

## Delivering Simplified Secure SD-WAN

There are many use cases for secure SD-WAN, and Fortinet's unique approach enables them to be most effective for all types of SD-WAN projects. Simplifying SD-WAN operations is core to successful implementation and expansion supporting digital innovation initiatives. Fortinet Secure SD-WAN with FortiManager and FortiAnalyzer offers best-of-breed SD-WAN management and analytics capabilities that help network leaders reduce operational costs and risks at the network edge.



The average total cost of a data breach (\$4.88 million) in 2024, a 10% increase from last year.<sup>4</sup>

<sup>1</sup> Jonathan Forest, Karen Brown, and Nauman Raja, [2024 Gartner® Magic Quadrant™ for SD-WAN](#), Gartner, September 30, 2024.

<sup>2</sup> [SD-WAN Market](#), Prescient & Strategic Intelligence, December 2024.

<sup>3</sup> Jonathan Forest, Karen Brown, and Nauman Raja, [Critical Capabilities for SD-WAN](#), Gartner, September 30, 2024.

<sup>4</sup> [Cost of a Data Breach Report 2024](#), IBM, July 2024.