

SOLUTION BRIEF

Complete Small and Midsize Business Protection

Consolidated Management. Proven Security. Maximum Value.

Executive Summary

With 43% of attacks in 2019 targeting small and midsize businesses (SMBs),¹ security is no longer a topic business leaders can ignore yet remains one of the most intimidating subjects for many leaders to tackle.

New technologies and working models expose new risks, meaning effective security must be complete security. The good news is security has gotten much better. Leading security vendors like Fortinet are continually validated by third-party testing groups to effectively prevent threats across a broad range of tactics. Built off the same underlying code and taking advantage of custom-built hardware, the Fortinet Security Fabric effectively stops attacks and automatically communicates to reduce false alerts and maintenance. By taking advantage of a single vendor approach, workloads drop, operational efficiency increases, and securing your business suddenly becomes much easier.

Designed to maximize simplicity, Fortinet Small and Midsize Business Security Solutions deliver a path to complete protection. Clear ROI is delivered without sacrificing security with tight integration, automation, and visibility across your entire cybersecurity footprint to improve effectiveness, reduce cycles, and scale as your company grows. Cloud-based, centralized management simplifies ongoing operations with business-driven rules and policies so you can quickly consume new technology while keeping your business safe from attack.

Fortinet SMB Security Solutions

Secure Office Networking

At the heart of any cybersecurity solution is its ability to protect the business from incoming network attacks. Next-generation firewalls (NGFWs) understand how the combination of the user, the device they're using, and the application they're interacting with *should* behave, analyze the traffic and ultimately understand how it should be transmitted, replacing the need for traditional routers.

The NGFW is just part of the solution. For traffic to ultimately reach the user, or for the user or device to reach the internet, traffic must travel through two key devices that help scale network access around the office—switches for wired devices and wireless access points (APs) for wireless connectivity.

The combination of these three devices—NGFW, switch, and wireless AP—form the core of network connectivity. Businesses need both high performance and strong security from their network, and with Fortinet, you can have both and enable safe access to the cloud with built-in Secure SD-WAN at no additional cost.

- **FortiGate:** The most cost-effective NGFW for performance and protection³ with built-in Secure SD-WAN to better control network performance to cloud-based applications and secure traffic.

Fortinet SMB Security Solutions Provide Affordable, Complete Security

- **Secure Office Networking:** Protect the traditional office network while enabling a hybrid work force.
- **Endpoint and Remote User Protection:** Enable your users to work from anywhere with leading endpoint security and secure access.
- **Secure Cloud Applications and Email:** Build out the secure cloud-connected office and take full advantage of the cloud.
- **Cloud-based Management and Analytics:** Streamline and simplify security, management, and ongoing operations.

Two-thirds of organizations are actively consolidating the number of cybersecurity vendors with which they do business for better operational efficiency and cost savings.²

- **FortiAP:** High-performance, Wi-Fi 6 ready APs ensure strong connectivity even in dense, highly populated environments.
- **FortiSwitch:** Stackable, Power over Ethernet (PoE) functionality delivers performance and scale to meet any need.

Unified security across firewalls, switches, and wireless access points

By consolidating Layer 7 routing and multiple security services into a single, industry-leading NGFW, many business are able to reduce the cost of multiple licenses and the oversight needed to maintain a strong security position as multiple needs are solved by one. With Fortinet, this exercise in simplicity extends even further thanks to proprietary technology that allows administrators to extend this security to FortiSwitches and FortiAPs, creating a truly secure connectivity environment for the office.

FortiGate NGFW consolidates security functions*

- **Anti-malware/antivirus:** Prevents basic malware, threats, and bot activity
- **Intrusion prevention (IPS):** Uncovers advanced threats hidden deep within packets missed by basic antivirus
- **Virtual private network (VPN):** Creates an encrypted, private communication through the public web between user and office network
- **Web and content filtering:** Enable SafeSearch and block traffic to explicit and malicious websites

*For a complete list of security services available to the FortiGate, please discuss with your Fortinet representative or authorized partner.

Simple, high-performance connectivity with built-in Secure SD-WAN

As your business grows and more users and devices need to connect in and around the office and to the cloud, network bottlenecks can quickly hinder productivity. Fortinet FortiGate NGFWs, along with FortiAP wireless access points and FortiSwitches, provide industry-leading network connectivity while maintaining enterprise-grade security. Additionally, built-in Secure SD-WAN helps improve cloud-based application performance over multiple paths while retaining strong security.

Fortinet Secure SD-WAN enables fast access to cloud-based applications and high-quality experiences in multi-cloud environments by self-healing for data loss and network speed before it affects the application. As an integrated component of the FortiGate, organizations are protected against the latest risk exposures and evolving sophisticated attacks included for no additional cost and without the headache of configuring and managing another point product.

Endpoint Protection and Remote User Protection

As workers increasingly move outside the traditional office environment on a permanent or semi-permanent basis, the need for strong endpoint protection, detection, and remediation increases in importance. With a combination of FortiClient and FortiEDR, businesses can obtain rich visibility and control over endpoint hygiene, network access, and discover and prevent malicious attacks like ransomware from spreading across the network.

Endpoint visibility and control

FortiClient was designed to natively integrate with the larger Fortinet Security Fabric. Tight integration with the FortiGate NGFW allows administrators to easily drill into user devices and assess risk level, network access, and ensure content filtering policies remain consistent even when users are offline.

Secure access and VPN

FortiClient also includes a free client VPN service to ensure users are protected anywhere they log in. With built-in auto-connect and split-tunneling capabilities, there is no need to purchase a standalone VPN solution and further complicate the environment.

Real-time breach protection and ransomware

With FortiEDR, businesses can raise their level of preparedness and block exploits, stop breaches, data exfiltration, and ransomware attacks automatically, without disrupting business operations. FortiEDR brings multilayer detection and prevention technology such as machine learning (ML), patented code-tracing technology, and automated response and remediation procedures.

Secure Cloud Applications and Email

The cloud offers businesses a wealth of efficiency and simplicity while trading out control. Protecting the information stored within these services often falls unknowingly on the business rather than the application vendor. With Fortinet, administrators can build out a secure cloud-connected office by securely accessing cloud-based applications with SD-WAN, virtual firewalls to protect data across AWS, Azure, GCP, and Oracle Cloud, and ensuring email is protected when using popular platforms such as Microsoft 365 and Google Mail.



Public and private cloud security

As more applications and data move from traditional on-premises implementations to private and public cloud deployments, ensuring security remains consistent regardless where or how the firewall is deployed is paramount to maintaining a streamlined environment to easily manage. Built for the cloud, FortiGate VMs deliver protection across public, private, and multi-cloud environments.

- Safely leverage cloud benefits of scalability, metering, and time to market with cloud-native security
- Seamlessly scale without increasing operational burdens
- Flexible consumption models include licensing and on-demand usage models

Enhanced email security

Email continues to be the top method of attack used by attackers to dupe unsuspecting users into running malicious files and clicking on malicious links through phishing and other business email compromise (BEC) schemes. FortiMail Cloud offers unparalleled protection to remove these risks from your workforce and provide additional protection to popular email platforms such as Microsoft 365 and Google Mail.

Cloud-based Management and Analytics

Security works on the premise of understanding what is good, what is not, and responding accordingly. When different vendor products perceive a threat differently, conflicts arise, leaving the burden of analysis on the administrator. With Fortinet, automated information sharing across the solution and the ability to manage it from a single pane of glass help streamline and simplify security, management, and ongoing operations.

Cloud-based management

Centralized, cloud-based management of the complete SD-Branch (NGFW, AP, Switch, SD-WAN, Security), FortiGate Cloud, is included with the purchase of the FortiGate NGFW. From here, administrators can simplify deployments, management, and troubleshooting with actionable insights and visual reports of their basic network.

As locations and implementations grow and/or additional Fortinet security products are installed, businesses can easily upgrade to FortiManager and FortiAnalyzer to centralize all administrative tasks.

A Solid Security Foundation on Which To Build Your Business

Technology both enables productivity and increases the risk of a breach as the attack surface grows. Looking across the security landscape, there are many options and closer inspection regularly finds critical holes in a vendor's offerings such as:

- Limited solutions forcing you to purchase from multiple vendors to protect everything and stitch them together yourself
- Confusing implementation and management that result in ineffective protection
- Expensive solutions that claim to protect everything and leave no budget for anything else

Fortinet SMB Security Solutions are engineered to scale as your business grows and give you the confidence of investing in a market-leading security platform designed to reduce workloads while maintaining security. Only Fortinet offers this breadth of small business offerings validated by security experts.

Curious where to start? Reach out for a quick 30-minute chat to better understand your goals and unique challenges and ask about our free [Cyber Threat Assessment Program \(CTAP\)](#) to help identify where your risks are and where to focus first.

¹ "2019 Data Breach Investigations Report," Verizon, April 2019.

² Jon Oltsik, "The cybersecurity technology consolidation conundrum," CSO, March 26, 2019.

³ <https://www.fortinet.com/products/next-generation-firewall.html#certifications>.



www.fortinet.com