



SMB Cybersecurity Solutions

Security built for scale, designed for you.



Your Security Blueprint

56%

of SMBs will experience one or more cyberattacks.

71%

of SMB employees do not understand phishing or malware.

\$3.3M

average impact of a data breach on a small business.

Cybercriminals motivated by ransomware profits and empowered by automation and AI are increasingly targeting SMB organizations that lack core security protections. And with distributed employees, offices, and cloud applications, today's SMB organizations share many of the same cybersecurity and networking challenges faced by large enterprises. To keep up with these evolving threats across your expanding attack surface, you'll need to focus on unified secure networking solutions that are enterprise-grade, yet affordable, simple to manage, and ready to scale with your future needs.

So, where to start? In the age of work from anywhere (WFA), employees are the most exposed and vulnerable attack point. Protecting user endpoints is a must, as well as their secured access to your company applications and data, whether located in the cloud or your offices. Office locations typically host applications and the data the attackers are targeting, so protecting the office network with a firewall remains the most critical aspect of your security strategy. Finally, as companies of all sizes embrace Software-as-a-Service (SaaS) applications and cloud computing, your cloud resources now need the same protections as the office.

In this brochure, we'll explore the security needs of users, offices, and cloud, the types of cybersecurity solutions required, the value of unified secure networking, and show you why Fortinet is the right technology partner to secure your business today and grow with you tomorrow.



SMB Cybersecurity Challenges

Secure users

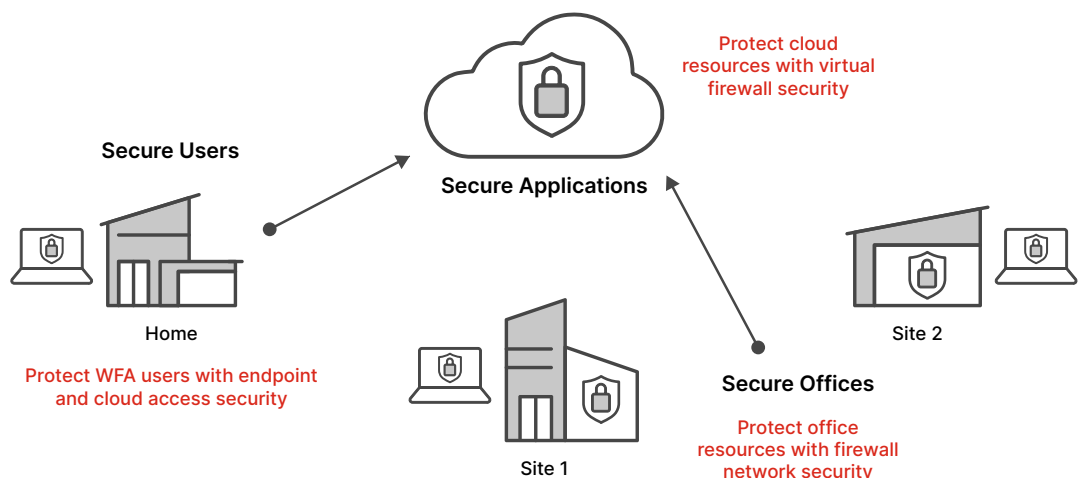
Whether at home, in the office, or anywhere in between, WFA employees need endpoint protection against malware, phishing, malicious websites, and other threats that lead to infection, credential theft, and a company data breach. And, with SaaS applications and company data and resources increasingly in the cloud, securing all user internet access, activities, and communications has also become essential. A secure access service edge (SASE) solution solves these challenges, offering all-in-one endpoint and cloud access protection to users regardless of location and activity.

Secure offices

Main and distributed offices remain the foundation of most organizations. They also typically house the sensitive data that is extremely attractive to cybercriminals. Your office network is undoubtedly under near-constant siege, with foes probing your defenses for a weakness they can exploit. Next-generation firewall (NGFW) protection against unauthorized access to your office network is the most fundamental and critical aspect of your security solution, providing a host of protections that shield your office users, data, and applications from outside attacks.

Secure cloud applications

Dependence on the convenience of cloud-based applications and data is most organization's current and future strategy. This is not news to cybercriminals, so access to your cloud resources merits the same critical NGFW protections as your offices. While public cloud providers may offer basic firewall security, their capabilities are limited, and they cannot provide consistent policies or management with your office networks. An independent virtual NGFW in the cloud works together with your office NGFWs and SASE solution for the best protection and access control across all locations.



Recent research shows organizations with fewer than 500 employees reported the average impact of a data breach has risen to \$3.3 million, a 13.4% increase.¹ Clearly, cybersecurity is no longer a topic that SMB proprietors can ignore.

¹ Cost of a Data Breach Report, IBM, 2023.

Critical Security Technology Defined

Endpoint protection

Endpoint protection provides a full range of user and device security capabilities designed to detect and block threats. It is delivered via an agent installed on the system itself (laptop, desktop, phone, server). Functions include:

- Antivirus malware blocking, malicious email protection
- Blocking malicious website access
- Operating system and communications protections
- Zero-trust, VPN, and other functions
- May work independently or as part of a SASE solution

Next-generation firewall

An NGFW provides a secure connection and control point between your office network and the outside world, connecting your offices to the internet and one other while inspecting and controlling all inbound and outbound traffic. Among its many functions, it:

- Blocks incoming illicit traffic, malware, and vulnerability exploits
- Controls user access to external applications and websites
- Can also be deployed in public-private clouds to protect cloud resources
- Can provide inter-office wide-area networking
- Is available as a hardware appliance as well as virtual or cloud-native software

Secure access service edge

SASE combines user security protections and access controls into a single cloud-based solution that protects user devices, their communications, and application access regardless of the user's location. SASE functions include:

- NGFW networking, traffic inspection, and control protections
- Zero-trust identity-based access controls
- Endpoint agent antivirus and other protections
- Monitoring of user experience quality
- Optional wide area networking capability

46%

of all data breaches are targeted at SMBs with 1,000 or fewer employees.





Fortinet products protect against the latest threats with real-time intelligence updates from FortiGuard Labs and millions of sensors around the world.

Fortinet Enterprise-Grade Solutions for SMBs

Fortinet delivers a total solution for SMB cybersecurity providing the same protections and scalable, high-performance technology used by large enterprise and government customers. Simple to manage and backed by expert Fortinet and partner services, Fortinet solutions are the right answer to your security needs of today and tomorrow.

FortiClient

FortiClient provides all the essential elements of endpoint security, including AI-based antivirus, endpoint quarantine, ransomware protection, and USB device control. In addition, FortiClient provides the required endpoint foundation for zero-trust and Fortinet SASE security functions. FortiClient is available as a standalone security product or as an integral part of the Fortinet SASE solution.

Fortinet SASE

Fortinet SASE secures user endpoints and communications from anywhere to anywhere by delivering critical security services and enforcing zero-trust authorized access. Endpoint protection from FortiClient combined with cloud-delivered security services provide a full range of protections in a unified solution ready for SMB adoption. The Fortinet SASE solution also includes SD-WAN functionality that can economically connect multiple office locations.

FortiGate NGFW

The FortiGate NGFW is the recognized industry leader, with a robust array of AI-driven protections, high performance, and integrated SD-WAN for high-speed inter-office and cloud communications. It also includes a Wi-Fi controller, and when combined with FortiSwitch Ethernet switches and FortiAP WIFI access points, you have a total solution for unified security and networking across the organization and within each location.

FortiGate NGFW Virtual Machine

The FortiGate NGFW virtual machine (VM) provides your cloud resources with the same robust AI-driven protection, management, and SD-WAN interoperability as your on-site FortiGate deployment. As the foundation of SASE and zero-trust enforcements, it also provides essential application control features as it adds full perimeter security and segmentation protections that complement a SASE defense.

FortiSwitch and FortiAP

FortiSwitch and FortiAP seamlessly integrate with the FortiGate NGFW to provide secure site connectivity. FortiSwitch offers secure ethernet access for wired users and equipment while FortiAP delivers secure WIFI access at any location served by a FortiGate NGFW.

40%

of small businesses reported they lost crucial data as a result of a cyberattack.

Management made simple

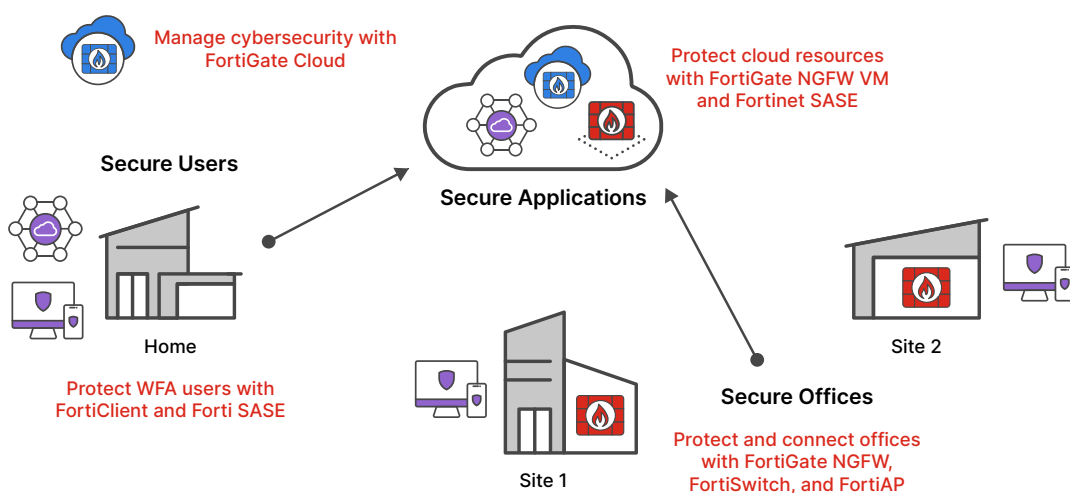
Your team needs to focus on business priorities, so managing your network security solutions should be as centralized and simple as possible. Zero-touch deployment, automated updates, and frictionless operations are essential. FortiGate Cloud provides centralized management for your entire FortiGate, FortiSwitch, and FortiAP infrastructure. An intuitive and automated cloud-based console combines network management with security analytics and intelligence to offer unified monitoring and control of your secure networking solution.

Cybersecurity services

Whether for staff augmentation services, selective outsourcing, or full turnkey operations, many SMB organizations turn to security and operations experts to help ensure their protection. Fortinet and our worldwide partner network provide the services and proven cybersecurity and Fortinet product expertise you need to keep your business secure while optimizing operations. Fortinet services include the Managed FortiGate Service, a complete managed service for your network security solutions, and FortiGuard SOC-as-a-Service, a managed service for FortiGate security and operations monitoring and alerting.

Fortinet SMB solution partners

Fortinet SMB solution partners specialize in a full range of expert guidance, sales, and value-added services to complete your Fortinet solution. From cybersecurity consultants to turnkey managed service providers, these partners are trained and supported by Fortinet to ensure your success.



The Secure SMB: Fortinet SMB solutions protect WFA users, company offices, and cloud applications.

Adopting new technologies and working models increases risks and creates new vulnerabilities. SMBs must have complete protection. Fortunately, cybersecurity from industry-leading security vendors like Fortinet effectively prevents threats across various tactics.

Why SMBs Choose Fortinet



Cybersecurity, everywhere
you need it.

SMBs trust Fortinet to deliver the best in proven, enterprise-grade security designed to meet the needs of small businesses with big plans.

The best security

Proven protection from the top-rated and most widely deployed next-generation firewall

Powered by FortiGuard Labs intelligence

Real-time product updates gathered from researchers and over 700,000 customers

Networking and security united

A single solution for protecting and connecting users, offices, and cloud resources

Designed for SMBs

An easy-to-manage end-to-end solution packaged and priced for the SMB budget

Ready to scale with you

Enterprise-grade performance and expansive capabilities that you'll never outgrow

Expert security services

Fortinet and trusted partners help optimize security and manage operations



Read Our Rave Reviews



Gartner Peer Insights™ Customers' Choice distinctions are based on the ratings of vendors by verified end-user professionals across a variety of industries and from locations around the world. These distinctions take into account both the number of end-user reviews a vendor receives, along with the overall ratings score a vendor receives from those end-users.

Fortinet is proud to be named a Gartner Peer Insights Customers' Choice in several critical areas:

- Wired and Wireless LAN
- Network Firewalls
- WAN Edge Infrastructure
- Email Security
- Secure Service Edge
- Endpoint Protection Platforms

The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.

About Fortinet

Founded more than 20 years ago in Sunnyvale, California, Fortinet continues to be a driving force in the evolution of cybersecurity and the convergence of networking and security. Securing people, devices, and data everywhere is our mission. To that end, our portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 730,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry.

