SMB Cybersecurity Solutions

Security Built for Scale, Designed for You

Your Security Blueprint

$3.3M

average impact of a data breach on a small business.[1]

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 small and midsize businesses (SMBs) share many of the same cybersecurity and networking challenges large enterprises face. To keep up with these evolving threats across your expanding attack surface, you'll need to focus on converged and integrated cybersecurity solutions that are enterprise-grade yet affordable, simple to manage, and ready to scale with your future needs.

So, where to start?

Office locations typically host sensitive data the attackers are targeting, so protecting the office network with an effective firewall remains the most critical aspect of your security strategy.

In the age of the hybrid workforce, employees are the most exposed and vulnerable attack points. Protecting user endpoints and their access to your company applications and data, whether located in the cloud or your offices, is a must.

Finally, as companies of all sizes embrace Software-as-a-Service (SaaS) applications and cloud computing, cloud resources and access to them must be afforded the same protections as those in the office.

In this brochure, we'll explore the challenges of and requirements for securing users, offices, and applications, best practices in implementing cybersecurity solutions, 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, hybrid workforce employees need endpoint protection against malware, phishing, malicious websites, and other threats that can lead to infection, credential theft, and a company data breach. With SaaS applications and company data and resources increasingly in the cloud, securing all user internet access, activities, and communications is also essential.

Secure offices

Office locations are the backbone of most organizations, often housing sensitive data that is a prime target for cybercriminals. As more devices and applications are added to the network, the complexity and associated security risks increase, leaving office networks under near-constant threat from attackers probing for vulnerabilities. Protecting your office network from unauthorized access is a fundamental and critical aspect of your security solution.

68%

68% of SMB employees do not understand phishing.[2]

Securing application access

Dependence on the convenience of cloud-based applications and data is the current and future strategy of most organizations. This is not news to cybercriminals, so access to your cloud resources merits the same critical 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.

Complex management

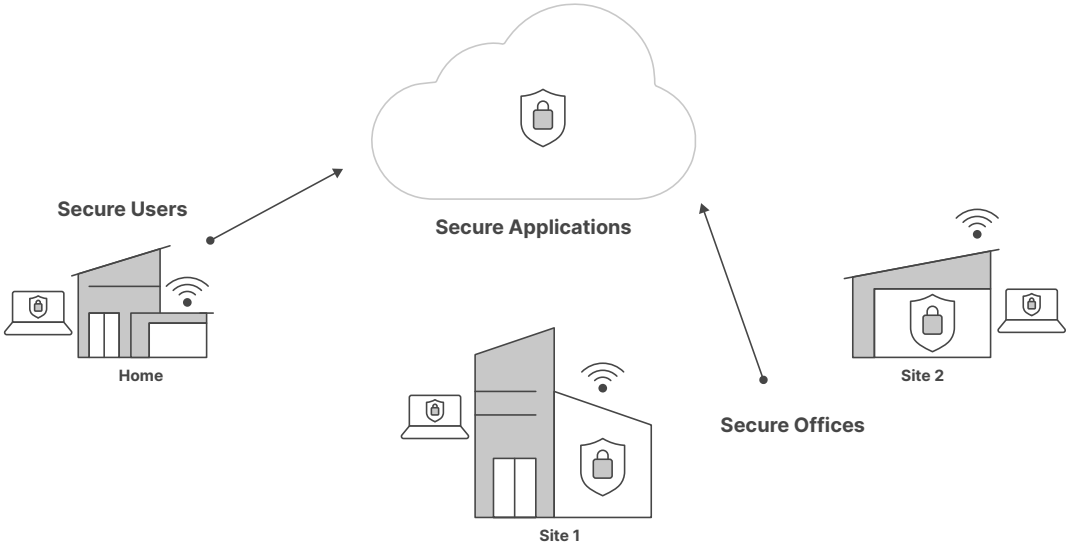
Learning and using multiple management consoles from multiple point products leads to complexity, lack of visibility, difficult troubleshooting, higher costs, and inconsistent security. This increases the risk of misconfigurations and breaches as well. Many breaches occur due to policy misconfigurations caused by managing multiple devices across a complex infrastructure.

Too many solutions

Digital transformation, cloud applications, and remote work expand the attack surface, increasing cybersecurity risks. Security operations become more complex, which puts a strain on even the most capable and well-staffed security and IT teams. This is more challenging for SMBs dealing with limited resources and tight budgets.

56%

of SMBs will experience one or more cyberattacks.[3]



Securing the modern SMB: protect your network, users, and apps everywhere

Recent research shows that organizations with fewer than 500 employees reported that the average impact of a data breach has risen to $3.3 million, a 13.4% increase.[4] Clearly, cybersecurity is no longer a topic that SMB proprietors can ignore.

Cybersecurity Best Practices for SMBs

Many SMBs rely on piecemeal security from multiple vendors, which leaves gaps in protection and visibility. With a broad portfolio of integrated security tools, the gaps are closed, and comprehensive protection can be achieved. An enterprise-grade solution will support growth and performance needs, meeting your business requirements at every stage. Deploying the following in an integrated platform is critical to stopping cyberattacks.

84%

of survey respondents declared their company takes a remote or hybrid approach.[5]

Next-generation firewall

A next-generation firewall (NGFW) is the first line of defense against new cyberthreats, keeping your network up and running for business continuity. When choosing a firewall, focus on solutions that can grow with your business and adapt to changing cybersecurity threats. Look for firewalls with security processing units that deliver strong security and high performance. Using a single vendor for security and networking needs is more efficient and simplifies management. Beyond the basic NGFW features, look for included DNS security, sandboxing, Internet-of-Things (IoT) visibility, Wi-Fi controller, and secure SD-WAN. Investing in the right firewall is essential for protecting your business now and in the future.

Secure remote user access

With a hybrid workforce, businesses need to allow users to securely access apps regardless of where they, or the app, are located. A high-performance and scalable cloud-delivered secure access service edge (SASE) solution is optimal. This will provide consistent security and user experience for your remote workforce while they access web, corporate, and SaaS applications.

Endpoint security

Endpoint solutions deliver security wherever employees work. It secures laptops, desktops, phones, and servers against threats by deploying an agent directly on each system. This solution should provide robust security features, including antivirus and anti-malware, protection against malicious emails, and block access to harmful websites. It also should safeguard the integrity of operating systems and communications while including connectivity features like zero-trust network access (ZTNA) and VPN support. For SMBs, endpoint protection offers a scalable way to defend users against cyberthreats, helping secure critical data and maintaining operational continuity.

Branch security

A software-defined branch (SD-Branch) approach solves the challenge of securing branch offices in the face of the rapid increase in IoT, operational technology devices, and BYOD, which typically lack proper security and visibility. By integrating security across both wired and wireless networks, businesses can achieve centralized control, greater visibility, and simplified management of branch infrastructure. This unified approach enhances performance and reliability while effectively securing distributed environments.

Security operations center services

Small businesses face constant security threats, and managing these risks with limited resources can be challenging. SOC-as-a-Service (SOCaaS) provides 24×7 protection by letting experts handle security monitoring, detection, and investigation. For SMBs without a dedicated security operations team, SOCaaS is an extension of the team, offering expert management, real-time guidance, and direct collaboration with security specialists to ensure robust protection.

>25%

By 2026, over 25% of SMBs with compliance requirements will have adopted a single dedicated platform to unify security and risk management services compared to less than 5% in 2022.[6]

Centralized management

SMBs can simplify device deployment and management by using a unified management and analytics platform to unburden limited IT staff. This approach provides visibility into your entire infrastructure, reduces operational complexity, and delivers consistent security policy management, reporting, and regulatory compliance. As a result, SMBs can lower cyber risk, improve security posture, and achieve a lower total cost of ownership, which is crucial for cost-conscious businesses.

Single-vendor solutions

Switching from disparate point products to a platform of integrated solutions improves the efficiency and efficacy of security, reduces management burden, and enables automation and full visibility. Look for proven products from a single vendor that work together to enable advanced threat protection and fast, coordinated response across networks, endpoints, and clouds.

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 cybersecurity solutions for SMBs provide enterprise-grade protection and performance tailored to meet SMB cybersecurity needs within budget and resource limits. Easy to manage and supported by expert services, Fortinet solutions are the right choice for your current and future security needs.

FortiGate NGFW

The FortiGate NGFW is the recognized industry leader, delivering top-tier protection and performance to safeguard your critical networks. Security capabilities include intrusion prevention system, deep-packet inspection, advanced malware protection, and application control. For networking, a Wi-Fi controller, SD-WAN for high-speed inter-office and cloud communications, and ZTNA proxy are included at no additional cost. Available as hardware, virtual machine, or as-a-Service, FortiGates offer on-premises and cloud networks the same robust AI-driven protection, centralized management, and SD-WAN interoperability.

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services offers protection against a wide range of threats, keeping your networks, applications, files, emails, employees, and web usage secure.

FortiSwitch and FortiAP

FortiSwitch provides secure Ethernet access for wired users and devices, while FortiAP offers secure Wi-Fi. Both FortiSwitch and FortiAP integrate seamlessly with FortiGate NGFWs, delivering unified security and networking across the organization and within each location.

FortiClient

FortiClient provides all the essential elements of endpoint protection, including AI-based antivirus, endpoint quarantine, ransomware protection, and USB device control. It proactively reports vulnerabilities, guides patching, and secures access to corporate and SaaS applications. FortiClient is available as a standalone security product or as an integral part of the Fortinet SASE solution to protect users wherever they work. Use FortiClient along with a virtual FortiGate NGFW to adopt a ZTNA approach.

Fortinet SASE

Fortinet SASE and its agent, FortiClient, extend zero-trust access and high-performance connectivity to users anywhere. It offers a simple, scalable, cloud-delivered security solution that provides always-on, AI-powered protection and secure web, cloud, and applications access.

FortiGate Cloud management and analytics

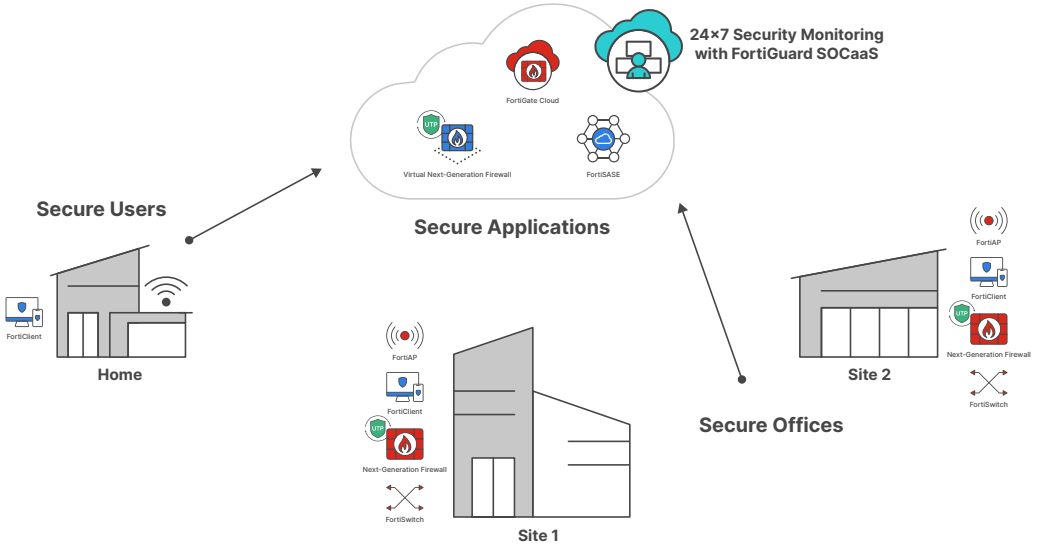
The FortiGate Cloud SaaS portal offers simplified, single-pane-of-glass network management of your entire FortiGate, FortiSwitch, and FortiAP infrastructure, improving operational efficiency. It also offers security analytics and reporting to reduce cyber risk.

FortiGuard SOC-as-a-Service

Whether for staff augmentation services, selective outsourcing, or full turnkey operations, many SMB organizations turn to security operations experts to help ensure their protection. FortiGuard SOCaaS offers 24×7 expert security management for SMBs, handling monitoring, detection, and investigation for their FortiGate devices. Whether offered by a partner directly or as a partner-branded service, Fortinet experts will manage your network security so you can focus on your core business.

87%

of small businesses reported increased efficiency due to technology platforms.[7]



The secure SMB: Fortinet SMB cybersecurity solutions

Fortinet SMB Solution Partners

Fortinet SMB solution partners specialize in a full range of expert guidance, sales, and value-added services to help you get the right solutions to fit your unique needs. From cybersecurity consultants to turnkey managed service providers, Fortinet trains and supports these partners to ensure your success.

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.

Fortify your cybersecurity.

Why SMBs Choose Fortinet

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 NGFW

Powered by FortiGuard Labs intelligence

Real-time intelligence updates gathered from researchers and millions of global sensors

A single-vendor solution for networking and security

A unified solution that protects and connects 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

Help with optimizing security and managing operations from Fortinet and trusted partners

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

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 775,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry.

[1] Andrew Rinaldi, The Cost of Cybersecurity and How to Budget for It, Business.com, August 13, 2024.

[2] Anurag Agrawal, Global US$84B spend on IT Security in 2023 by SMB and Midmarket firms, Techaisle, March 23, 2023.

[3] Ibid.

[4] Andrew Rinaldi, The Cost of Cybersecurity and How to Budget for It, Business.com, August 13, 2024.

[5] 2024 State of the Digital Workplace & Modern Intranet Report, Akumina, February, 2024.

[6] Ajit Patankar, et al, Top 10 Trends in Enterprise Communication Services for 2024, Gartner, February 19, 2024.

[7] Empowering Small Business: The Impact of Technology on U.S. Small Business, U.S. Chamber of Commerce, September 14, 2023.