

Fortinet Security Fabric for SMBs

Engineered for Simple, Cost-effective Security Across Your Growing Business

Executive Summary

A successful small business needs to focus on two primary themes—growth and a shrewd oversight of cash flow. A successful security breach can instantly derail both of these, and 43% of attacks target SMBs.¹ With the rapid adoption of new technologies and instantaneous data-sharing in and out of your traditional networking perimeters, breaches are easier than ever and can impede critical productivity cycles and/or result in sensitive data being lost and your customers’ trust coming into question.

At Fortinet, we strive to ensure you are able to protect what you have worked so hard to build and enable you to keep growing through intelligent security designed to maximize your limited resources.

Improving Security for Growing Businesses

Technology both enables our productivity and spreads the attack surface, increasing the challenge of ensuring both our business’s and customers’ data is protected. Looking across the security landscape, there are lots of 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
- Confusing implementation and management that result in ineffective protection
- Expensive solutions that claim to protect everything and leave no budget for anything else

The Fortinet Security Fabric is designed to scale as your business grows and gives you the ability to build an enterprise-grade security platform that gives you:

- **Broad** coverage and visibility of the entire digital attack surface to better manage risk
- **Integrated** solutions that reduce the complexity of understanding and supporting multiple vendor point products
- **Automated** workflows to increase the speed of operations and reduce management and response times

And unlike others, Fortinet has always believed that enterprise-grade security should be affordable and widely available. In both our engineering and our pricing, we aim to protect your growing business throughout and across all your digital initiatives.

Fortinet SMB Security Solutions

Security and SD-WAN

As users interact with data in new ways across multiple devices and cloud-based applications, your business can quickly become exposed to attack if left unprotected. Ensure your users are performing their best while keeping them safe by combining industry-leading next-generation firewall (NGFW) technology with software-defined wide-area networking (SD-WAN) with the Fortinet FortiGate available as a hardware appliance or virtually for deployment in the cloud.

Fortinet Security Fabric for small business provides security affordably

- **Security and SD-WAN:** Industry-leading NGFW technology and SD-WAN capabilities in a single device
- **Secure Access:** Extends security across wired and wireless connections
- **Secure the Cloud-connected Office:** Shift operations and applications to the cloud safely
- **Management and Analytics:** Simple, cloud-based oversight for basic and advanced deployments
- **Preventing Ransomware:** A comprehensive approach to preventing the most insidious attack strategy

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

Up and running in a matter of minutes, FortiGates deliver proactive threat protection, including inspection of encrypted traffic (secure sockets layer [SSL] and the industry's latest encryption standard, transport layer security [TLS] 1.3), at an industry-leading \$2 per protected Mbps and can be entirely managed from the cloud.

Industry-leading \$2 per protected Mbps³

Consolidated Networking and Security Functions

- Intrusion prevention (IPS)
- WAN optimization
- Application control
- Anti-malware
- Web filtering
- Virtual private network (VPN)

Connect to the Cloud Faster with Secure SD-WAN Integrated at No Additional Cost

Regardless if you have a single location or many, implementing SD-WAN to gain multiple ways of connecting to the cloud will ensure your business is always operating at peak performance.

Fortinet Secure SD-WAN enables efficient adoption of Software-as-a-Service (SaaS) applications, fast access in multi-cloud environments, and high-quality experiences by adjusting for any data loss before it impacts the application. As an integrated component of the FortiGate, security is easily extended to protect organizations against the latest risk exposures and evolving sophisticated attacks.

Fortinet Secure SD-WAN Advantages

- Purpose-built chip delivers 10x the performance of competitive solutions
- Automatically recognizes and routes 5,000+ applications
- Automated path intelligence
- WAN overlay support for VPN
- Direct connectivity via cloud on-ramping

Secure Access

Your growing business demands technologies that enable your employees to move faster and give your customers experiences they will love, but supervising disparate security devices and management portals quickly becomes cumbersome and inevitably leads to gaps in protection. To perform at your best, you need your network up and running fast, an easy way to control what's happening and to make sure it's safe.

Quickly Expand Your Network Safely

The Fortinet Secure Access solution effortlessly extends security policies from the FortiGate to attached FortiSwitches and accompanying devices such as FortiAPs and FortiExtenders, for wireless access and LTE coverage, respectively.

Proprietary engineering within the FortiOS operating systems, known as FortiLink, allows our FortiGates to also manage any FortiSwitch, FortiAP, or FortiExtender, granting a near plug-and-play experience for administrators looking to quickly expand their network while maintaining security across wired and wireless devices and providing a single-pane-of-glass management experience.

In addition, two-factor authentication can be added with FortiToken Cloud for enhanced credential security of any user attempting to enter the network.

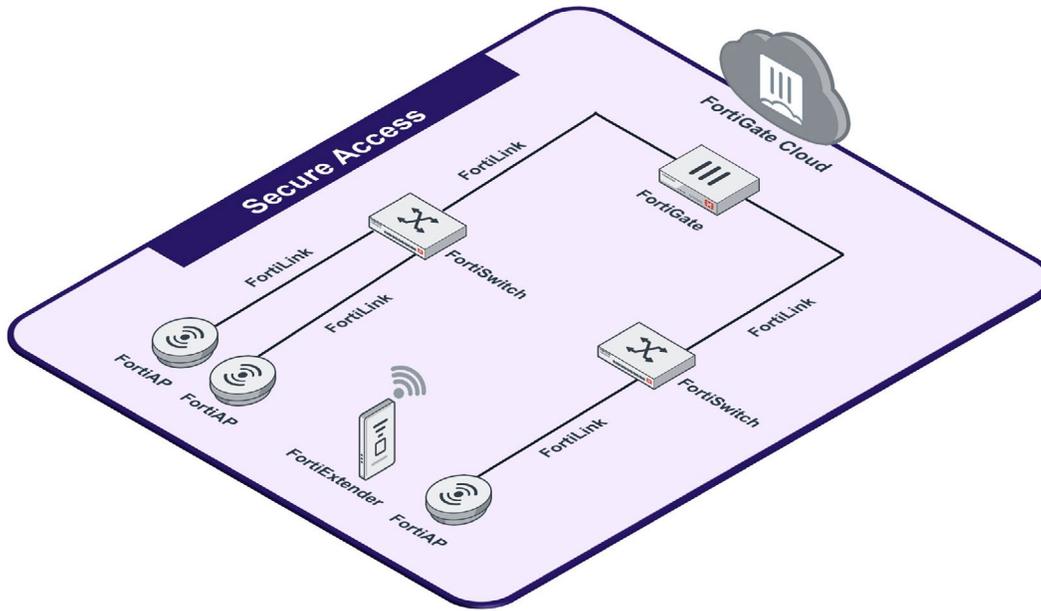


Figure 1: Secure Access Architecture Diagram.

Secure the Cloud-connected Office

Both public cloud infrastructures and SaaS applications offer tremendous advantages for growing businesses and increasingly, your sensitive, proprietary data is being scattered across these platforms, making it more difficult to ensure visibility and control.

Take Advantage of the Cloud Safely

As the leader in multi-cloud security, Fortinet gives you the confidence to deploy any application in any cloud.

- Automates common actions and reduces the need for trained staff
- Configuration templates both reduce errors and help automate key processes
- Offers visibility across all applications, networks, infrastructures, security events, and logs

Cloud Security Services Hub

Share a centralized security hub that enforces security policies and provides visibility into inbound and outbound traffic between connected networks and clouds.

Public Clouds

Fortinet delivers broad, integrated, and automated security along with the necessary visibility and control that users demand for cloud and hybrid-cloud infrastructures. Security policies are enforced across all environments and controlled using single-pane-of-glass management to secure both applications and connectivity. Administrators can easily obtain consistent compliance reporting across multi-cloud environments and perform streamlined incident investigation when needed.

Available across:



SaaS Applications

Fortinet enables organizations to have uniform access control, resource consumption, configuration, and security policies. Our solutions scan stored files for malware and advanced persistent threats to reduce the risk of unchecked malicious files spreading throughout the network.

Centralizing control of SaaS applications with Fortinet enables organizations to enforce best practices for compliance and governance in order to protect sensitive application-based data from advanced threats. At the same time, Fortinet solutions also help reduce latency to support application performance that drives business productivity.

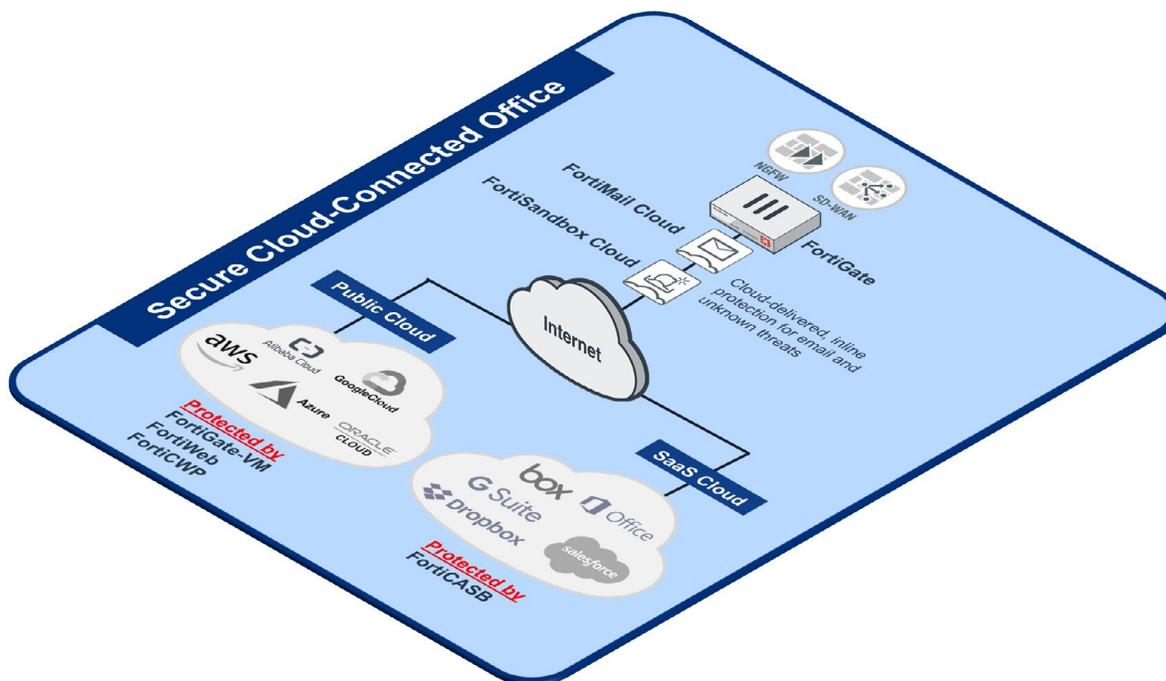


Figure 2: Cloud-connected Office Architecture Diagram.

Management and Analytics

While the opportunity for increased revenue through growth and expansion is appealing, network administrators must ensure the network can support the organization’s progress. Growing quickly means more users, devices, and technology to manage. Understanding how security and understanding how security all fits together and being able to handle changes easily—especially if the devices were not intended to be managed as a whole—becomes more difficult as staff must correlate data using each vendor’s tools.

Single pane of glass SaaS Management

Fortinet delivers growing organizations single-pane-of-glass management across their entire security architecture delivered as-a-service.

Basic Deployments with FortiGate Cloud

FortiGate Cloud offers a range of management and services across FortiGate (NGFW and SD-WAN), FortiSwitch, FortiAP, and FortiExtender.

Includes:

- Zero-touch provisioning
- Configuration management
- Reporting and analytics
- Multitenancy
- Sandboxing
- Indicators of compromise
- Two-factor authentication

Advanced Deployments

With FortiManager, administrators can easily address key use cases for effective network operations across distinct and differentiated deployments. By enabling FortiAnalyzer, administrators get even more control across the entire Security Fabric.

Includes above plus:

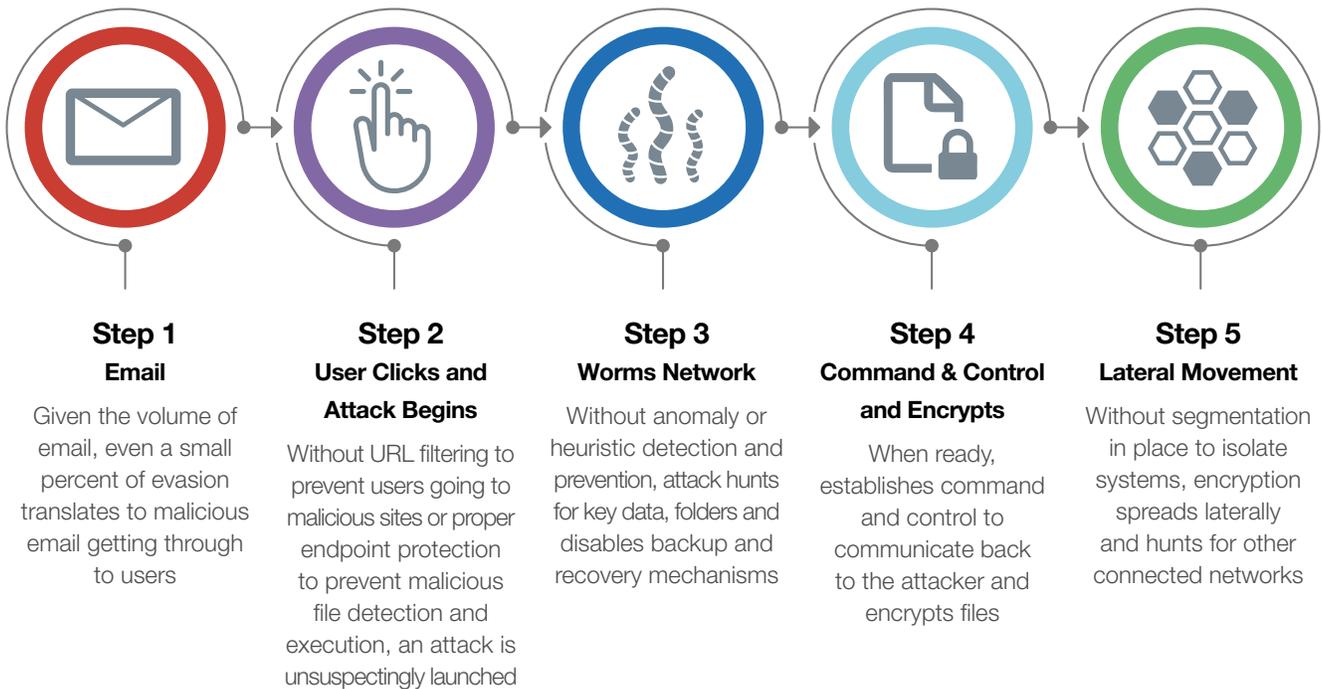
- Management and analytics across the entire Security Fabric
- Device grouping and management
- Aggregated logs across Security Fabric
- Optional administrative domains (ADOMs)
- Real-time reporting on industry standards such as PCI DSS and NIST
- Targeted executive dashboards

Preventing Ransomware and Phishing

71% of ransomware targets SMBs⁴ and continues to be the prevailing form of malware used by attackers for illicit gain and to cause disruption. For many organizations, the loss of critical business cycles and revenues from systems that have ground to a halt far outweighs the price of the ransom itself. With so many potential points of entry, businesses need complete security to ward off this ongoing threat.

71% of ransomware targets SMBs.⁴

How Ransomware Attacks



Ransomware Prevention and Remediation: Fortinet Security Fabric

The Fortinet Security Fabric enables organizations to stop known and unknown ransomware across their environment through automated sharing of actionable intelligence. With Fortinet, SMBs gain advanced capabilities and threat-intelligence sharing to help them prevent, detect, and remediate ransomware and other sophisticated modes of attack.

Phishing—FortiMail

FortiMail brings powerful antispam and anti-malware capabilities. These are complemented by advanced techniques like outbreak protection, content disarm and reconstruction, sandbox analysis, and impersonation detection to stop unwanted bulk email, ransomware, phishing, business email compromise, and targeted attacks.

Malicious URLs—FortiGuard Web Filtering

The FortiGuard Web Filtering Service enhances the core web-filtering capabilities of FortiGate NGFWs by sorting billions of webpages into a wide range of categories that users can allow or block. It includes over 45 million individual ratings of websites that apply to more than 2 billion pages.

Endpoint Execution—FortiEDR

FortiEDR real-time endpoint security solutions proactively reduce the attack surface and protect endpoint devices using machine learning anti-malware and behavior-based detection technology.

Lateral Movement—FortiGate Intent-based Segmentation

Fortinet intent-based segmentation provides end-to-end protection across the network. It intelligently segments network and infrastructure assets, whether on-premises or across multiple clouds. Policy-based access controls continuously monitor the trust level of users and devices to keep sensitive data and assets safe. Analytics and automation capabilities ensure quick detection and neutralization of threats.

Recover and Reset—Fabric-Ready Integration

Fortinet's Open Fabric Ecosystem was designed to connect traditionally disparate security solutions into an integrated framework. This enables evolving IT infrastructures to stay connected across the entire organization, share information in real time, and defend against a rapidly changing attack surface. Fabric-Ready Partners (such as Rubrik and BackBox) offer organizations quick recovery of lost data and device configurations to ensure minimal downtime with little to no integration effort.

Detection and Response

FortiEDR delivers threat protection both pre- and post-infection in real time. It detects and defuses potential threats in real time to stop breaches and prevents ransomware damage. It automates response and remediation procedures with customizable playbooks.

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>

⁴ "Beazley Breach Briefing – 2019," Beazley, March 21, 2019.

