SOLUTION BRIEF

Fortinet Delivers Powerful, Consolidated Security Solutions for SMBs

Grow Your Business, Protect Your Assets, Consolidate Your Investments

Executive Summary

In the digital transformation (DX) era, small and midsize business (SMB) owners juggle multiple security and networking challenges as they grow their businesses. SMB owners and leaders need security solutions that offer comprehensive protection, are easy to use, and are simple to manage. The Fortinet Security Fabric includes solutions for Secure Access, Secure Productivity, and secure software-defined wide-area network (SD-WAN)—offering exceptional threat protection for growing businesses.

Fortinet Security for Small and Midsize Businesses includes:

- **Secure Access** for all devices, applications, and users
- **Secure Productivity** for using cloud-based tools and services
- **Secure SD-WAN** for expanding the network to branches/remote offices

Improving Security for Growing Businesses

SMBs are under attack. Verizon reports that 43% of data breaches involve small businesses.[1] Another survey from ESG shows that two-thirds of SMBs experienced at least one cybersecurity incident over a two-year period.[2]

In response to an expanding attack surface caused by rapid adoption of new technologies (such as cloud-based services and Internet-of-Things [IoT] devices), many SMBs have added point security products to address individual attack vectors. But this approach often results in complexity that inhibits overall security by increasing manual workflows for management and maintenance—not to mention lack of visibility for pinpointing the root causes of attacks or tracking potential issues because the different products cannot share information. The added pressures of limited staff and budget resources compound these problems. To keep up with these ever-increasing security threats, SMBs need to simplify, integrate, and automate their defenses for more effective protection across their entire network.

Market-leading Solutions for SMBs

Fortinet understands SMBs and their security requirements and continues to lead the market with a robust portfolio of security solutions. Core attributes of the Fortinet Security Fabric include:

- **Broad** visibility of the entire digital attack surface
- **Integrated** artificial intelligence (AI)-driven breach prevention
- **Automated** operations, orchestration, and security responses

As growing businesses add employees, offices, devices, and/or applications, these additions bring unforeseen risks. The Fortinet Security Fabric is designed to scale with business needs—providing top-rated protection from on-premises, to the cloud, to remote/branch locations, to end-user devices. And it is all managed through a unified console for simplified visibility and consistent control.

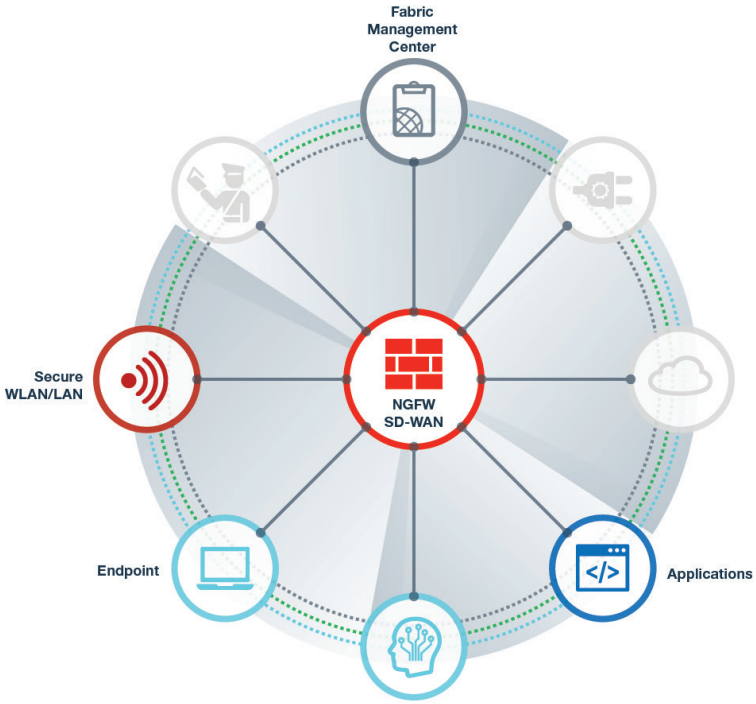

Figure 1: The Fortinet Security Fabric for the SMB enables multiple security technologies to work seamlessly across all network environments. This helps to eliminate security gaps and accelerate responses to attacks.

The Fortinet Security Fabric for the SMB includes three essential solution areas that correspond to the cyber-risk exposures of most SMBs:

Secure Access

The volume and variety of connected devices continue to increase for SMBs. This includes employee-owned mobile devices (which may have unpatched security vulnerabilities) and IoT devices such as "smart" office equipment and environmental controls (which frequently have no built-in endpoint defenses of their own). Greater network access demand from these kinds of sources means that there are many more opportunities for threats to breach the network.

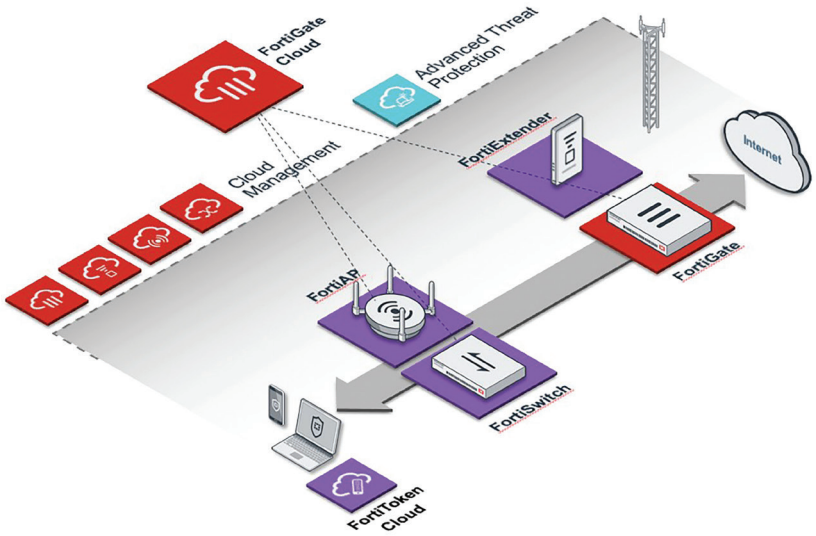

Figure 2: Fortinet Secure Access.

The foundation for the Fortinet Secure Access solution is the **FortiGate next-generation firewall (NGFW)**. A FortiGate NGFW consolidates several network and security operations functions in a single platform, including network firewall, intrusion prevention (IPS), anti-malware, virtual private network (VPN), WAN optimization, web filtering, application control, and wireless local-area network (WLAN) control. FortiGate NGFWs deliver high-performance protection that can extend to other parts of the Security Fabric architecture.

FortiGate Cloud provides a cloud-based management platform for FortiGate NGFWs. FortiGate Cloud enables the FortiGate to manage device connectivity via **FortiSwitch** (wired) switching and **FortiAP** (wireless) access points, enhance connection security, and deliver rich analytics and actionable reports. FortiGate Cloud also helps simplify the initial security deployment, setup, and ongoing management while providing transparent visibility of the infrastructure. Fortinet Secure Access also includes **FortiToken Cloud** user authentication to enforce access controls that prevent unauthorized users from gaining access to the network.

As a secondary WAN connection, **FortiExtender** uses LTE cellular phone connectivity to provide broadband speeds that can be used as a failover or for load balancing. For locations without a wired broadband option, FortiExtender can be used as the primary internet connection.

Secure Productivity

The Fortinet Secure Productivity solution includes strong endpoint device protection, email security, and protection against advanced threats, as well as cloud-based application controls.

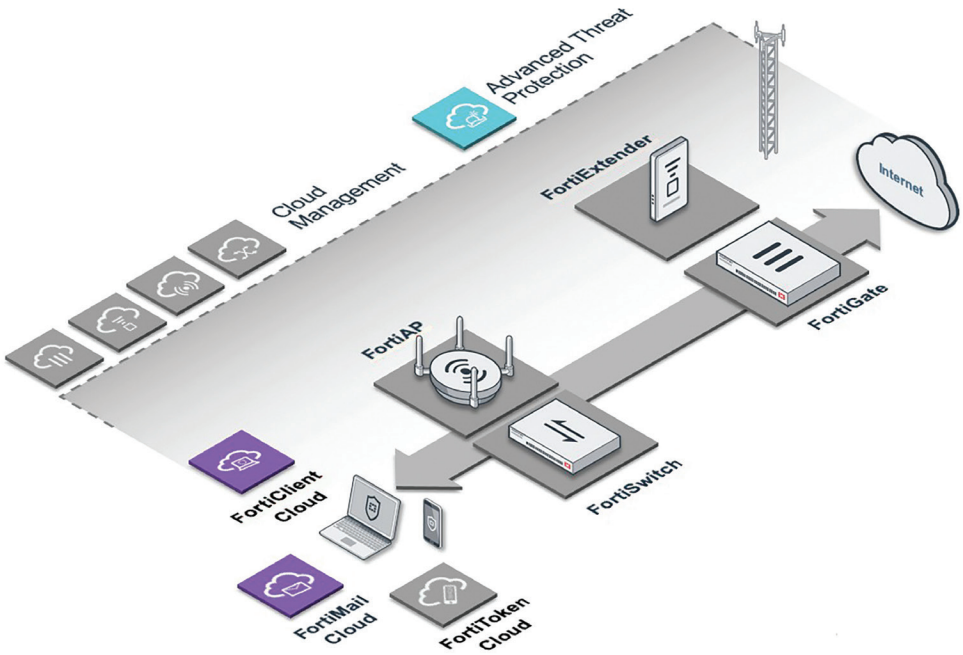

Figure 3: Fortinet Secure Productivity.

FortiClient Cloud provides businesses with cloud-managed advanced endpoint protection for mobile devices as well as IoT devices. Security Fabric integration helps FortiClient Cloud provide instant endpoint visibility through real-time telemetry and risk status—including unpatched vulnerabilities. It can then automatically contain threats by mitigating risky or compromised endpoints and alerting users. FortiClient Cloud also supports remote employee login with always-on secure VPN and two-factor authentication capabilities.

FortiMail Cloud inspects incoming and outgoing email to stop threats and prevent data loss. It provides comprehensive coverage, including antispam, antiphishing, anti-malware, data loss prevention (DLP), encryption, and message archiving. Fortinet Secure Productivity also includes **Advanced Threat Protection** in the form of top-rated sandboxing capabilities using **FortiSandbox** solutions for continuous analysis of suspicious email file attachments and URLs for previously unknown cyberattacks.

Businesses of all sizes also need application security for the popular cloud-based productivity suites they depend on every day—such as Microsoft Office 365 and Google G Suite. These applications deliver core business functions such as email, data storage, and office productivity tools employees need to access at all times and without fail. To secure use of these Software-as-a-Service (SaaS) applications, Fortinet also offers a cloud access security broker (both **FortiCASB-Cloud** and **FortiCASB-SaaS**) that inspects content in transit or at rest for threats using the latest threat-intelligence research findings from FortiGuard Labs.

Secure SD-WAN

SD-WAN helps distributed businesses with multiple locations or offices achieve faster connectivity, cost savings, and improved cloud application performance versus traditional WAN environments.

As a core Security Fabric element, FortiGate NGFWs also include **Fortinet Secure SD-WAN** capabilities. Secure SD-WAN combines branch networking and firewall security in a single, unified solution. It provides application visibility and control, high-quality voice and video delivery, as well as consolidated management of both networking and security operations.

Delivering Complete, Flexible, and Scalable Security

The dynamic business benefits of digital innovations mean very little if they lead directly to a loss of sensitive data, a compliance violation, and/or negative publicity that damages customer trust. With cyber-criminal attention focused on the perceived "low-hanging fruit" of smaller companies, decision-makers must find ways to do more with less. The Fortinet Security Fabric does precisely that—by integrating the disparate solutions that protect networks, it closes the gaps that threats can slip through.

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

[2] Jon Oltsik, "The state of cybersecurity at small organizations," CSO, August 16, 2018.

January 27, 2020 10:40 AM

304372-0-0-EN

C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\sb-smb-solution-selection\sb-smb-solution-selection Folder\sb-smb-solution-selection