FORTINET

WHITE PAPER

Small and Mid-Size Business Security: 4 Steps to Success

Executive Summary

A successful SMB focuses on two things above all: growth, and a shrewd oversight of cash flow. SMBs are attractive targets for hackers, and in the modern age, weak security can put a stop to both of those things.

Many SMBs struggle to implement strong, holistic security across their business for a variety of reasons and too often rely on piecemeal security cobbled together with multiple vendor point products that don't operate cohesively. Ultimately, this results in inflated costs and stagnating growth, as investing in technology that would help the business be more productive is delayed by security.

Fortunately, even with limited budgets and manpower, SMBs can significantly reduce their risk using the right technologies that were designed to work together and offer strong protection while maintaining ease of use. Here are four steps to modernize your business and set it up for future success so security remains tight without impacting growth.

What Is SD-WAN?
Software-defined wide-area networking enables businesses to take advantage of locally available internet pathways to reduce costs and gain better performance from cloud-based applications. Secure SD-WAN enables this with security applied to incoming and outgoing traffic.

Step 1: Invest in secure connectivity and protect data across your network

With the right investment in next-generation firewall (NGFW) technology, you can consolidate your product portfolio, reduce licensing costs needed to operate several different products, and make overall management of your IT environment easier and more cost-efficient.

Think of your NGFW as your most critical security tool. NGFWs monitor the network and provide understanding and insight into users, devices, and applications. This is Layer 7 inspection and means businesses can consolidate legacy routers and multiple security devices into a single device. Some NGFWs even enable SMBs to take advantage of networking technologies such as secure SD-WAN.

TCO per Protected Megabyte

Security Effectiveness
= Exploit Block Rate x Evasions x Stability and Reliability

TCO per Protected Mbps
= TCO / (Security Effectiveness x NSS-tested Throughput

What to Look For:

Understanding your business's bandwidth needs and accurately sizing the NGFW to ensure it can handle both incoming and outgoing traffic as well as analyze that traffic for threats is critical. NGFWs can get expensive, but they don't have to be. Paying close attention to security effectiveness and buying based on validated performance and total cost of ownership (TCO) per protected megabyte will set your business up for long-term success. Additionally, the ability to extend this security through other networking components like switches and wireless access points can further reduce your business risk.

The following considerations provide a basic checklist for evaluation:

- **Credible third-party validation:** Vendors will always put their products in the best light but should be tested by reliable sources. A credible third-party evaluator, such as Gartner or NSS Labs, provides detailed validation of NGFW solutions and other products.
- **Threat protection performance:** When the NGFW has all its security enabled—meaning providing firewall, intrusion prevention, antivirus, decryption, and application control capabilities among others—what impact does it have on network speed? Is it capable of maintaining security without sacrificing performance?

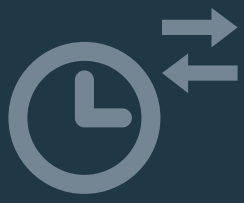
- **Price vs. performance:** Balancing an NGFW's cost with its performance can be tricky. While some NGFWs were designed with advanced capabilities for global enterprises, most SMBs simply don't need that. Finding a vendor that can provide right-sized solutions and modular functionality will ensure your team can consume the technology they have without overspending.
- **SSL inspection capacity:** By most accounts, roughly 80% of all internet traffic is now encrypted. Without decrypting and analyzing this traffic, threats can hide and invade your business. NGFWs need to offer adequate SSL inspection and decryption capabilities while still able to perform analysis and adequate throughput.
- **IPsec VPN performance:** Can you provide secure connections to company resources when users are not at the main office—whether they be at a branch location or working remotely?
- **Extensible security:** While the NGFW can analyze traffic coming in and leaving the office, non-internet-based attacks can quickly propagate to other users and devices via switches and access points. Can you enable these devices to act as additional security sensors stemming from the NGFW?
- **Easy, single-pane-of-glass management:** If you can't manage all of your NGFWs from a single application, you're hampering productivity of your team as they switch from portal to portal.
- **Future-proofing:** As your business grows and more advanced capabilities are needed, like secure SD-WAN to effectively and securely access cloud-based applications, does your NGFW provide these capabilities and features or will you need to replace it with a more capable vendor later and have to learn a different platform all over?

Step 2: Invest in securing applications delivered from the cloud

As cloud computing and Software-as-a-Service (SaaS) offer businesses flexibility and affordability, many SMBs are caught unaware that the responsibility for protecting information flowing through these services and their users rests on their shoulders. SaaS takes much of the oversight and ongoing maintenance responsibilities off the customer's shoulders but with that comes a loss of visibility into what's happening and the ability to control how data is being used. A good cloud access security broker (CASB) solution helps fix this.

What to Look For:

Just like you are able to scan your network for compliance and threats, and drill into user, device, and application usage on your own network with a well-designed NGFW, a CASB solution with application programming interface (API)-based access gives administrators the ability to do the same with SaaS applications. Additionally, out-of-the-box reports for common compliance and regulatory requirements help speed up audits and can monitor if users are sharing information within the application they shouldn't be.



Throughput: How much data can be transferred from one location to another in a given amount of time.

Enhanced Security for SaaS Email

As more businesses turn to Microsoft Office 365 and Google Mail to handle their email needs, so do attackers. Multiple threats now exist designed to circumvent the security included with these services like ShurL0ckr and Cerber. In fact, ransomware most commonly attacks businesses using email,[1] and 46% of all SMBs have been the targets of a ransomware attack.[2] As a best practice, introducing security specifically designed to handle email and weed out spam and other malicious communications is a solid step in protecting your business from the leading method of attack.

Step 3: Invest in protecting your users wherever they're working

More and more, users are working and accessing company resources outside the office. Ensuring they have the ability to communicate via a virtual private network (VPN) ensures the network security you have invested in keeps them safe. Combined with security on the endpoint, your users will be protected regardless if they forget to use VPN or if the attack originates from a source other than the internet.

What to Look For:

VPN capability shouldn't be an additional service, rather, it should be included as part of the NGFW and/or endpoint solution. What is important is the NGFW be able to decrypt incoming VPN traffic at a rate that doesn't impact user performance (making them want to disable it) and users can quickly verify their identity with easy two-factor authentication.

Search for endpoint security that not only offers machine learning and artificial intelligence to detect and stop new attacks but also communicates with your network security and other security products to reduce false alerts and enhance your entire solution's ability to identify threats.

Step 4: Control costs by streamlining and simplifying security, management, and ongoing operations

One of the biggest productivity killers all IT teams face is management, especially when multiple vendor products and solutions weren't designed to work together out of the box. While best-of-breed solutions can be stitched together with security information and event management (SIEM) technology or by creating a security operations center (SOC), these require significant resources to deploy and maintain.

What to Look For:

When products were designed to be used together with the same policies and rule sets, managing an entire security solution from a cloud-based, single-pane-of-glass view—that is, one window—enables teams to monitor network health and user activity from anywhere they have internet access and remediate issues with a few clicks.

Similarly, if your business is already investing in SaaS and comfortable with foregoing granular features and controls, Security-as-a-Service (SECaaS) is another cost-controlling option. However, unlike typical SaaS applications—whose effectiveness isn't impacted by integrated threat intelligence—a vendor who is able to provide a complete SECaaS platform will allow you to maintain a strong, proactive security platform based on automation and intelligence sharing to reduce both risk and long-term costs.

Conclusion

SMBs are popular targets for hackers, but they don't have to be. By investing in the right networking and security tools, SMBs can significantly reduce their risk using the technologies that were designed to work together, offer strong protection, and are easy to use and manage. Good investment decisions now will set you up well for the future and ensure your needs are met at every stage of growth.

[1] J. Clement, "Leading cause of ransomware infection, 2019," Statista, December 3, 2019.

[2] "More Than 1 in 5 SMBs Lacks Proper Data Protection," Infrascale, April 1, 2020.

September 18, 2020 1:21 PM

700979-A-0-EN

D:\Fortinet\Work\2020\September\091820\wp-small-business-security