WHITE PAPER

Small and Midsize Business Security: 4 Steps to Success

Executive Summary

A successful small to midsize business (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 resources, SMBs can get the complete protection they need without having to sacrifice functionality critical to growth or performance. With technology based off the same underlying code, businesses can better integrate and automate their security ecosystem and make the most of their resources to achieve maximum value from their investments. Here are four steps to modernize your business and set it up for future success.

Step 1: Create a Secure Office Network

Even as most companies pivoted to support a hybrid workforce, the main office remains a cornerstone of the business with the next-generation firewall (NGFW) sitting at its heart protecting and controlling traffic going in and out. While many NGFW vendors advertise their firewalls as "simple," this often comes at the expense of performance, interoperability, and limitations in functionality that impede growth. Choosing the right NGFW not only saves you time and money in the short- and long-term but it can make overall management of your environment easier and more cost-effective. Some NGFW vendors even include integrated SD-WAN and cloud management at no additional cost.

Once inside the perimeter, data must effectively move from place to place and users must be able to get online as they move around. This is accomplished through the network switch and wireless access points, respectively.

What To Look For

While a multi-vendor solution between these three critical components is an option, a single-vendor solution designed with the same underlying software eliminates many of the administrative hassles that stem from a multi-vendor approach, such as troubleshooting connectivity, security effectiveness, and licensing.

Across all three, however, the NGFW is the most powerful and important piece of a secure office network.

What Is SD-WAN?

Software-defined wide-area networking (SD-WAN) 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.

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)

The following considerations provide a basic checklist for evaluation:

- **TCO per protected megabyte:** NGFWs can get expensive, but they don't have to be when properly engineered. 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.
- **Credible third-party validation:** Vendors will always put their products in the best light but should be tested by reliable sources. An evaluator like Gartner 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?
- **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 secure sockets layer (SSL) inspection and decryption capabilities while still able to perform analysis and adequate throughput.

- **IPsec virtual private network (VPN) performance:** Can you provide secure connections to company resources when users are not at the main office?
- **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 (APs). 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: Support a Work-from-anywhere, Hybrid Workforce

When COVID hit, many businesses continued to grow by pivoting their infrastructure to support an entirely remote workforce. VPN technology enabled secure access for remote employees to company resources, and better NGFWs were purchased to handle the sudden demand for greater VPN throughput. SD-WAN was used more effectively to maintain application performance across videoconferencing and other bandwidth-hungry applications. Additionally, endpoint protection, detection, and response gained in notoriety as users were no longer protected by company-owned network security.

Regrettably, when the dust settled and employees went back to the office, now in a hybrid work environment, a significant obstacle was often discovered. The technology driving the secure office network did not easily integrate and communicate with the endpoint and remote user protection technologies. This separation of systems added to complexity and ultimately raised operational costs. To avoid this and build a more streamlined, easy-to-manage solution, find a vendor who delivers both of these critical pieces.

What To Look For

When technologies share a common operating system, their ability to quickly and easily share information is naturally better and easier than technologies that require additional integrations and configuration to communicate. The more components closely operating together, the more cohesive the security fabric, the more effective the security, and the more streamlined operations become.

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 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.

Native network and endpoint integration: With tight integration between the NGFW and endpoint protection, network policies continue to be enforced through the endpoint agent even when off-network. Additionally, management can be consolidated through the NGFW enabling network access controls based on endpoint risk reducing the attack surface.

Endpoint protection: Differentiating between when only basic antivirus is needed versus more advanced threat protection and endpoint detection and response (EDR) has become much more blurry. Despite their relative size, many SMBs are utilizing much more mature technology than was once unavailable to them years ago. This adoption has led to a much wider attack surface and more sophisticated threat risk. Businesses would be wise to seek out a vendor that offers differing levels of protection while paying close attention to third-party validation to ensure it really works.

Secure access and VPN: For most businesses, an easy-to-use client VPN solution is necessary to safely operate in a hybrid environment, but it should not be a disconnected point solution. Finding a solution that is included with capabilities, such as always-on, to ensure employees are properly using VPN and split tunneling to reduce load will go a long way.

Two-factor authentication: Even with all of a business's security, credential theft remains a predominant threat with usernames and passwords going for pennies on the black market. Two-factor authentication is one of the easiest, least expensive methods of protecting against this problem.

Step 3: Secure Cloud Applications and Email

No matter your business size, taking advantage of the operational savings and scalability the cloud offers is often on the top five strategic priorities IT teams have on their list. Though the possibilities are exciting, what isn't is managing a consistent security posture as data fluidly moves across different cloud vendor infrastructures. When comparing cloud providers, the decision to choose a single- or multi-vendor cloud infrastructure is hard enough; with the right security vendor, however, at least managing security across these platforms can be easy.

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 cloud access security broker (CASB) solution with application programming interface (API)-based access gives administrators the ability to do the same with Software-as-a-Service (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.

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 rulesets, 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] Joseph Johnson, "Leading cause of ransomware infection, 2020," Statista, February 16, 2021.

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

May 22, 2021 4:10 AM

700979-B-0-EN