FORTINET

EXCLUSIVE NETWORKS

WHITE PAPER

How SMBs Can Secure Endpoints and Remote Workers for the Long Haul

4 Pieces of a Successful Solution

Executive Summary

Like their larger counterparts, small and midsize businesses (SMBs) have had to build or scale a work-from-home infrastructure. Many have seen great benefit from remote workers, but having a large number of users outside the corporate network changes cybersecurity priorities and increases risk.

In this "new normal," SMBs do well to pay attention to four pieces as they work to secure their remote work infrastructure: an easily managed virtual private network (VPN) solution, effective two-factor authentication, robust endpoint security, and end-to-end security integration. Delivering all four of these priorities will put SMBs in a good position to protect their assets, enabling them to survive and thrive in growing competitive market.

83% of consumer routers sampled had at least one unpatched vulnerability and the average device had an astounding 186 unremediated security flaws.[1]

Working from Home: A New World for Many SMBs

Starting in 2020, enabling a remote workplace was necessary for businesses of all sizes to continue operations. While many SMBs already had some employees working remotely with limited risk prior to this shift, running an entire organization remotely was a big change for many of them. According to one study, only 46% of SMBs had remote workers before the spring of 2020.[2] Now, 70% of SMBs have employees working from home—and 62% expect to continue supporting at least some remote workers indefinitely.[3]

Remote Work: New Security Challenges for SMBs

Of course, remote work at its current scale is not without its challenges. For one thing, it greatly impacts an organization's cybersecurity posture. Even when users are purely within the perimeter of a business's network, many small information technology (IT) teams have difficulty maintaining visibility and control, given the pace of new technology adoption and shifting business requirements. Still, corporate IT at least had the ability to control patch management across network devices like wireless access points, switches, and other office equipment.

With most office workers now working remotely, SMBs no longer enjoy this level of control. Users now connect through home office devices and networks that corporate IT does not own or manage, and into which they have no visibility. Unlike IT members at the office, regular users typically do not think twice about the security of their internet connection—whether for personal or work use. One study found that 79% of SMBs are worried about their remote devices or remote employees being breached.[4]

When employees work from home, their work traffic travels through these largely unsecured devices and across the public internet before reaching the corporate network and the company's cloud-based resources. This makes them easy targets for man-in-the-middle (MITM) attacks, in which a cyber criminal eavesdrops unsecured communications and monitors the data moving between. Breaking through the limited defenses of a consumer-grade router and spying on their traffic is simply not that difficult for most hackers—especially when the device is unpatched.

Four Keys To Success

This white paper delves into this new world of endpoint and remote worker protection from the perspective of the SMB. On the coming pages we discuss four essential pieces of a successful program. Focusing on these priorities will help resource-strapped businesses hone their financial and human investments where they will matter most.

Secure Communications: Not All VPNs Are Created Equal

In many ways, VPNs made remote work possible for larger enterprises two decades ago. They have seen mainstream use for at least 15 years.[5] The idea is that a remote worker can use an encrypted connection (called a "tunnel") to a server in the employer's data center, enabling secure access to corporate resources, regardless of the security of the remote internet connection.[6]

The growth in the number of remote workers and the increasingly advanced threat landscape mean that all businesses, regardless of size, need a VPN solution.[7] However, purchasing a disconnected point product may not be the best approach. Like the addition of any standalone product, IT teams should consider the additional management cycles that come with such a purchase along with whether or not functionality like auto-connect and/or always-on mode is available or split tunneling is offered.

"70% of SMBs have employees working from home—and 62% expect to continue supporting at least some remote workers indefinitely."[8]

Without a VPN, hackers can see the data that's in transit and follow the trail to identify and reach your IP address.[9]

Auto-connect and/or Always-on: Enforcing VPN Usage

As discussed, MITM attackers take advantage of a poorly secured endpoint to eavesdrop on traffic or even impersonate the legitimate user in communications with others. Companies are protected against such attacks when their remote workers access corporate resources through a VPN tunnel. However, if activating the VPN requires action on the part of the user, this introduces the risk of human error—namely, forgetting to turn on the VPN. Given that most users have multiple personal devices that do not require this step, this oversight is not uncommon.

This means that SMBs need to ensure that their VPN solution enables administrators to enforce VPN usage—either with an always-on setup or with automated activation of the VPN any time the device is outside the corporate network. By ensuring that the VPN is activated when an employee is off-site, organizations can protect their network traffic from prying eyes—regardless of the security of the internet connection it is using.

Split Tunneling: Directing Traffic To Address Performance Issues

Historically, when remote users needed to access the public internet, they would do so from the corporate data center via the VPN tunnel, rather than from their own home connection. This system worked well when internet use was largely limited to browsing, but the cloud computing revolution changed that calculation. Since resources like Software-as-a-Service (SaaS) applications, streaming services, and cloud-based storage are accessed via the internet and require substantial bandwidth, corporate internet servers see much more traffic than in the past.

Legacy VPN solutions often have problems with latency, as limitations in firewall bandwidth and the extra computing required by encryption created bottlenecks. This problem is compounded exponentially as the number of remote workers—and the amount of cloud traffic—increases. VPN solutions with split tunneling distinguish between traffic that is destined for resources in the corporate data center and internet-bound traffic. The latter is directed away from the VPN tunnel and directly to the internet. SaaS applications and other cloud-based resources would then be protected by security protection at the cloud edge or directly through the SaaS vendor.

Two-factor Authentication: User-friendly Protection Against Credential Theft

By definition, every login credential provides access to something that an organization does not want to be available to the general public. While some may be relatively low risk, think of what would happen if a single login to a VPN tunnel were compromised. The benefits of the VPN's secure encryption would be annulled, and a hacker could conceivably move laterally around the network undetected for days, weeks, or months.

This risk is not merely theoretical. The unauthorized use of login credentials is behind numerous intrusions and breaches. Verizon's latest Data Breach Investigations Report found that 37% of overall breaches involved the use or theft of credentials.[10] This includes 73% of cloud breaches and 80% of breaches in the "hacking" category. For many companies, the risk of credential theft has grown in recent months as more employees are working from home and are more susceptible to phishing and other credential-stealing strategies.

Two-factor authentication enables an extra step of user verification without slowing down the business. In addition to providing a username and password, those logging in are also required to enter a unique code sent to a physical device on the user's person—usually either a small physical token, or more commonly, a software-based token on the user's mobile device.

Again, buying another standalone solution has its challenges when it comes to identity and access management. It is best to seek a solution that is a part of an integrated security architecture. This way, policy control and workflows are natively integrated as part of the network security design. As a business grows, this also provides a foundation on which a more robust zero-trust access strategy can be built. To improve the user experience, IT teams should also look for options that include the use of software-based tokens on mobile devices.

As time goes on, it appears that attackers become increasingly efficient and lean more toward attacks such as phishing and credential theft.[11]

Endpoint Security: Adding Protection Where Users Are

As more remote users spend some or all of their work time outside the corporate network, a perimeter-based approach to security makes less and less sense. For leading SMBs, the reality is that the traditional concept of a perimeter is no more. Employees are likely already accessing corporate email and other resources on their mobile devices. Now, they may spend all day working at their corporate laptop from home—or even from a parking space near a public Wi-Fi hotspot. At the same time, even some of the smallest businesses now have Internet-of-Things (IoT) devices connected to their networks, gathering and monitoring metrics and sharing data with larger centralized systems to improve productivity and efficiency. While all these trends support corporate growth, they also shift how the company must approach endpoint protection.

Endpoint Visibility and Hygiene: No Longer Optional

Unmanaged devices and bring-your-own-device (BYOD) policies and controls are often less formal at smaller organizations, which leads to risk. There are many ways attackers can learn what applications are in use at an organization. They use that knowledge to target those applications, exploiting vulnerabilities through drive-by downloads, phishing campaigns, or other means of injecting malicious code. Drive-by downloads are unauthorized transmissions of software onto a laptop or mobile device. Once the software is installed, adversaries can spy on the user, erase or corrupt data on the device, or even hijack a device to become part of a botnet to infect other devices.

Such attacks are much easier when an organization lacks awareness of what devices are connected to the network, which user each device is associated with, and whether each device is current on patching for each of its applications. SMBs should seek an endpoint security strategy that brings full visibility to each device and automates patching policies to ensure applications are up to date with the latest fixes.

Achieving this visibility and control without disrupting workers' productitivy requires tight integration to ensure that policies are not conflicting, data is properly shared to understand the full context of a request, and less time is spent troubleshooting. SMBs should seek a vendor that can provide a broad set of security tools that natively integrate and provide consolidated management to provide a centralized view of every device, its compliance with security policies, and the identity of its user.

Advanced Threat Protection and Automation: Combating Malware, Exploits, and Ransomware

As with larger businesses, basic signature-based antivirus is no longer adequate for most SMBs as they adopt more sophisticated technology that expands their attack surface. Attackers are now capable of creating tens of thousands of malware variations in a matter of seconds, requiring a more advanced form of analysis. Additionally, advanced threats considered "old" when used against enterprise-size targets have found new life and are successful when used against SMBs that have failed to implement more advanced protection.

In a recent analysis of SMB Cyber Threat Assessment Programs (CTAPs) run on potential clients, Fortinet found that 56% of those participating had one or more significant application vulnerabilities, malware, or botnets in their ecosystem. It is no wonder ransomware attacks against SMBs are on the rise, and many see no alternative but to pay the ransom.[12] This is why companies should also seek out a solution that is capable of rolling back systems to a state prior to an attack as a last resort.

Ideally, however, the attack would never get through in the first place. An ideal solution should prevent threats with multiple layers of protection and be continually updated with the latest real-time threat intelligence. Technology such as artificial intelligence (AI) and

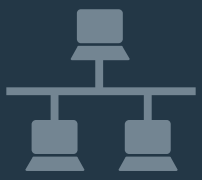
machine learning (ML) should be used to understand and dissect known threats in order to prevent unknown future ones—but a model is only as good as what it learns from. The vendor's threat intelligence network should be built from a wide range of customers of different industries, sizes, and geographies—and this information needs to be shareable, in real time, across a company's security architecture automatically.

Web Filtering: Extending Protection To the Endpoint

When everyone is working in the office, corporate policies established at the firewall can block access to malicious, risky, or inappropriate websites, protecting the network against web-based attacks. But when employees use a corporate device outside the network, those protections often fall away as the users' traffic is no longer necessarily traveling through those firewalls.

The best practice is to find a solution capable of shifting corporate web policies to the endpoints even as users work remotely. With this, a device benefits from the same policy-based protection no matter where it is located.

As organizations expand and more employees work remotely, the number of vulnerable endpoints grows.[13]



"Now more than ever, it is essential that security tools no longer be deployed as separate pieces of the network."[14]

Integration: Ensuring Complete Security

It may seem natural to choose the "best of breed" for each security element—based on whatever parameters make sense for a particular business and department. However, for SMBs with limited staff to properly configure and maintain a unique mixture of technology pieces, the resulting security is often much weaker than that of a single-vendor approach. Lack of full visibility and understanding of the impact of change leads many IT teams to fear making improvements while attackers continually modify and tune their approaches.

Ultimately, integration and automation are necessary to maintain and operate a complete security solution with limited staff. An integrated security architecture almost always requires less staff time to administer. Further, when each part of your ecosystem was built with the intention of working together, security complexity is minimized. Single-pane-of-glass visibility enables quick decision-making and timely threat response, and additional pieces can be added as the company's needs mature. This allows cybersecurity protection to easily scale as a business grows—without ripping and replacing infrastructure.

Conclusion: A Holistic Strategy

2020 was among the most challenging years in recent memory for many SMBs: Businesses not only had to adapt how they went to market but also faced increased risk as attackers preyed on the unprepared. In such an environment, where the sheer survival of the company may be in question, it may be tempting to seek a "quick fix" to individual cybersecurity issues—or even defer doing anything at all. However, with cyber threats increasing, the best approach is a strategic, holistic approach.

SMBs that focus on the four pieces of remote worker cybersecurity that we have discussed in this white paper will be well-positioned to take advantage of the coming recovery and thrive as a business. Getting this right may be the best investment of time and resources that a company can make right now.

[1] "Securing IoT Devices: How Safe Is Your Wi-Fi Router?" American Consumer Institute, September 2018.

[2] "Key statistics for small business and coronavirus," ZenBusiness, accessed November 22, 2020.

[3] Ibid.

[4] Jay Ryerse, "The State of SMB Cybersecurity in 2020," ConnectWise, September 24, 2020

[5] Chris Partsenidis, "A history of VPN: Disadvantages of early virtual private networks," TechTarget, accessed November 29, 2020.

[6] Jeff Tyson, et al., "How a VPN (Virtual Private Network) Works," HowStuffWorks, May 24, 2019.

[7] Gitanjali Maria, "The Benefits of VPN and Why All Businesses Need One," GetApp, April 30, 2019.

[8] Sandeep Rathore, "57% of Small Business Owners Believe Remote Work Will Continue After Stay-at-Home Orders Lifted," Small Business Trends, July 22, 2020.

[9] Gitanjali Maria, "The Benefits of VPN and Why All Businesses Need One," GetApp, April 30, 2019.

[10] "2020 Data Breach Investigations Report," Verizon, April 2020.

[11] Ibid.

[12] "46% of SMBs have been targeted by ransomware, 73% have paid the ransom," Help Net Security, April 21, 2020.

[13] "The Importance of Endpoint Security," Security Boulevard, August 13, 2020.

[14] John Maddison, "Securing Remote Workers Requires an Integrated Approach," Fortinet, September 14, 2020.

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

December 23, 2020 4:33 AM

870512-0-0-EN

D:\Fortinet\White Paper\Grey White Paper\GREY - Endpoint and Remote User Protection\wp-FA-how-smbs-can-secure-endpoints-12322020\wp-FA-how-smbs-can-secure-endpoints-12322020