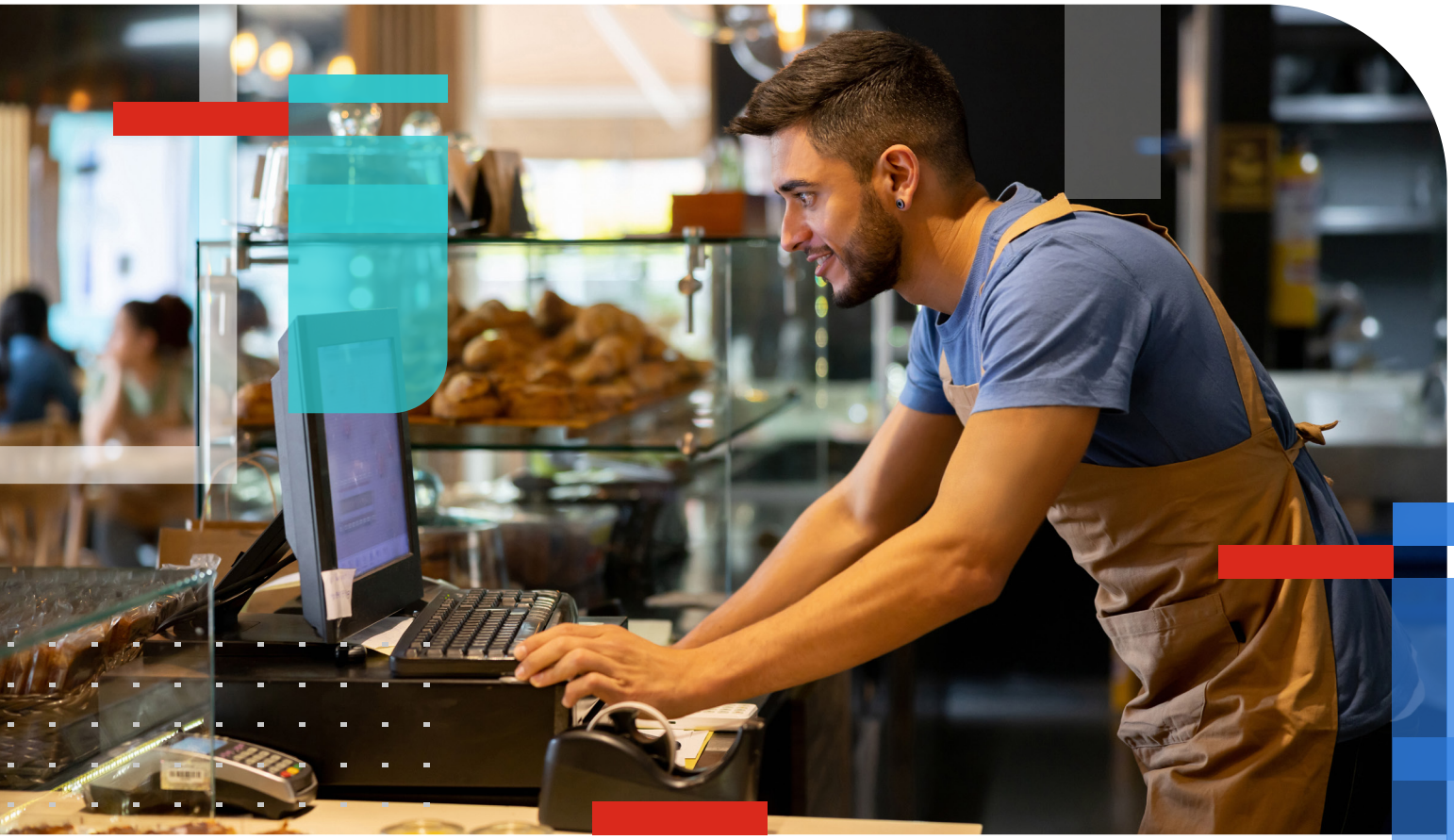
WHITE PAPER

4 Steps to Successful Small Business Cybersecurity



Executive Summary

A successful small business focuses on two things above all: growth and cash flow. However, if it has weak cybersecurity, the company can quickly lose focus on these priorities. Smaller enterprises are attractive targets for cybercriminals, and a successful attack can devastate them.

For various reasons, many small and midsize businesses (SMBs) struggle to implement strong, holistic security. Too often, they rely on piecemeal cybersecurity cobbled together with multivendor point products that don't operate cohesively. Ultimately, this results in inflated costs and stagnating growth. Security concerns, delays, waste, and extraneous expenses delay investment in technology that would help the business be more productive.

Organizations with fewer than 500 employees reported that the average impact of a data breach had reached $3.31 million, a 13.4% increase from 2022.[1]

Fortunately, even with limited budgets and resources, SMBs can get the complete protection they need without sacrificing functionality critical to growth or performance. With technology based on the same underlying code, businesses can better integrate and automate their security ecosystem and make the most of their investments.

4 Steps to Modernize Your Business Protection

Step 1: Create a Secure Network

Even as most companies have 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.

Building a secure office consists of seamlessly integrated NGFWs, switches, and wireless devices working together with the same consistent security policy across users and devices. This convergence saves time and money and can also make the overall management of your environment easier and more cost-effective.

Once inside the perimeter, data must effectively move from place to place, and users must be able to get online. This is accomplished via the network switch and wireless access points (APs), respectively.

What to look for

One option is a multivendor solution with these three critical components: firewall, switch, and wireless access points. However, a single-vendor solution designed with the same underlying software eliminates many of the administrative hassles that stem from a multivendor approach, such as troubleshooting connectivity, security effectiveness, and licensing.

An NGFW is the most powerful and important piece of a secure office network. The following considerations provide a basic checklist for evaluation:

- **Credible third-party validation:** Vendors will always put their products in the best light, so they should be tested by reliable sources. Analysts such as Gartner provide detailed validation of NGFW solutions and other products.
- **Security enriched by artificial intelligence and machine learning:** Today's cybercriminals use emerging technologies to create advanced attacks. AI in cybersecurity can help analyze network traffic, detect malicious behaviors, and provide your business with more comprehensive protection against cyberattacks.
- **Threat protection performance:** When the NGFW has all its security enabled—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?
- **Secure sockets layer inspection capacity:** Google estimates that 95% of website traffic is encrypted.[2] Without decrypting and analyzing internet traffic, threats can hide and invade your business. NGFWs must offer adequate secure sockets layer inspection and decryption capabilities while performing analysis and adequate throughput.

- **Secure connectivity:** 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 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 your security solutions with the coordinated policy from a single application, you're hampering team productivity and increasing security risks.
- **Future-proofing:** As your business grows and more advanced capabilities are needed, such as secure SD-WAN to access cloud-based applications effectively and securely, does your NGFW provide the needs? Or will you need to purchase and integrate additional solutions to support the growth?

Organizations with extensive use of security AI and automation reduced 66% of the time to identify and contain a breach when compared to organizations with no use.[3]

Step 2: Enable Work-from-Anywhere Users with Secure Access

With the increase of their work-from-anywhere (WFA) users, SMBs must ensure their employees have secure access to the network and applications. VPN and zero-trust network access (ZTNA) technologies can connect WFA users and devices to corporate networks. While VPN provides direct tunneled access to an endpoint on a corporate LAN, ZTNA provides more granular access to explicitly authorized applications and services.

The technology driving many secure office networks does not easily integrate and communicate with endpoint and WFA user-protection technologies. This separation of systems adds to complexity and ultimately raises operational costs. To avoid this and build a more streamlined, easy-to-manage solution, find a cybersecurity vendor delivering both critical pieces.

What to look for

When technologies share a common operating system, their ability to share information quickly and easily 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.

- **Native network and SASE integration:** For WFA users, direct internet access expands security risks. With tight integration between NGFW and secure access service edge (SASE), businesses can ensure that security policies are applied and enforced consistently for users regardless of their locations.
- **Endpoint protection:** As an increasing trend of the hybrid work model, employees are accessing their email, applications, and corporate resources outside of their workplaces. This shift has led to a much wider attack surface and more sophisticated threat risk. An endpoint agent integrated with NGFW can help detect and defuse malicious events on their devices efficiently to reduce cyber risk and provide end-to-end protection with a cohesive corporate security posture.
- **Secure access and ZTNA:** For most businesses, a SASE approach helps address challenges from today's hybrid workforce by providing secure access and high-performance connectivity. Deploy a solution that provides integrated SASE with ZTNA to provide consistent protection for WFA users.
- **Two-factor authentication:** Credential theft is 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: Enforce Consistent Cloud Application Security

No matter the size of your business, taking advantage of the cloud's operational savings and scalability is often one of the top strategic priorities IT staff have on their list. Though the possibilities are exciting, there are challenges. One of the biggest is managing a consistent security posture as data fluidly moves across different cloud infrastructures.

Choosing a single- or multivendor cloud infrastructure is difficult when comparing cloud providers. However, managing security across these platforms can be easy with the right security vendor.

What to look for

Just like you can scan your network for compliance and threats and drill into user, device, and application usage on your network with a well-designed NGFW, a cloud security solution with application programming interface-based access gives you 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 alert users if they are sharing information within the application they shouldn't be.

Step 4: Simplify Security, Management, and Ongoing Operations

Managing the sophisticated network security solutions necessary to protect organizations from cyberthreats is critical. However, it can be challenging for SMBs with limited resources and expertise to deal with the increasing numbers of devices, users, and cloud applications. Deploying and configuring multiple network security devices—in some cases across multiple sites—can be time-consuming. The dynamic threat landscape requires security solutions to be continuously updated to protect from the latest threats.

What to look for

When products are designed to work together with the same policies and rulesets, managing an entire security solution from a cloud-based, single-pane-of-glass view enables IT people to monitor network health and user activity from anywhere they have internet access and remediate issues with a few clicks.

Similarly, cloud-based management is another cost-controlling option if your business is already investing in SaaS and is comfortable with the foregoing granular features and controls. Look for a vendor who can provide a simple, integrated platform that allows you to maintain a strong, proactive security ecosystem based on automation and intelligence sharing to reduce both risk and long-term costs.

Conclusion

SMBs are popular and enticing targets for cybercriminals because they are "low-hanging fruit." But they don't have to be. By investing in the right networking and cybersecurity tools, SMBs can significantly reduce their risk using 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 for the future and ensure your needs are met at every growth stage.

[1] Cost of Data Breach Report 2023, conducted by Ponemon Institute and sponsored and published by IBM Security, 2023.

[2] "HTTPS encryption on the web," Google Transparency Report, accessed January 25, 2024.

[3] Cost of Data Breach Report 2023, conducted by Ponemon Institute and sponsored and published by IBM Security, 2023.

January 30, 2024 12:01 PM

2527268-0-0-EN