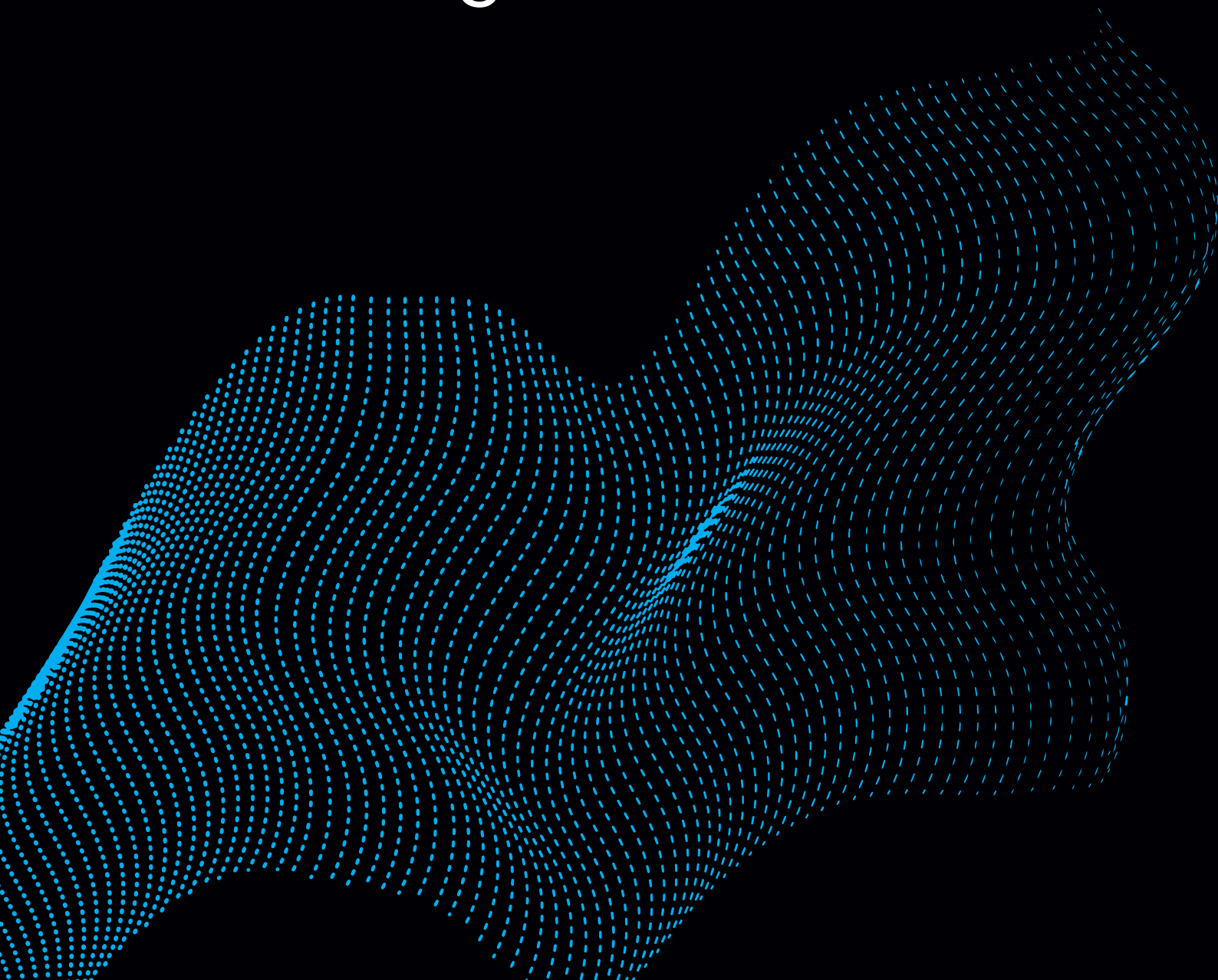
CyberFOX™

eBook

Beyond the Firewall and VPNs:

The Ultimate SMB Guide to Securing Data and Minimizing Business Risks



Why data breaches and ransomware are popular in the worst ways, and how SMBs can fight back.

In this eBook, we examine the current threat landscape facing small and mid-sized businesses (SMBs) in the US, providing detailed statistics on the latest figures. We delve into the common reservations SMBs express regarding the adoption of the latest cybersecurity measures available to them, and we address these concerns with clear, data-driven arguments.

The discussion continues with an overview of proactive steps SMBs can undertake to counteract bad actors. We then detail how Zero Trust Network Access (ZTNA) solutions, like Timus SASE, serve as a formidable tool in the arsenal of SMBs to safeguard themselves, their employees, and their clients within the ever-evolving risk economy.

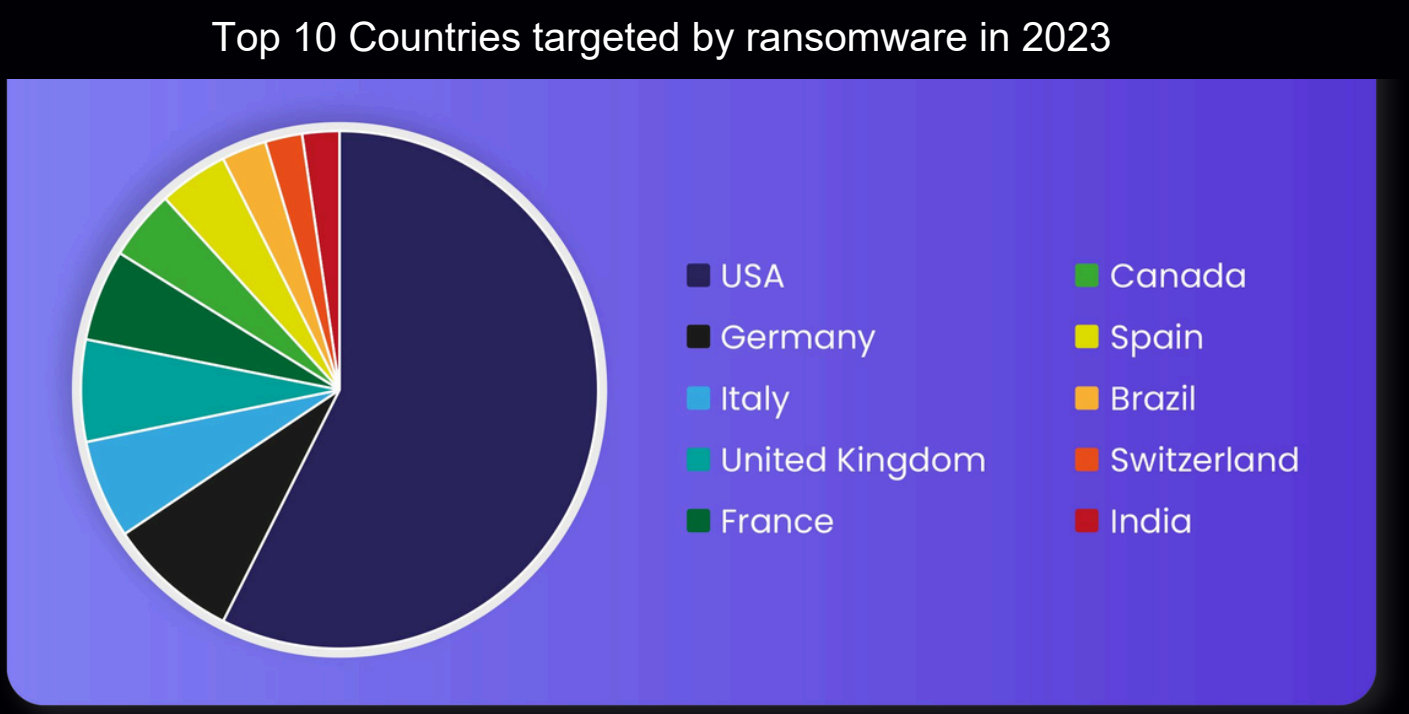


Figure 1: US remains as a robust playground for bad actors

In 2024, the top five causes of loss for SMBs continue to be ransomware, business email compromise, hacking, theft of money, and staff errors. As a committed ally to businesses of all sizes, our aim with this ebook is to steer SMBs towards adopting stricter security protocols.

Let's begin by addressing some of the most prevalent objections from SMBs regarding the adoption of modern cybersecurity measures.

Common SMB Objections to Modern Security Measures:

1. "We are not big enough for hackers to care"

More than half of SMBs think that they are too small to be hacked; hence the reason they say for not needing to move to the latest cybersecurity measures like ZTNA. This is the result of a misunderstanding of how varied and effective the current hacking methods are. If we use the analogy of a bowling alley, hackers today can easily send out a "ball" to hit whatever "pins" they can hit - in fact using this technique, they can steal more data in less time than going after a bigger target.

In fact, according to the Verizon 2023 report, 43% of all cyberattacks actually target small businesses, and this number is only increasing as we will see below.

> "While bigger businesses can often dedicate greater resources towards cybersecurity, small and medium-sized businesses and entrepreneurs face **the same cybersecurity challenges and threats** with limited resources, capacity, and personnel."
>
> - *US Department of Homeland Security*

2. "I never hear about it!"

In this case, it is true that we hardly hear about smaller businesses getting hacked, in between the news about major company data breaches like MGM, Okta, or the world's largest bank ICBC. A key reason for this is that the large enterprises are required by law to disclose data breaches to consumer reporting agencies. Plus it brings in more ratings. Therefore, you will never hear about the 100s of SMBs having all their data stolen and going out of business because of it.

Contrary to common belief, for example in 2023, 82% of ransomware attacks were against companies with fewer than 1,000 employees. And 37% of companies hit by ransomware had fewer than 100 employees.

There is then no wonder why SMBs are in the sweet spot for hackers. Not only do they get less resistance, but also less scrutiny from the FBI, Homeland Security, or other government entities with a lower risk of capture.

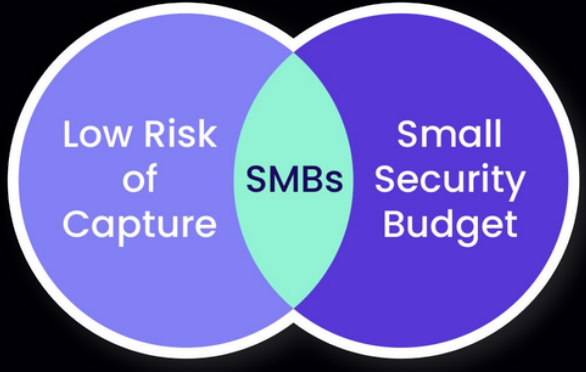


Figure 2: SMBs are a sweet spot for hackers

Common SMB Objections to Modern Security Measures:

3. "We don't have sensitive data"

Some SMBs think that they have no data that would be of interest to hackers. This would be true if not every company had HR, payroll data, and a business email address! Add on top of this, if the company is accepting payments, then there is the customer data, along with compliance considerations like PCI.

4. "We have cyber insurance!"

Another objection from SMBs for why they don't need enhanced cybersecurity measures is that: "We have insurance, we'll just file a claim." This is again a misunderstanding of how cyber insurance works. Firstly, not all cyber insurance is created equal. Unless it is a standalone policy, vs an add-on to another line of coverage, the limits for claims will be way less than needed to cover the overall cost of a successful cyberattack. The standalone cyber insurance rates have been increasing 25%+ per quarter since 2021, and it is significantly higher for companies with a previous claim, or even worse, it might result in non-renewal! Additionally, security requirements that are needed to be eligible for a successful claim or a renewal are becoming stricter each year.

In fact, the numbers are sobering. SMBs accounted for a staggering 98% of cyber claims from 2018 to 2022, with an average incident cost of $865,000 in 2022. Ransomware has emerged as the biggest threat, with SMB claims rising from $514,000 in 2021 to $555,000 in 2022.

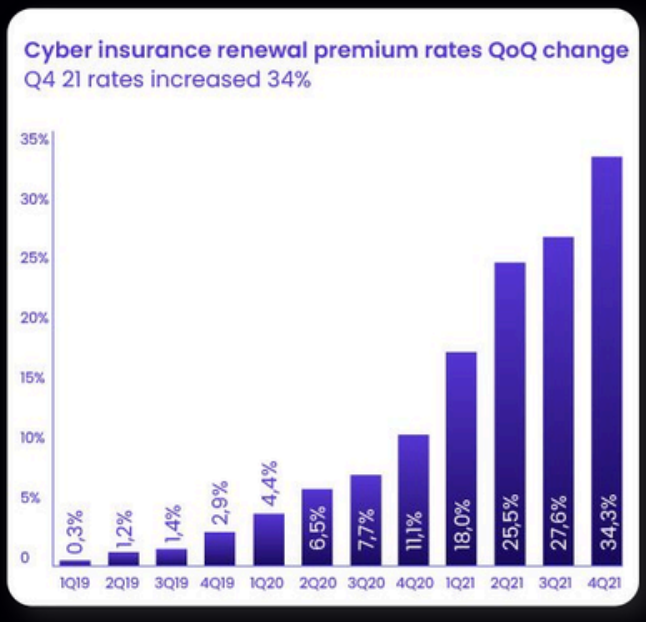


Figure 3: Rates have been increasing 25%+ per quarter

Figure 4: US cyber insurance premiums surged 50% in 2022 as ransomware attacks and online commerce drove demand for coverage

Figure 5: Getting claims approved is not guaranteed

Common SMB Objections to Modern Security Measures:

5. "We only use SaaS apps"

Another frequently heard objection from SMBs is that they don't have on-premise or cloud data other than what exists in the SaaS applications they frequently use, and that these apps are already protected.

Any short google search will show the myriad tools bad actors have in their arsenal to steal SaaS credentials and access the company network. In fact, business email compromise is one of the worst breaches that can befall an organization in this way, as you can see in the example scenarios below.

There are many ways to steal SaaS system/app credentials; most used ones remain email/SMS phishing and credential stuffing, because they still work! Add to this the Multi-Factor/2-Factor Authentication (MFA/2FA) fatigue among employees, plus the ways to circumvent them by hackers, the situation becomes no joking matter.

Credential stuffing is the re-use of stolen credentials, often from leaked password databases, in an attempt to login to other apps. This is often successful due to the tendency of users to utilize the same password between multiple systems, and accounts. This is particularly effective against heavy users of SaaS apps as the higher the number of accounts in use, the greater the chance that a compromised password hasn't been changed.

These attacks can be made even more effective by matching personal and corporate email addresses, as well as guessing likely similar/incremental passwords.

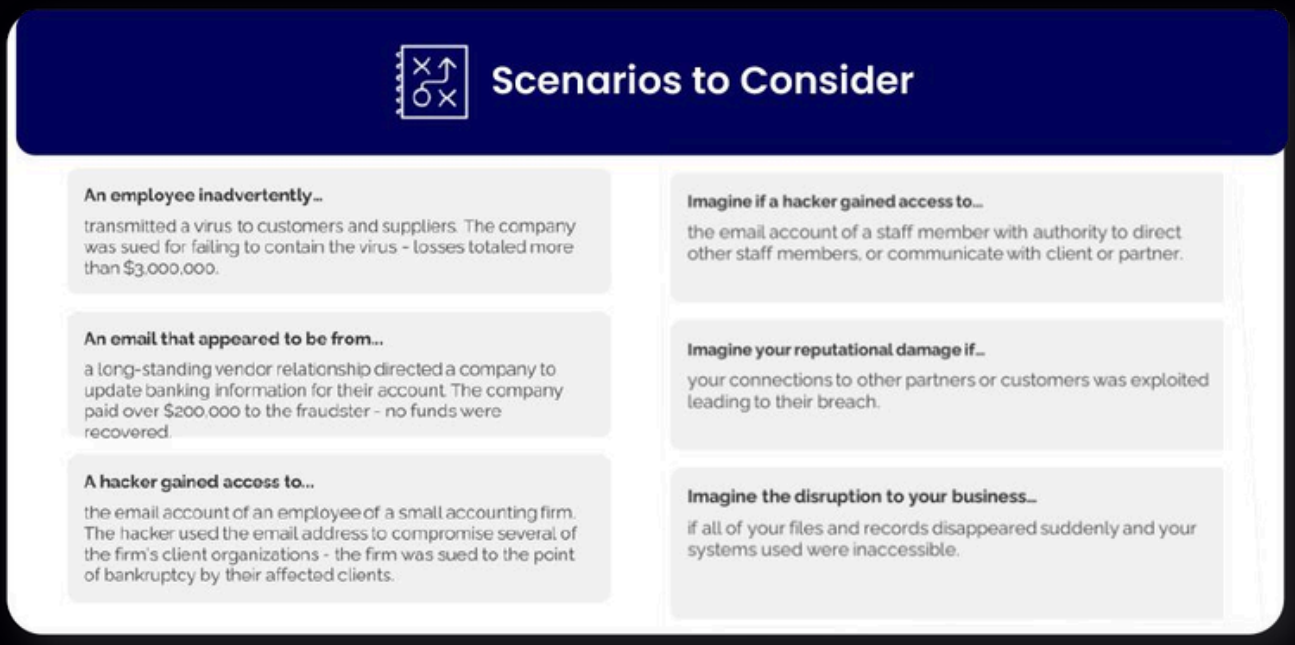


Figure 6: Business email compromise can result in serious consequences

Common SMB Objections to Modern Security Measures:

It is thus not surprising that SMBs get **400% more phishing attempts than enterprises.** Why? It's because hackers are smart entrepreneurs and know that their ROI will be higher with SMBs due to limited employee training, resource constraints, limited number of cybersecurity tools, limited expertise in cybersecurity, and poor configuration of existing systems in place.

Human error still accounts for more than 90% of cyber instances within a company. If a business employs people, no matter the business size, there's always risk. Whether unintentional or malicious, the human factor in security must be accounted for and proactively addressed with a security strategy that includes prevention, response, and recovery measures.

6. "Our company uses VPNs for remote users"

As much as traditional VPNs are better than not using any type of encrypted access to company resources, they still come with several disadvantages and real security risks. Firstly, traditional VPNs are clunky, frequently affecting user experience on their devices. This is one of the main reasons users don't like to use VPNs, and often will forgo using it. Since VPN usage is left to an employee, in addition to leaving the user exposed to man-in-the-middle attacks on public Wi-Fi, it also causes gaps in security and network visibility from the IT admin side. Traditional VPNs cannot be configured to be always-on. To top it off, VPN credentials are easily stolen by social engineering and phishing, and once a hacker is in via stolen VPN credentials, he or she can move laterally within the network potentially resulting in catastrophic consequences.

Cost Considerations of a Data Breach for an SMB

Unfortunately, we are all living in an ever-evolving risk economy, and it is not a question of if but when there will be a data breach.

In the US, ransomware-related insurance claims rose 77% in the first quarter Q1'23 compared to Q4 2022. Paying the ransomware is often just the tip of the iceberg. A lot of states have requirements about informing affected customers requiring costly legal forensics, and hiring data scientists. Add to this the time and effort lost while getting the operations back up, reputation hit to the brand, along with the cyber insurance premiums that will skyrocket, it is no wonder that often an SMB is severely affected by the data breach if not going bankrupt.

Figure 7: Lifecycle of a breach and its effects on a business

Figure 8: Ever-evolving Risk Economy

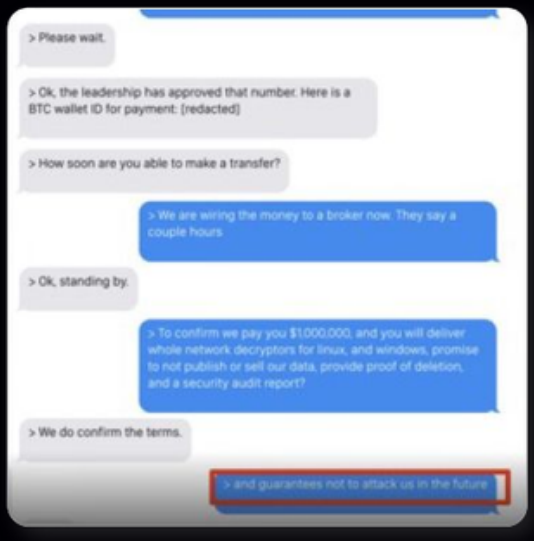


Figure 9: Actual conversation between a hacker group and a hacked company, negotiating the ransomware amount

How SMBs can fight back:

Hopefully, it is now clear, by reading the above sections, that like the saying goes, “it’s not a matter of if, but when” for when an SMB might face stolen credentials, or the possibility of ransomware. Even if a company does everything right, there’s no guarantee of immunity to a breach or cyberattack.

Thankfully for SMBs, they have more and more powerful allies on their side when it comes to protecting their networks, apps, and data. Some of the key initiatives an SMB can take to protect themselves are:

Work with a Managed Service or a Security Service Provider (MSP/MSSP):

There are three key areas affecting most SMBs today that could be mitigated by working with an experienced MSP/MSSP: limited in-house resources and cybersecurity expertise, misconfigurations of existing tools and other vulnerabilities, and the absence of comprehensive cybersecurity measures.

According to a 2023 report from the International Information System Security Certification Consortium (ISC^2), the gap in the trained cyber workforce has widened to nearly 4 million, with a global workforce estimate at approximately 5.4 million. With rapid economic and technological changes, it is a challenge for many businesses to find and retain the necessary resources to proactively protect against, monitor for, and respond to incidents. As previously mentioned, small to medium-sized businesses are particularly vulnerable to adversary attacks. The constraints and lack of preparedness make SMBs attractive targets for cybercriminals seeking easy entry points into company networks.

Regular system updates and configuration reviews are often overlooked due to limited IT resources, contributing to the vulnerability of SMBs to cyber threats. MSPs/MSSPs offer a cost-effective, reliable, and sustainable solution to obtain the right expertise and cybersecurity measures to meet business needs for long-term success.

How SMBs can fight back:

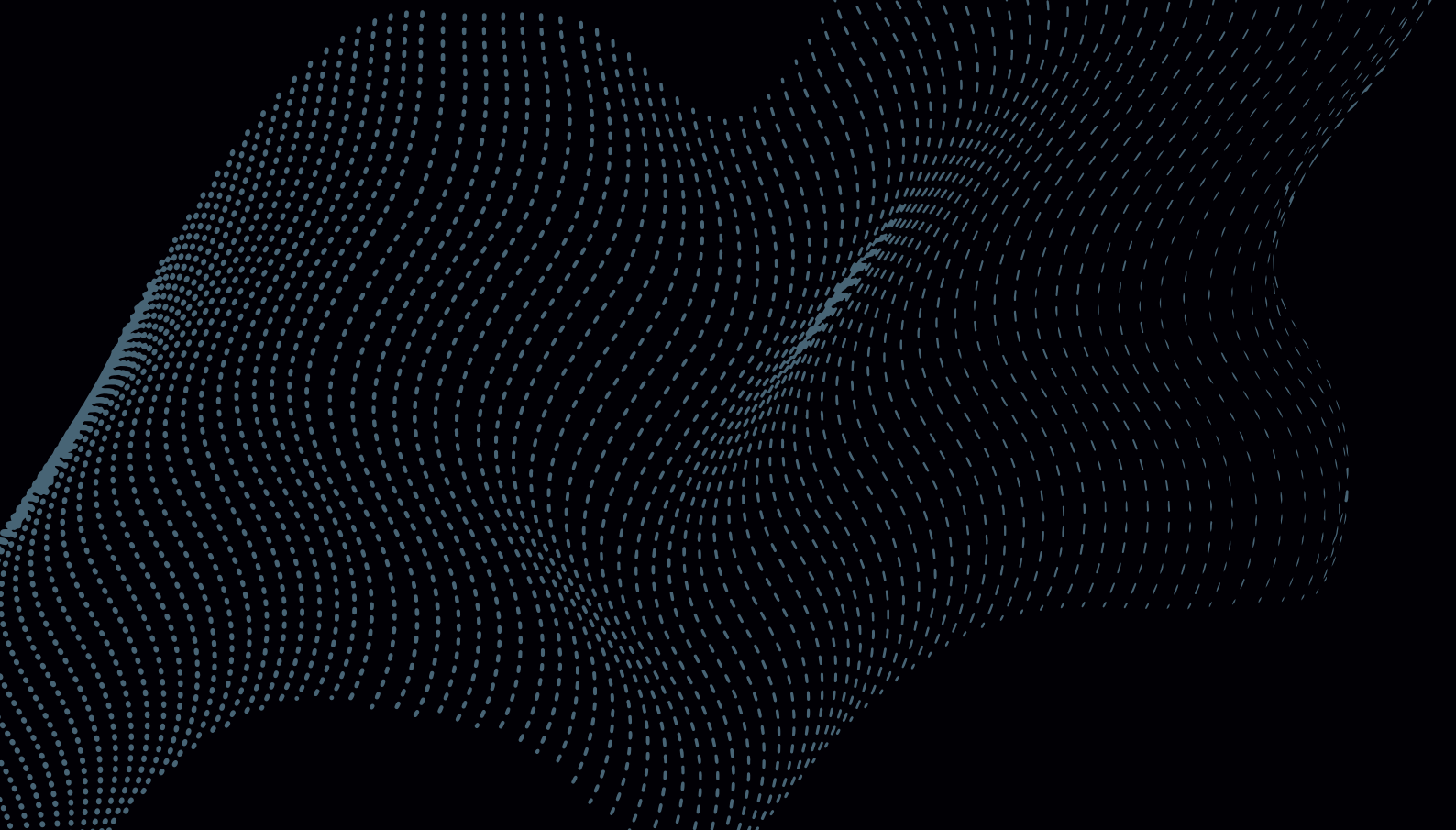
Enforce zero trust network security:

Given the frequency at which SMBs are targeted by phishing and social engineering attacks, it is crucial for them to ensure that their security perimeter around resources and data is robust. Relying solely on SaaS credentials or VPNs is not sufficient!

Instead, it is imperative to always enforce secure connections to the company network and business SaaS applications, with mandatory encryption, regardless of whether employees are accessing the network from business sites, conferences, airports, or while traveling. One of the most effective, easy to deploy, and modern methods for enabling secure, always-on access is through the Zero Trust Network Access (ZTNA) technology, such as that provided by Timus Networks.

ZTNA operates on the principle of "never trust, always verify," which means that trust is not assumed until a user is thoroughly verified. This includes not only credential checks but also an assessment of contextual behaviors such as a user's location, IP address, impossible travel check compared to the last known location, breached email check on the dark web, and more —all of which Timus SASE verifies before granting access, be it to the company network, or a SaaS business app.

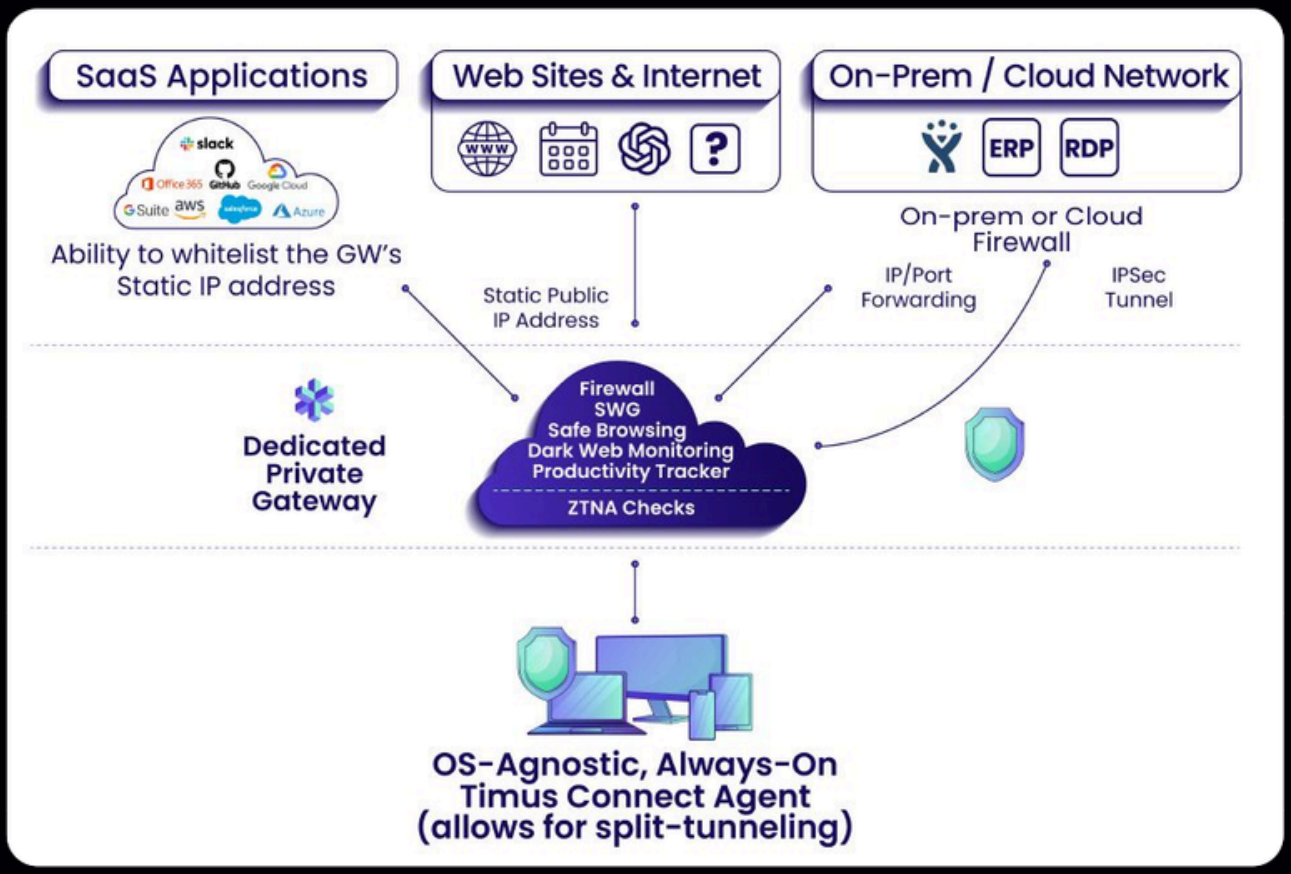
Humans will remain as a significant vulnerability factor in modern cybersecurity defenses. If network access relies solely on credentials, a single human error could lead to exposure to criminals or worse.



How Timus SASE helps SMBs stay protected and productive

Timus SASE, via a lightweight app installed on devices (supporting laptops, tablets, and mobile), provides secure, always-on seamless connectivity to company resources at all times, based on the richest set of behavior driven conditional access policies. Access is granted granularly on the least privilege principle, where a user can only access explicitly authorized resources and data.

Timus SASE users connect to company data or the SaaS apps through private, never shared gateways, with the gateways acting as a single point of network entry to all resources. Allowlisting the Timus SASE static IP within the commonly attacked SaaS business apps (think Google Workspace, Microsoft 365, Salesforce, etc) makes things further hacker-proof, meaning that even if the bad actors stole all the credentials of all the users, they still would not be able to access the apps, and sensitive data.
Timus SASE also uses an adaptive MFA, where the MFA is only pushed if the risk profile warrants it for the specific access request - significantly helping with increased user experience and reduced MFA fatigue.



How Timus SASE helps SMBs stay protected and productive

Timus SASE Productivity Tracker

Another way Timus SASE paves efficiency and growth for SMBs in the times of hybrid work is the way the IT admins and managers can get deep visibility into their network usage on the user and app level. The Timus SASE Productivity Tracker feature consolidates company-wide productivity metrics to inform business leaders of the user and team activities.

The Timus SASE Intelligent Agent captures traffic along with granular information pertaining to users' productivity during business hours, additionally allowing for custom automated reports.

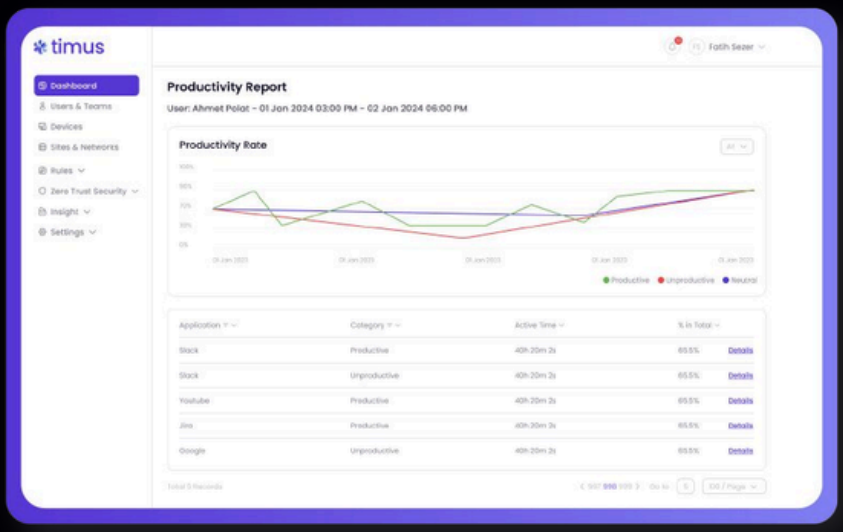


Figure 10: Timus Productivity Tracker

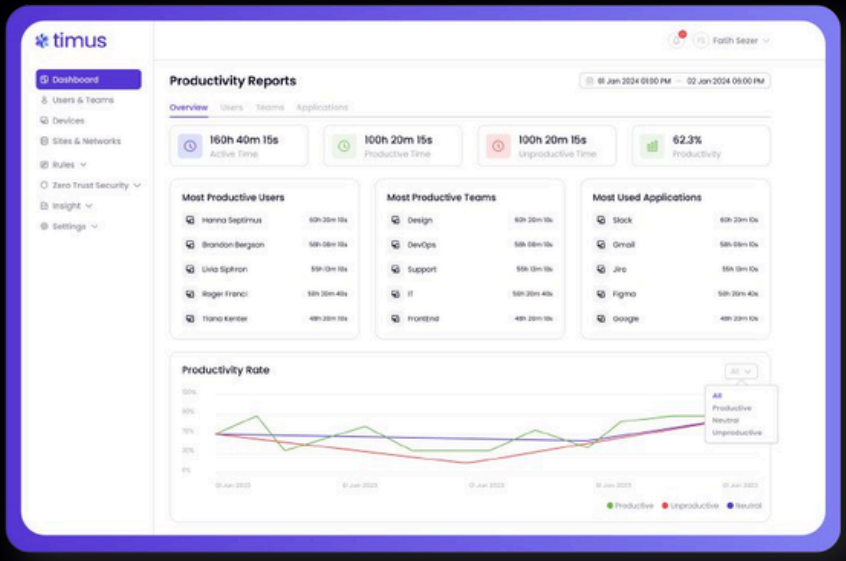


Figure 11: Timus Productivity Tracker

The Business Case for ZTNA in addition to Peace of Mind

For SMBs, implementing ZTNA is not just about enhancing security; it's also a strategic business decision. With cyber threats evolving rapidly, customers and partners are increasingly concerned about the security posture of the businesses they engage with. By adopting ZTNA, SMBs can demonstrate a commitment to robust cybersecurity, which can be a competitive differentiator in the market.

Moreover, ZTNA can lead to cost savings in the long run. The costs associated with a data breach or ransomware attack – including downtime, legal fees, regulatory fines, increase in cyber insurance premiums, and loss of customer trust – can be crippling for SMBs. Investing in ZTNA can significantly reduce the likelihood and potential impact of such incidents.

Finally, the regulatory landscape is constantly evolving along with the requirements to qualify for cyber insurance. Deploying a robust modern secure access mechanism like ZTNA prepares SMBs for tomorrow's landscape that is fast approaching.

Conclusion

SMBs are right in the hacking sweet spot for bad actors as they usually lack the necessary preventive cybersecurity measures, with the added benefit of a low risk of capture for hackers. For SMBs, the adoption of Zero Trust Network Access is a critical step in safeguarding against the increasingly sophisticated threats of data breaches and ransomware. By moving away from using simple SaaS credentials to rely on access or traditional VPNs, and instead embracing the more secure and dynamic framework of ZTNA, SMBs can not only protect their digital assets but also strengthen their market position by showcasing a strong commitment to cybersecurity. The transition to ZTNA is not just a technological upgrade; it's a strategic move towards a more secure and resilient future in the digital age.

References and Additional External Resources:

- Cyber Insurance Claims for SMBs: https://www.ioausa.com/blog/focus-report-2023-cyber-market-outlook/ https://www.techtarget.com/searchSecurity/news/366552773/Cyber-insurance-report-shows-surge-in-ransomware-claims
- Verizon DBIR Reports: https://www.verizon.com/business/resources/reports/dbir/
- SMB Ransomware Statistics: https://www.techtarget.com/searchSecurity/news/366552773/Cyber-insurance-report-shows-surge-in-ransomware-claims
- 64 Cyber Insurance Claims Statistics 2023-2024: https://www.getastra.com/blog/security-audit/cyber-insurance-claims-statistics/

About Timus SASE, a CyberFOX Platform

Timus SASE simplifies network security and access for SMBs and mid-market enterprises helping to significantly reduce business risks and bolster compliance.

Timus SASE transforms complex setups involving multiple tools into a single, unified solution that secures networks and safeguards users, regardless of their location or device.

Developed by firewall experts with decades of cybersecurity experience, Timus SASE offers simplicity and rapid deployment, with installation in under 30 minutes.

Learn more at https://www.cyberfox.com

About the Authors

David Bellini
Chief Executive Officer

Andrew Bensinger
Chief Technology Officer