See. Control. Secure.

Allot Secure

Report

CSP-Driven Cybersecurity for SMBs

H2 2024

Executive Summary

Cybercriminals are targeting businesses of all sizes these days. However, small and medium businesses (SMBs) with 10–50 employees are among the most sought-after and vulnerable groups to attackers. Think of the local coffee chain around the corner or a mid-sized law firm. These organizations typically lack the resources and budget that larger organizations can afford to protect against cyberattacks. Luckily for SMBs, however, they still have a way to fight back. By partnering with Communications Service Providers (CSPs) using network-native cybersecurity solutions, they can tap into affordable protection to defend against threats and meet compliance standards — all within their budget.

The 2024 SMB Cybersecurity Protection Report by Allot offers a comprehensive guide for CSPs with SMB customers seeking to enhance their network security in a cost-effective and comprehensive manner. The report draws on the most recent findings by Coleman Parkes from July 2024, comparing the updated survey with its earlier version from 2023. For reference, the most up to date 2024 version by Coleman Parkes was conducted with 450 SMB owners and managers from the United States, Canada, the UK, Germany, Sweden, Norway, Denmark, Finland, and the Philippines. It provides top recommendations for selecting affordable, easy-to-maintain, and highly effective network-native solutions for SMBs.

SMB Protection Is No Longer "Optional"

Cybercriminals have figured out that targeting multiple small businesses with weaker protection is often easier than attacking large, well-secured enterprises. In previous reports, the 2023 SMB and SoHo Security Study [1] showed us that, despite significant concern, many SMBs in the US (69%) and Canada (56%) were not adequately protecting themselves. This same survey also showed that:

- ⇒ 1 out of 4 of SMBs in the US were under attack in 2023
- ⇒ Companies relying solely on mobile internet access are more vulnerable, with 21% of such businesses worldwide facing security incidents last year.

The figures are still relevant in 2024, and even more alarming when considering that 300 million businesses fall under the SMB category worldwide, according to the MSME Forum. Particularly, SMBs are often vulnerable to attacks because they have either inadequate or no security measures in place. For example, when it comes to protecting their networks and cloud systems, SMBs typically rely on routers with built-in security features, firewalls from their CSPs, and web filtering. However, these methods still leave them exposed to threats because:

- They lack the internal IT expertise needed to properly configure devices and networks, such as firewalls and endpoint security systems.
- The high total cost of ownership (TCO) forces them to depend on off-the-shelf solutions, which are often poorly set up and maintained.
- They fail to protect the entire network by only securing certain devices, leaving gaps in their defenses.

The increased number of attacks and potential repercussions to third parties means that SMB protection is no longer an option — it is a must. Worse yet, attackers view SMBs as entry points to reach larger organizations. Once they infiltrate an SMB, they can exploit the connection to bigger third-party vendors, potentially compromising more extensive and critical security systems.

Keep in mind, however, that security gaps don't always result from a lack of resources and skills. Sometimes, employees might be the weakest link in the security chain. According to the 2023 SMB and SoHo Security Study, despite a slight decrease since 2022, 7 in 10 small businesses are still concerned about employees putting IT security at risk. Why is that the case?

The Unwanted Risks of Working from Home

The shift to work-from-home has drastically increased security risks. From a business perspective, working from home is a win-win situation for the business and the employee. On the one hand, SMBs with limited budget don't have to spend on expensive office space and can foster a more relaxed working environment. On the other hand, the employees can save commuting hours and get unmatched flexibility in their day-to-day job. While this new work model looks great on paper, it introduces several challenges from a cybersecurity standpoint.

Once an employee is able to take a company device (smartphone, laptop, hard drive, etc.) those devices are no longer in the office, which can be a 24/7 controlled environment. Rather, any device that leaves the office and is used at home or in public places connect to unsecured networks, increasing the chance of infection.

For example, when employees take their laptops and connect to a coffee shop Wi-Fi (public) network, there are very high chances that the device will now become a vulnerability for

the entire office. The statistics from the 2023 SMB and SoHo Security Study clearly depict the truth; SMBs in the USA reported that the types of cyber-related risks which are considered the biggest threat were:

- ⇒ (69%) Threats from laptops and mobile devices connecting remotely to corporate assets (e.g., working from home and mobile security)
- ⇒ (59%) Vulnerabilities introduced to the business network through personal devices.

All in all, the recommendation in 2024 remains the same as last year: to have proper security policies in place at the office, and to protect these devices everywhere we go. However, there are still barriers for SMBs to achieve robust security. The question is, how can a small business afford that protection when lacking the funds and know-how? Let's explore in the following section.

SMBs Are Choosing MSPs and CSPs For Their Cyber Protection

As cybersecurity threats grow more complex, SMBs are turning to CSPs for affordable, reliable solutions that can be easily tailored to their needs. This shift is evident when comparing our 2023 survey to the latest 2024 results, with the use of MSPs or CSPs rising from 26% in 2023 to 36% in 2024.

CSPs not only provide flexible pricing models that fit SMB budgets, but they also offer solutions that require minimal in-house technical expertise. For instance, the 2023 Coleman Parks survey reinforces this last point, showing that 80% of small businesses in the US and 75% of small businesses in Canada would switch to a new internet service provider if it offered a security service. For smaller businesses, this means avoiding the expense of hiring full-time IT staff or investing in costly infrastructure while still benefiting from enterprise-level security measures. This makes sense — especially when cost is still one of the main deciding factors for SMBs.

Cost Is Still a Big Concern for SMBs

There are still barriers for SMBs to achieve robust security. When looking at the 2023 SMB study by Coleman Parkes, the most common roadblocks to improving a company's current IT security position were:

1. Cost of technology and services (68% in the US and 66% in Canada)
2. Too many products and services to secure (54% in both the US and Canada)
3. Cost of hiring IT security professionals (47% in the US and 51% in Canada)

Comparing those numbers in 2024, when SMBs were asked about the key factors in choosing a cybersecurity solution, **48% prioritized performance**, while **43% still focused on cost**. This shows that the financial barriers identified in 2023 are still relevant. Although performance got the first place, cost is still a big concern for SMBs.

Notably, the amount SMBs are willing to spend on cybersecurity solutions directly impacts the type of protection they can implement. According to our 2024 survey, SMBs allocate an average of $1,400 annually for cybersecurity protection. While this budget limits their options, it does not necessarily mean they have to compromise on quality — especially when they choose a CSP to handle their cyber protection. CSPs are in a unique position to provide effective cybersecurity solutions because they control the internet connectivity where most threats originate, allowing them to:

- Intercept cyber threats at the network level before they reach the end user.
- Offer mass-market solutions that are zero-touch for the end user.

Here’s the most interesting insight: almost two-thirds of SMBs surveyed (64%) are still not utilizing CSP-provided cybersecurity services in 2024. This gap offers a significant opportunity for CSPs in a market that is increasingly seeking affordable and effective cybersecurity solutions.

There is a Massive, Untapped Market for CSPs

A bundled cybersecurity solution from a CSP combines multiple security services into one package, eliminating the need for businesses to buy separate tools like firewalls, malware protection, or encryption. Instead, they get an all-in-one solution covering various cybersecurity needs, such as network security, threat detection, antivirus protection, and data encryption, all managed by the CSP.

Interestingly, 62% of SMBs expressed a preference for bundled services over standalone solutions in 2024. The outlook for CSPs in the SMB market is even more encouraging, with 65% of SMBs surveyed planning to purchase or upgrade their cybersecurity solutions in the next 12 months. This indicates a market that is not only increasingly aware of CSP-offered cybersecurity services but is also ready to invest in them in the near future.

On top of offering cybersecurity packages, CSPs can gain a competitive advantage by adding compliance solutions for SMBs. Many small and medium-sized businesses struggle with keeping up with regulations, so by providing this level of service and support, CSPs can stand out as *all-in-one* providers. This not only covers security but also ticks the regulatory box, making customers stick around longer and boosting potential recurring revenue.

Compliance Could Be the Next Big Opportunity

Our 2024 survey shows that 92% of SMBs have at least a basic understanding of the benefits of network-based security solutions. However, many SMBs still remain largely unprepared and are at significant risk of non-compliance with regulations. The latest findings also show that only 1 in 3 SMBs feel fully ready for upcoming regulatory changes, and just 24% have hired compliance experts in 2024. These gaps are particularly concerning for SMBs that handle digital payments, collect personal data, or work with key federal agencies. In addition, the lack of preparedness exposes them to compliance risks, potential fines, and business disruptions.

While no single cybersecurity solution can fully address all the regulatory compliance needs of an SMB, a network-native cybersecurity solution provided by a CSP can help mitigate a significant portion of these concerns. For example, with NetworkSecure by Allot, small businesses and CSPs worldwide can implement a compliance-friendly solution, while enjoying the advantages of a reliable, robust, and easy-to-use service already trusted by millions of subscribers.

Network-native Means Effective Security for SMBs

Allot offers NetworkSecure — a zero-touch, network-native solution implemented directly within the CSP's network. This means that it not only effectively intercepts cyberthreats before they reach the end user's device; it also eliminates the need for end users to install or update any software to enjoy the protection of the network-native solution. Allot brings enterprise-grade protection to SMBs at a significantly more convenient price point. Here's how:

1. Network-Based Security: Allot provides network-native security services — accessible to any device, without requiring client software, and without impacting performance or battery life.

2. Comprehensive Threat Protection: Our platform protects every employee and device, regardless of location. NetworkSecure provides comprehensive protection by filtering domains, URLs, DNS security, and IP addresses for the latest Internet security threats, including ransomware, Trojans, adware, viruses, bots, and phishing attacks.

3. Robust Content Filtering: The platform offers numerous content filtering categories, allowing CSPs to group them as desired. It also enables on-demand and scheduled Internet access pausing and provides allowed and blocked lists for tailored content control — ensuring a safer and more controlled Internet experience for users.

4. Customer Engagement: Allot NetworkSecure enhances customer engagement by giving subscribers a value perception of the service. It offers multiple engagement options, including personal reports and security alerts, redirection to notification pages, and promotion of other services to increase adoption.

5. 5G Ready: The security sits in the telco network, eliminating the need for application management. Our NetworkSecure solution is designed to protect existing 4G subscriber connections and new 5G connections. This ensures minimal latency impact and the capacity to protect devices without requiring any installations and achieve security convergence.

Key Takeaways

The conclusions are straightforward: SMBs are greater targets for cybercrime than ever before. They are concerned with the budget and performance of solutions to protect their businesses, and they are ready to purchase cybersecurity solutions from CSPs. With Allot, SMBs and CSPs alike can seize the benefits of a proven, robust, yet simple, transparent, zero-touch service that is already used by many millions of subscribers.

About Allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and converged security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-native security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed, and cloud service providers and over 1000 enterprises. Our industry-leading network-native security-as-a-service solution is already used by many millions of subscribers globally.

Allot. See. Control. Secure.

If you're interested in learning how to offer network-native, zero-touch cybersecurity solutions to your SMB subscribers, book a demo with one of our experts today.

References

[1] Don't Miss the Growing SMB Security Services Opportunity: Allot Consumer Security Survey, Q3 2023

[2] Allot SMB Cybersecurity Survey Insights: Guiding SMBs Through the Cybersecurity Maze, H2 2024