allot

Small Businesses, Big Cyber Targets

Global SMB Cybersecurity Snapshot and the Emerging Role of Telecom Providers

SMB Security Survey, Q2 2026

Table of Contents

Introduction

Small businesses have moved decisively into the digital mainstream. Cloud adoption, mobile-first workflows, online payments, and remote collaboration tools have enabled even the smallest firms to operate at unprecedented scale and speed. At the same time, this digital dependence has quietly elevated small and medium-sized businesses (SMBs) into prime cyber targets.

This report analyzes findings from a multi-market survey of SMBs, conducted in partnership with Dynata, across the United States, Canada, the United Kingdom, Germany, Japan, South Korea, and Indonesia. The data reveals a consistent global pattern; SMBs are increasingly aware of cyber risk but remain structurally under-prepared. As threats escalate, many are rethinking not just what cybersecurity they need, but who they expect to deliver it.

One conclusion stands out clearly. SMBs increasingly view their telecom providers, and not traditional security vendors, as natural partners for cybersecurity protection. Trust, simplicity, embedded delivery, and predictable pricing are emerging as decisive factors. This shift signals a strategic moment for telecom operators as cybersecurity becomes a core component of the connectivity relationship.

Small Businesses at the Center of the Cyber Risk Map

For many years, cybercrime narratives focused on large enterprises and critical infrastructure. That focus has shifted. Attackers today pursue scale, automation, and ease of entry, making small businesses highly attractive targets. With hundreds of millions of SMBs worldwide, they make up more than 99% of all enterprises in the US, Europe and Asia. Many SMBs collect and store sensitive customer data like credit card information and personally identifiable information (PII), which can be valuable to cybercriminals, making SMBs good targets for cybercrime. The likelihood of SMBs being unprepared for those crimes makes them even more attractive targets.

Further expanding the cyber risk landscape, SMBs in the recent Allot SMB Cybersecurity Survey reported that 95% used their personal mobile devices for tasks, including business communication and work emails (58%), accessing work documents (44%) and accessing desktops and other remote work activities (35%). This potentially leaves those business assets open to attack via personal devices.

Indonesia

BYOD is far more prevalent than in the other countries surveyed

67% For work email (vs. 58% WW)

70% For financial transactions (vs. 49% WW)

48% For remote work (vs 35% WW)

Survey respondents across all regions consistently rank phishing (39%), data theft (38%), financial fraud (36%), malware (36%), and ransomware (25%) among their top cyber concerns. Importantly, these fears are not theoretical. Approximately 1 in 3 SMBs report having already encountered a cyber threat tied directly to their business operations. (This compares to just 21% reporting cybersecurity incidents in the Allot 2024 SMB Cybersecurity Survey.) Another 5% say they are unsure whether they have been attacked at all, suggesting that limited visibility, rather than absence of incidents, may be masking true exposure.

Downtime anxiety further reinforces perceived risk. Many SMBs estimate that a single day of operational disruption could cost them as much as $10,000 (45%) to $25,000 (28%), with higher losses cited among companies with greater digital dependency. For firms operating with limited cash buffers, these losses threaten long-term viability.

South Korea

The Threat Environment (vs. Worldwide)

46% Phishing (vs. 39% WW)

37% Ransomware (vs. 25% WW)

26% DDoS Attacks (vs. 13% WW)

BYOD | An Open Door for Cyber Threats

Bring-your-own-device (BYOD) practices have become the norm for small and medium businesses. But they come with a steep cybersecurity cost. Nearly all SMB decision-makers (95%) report using personal devices for work, dramatically expanding the attack surface beyond the reach of traditional IT controls. While this flexibility boosts productivity, it also shifts critical business activity onto devices that are rarely built or configured for business-grade security.

The risk is amplified by how these devices are used. SMB decision-makers reported that they used messaging apps (60%), business email (58%), video conferencing (55%), and social media (54%), though each represents a high-value entry point for attackers. Personal devices often lack advanced threat protection, centralized policy enforcement, or real-time monitoring, making them ideal targets for phishing, credential theft, and malware. A single compromised smartphone can expose corporate email accounts, business conversations, customer data, and internal systems.

Even more concerning, personal and professional use routinely overlap. An employee might let a child play a game on their phone or download a new app for personal use, unknowingly introducing a malicious application. From that moment on, the device becomes a silent vulnerability inside the business. Without strong protection, malware can access messages, harvest credentials, or spy on communications, turning an everyday convenience into a gateway for cybercriminals.

For SMBs, where IT resources are limited and security management is often reactive, BYOD risk is immediate and operational. As work continues to shift toward mobile-first and app-driven environments, unmanaged personal devices increasingly serve as the weakest link in an SMB's security chain, exposing businesses to outsized cyber risk with very little warning.

The Preparedness Paradox

Despite high awareness, most SMBs operate with minimal cybersecurity infrastructure. Built-in operating system protections and basic antivirus software remain the most common defenses. Adoption rates decline sharply for more advanced tools such as DDoS protection, endpoint detection and response, DNS protection, intrusion protection, or managed security services.

62% Antivirus software

49% Firewall

25% MSS

19% Intrusion protection

19% DNS protection

15% EDR

15% DDoS protection

Although SMBs adopt DDoS protection solutions at a lower rate than other cybersecurity solutions, there is greater risk of DDoS attack to SMBs than to any other sector. DDoS protection is often considered to be too expensive or too complicated in relation to the risk. However, a properly educated SMB with a small cybersecurity budget can find DDoS protection to be affordable, easy to manage and worthwhile when acquired through the telecom provider as a service. Therefore, today's high rate of increase of DDoS attacks on SMBs and the currently low adoption rate of DDoS protection should represent an opportunity for telcos.

Two constraints dominate in the adoption of cybersecurity solutions among SMBs: resources and expertise. Many SMBs lack formally defined cybersecurity budgets or allocate only modest annual spending toward protection. 41% of SMBs reported that their annual cybersecurity budget was under $1,000. This number increases with the size of the small business to an average of $2,000 for business with 11-50 employees. As we will see later in this report, 84% of SMBs indicated that they would be willing to pay their telecom provider for a cybersecurity solution for their business. These findings indicate that small businesses, though price-sensitive, are willing to invest in cybersecurity, particularly when the value case is clear. That's good news for effective low-cost services.

Small businesses rarely employ dedicated security personnel. Owners, founders, or general managers often serve as sole decision-makers on technology investments. They have neither the time nor the expertise to properly address cybersecurity protection needs. When queried about those needs, SMB managers indicated that the following are their top concerns when purchasing a cybersecurity solution:

59%

Efficacy & Protection:
Proven ability to stop modern threats like ransomware

47%

Total Cost of Ownership:
Not just the sticker price, but renewal costs and resource requirements.

41%

Ease of Use & Management:
A 'set-and-forget' interface that doesn't require constant monitoring.

37%

Technical Support:
24/7 availability or a dedicated account manager.

When it comes to technical support calls, network-based cybersecurity actually has the potential to reduce the volume. In a situation where telco customers have telco-supplied security apps installed, there are pop-ups for problems, updates, upgrades and the like. These all inevitably lead to support calls from confused and frustrated customers. With network-based cybersecurity, since there is no software installed, there are no requests for updates and upgrades. Additionally, because the solution is not embedded in the device, network-based cybersecurity protection does not affect device performance or battery life.

When asked whether it was important to them if they could purchase all their cybersecurity solutions from a single vendor, 66% of SMBs answered in the affirmative.

Security competes with sales growth, staffing, compliance, and customer experience for attention. When protection requires multiple vendors, complex setup, or ongoing management, it becomes a low-priority burden. The result is not indifference to risk, but paralysis driven by complexity.

Japan

Top concern when purchasing cybersecurity:

57% Total Cost of Ownership

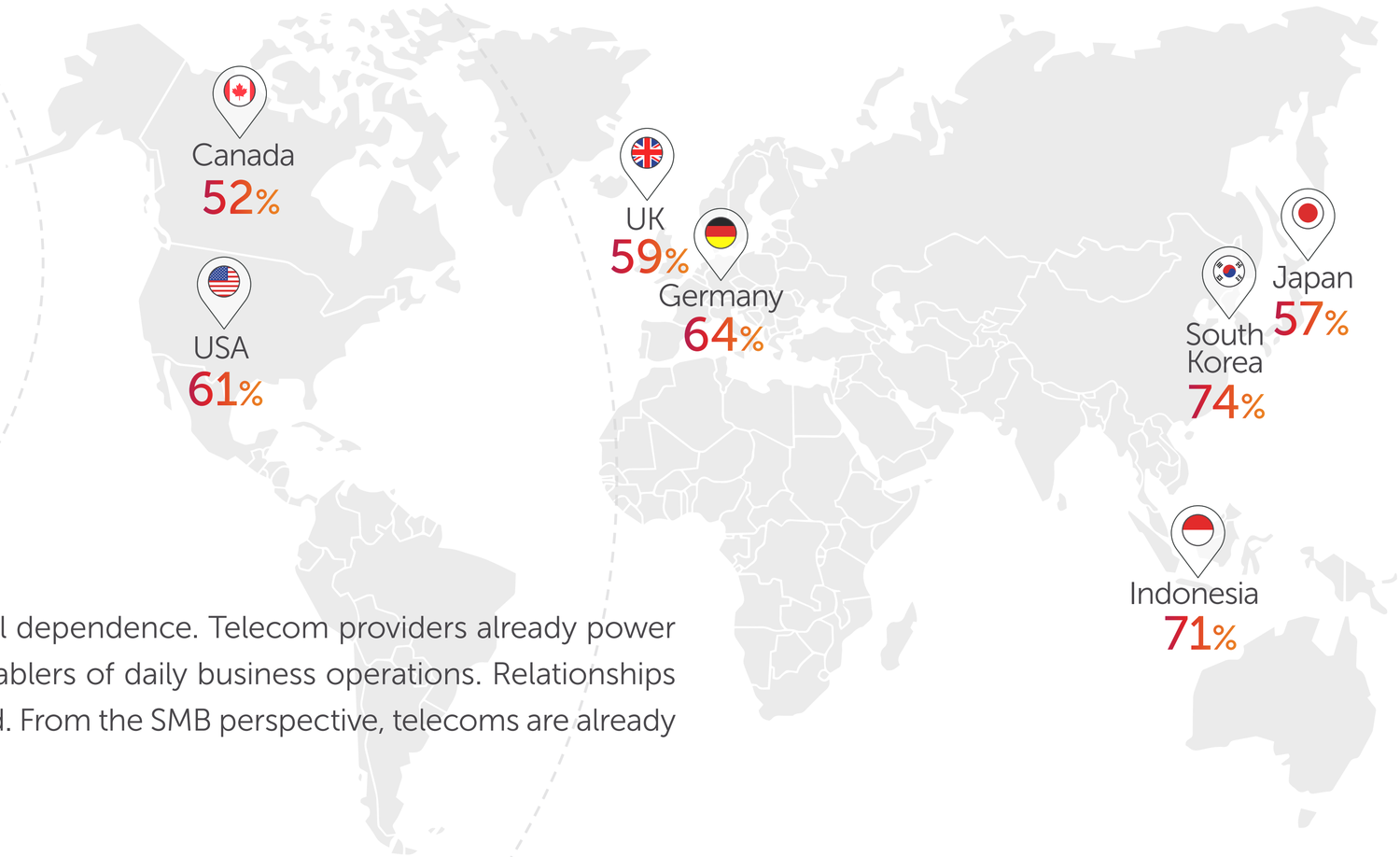
51% surpasses efficacy

This aligns with Japan's lower willingness-to-pay for cybersecurity and highlights the importance of a value-oriented positioning and transparent pricing in Japan.

Why Telecom Providers Enter the Cyber Conversation

Within this context, telecom providers emerge as unexpected, but logical, security partners. Across all markets surveyed, a majority of SMBs say they would trust their mobile or telecom service provider to offer cybersecurity solutions for their business.

Worldwide, 63% of SMBs said that they would trust their mobile service provider if they offered a cybersecurity solution for their business.



This trust is rooted in familiarity and operational dependence. Telecom providers already power connectivity, voice, data, and mobility: core enablers of daily business operations. Relationships are long-standing, contractual, and billing-based. From the SMB perspective, telecoms are already mission-critical.

Crucially, telecom infrastructure sits directly in the path of business traffic. This creates a perception that telecom providers are well positioned to observe, filter, and protect digital activity. For small businesses seeking protection without complexity, this proximity matters.

Trust is highest among the larger SMBs and sole decision-makers—segments most likely to have a mature relationship with their telecom provider. This positions telecom-delivered cybersecurity not as a replacement for enterprise platforms, but as an accessible alternative for underserved SMBs.

Trusting the mobile service provider to offer a cybersecurity solution for the SMB

Willingness to Pay, Redefined

The data dispels a long-held assumption that SMBs are unwilling to pay for cybersecurity. In reality, willingness exists, but under specific conditions.

A majority (84%) of respondents state they would probably or definitely pay their telecom provider an additional monthly fee for cybersecurity protection that reduces downtime, fraud, and data loss. Resistance grows only when pricing lacks transparency or delivery feels complex.

- 91% USA
- 78% Canada
- 86% UK
- 90% Germany
- 68% Japan
- 81% South Korea
- 94% Indonesia

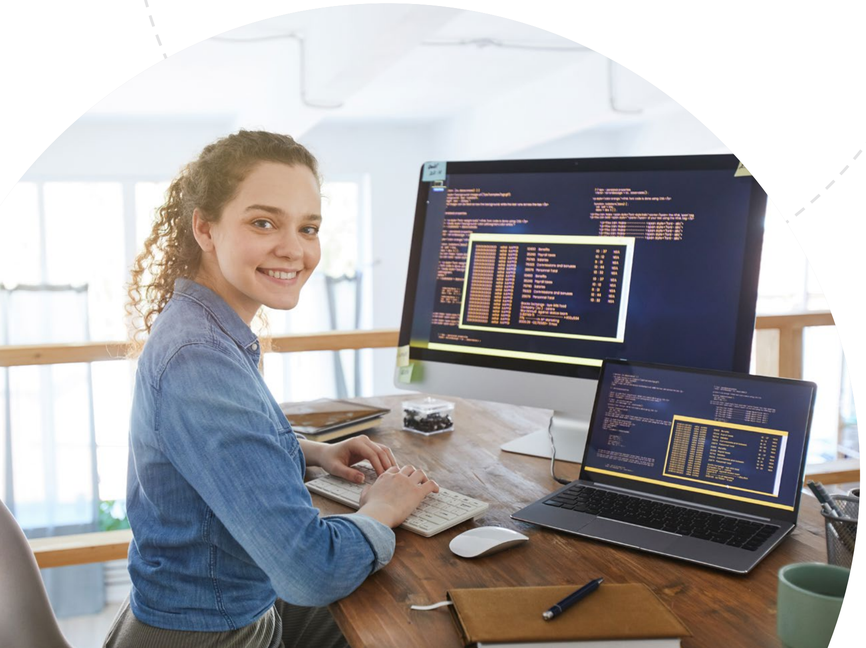
Pricing preferences cluster around low, predictable, per-device monthly fees. Global data indicates that price points of $10–$18 per device per month are the optimal "sweet spot". That's high enough to drive meaningful Average Revenue Per User (ARPU), yet low enough to be easily approved by SMB decision-makers without a formal procurement process. SMBs consistently favor operating expenditure over capital expenditure, mirroring how they already purchase connectivity services. Large upfront costs or multi-year commitments are far less attractive

Average Maximum Monthly Per Device Spend on a Security Solution, By Country

Equally important is frictionless deployment. Likelihood of purchase increases significantly when solutions require no installation, no agents, and minimal configuration. In effect, SMBs want cybersecurity that behaves like connectivity: always on, invisible, and dependable.

What SMBs Truly Value in Cybersecurity Solutions

When evaluating cybersecurity offerings, SMBs prioritize outcomes over features. Understandably, efficacy ranks first; solutions must demonstrably stop modern threats such as phishing, ransomware, and fraud. Cost, specifically total cost of ownership, follows closely.



Ease of use consistently ranks among top decision factors. SMBs seek "set and forget" protection that does not demand constant oversight. Technical support, particularly 24/7 availability, also plays a meaningful role in purchase decisions. While the heavily favored categories of solution efficacy and cost generally conflict with one another when it comes to cybersecurity, this conflict can create an opportunity for telecom operators who are able to offer lower-cost cybersecurity services.

Top three cybersecurity solution purchasing criteria:

59% Efficacy & Protection

47% Total Cost of Ownership

41% Ease of Use and Management

By contrast, advanced automation (12%) and regulatory alignment (8%) rank lower for most SMBs, except in regulated verticals. This reinforces a crucial point; SMB cybersecurity adoption depends more on operational fit than technical depth.

Why SMBs Struggle with Cybersecurity

The most significant hurdles reported by SMBs which make it difficult for their business to maintain a strong cybersecurity posture include:

48% Threat Evolution

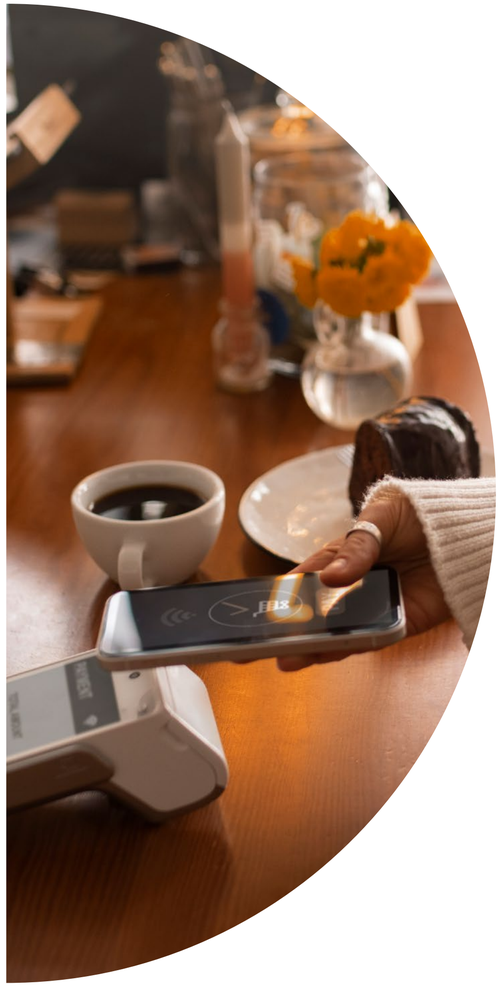
40% The “Human Element”

38% Financial Constraints

28% Expertise Gap

These findings are aligned with what we know about small businesses regarding cybersecurity; they lack the expertise, knowledge and time and they do not have the big budgets to keep up with current cyberthreats.

Whereas the ‘Human Element”, pointing toward a need for education, and Financial Constraints speak for themselves, the prominence of Threat Evolution as the primary global challenge highlights the need for network-level, AI-powered security; if threats develop faster than SMBs can manually respond, then a solution that updates automatically, and requires no ongoing management, is not just a convenience, it becomes essential.



Consolidation as a Strategic Preference

Vendor sprawl has become synonymous with security complexity. The survey data shows a clear desire among SMBs for consolidating cybersecurity with a single provider whenever possible, with 66% of SMBs reporting that this would be their preference.

Managing multiple dashboards, subscriptions, and support channels introduces friction that small teams cannot absorb. Every additional vendor increases cognitive and operational load.

Telecom providers are structurally positioned to respond to this preference. By embedding cybersecurity within connectivity services, operators can reduce fragmentation while strengthening customer relationships.

A Strategic Opening for Telecom Operators

Taken together, the data indicates a structural shift. SMBs are facing enterprise-level cyber threats without enterprise-level resources. Traditional security procurement models do not align with their realities. The tools available to them are either too complex, too expensive, or too poorly matched to SMB needs.

While 63% of SMBs surveyed said that they would trust their current mobile service provider to offer a cybersecurity business solution, 72% of SMBs indicated that they were likely to purchase a comprehensive cybersecurity business solution if it did not require any installation, a characteristic unique to network-based services.

In the Allot SMB Cybersecurity Survey from 2024, conducted by Coleman Parkes, only 36% of SMBs surveyed were using managed cybersecurity services. In the 2026 survey, that number dropped to 25%. This drop also represents an opportunity for telecom operators who are bold enough to offer cybersecurity services to the under-provided SMB market for whom network-based cybersecurity services are not yet available.

This creates a strategic opening for telecom operators to evolve from connectivity providers into digital guardians. The opportunity is not about feature parity with enterprise platforms, but about delivering the right level of protection in the right way: embedded, affordable, and trusted.

Cybersecurity becomes a logical extension of the network layer: filtering threats before they reach endpoints, protecting identities and communications, and reducing downstream risk.

Alignment with Network-Based Security Approaches

From a portfolio perspective, the SMB expectations surfaced in this research align closely with network-based cybersecurity models. Solutions that operate at the network layer, requiring no endpoint installation, directly address SMB preferences for simplicity and invisibility.

Capabilities such as network-level threat detection, malicious traffic blocking, phishing protection, and behavioral anomaly analysis resonate because they reduce reliance on user action. For SMBs with limited security awareness or training, this passive protection model is especially valuable.

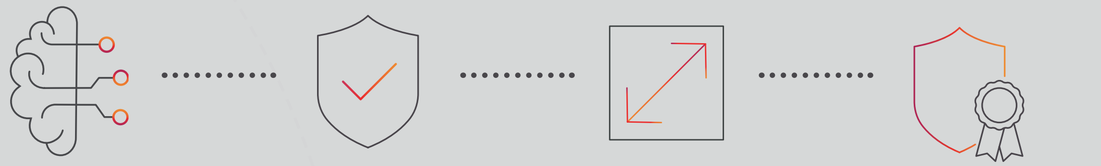
Importantly, bundled delivery through telecom channels enables security adoption without altering existing workflows. Protection becomes inherent rather than optional.

Erasing the Target

The survey insights naturally map to several portfolio design principles relevant to Allot's approach.

1. network-based protection addresses SMB deployment constraints by eliminating installation and management barriers.
2. subscription-based consumption aligns with SMB pricing expectations and telecom billing models.
3. centralized visibility and policy enforcement support consolidation goals.

Allot's emphasis on network intelligence, inline threat mitigation, and telecom-grade scalability reflects the direction SMBs implicitly signal; cybersecurity that is embedded, always on, and delivered by trusted service providers rather than standalone tools.



Network Intelligence | Inline Threat Mitigation | Telecom-Grade Scalability | Trusted Service Providers

From an ecosystem perspective, such approaches allow telecom operators to offer meaningful protection while preserving simplicity, meeting SMB needs without overwhelming them. This can lead to significant reduction in cyber risk for SMBs that subscribe to cybersecurity services offered by their telecom providers.

Key Takeaways

SMBs make up most of the world's businesses but are under-served when it comes to cybersecurity. This leaves a wide gap that telecom providers can fill with network-based cybersecurity services.

- SMBs have become prime cyber targets, but remain structurally under-prepared
- There is a widening gap between threat reality and cyber readiness
- Simplicity and consolidation matter more than advanced features
- SMBs trust telecom providers as cybersecurity partners
- Willingness to pay exists if pricing is predictable and friction is low
- Network-based security aligns closely with SMB expectations

Conclusion

Small businesses have become some of the most attractive cyber targets in the digital economy. They are connected, data-rich, and operationally vulnerable. The survey data shows that SMBs understand this risk clearly, but struggle with conventional cybersecurity models.

As threats intensify, expectations are shifting. SMBs increasingly look to their telecom providers, not as a convenience, but as strategic partners in protection. Trust, cost, simplicity, and embedded delivery now matter more than feature checklists.

For telecom operators, this transition represents a defining opportunity. In their competition with other communication providers, the cybersecurity differentiator for SMBs is whether or not they offer comprehensive protection services that do not tax their resources, both human and financial. Cybersecurity is no longer adjacent to connectivity; It is becoming inseparable from it.

Survey Methodology

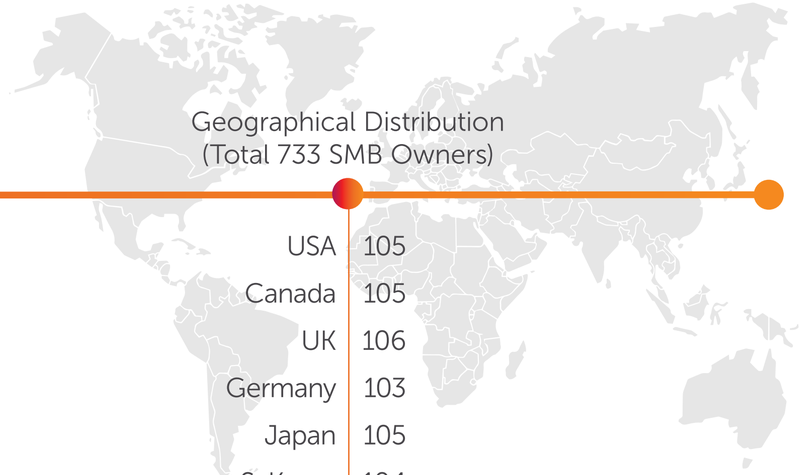
During March-April of 2026, Dynata, the world's largest first-party data company, together with Allot, set out to gain insights into SMB perspectives on cybersecurity and to discover how they protect their mobile devices, data and money against cyberthreats. The survey included 733 SMB owners, managers and IT managers from the USA, Canada, UK, Germany, Japan, South Korea and Indonesia. These participants were surveyed online about the current state of their cybersecurity awareness and preparedness, their willingness to invest in cybersecurity solutions, and their views on cybersecurity offerings from their telecom service providers.

Types of SMBs

Professional Services	12%
Retail & E-commerce	13%
Construction & Trades	13%
Technology & Software	13%
Finance, Insurance & Real Estate	6%
Manufacturing & Industrial	10%
Hospitality & Food Service	9%
Other	24%

SMB Size

Geographical Distribution (Total 733 SMB Owners)



USA	105
Canada	105
UK	106
Germany	103
Japan	105
S. Korea	104
Indonesia	105

Allot (NASDAQ & TASE: ALLT) makes networks safer, smarter and more valuable. We make it our mission to help telcos and enterprises gain deep network insight, defend against evolving cyber threats, and unlock new value for their customers. At the core of Allot's solutions is Deep Network Intelligence, powered by advanced AI/ML technologies, enabling unmatched app-aware visibility, even when traffic is encrypted. The same intelligence that drives precise traffic control and Quality of Experience (QoE) optimization enables real-time protection against DDoS and cyber threats, and the market's only comprehensive network-native platform that turns security into revenue-generating services. Through these services, we enable telecom providers to offer accessible and affordable cybersecurity protection services to their consumer and small business customers who do not have the resources or expertise to protect themselves otherwise. Leveraging 30 years of advanced telecom and enterprise network expertise, Allot partners with more than 500 communication service providers, including many of the world's top 10 telcos, and over 1,000 enterprises. Recognized by top analysts and trusted globally, Allot is at the forefront of secure, intelligent network experiences.

June 2026

allot

www.allot.com »