Mind the Gap

A Telco Revenue Growth Opportunity

Global Consumer Security Survey, Q4 2025

Table of Contents

Introduction

This report summarizes and analyzes the results of Allot's Q4 2025 Consumer Cybersecurity Survey, conducted in September 2025. The study captures attitudes, experiences, and behaviors of mobile device users across the US, UK, Germany, France, Italy, and Sweden. With over 3,100 respondents, the research sheds light on how consumers perceive cybersecurity risks, what actions they take (or fail to take), and where they place responsibility for safeguarding their digital lives.

According to the responses in this survey, mobile subscribers are highly aware of the cyber threats that put their devices, data, and daily lives at risk. Yet most fail to take the proper steps to protect themselves.

The findings in this report reveal a paradox: While concern about mobile cybersecurity is rising, consumer adoption of protective measures remains relatively low. This gap represents a risk for individuals and a market opportunity for mobile service providers.

By offering affordable, zero-touch cybersecurity services that are seamless and easy to understand, telcos can strengthen customer trust, and unlock new recurring revenue streams.

Key Findings

The survey which serves as the basis for this report presents interesting results with implications for telcos who are looking for ways to provide customer-pleasing services that generate significant levels of recurring revenue. In this comprehensive study, you will find insights into consumer perceptions regarding cybersecurity and what they think about their telecom service providers as the channel for protection services. These insights serve to build a case for telcos to actively target their consumer customers for network-based cybersecurity services.

Rising Consumer Anxiety Around Mobile Security

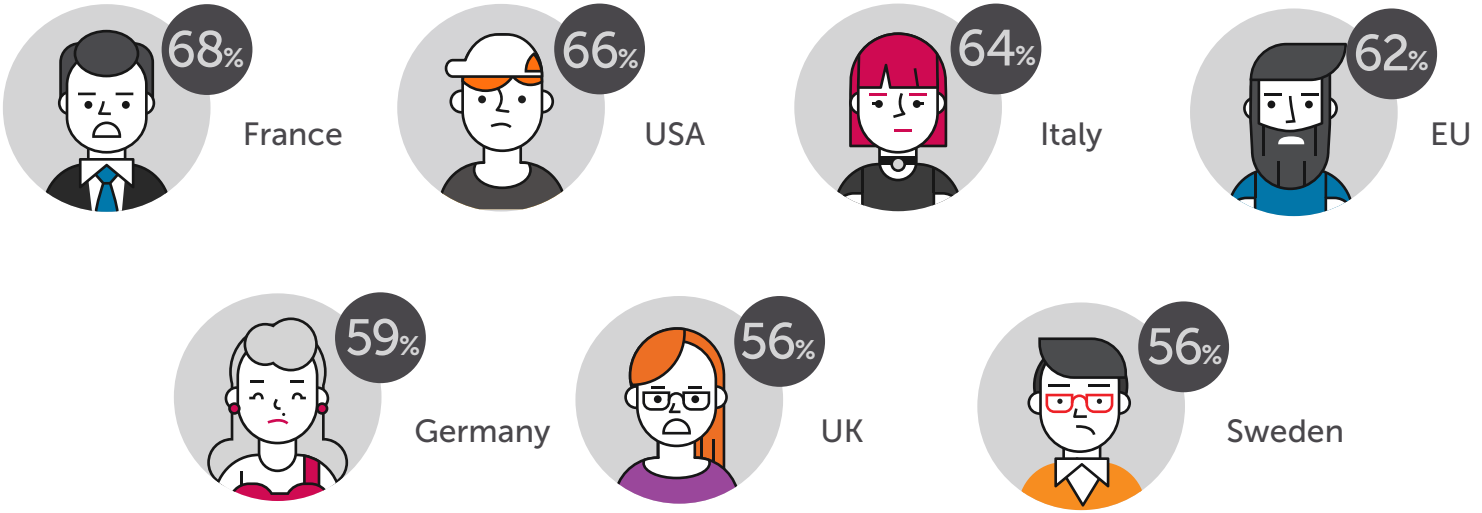
Mobile cybersecurity is no longer a niche concern for the consumer market. It is a mainstream phenomenon that is growing, and is particularly acute among digital natives who rely most heavily on mobile devices.

A clear majority of mobile users, 61.4%, recall actively thinking about or being concerned with the security of their mobile device within the last 12 months. This figure confirms that digital insecurity has moved beyond the technically knowledgeable and is now a widespread concern for the general population.

Mobile Device Security Concerns

This result is echoed in a Deloitte study – the 2025 CONNECTED CONSUMER SURVEY – which found that 70% of respondents are concerned about data privacy and security when using digital services on their mobile devices. This is compared with 60% the year before. Moreover, in actual implementations of Allot's cyber threat protection solutions, depending upon the region, between 70 and 90 percent of subscribers risk encountering a cyber threat during the next 6 months.

61%
are concerned with the security of their mobile device within the last 12 months



The Anxious Generation

Furthermore, the data challenges the stereotype of younger, "digitally native" users being more complacent about security risks. In fact, younger demographics express the highest levels of concern, with **73.2%** of 18-24 year-olds and **70.7%** of 25-34 year-olds reporting anxiety, figures that are significantly higher than for the 65+ age group (51.6%). This indicates that the users who are most deeply integrated into the mobile digital ecosystem are also the most acutely aware of its inherent vulnerabilities.

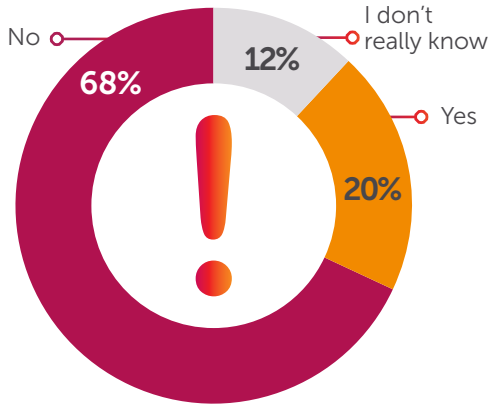
Growing Anxiety

The survey data also demonstrates that user anxiety is not a static condition but is actively growing. When asked to compare their current level of worry to a year ago, a combined 49.5% of users report being more concerned. In stark contrast, a mere 4.8% feel less concerned about mobile cyber threats.

No One Likes Being Targeted

The research consistently shows that a prior negative experience is a powerful motivator for future protective behavior. Users who have previously been victims of a security incident appear to be more likely to use a security solution actively. This divides the market into two profiles – a large, proactive segment that is concerned but has not yet acted, described in the previous section, and a smaller, highly motivated reactive segment that has learned the risks firsthand.

Deeper analysis reveals that personal experience is the single most powerful factor in shaping this perception. While the overall average of those who believe an attack is likely is **44.2%**, this figure is not evenly distributed. The **20.4%** of users who have previously experienced a security incident on their mobile device exhibit a dramatically heightened sense of future vulnerability (**73.4%**).



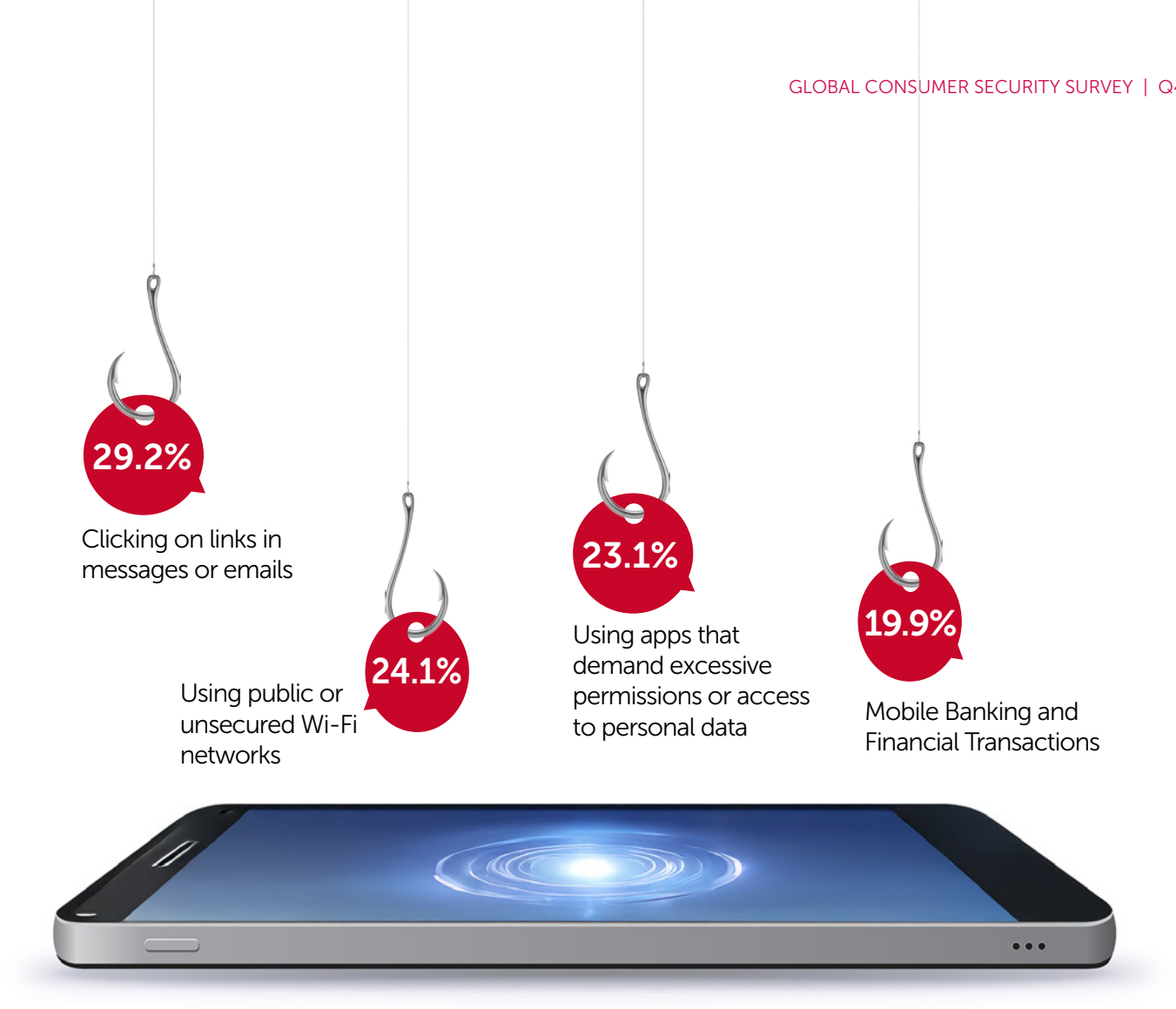
Personal Experience with Security Incidents

Dangerous Moves:

Perceived Risk of Mobile Activities

Mobile consumers report feeling most vulnerable when engaging in common, everyday mobile activities that inherently involve a degree of risk and data exchange. Top activities that make users feel the "least secure" are foundational to the modern mobile experience.

The prevalence of these activities means that the feeling of insecurity is not an occasional event but a frequent, recurring experience for a large portion of the consumer base.



The Cybersecurity Perimeter: Personal Devices for Business Activities

Mobile devices are no longer peripheral tools but are central to the modern workflow. The most common work-related tasks performed on these devices are core communication and collaboration functions, meaning sensitive corporate data is constantly in transit through them: The top business tasks performed on personal devices include:

43.7% Messaging colleague

31.8% Work-related calls & video conferences

30.6% Business Communication & Work Emails

The prevalence of these activities indicates that the traditional corporate security perimeter has effectively dissolved. The new cybersecurity perimeter is the employee's mobile device, wherever it may be.

The Trojan Horse Effect: Business Devices for Personal Activities

This blurring of boundaries is mutual, resulting in what can be called a "Trojan Horse" effect. A significant number of users admit to using their work-provided mobile devices for personal activities, including those that pose a high cybersecurity risk.

16.7% Online shopping

15.6% Social media & online communities

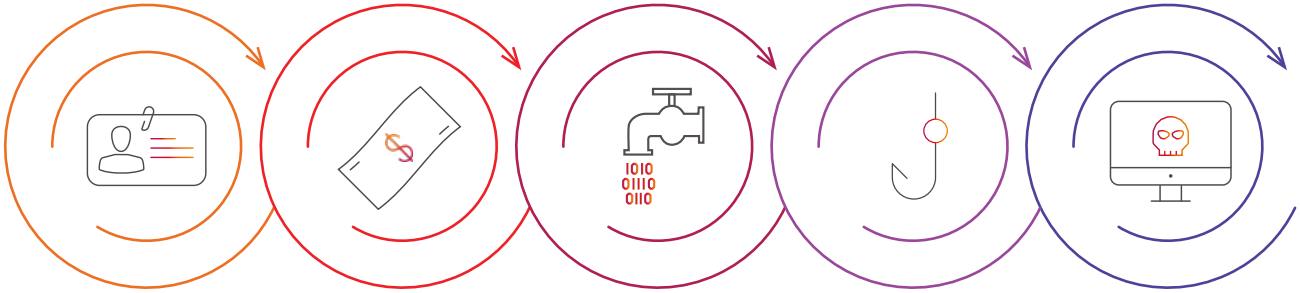
13.9% Personal banking & financial transactions

When an employee uses a corporate device for personal shopping, they might accidentally click a malicious link in a fake shipping notification. This action brings a threat from the less-controlled personal sphere directly into the corporate environment, potentially bypassing enterprise security measures, posing a persistent risk for businesses.

This “Trojan Horse” effect exposes corporate systems to consumer-level risks. Enterprises face growing threats from employees’ hybrid use of mobile devices, underscoring the importance of telco-provided, network-level protection.

The Threat Perception Spectrum

When presented with a comprehensive list of potential security threats, mobile consumers demonstrate a multifaceted understanding of the risks they face. The concerns span issues of identity, finance, and data privacy. The most concerning threats are:



When forced to choose, users overwhelmingly focus on the damaging outcome and less on the risky technical activity (e.g., Public Wi-Fi, IoT), which can have profound implications for how to approach consumers with cybersecurity service offerings.

The most significant perceived threat differs from market to market. For example:

- In the **United Kingdom** and **Sweden**, the primary concern is **Financial Theft**, which is a significantly higher priority there than in most other surveyed nations.
- In the **United States** and **France**, the dominant fear is **Identity Theft**. The US also shows a uniquely high concern for the broader category of "Exposure of personal information" (11.5%).
- In **Germany**, concerns are more evenly distributed, but users show a significantly higher preoccupation with the attack vectors of **Phishing** and the risks of **Public Wi-Fi** compared to their international peers.

Beyond the overall concern for cybersecurity threats in general, when selling security services to the consumer market, messaging and service positioning should be localized to match regional concerns. For example, identity protection in the US versus financial safeguards in the UK.

The Behavior Gap: Awareness vs. Action

Earlier in this report, we presented survey results that unequivocally revealed that a majority of consumers are concerned with cyber threats aimed at their mobile devices. Despite high awareness:

- **36.3%** of consumers currently use a dedicated mobile security app or service.
- **50.4%** of consumers admit they have no protection at all.
- Regional differences also exist: **Germany** shows higher mobile cybersecurity solution adoption (**41.2%**) than the **UK** (**30.1%**), despite UK consumers being more worried about financial theft. This may reflect a lack of trusted or effective solutions in the UK.

Despite the aforementioned high rate of concern about mobile cyberthreats, these findings point to barriers to adoption of cybersecurity protection solutions. Those barriers include cost sensitivity, complexity of setup, and skepticism about third-party apps. Mobile service providers have a unique opportunity to bridge this gap with zero-touch, trusted solutions.

The market for mobile security is far from saturated. It seems that the primary challenge for providers is not to create awareness of the problem, which already exists in abundance, but to overcome the inertia and specific barriers that prevent concern from converting into a purchase.

Adoption is lowest among 18–24-year-olds (30.4%), even though they report the highest concern (73.2%) about cyber threats.

Trust is the New Currency

Crucially, users have a clear preference for whom they want to provide cybersecurity service. An overwhelming 84% of respondents would trust their own mobile service provider to offer a cybersecurity solution. This is in contrast to the tendency for consumers to admit personal responsibility (40%) for the cyber hygiene of their mobile devices while only 16% blame their mobile service provider. By taking responsibility, yet not finding blame in the telco, consumers are likely saying that they want a cybersecurity solution that they can count on, but they want to decide where to acquire it.

Easier to Use Means Easier to Sell

The ideal product is not only trusted but also effortless. 47.4% of mobile users are more likely to purchase a security solution if it does not require any manual app installation on their device. This signals a strong market demand for network-level security. Users are often wary of installing additional applications due to concerns about device performance, battery drain, and installation and configuration complexity. The data shows a clear preference for a solution that "just works" in the background, protecting the device at the network level without requiring any user intervention.

Purchasing a security solution from a third-party vendor in an app store requires the user to conduct research, vet an unfamiliar company, download, install, maintain and update software and establish a new payment relationship. These are all points of friction that can deter a purchase. A network-based, zero-touch onboarding, hassle-free service is a strong differentiator in the crowded market of standalone security apps. This affords the telco a brand perception that evolves from a connectivity provider to a comprehensive guardian for the consumer's digital life.

84% would trust their own mobile service provider to offer a cybersecurity solution

From Concern to Conversion

Consumer willingness to pay for a mobile cybersecurity solution is strong. The data presents a robust commercial signal, with a combined 67.1% of respondents indicating they would be willing to pay their mobile service provider a monthly fee for a comprehensive cybersecurity protection solution. What's more, telcos are well positioned to offer the fundamentals of cybersecurity services that consumers want.

Simplicity

Nearly half (47.4%) of consumers are more likely to buy a solution that does not require app installation, favoring zero-touch network-based protection. Consumers are looking for security solutions that work in the background without requiring constant attention or manual intervention. Simplicity is embodied by the network-based approach to cybersecurity protection.

Trust

As mentioned above, 84% of consumers trust their mobile provider to deliver such a solution, far higher than their trust of independent vendors. Consumers perceive their mobile providers as reliable and capable of delivering effective security services. This trust can be leveraged to drive adoption and build customer loyalty.

Affordability

The optimal pricing point is clear: around $5 / €5 / £5 per month across all major markets. Across all surveyed markets, consumer willingness to pay is concentrated at the lower end of the pricing spectrum. While some users are willing to pay a premium, the volume opportunity lies in an affordable, mass-market price point.

The Telco Opportunity

Simplicity and price sensitivity are paramount to unlocking this market. For telcos, the commercial opportunity lies in offering affordable, frictionless, network-level security as a service. This leverages the telco's existing trust (established in this report), billing relationship, and distribution channels.

High motivation and trust responses indicate that the opportunity is not for a niche, high-margin product but for a mass-market, volume-based service integrated seamlessly into the user experience.

Beyond trust, a simple, hassle-free solution and customer awareness about cybersecurity threats, the final key to success for the telco is the sense of urgency that can be imparted to the customer by properly educated and motivated sales and support staff at the point of sale and on service engagements. When the customer understands that they have a problem and the telco has the solution right now, the cybersecurity protection solution becomes a high-value win-win scenario.

The gap between consumer awareness of cybersecurity threats and the inaction toward acquiring solutions to protect themselves from those threats illustrates the lack of the basic factors in the choices made by consumers. Those factors – Simplicity, Trust and Affordability – are all elements that telcos can deliver, enabling them to close the gap and attract the mass market to their network-based cybersecurity services.

Conclusions

The results of the Q4 2025 Global Consumer Security Survey point to seven primary conclusions for telcos:

Security Concerns

Concern is widespread and rising: Security is now a mainstream consumer issue.

Price Sensitivity

Mass-market adoption depends on affordability (~$5/month).

Zero-Touch Solutions

Consumers are reluctant to adopt third-party apps; zero-touch solutions win.

Localized Approaches

Perceptions differ by market, demanding localized approaches.

Blurring Perimeters

Mobile devices are the new security perimeter, blurring personal and work risk.

Channel Advantage

Mobile providers enjoy a built-in channel advantage based on trust and billing.

Revenue Opportunity

The opportunity is ripe for providers to convert concern into adoption, imparting a sense of urgency to turn passive anxiety into recurring revenue.

The 2025 consumer cybersecurity landscape is defined by high anxiety but low adoption. While users are acutely aware of risks like identity theft, financial loss, and phishing, most still lack effective protection. This gap between awareness and action creates a dual narrative:

A RISK STORY where personal and corporate data remain vulnerable.

A GROWTH STORY where mobile service providers can step in as trusted digital guardians.

In Q4 2025, this study explored an intriguing paradox: While mobile consumers expressed considerable concern about digital threats, most still fail to adopt protective measures, creating a large, untapped market. It indeed confirms that widespread anxiety has not yet resulted in the adoption of security solutions.

Concern is both widespread and passive. Over 61% of users worry about mobile security, and nearly 50% feel more concerned than they did a year ago. Despite this, only 36% currently use a security application or service, highlighting significant barriers to adoption.

This study highlights a growing concern that intensifies year after year, underscoring a market with increasing urgency. This momentum, likely driven by continuous news cycles of data breaches, high-profile scams, and more sophisticated phishing attacks, creates fertile ground for providers to introduce solutions to a population that is becoming progressively more receptive to messages of protection.

This report emphasizes the inherent channel advantage held by mobile providers. Consumers already have an established billing relationship, a customer service history, and a foundational level of brand trust with their mobile providers.

And indeed, the data points to a clear and trusted market channel - the Mobile Provider. A remarkable 84% of users trust their provider to offer a security solution, and a commercially significant 67% are willing to pay a monthly fee for it. This positions the mobile provider as the ideal and most trusted partner to bridge the Awareness-Action Gap and deliver security at scale.

This study advocates for Mobile Providers to adopt and promote simple, network-integrated, and affordably priced security solutions that deliver zero-touch provisioning and operation. Success relies on leveraging inherent user trust and addressing specific regional threat concerns to turn passive worry into active, protected, and recurring-revenue customers.

Strategic Recommendations

Once a telco has chosen a cybersecurity protection service solution for their consumer customers, they may want to consider the next steps to get their organization prepared to take advantage of the new revenue-generating opportunity. The following recommendations are based on findings from the global consumer survey described in this report:

Acknowledge Customer Concerns

Your customers are worried about cybersecurity threats. It is the obligation of the telco to acknowledge their concerns and to relate to them as such. Without executing a fear campaign, which research shows is ineffective, the telco can build a sense of urgency at the point of sale and in service engagements. In order to tap into the reality that customers experience, the telco can offer a simple solution that is available immediately, rather than a campaign that deepens fears.

Leverage Trust in the Telco Brand

The telco should highlight their role as both a concerned service provider who offers easy-to-use, reliable and comprehensive services, and also as a digital guardian, perceived as the primary protector by over 84% of consumers. This differentiates the telco from its competitors and from third-party bundled and app-store solutions.

Offer Network-based Protection

When offering a network-based cybersecurity solution to consumer customers, the telco should focus on presenting it as a solution that requires no app download, installation, configuration or updating and runs seamlessly in the background. This translates into benefits such as zero-touch onboarding, hassle-free, battery-friendly and always-on protection.

Price the solution for the Mass Market

Research shows that the maximum price point that is acceptable to consumers around the globe centers around $5/€5/£5. While final pricing should be assessed on a case-by-case basis, when priced at or below this level, and combined with the zero-touch onboarding and hassle-free operation messages, the telco can expect high service adoption rates.

Tailor Regional Messaging

The survey laid out in this report identified differences in priorities among consumers across various regions. By tailoring security messages for each region, a telco can achieve greater impact when it comes to persuading customers to subscribe to cybersecurity services. A few examples of how to take advantage of these regional differences are below:

- Emphasize identity protection in the US and France.
- Stress financial protection in the UK and Sweden.
- Highlight phishing protection in Germany.

Address the Youth Gap

Younger respondents to the survey expressed higher concern for cyber threats while responding that they were there least protected. Use campaigns that resonate with younger subscribers' digital-first lifestyle and emphasize simplified service onboarding.

Take Advantage of Cybermarketing Professionals

When preparing to go to market and promote network-based consumer cybersecurity services, the telco can leverage Allot's experience deploying cybersecurity projects with tier-1 and other CSPs worldwide. Allot's 'Cybermarketing' experts and programs take the guesswork out of launching services and building a highly profitable revenue stream. The Allot Cybermarketing team can help develop the business case, evaluate commercial models and marketing channels, define technical requirements, develop a communication strategy, offer valuable business intelligence and more. Their knowledge base has been accumulated over years of successfully launching such services worldwide.

The Allot Secure Offering

Allot offers a comprehensive 360-degree, network-native cybersecurity solution that delivers services that telcos can provide their consumer customers for hassle-free protection from cyber threats on any device, at anytime and anywhere the device is connected. Customers benefit from peace of mind with a comprehensive set of services that they can afford, and telcos benefit from satisfied customers with a branded solution that generates recurring revenue and reduces churn. This industry-leading solution is trusted and deployed by many of the world's leading telecommunications companies. It includes the following services:

Allot NetworkSecure

Enables the telco to deliver robust network-based security and content filtering services effortlessly to the mass market.

Allot DNS Secure

DNS-based, network-native security solution providing threat protection and parental control functions for the consumer market

Allot HomeSecure

Leveraging the home router, provides zero-touch security for home networks, protecting PCs, tablets, smartphones, and IoT devices from increasing cyber threats.

Allot OffNetSecure

OffNetSecure SDKs can be integrated into the telco customer care or any other app that is already on the customer's mobile devices. It keeps users safe when they are away from the telco network.

Allot Identity Theft Monitoring

Tracks stolen identity and personal data on the Dark Web and alerts end customers with information and recommendations so that they can take steps to protect themselves.

Methodology

During September of 2025, Dynata, the world's largest first-party data company, together with Allot, set out to gain insights into consumer perspectives on cybersecurity and to discover how they protect their mobile devices, data and money against cyberthreats. The survey included 3,111 mobile service customers from the United States, the UK, Germany, France, Italy and Sweden. 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.

Target profile

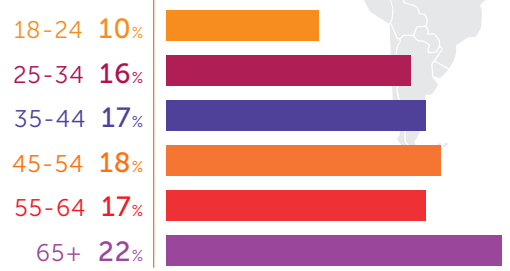
100%
Mobile device users subscribed to any paid digital subscription service

Gender

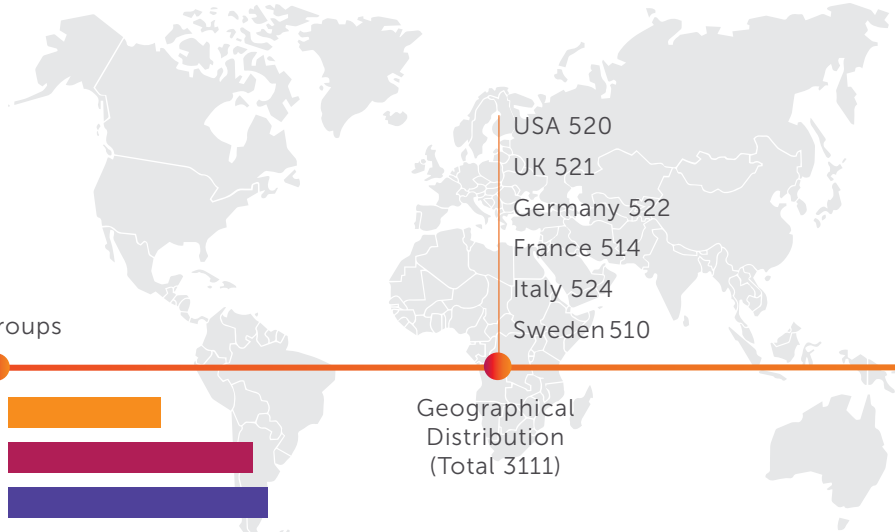
51% Male

49% Female

Age groups



Geographical Distribution (Total 3111)



Resources

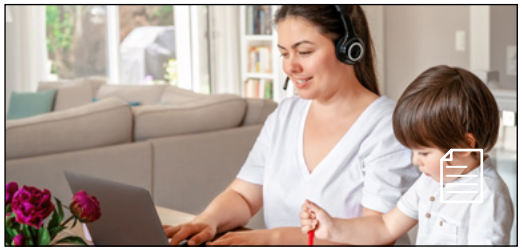
The following resources provide additional insight to CSPs considering converged security solutions for their customers.

Allot Secure Brochure
Learn more

On-demand Webinar: The Cybersecurity Awareness–Action Gap: A Telco Revenue Growth Opportunity
Learn more

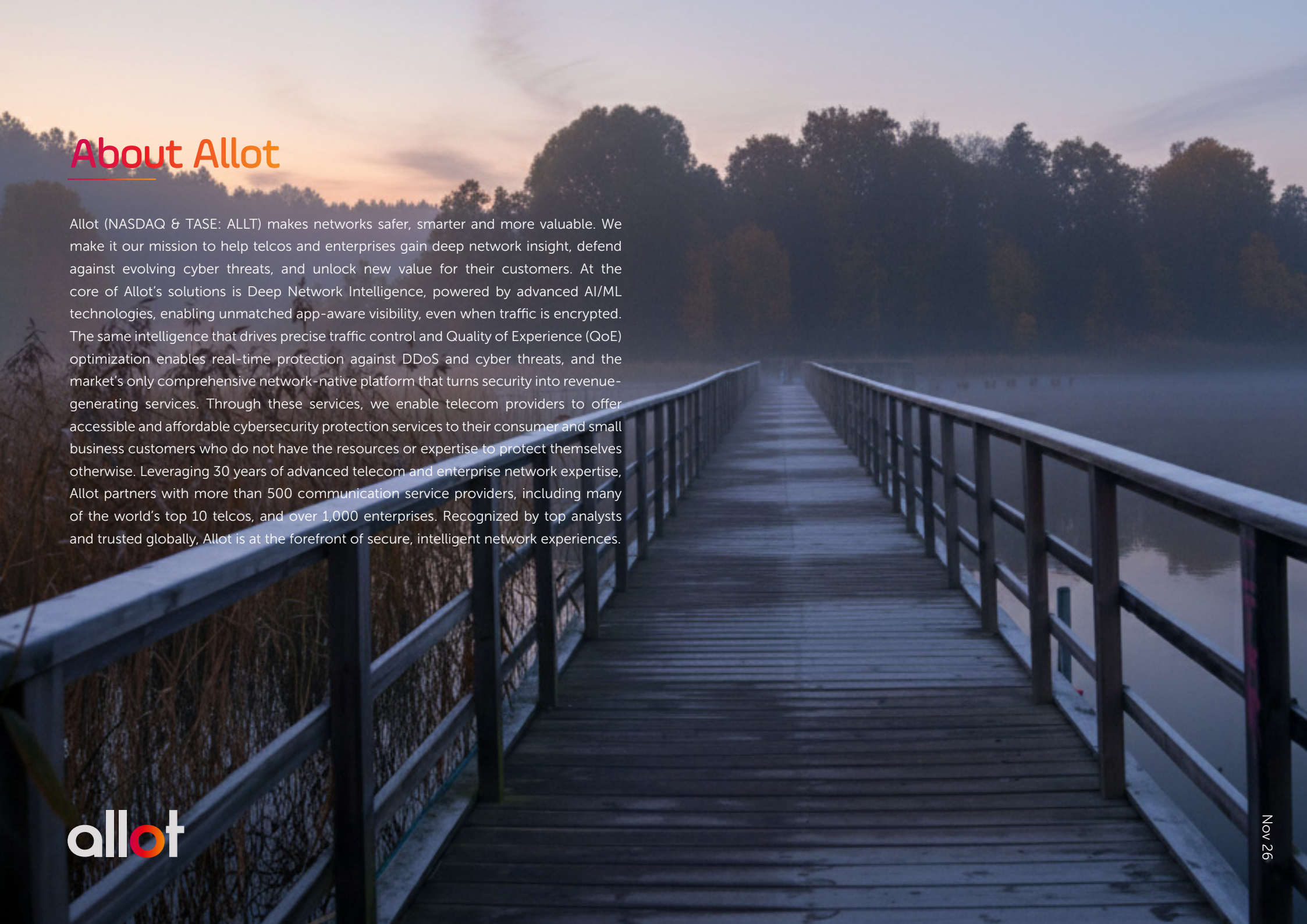
Allot NetworkSecure Brochure
Learn more

Allot OffNetSecure Brochure
Learn more



Allot HomeSecure Brochure
Learn more

OMDIA Market Radar: Total consumer cybersecurity solutions for telcos
Learn more



About Allot

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.

allot