Omdia
by informa techtarget

Digital Guardians: The CSP Advantage in Delivering Consumer Cybersecurity

Author: Mariana Zamoszczyk and Michael Philpott

September 2025

In partnership with:

F-Secure®

Contents

Executive summary

As digital threats continue to grow in sophistication and scale, communication service providers (CSPs) are uniquely positioned to become trusted guardians of consumer cybersecurity. This research study explores how CSPs can leverage their existing infrastructure and customer relationships to develop a comprehensive cybersecurity offering that not only protects consumers but also creates substantial business value.

By implementing comprehensive cybersecurity services, CSPs can transform security from a cost centre into a growth engine—generating new revenue streams, increasing average revenue per user (ARPU), enhancing customer loyalty, reducing operational costs, establishing meaningful market differentiation, while building brand trust, and boosting customer confidence.

The question is no longer whether CSPs should offer cybersecurity services, but how quickly and comprehensively they can bring these critical value-added services (VAS) to market. Those who act decisively will establish competitive advantages that extend far beyond the immediate revenue opportunity, positioning themselves as strategic partners in their customers' digital lives.

Key recommendations for CSPs

- **Transform security positioning from fear-based add-on to essential digital lifestyle enhancement.** CSPs should adopt a benefits-focused narrative that emphasizes how security enhances digital experiences rather than merely preventing negative outcomes. They also should replace technical terminology with accessible language that connects security features to everyday digital activities and tangible lifestyle improvements. This includes integrating security seamlessly into core connectivity offerings to establish protection as an expected component of the digital experience rather than an optional extra, while creating tiered security packages that align with different customer segments' digital lifestyles and usage patterns.

- **Empower digital safety by reinforcing consumer education and transparency.** Help consumers to identify devices that need greater protection as well as new potential threats. For example, offer personalized device security assessments by developing interactive tools that scan customers' connected environments and provide customized security recommendations for each device. Also, implement proactive alerts about emerging threats specifically relevant to customers' device profiles and usage patterns. For greater transparency, remind consumers of all the different CSP initiatives that are taking place in the background to keep them safe. This includes regularly sharing information about investments in security infrastructure and capabilities.

- **Develop a comprehensive artificial intelligence (AI) security framework, transforming AI into a competitive advantage while protecting consumers from emerging threats.** CSPs should implement a proactive, multi-faceted approach to address the double-edged nature of AI in cybersecurity, focusing on consumer education about emerging threats while building trust through transparent communication about AI-powered security measures. This includes providing clear, actionable guidance on adapting digital behaviors to counter AI-powered threats, while clearly communicating where and how AI is being deployed in the CSP's security infrastructure.

- **Create a multi-layered cybersecurity defense offering that can protect customers against all threats no matter where they are.** CSPs should implement a comprehensive, adaptive cybersecurity framework that integrates multiple protection layers, leverages advanced technologies, offers protection anywhere, and evolves continuously to address the full spectrum of digital threats. This includes developing a centralized security management system that coordinates across network, endpoint, cloud, and application layers. This approach will help CSPs to maximize the growing cybersecurity monetization potential by creating differentiated security offerings that drive significant new revenue streams.

- **Promote a household security command center that provides comprehensive protection while offering a single, intuitive control interface.** As traditional fragmented security approaches are becoming inadequate, the key is to provide comprehensive protection through multiple security touchpoints. Therefore, CSPs should develop a centralized control interface capable of managing protection across all household devices, applications, and networks. This unified approach will significantly enhance consumer protection while simplifying the user experience.

- **Integrate cybersecurity features directly into existing apps to drive efficiency and greater engagement.** Encourage active engagement with embedded security features rather than continuing to offer standalone security solutions. This approach will help CSPs to address the critical challenge of low adoption rates for specialized security apps while supporting the industry-wide movement toward application consolidation. Moreover, by embedding protection directly into applications customers already use and value, CSPs will be able to increase overall security adoption levels, while driving additional engagement to their core service app and supporting broader application consolidation strategies.

The cybersecurity imperative: Why is it so important for CSPs?

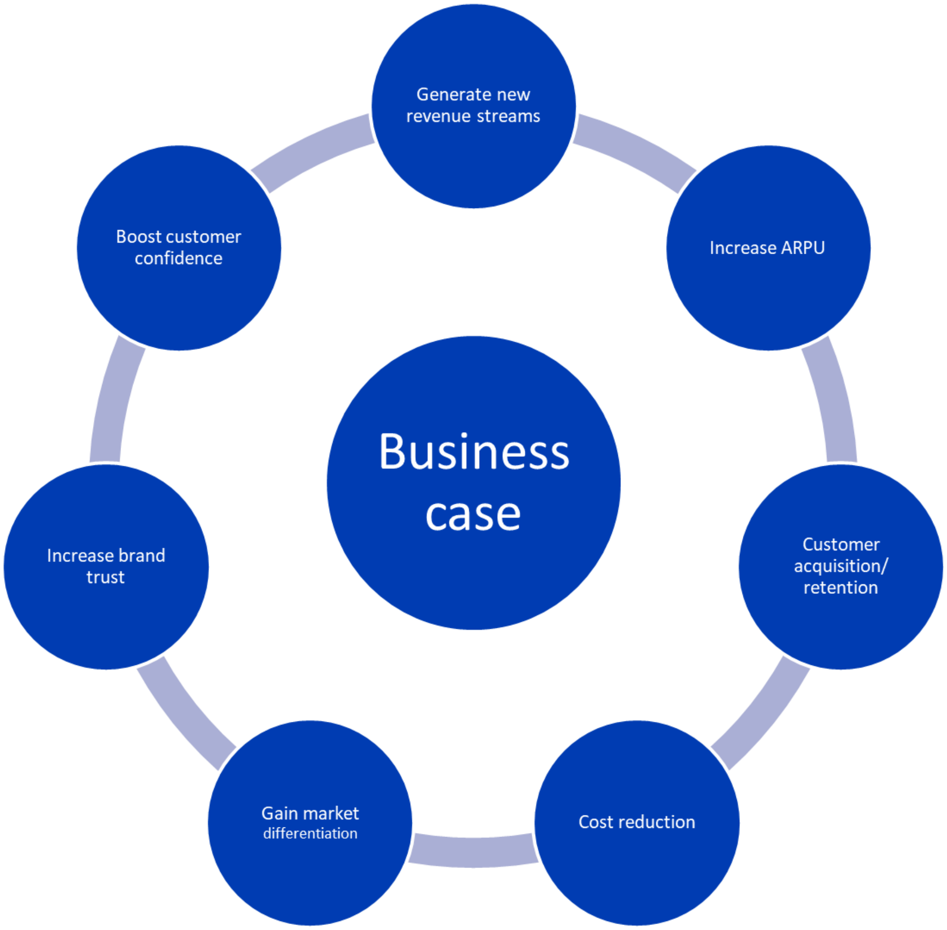
Today's consumers face an unprecedented array of digital threats—from sophisticated phishing schemes and malware to identity theft and smart home vulnerabilities. As the digital footprint of the average household expands through multiple connected devices, the attack vectors for cybercriminals grows proportionally. According to the Global Anti-Scam Alliance[1], consumers lost $1.03 trillion to scammers in 2024. Moreover, when looking at recent self-reported cybercrime victim figures, SMS scams have increased by 70.3% from 2024 to 2025, while E-mail scams have increased by 44.2% during the same period, according to F-Secure Consumer Market Research 2025 survey. This threat landscape creates both a challenge and an opportunity for CSPs.

CSPs serve as the fundamental gateway to the digital world for millions of consumers. This privileged position at the network level gives them unique visibility into traffic patterns and potential threats, creating an opportunity to offer value-added security services that protect customers across their entire digital footprint. This is particularly important as 81% of consumers expect their Internet service provider (ISP) to give them some level of protection (either full or basic protection), according to F-Secure Consumer Market Research study, published in June 2023.

Figure 1 highlights the business case for consumer cybersecurity services.

[1] “Global State of Scams Report 2024”, Global Anti-Scam Alliance

Figure 1: Developing a comprehensive cybersecurity strategy can help CSPs to achieve strategic business outcomes


Business case
Generate new revenue streams
Increase ARPU
Customer acquisition/ retention
Cost reduction
Gain market differentiation
Increase brand trust
Boost customer confidence

Source: Omdia

Opportunity to grow APRU

By developing a comprehensive cybersecurity offering, CSPs can tap into the rapidly growing consumer security market, generating new revenue streams. This includes services such as identity protection, scam protection, and password management, among others. Each of these offerings represents a potential subscription stream that extends beyond traditional connectivity, allowing CSPs to diversify their revenue sources and reduce dependence on commoditized connectivity services.

In mature markets where subscriber growth has plateaued, increasing ARPU has become critical. Therefore, consumer cybersecurity services represent high-margin additions to existing service bundles that can help CSPs to justify higher overall mobile and broadband package prices.

Increasing loyalty

In terms of customer acquisition and retention, offering consumer cybersecurity solutions can help CSPs to create strong service differentiation. This can improve retention metrics by lowering churn rates when compared to standard offerings. Moreover, offering cybersecurity protection is instrumental to prevent security incidents that can potentially trigger customers to change their service provider. For example, the time spent on entering credentials into the password manager and/or dark web monitoring creates a link with the solution that increases switching costs. Therefore, CSPs are in a key position to become trusted partners and digital guardians, promoting a relationship based on confidence rather than merely transactional connections based on price and speed.

Fewer support calls

The efficiency effect gained from the supply of consumer cybersecurity services extends far beyond its immediate security benefits. Fewer security-related support calls, with improvements in the handling time driven by diagnostic tools, and containment of security incidents affecting multiple customers through automated intervention, are some key examples of operational efficiencies that result from the development of a proactive consumer cybersecurity strategy.

This efficiency dividend creates a virtuous cycle where better security leads to more efficient operations, which enables more resources for security innovation and improvement. The most successful CSPs are leveraging these operational efficiencies not just as cost-saving measures, but as strategic capabilities that can enable faster innovation, better customer experiences, and sustainable competitive advantages in an increasingly security-conscious market.

Meaningful differentiation

Another important benefit for CSPs is that offering consumer cybersecurity solutions provides meaningful differentiation in markets where connectivity services have become increasingly commoditized. This allows CSPs to enhance brand perception and become a digital lifestyle partner rather than just a telecommunications service provider.

Higher customer lifetime value

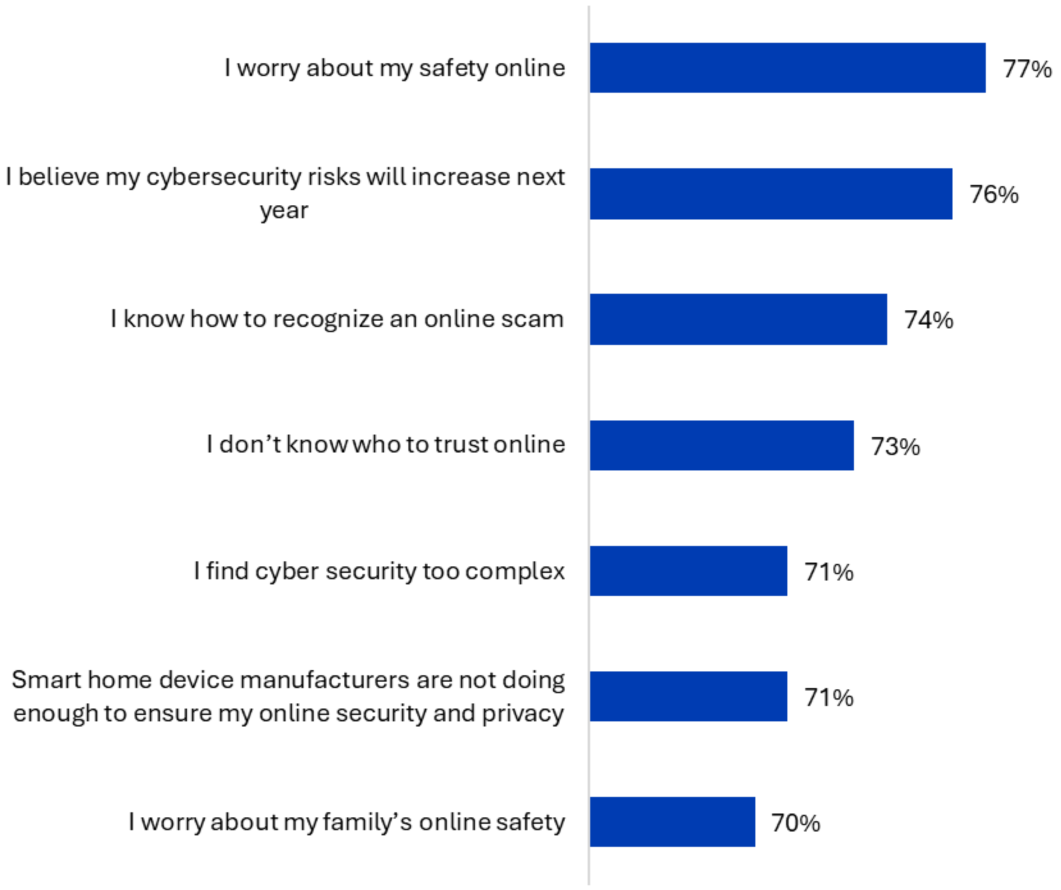
Finally, by providing comprehensive protection, CSPs can empower customers to fully embrace digital services. As a result, protected customers are more likely to try new digital offerings and reduce cybersecurity anxiety. This increased confidence translates directly into higher service utilization rates and greater customer lifetime value.

Digital trust in crisis: Consumer cybersecurity fears reach record levels

As digital services become an integral part of daily life, consumers find themselves navigating an increasingly complex security landscape. From managing finances and healthcare to conducting routine shopping and social interactions, today's digital lifestyle has transformed from convenience to necessity—bringing with it greater consumer awareness of its risks and threats.

As F-Secure Consumer Market Research 2025 survey highlights, consumer view of the digital world’s future is worrying (**see Figure 2**). Another key finding of this survey is that more people expect cybersecurity risks to increase next year. Consequenly, security consciousness is expected to grow as more consumers become vigilant about threats like phishing attacks that mimic trusted institutions, identity theft schemes that can destroy people’s financial stability, and scams messages that are becoming more contextual through AI.

Figure 2: The consumer view of the digital world is worrying


F-Secure Consumer Market Research survey: Online security related statements

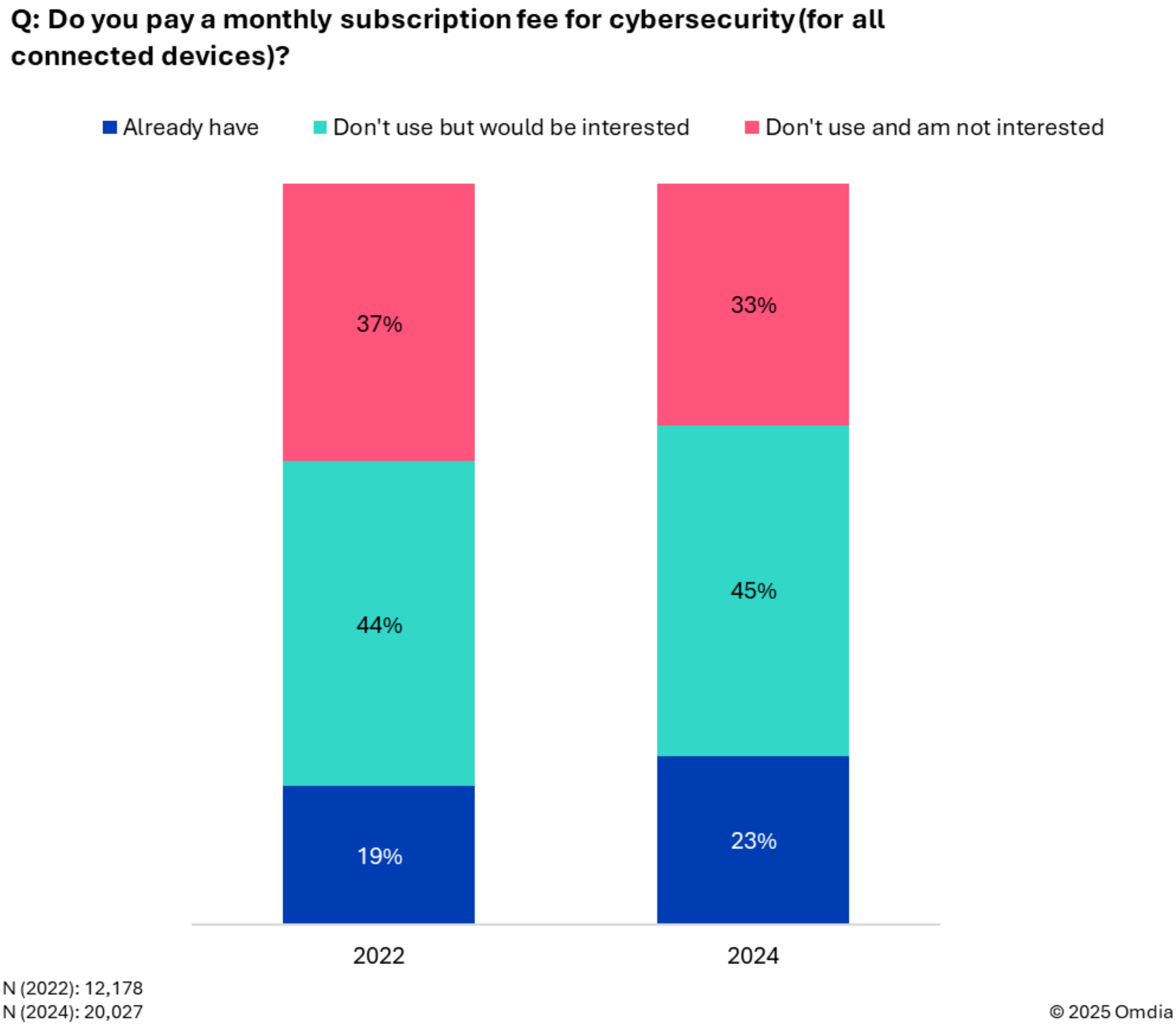
Source: F-Secure Consumer Market Research, January 2025 (N:11,000)
Responses: Strongly + somewhat agree

The fact that scams are becoming significantly more sophisticated due to AI is also fueling the current digital trust crisis. The phenomenon of AI-powered scams will make it harder for consumers to identify threats because most of the traditional cybersecurity red flags are now being eliminated by AI. Omdia believes that the full extent of AI's role in consumer cybersecurity is still emerging, but it will enable fraudsters to refine current psychological manipulation techniques introducing new efficiencies to the existing problem. This fundamental transformation is making traditional detection methods increasingly obsolete, a situation that requires urgent attention from all cybersecurity market participants.

The price of peace of mind promotes a surge in cybersecurity spending

The increasing scam frequency and sophistication together with the vulnerability of human intuition are driving consumers to reconsider their security practises. The rise in fraudulent activity has indeed encouraged consumers to spend more on cybersecurity as Figure 3 shows. This spending is likely to increase driven not only by the growing number of connected devices in our homes, but also by the proliferation of AI-enhanced scams, such as crypto fraud, scam messages and phishing campaigns.

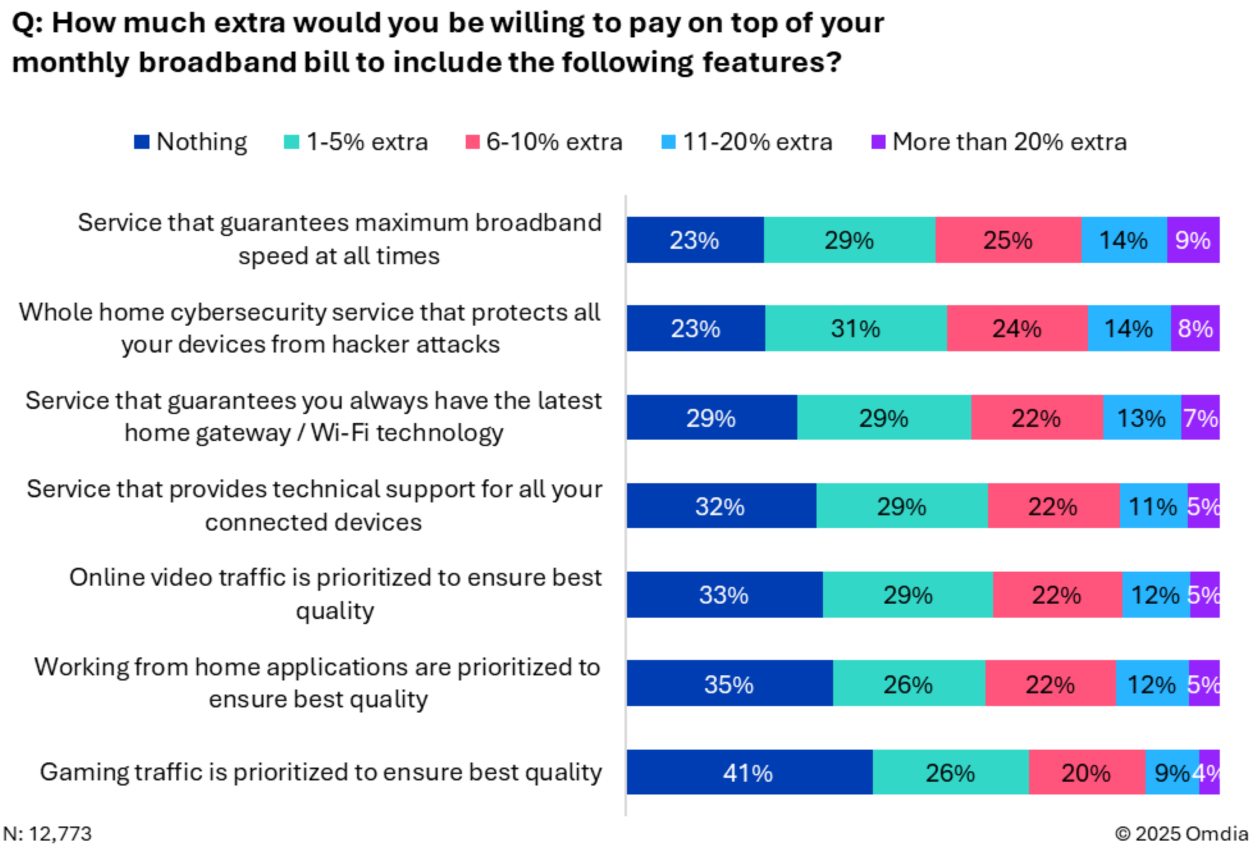
Figure 3: Consumer cybersecurity spending reaches new heights



Source: Omdia

As consumer spending accelerates, CSPs find themselves well-positioned to capitalize. **Figure 4** illustrates that alongside mobile and broadband speed guarantees, cybersecurity is the most likely mobile or broadband VAS that consumers would be willing to pay. This is increasingly the case for consumers living with children, or those with installed Internet of things (IoT) devices.

Figure 4: CSPs can harness the consumer spending momentum to accelerate cybersecurity adoption



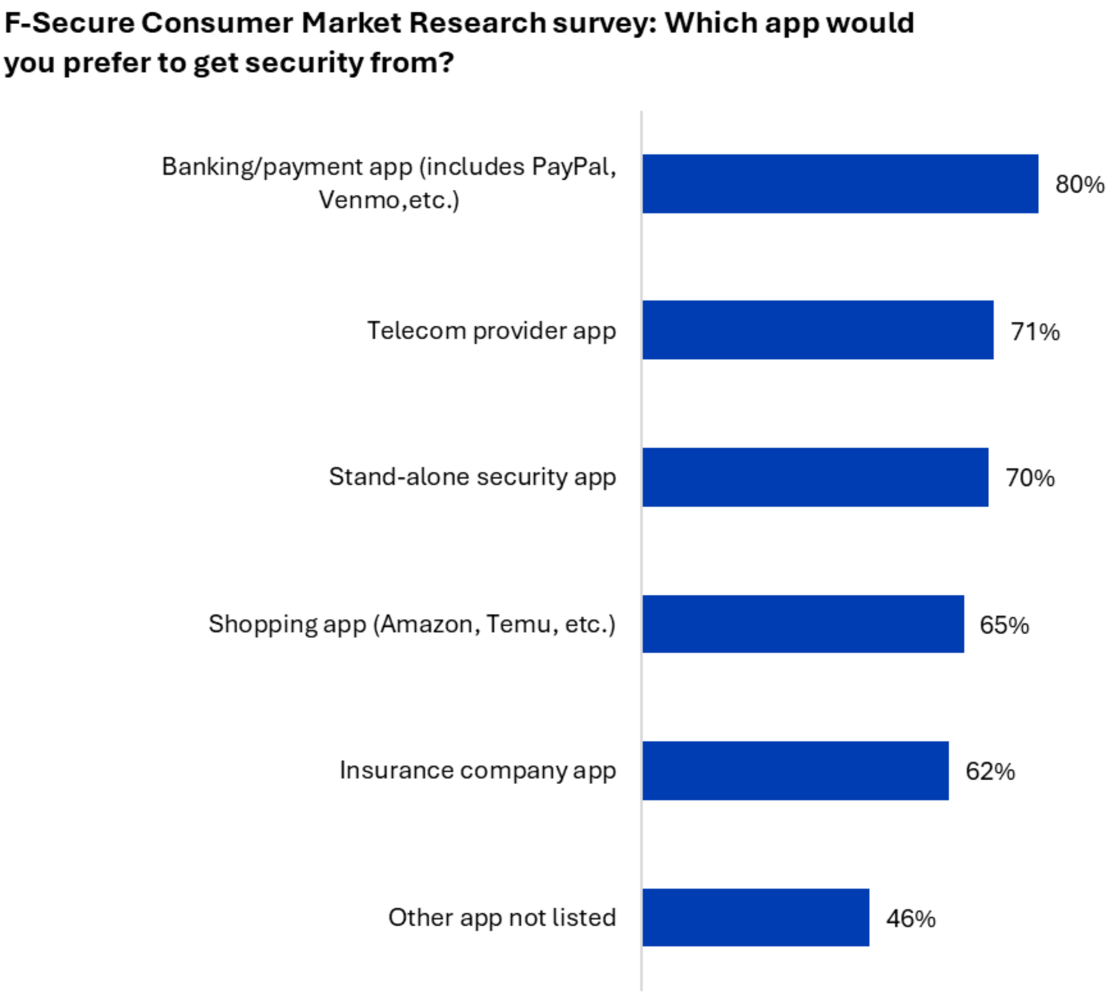
Source: Omdia

The Trust Advantage: Why consumers choose CSPs based on confidence

Feeling secure is imperative for consumers in today's digital landscape. The rise in scams has shifted how people approach digital protection, making them more aware of who to trust and what to look for in a cybersecurity service provider.

In this context, CSPs possess inherent advantages that make them natural cybersecurity guardians as Figure 5 highlights. The F-Secure Consumer Market Research 2025 survey shows that 71% of consumers preferred or would consider getting security protection from their CSP app as opposed to the app of other types of companies. When making this comparison with other types of market participants, CSPs not only have direct network access that allows them to detect and neutralize basic level of threats before they reach consumer devices, but they also have greater visibility across the entire connection path, enabling them more comprehensive threat detection than endpoint-only solutions. This network-native position allows CSPs to offer "zero-touch" cybersecurity solutions that protect consumers automatically, addressing the growing problem of security fatigue.

Figure 5: Consumers view CSPs as trusted advisors in the cybersecurity space



Source: F-Secure Consumer Market Research, January 2025
Responses: Preferred o would consider

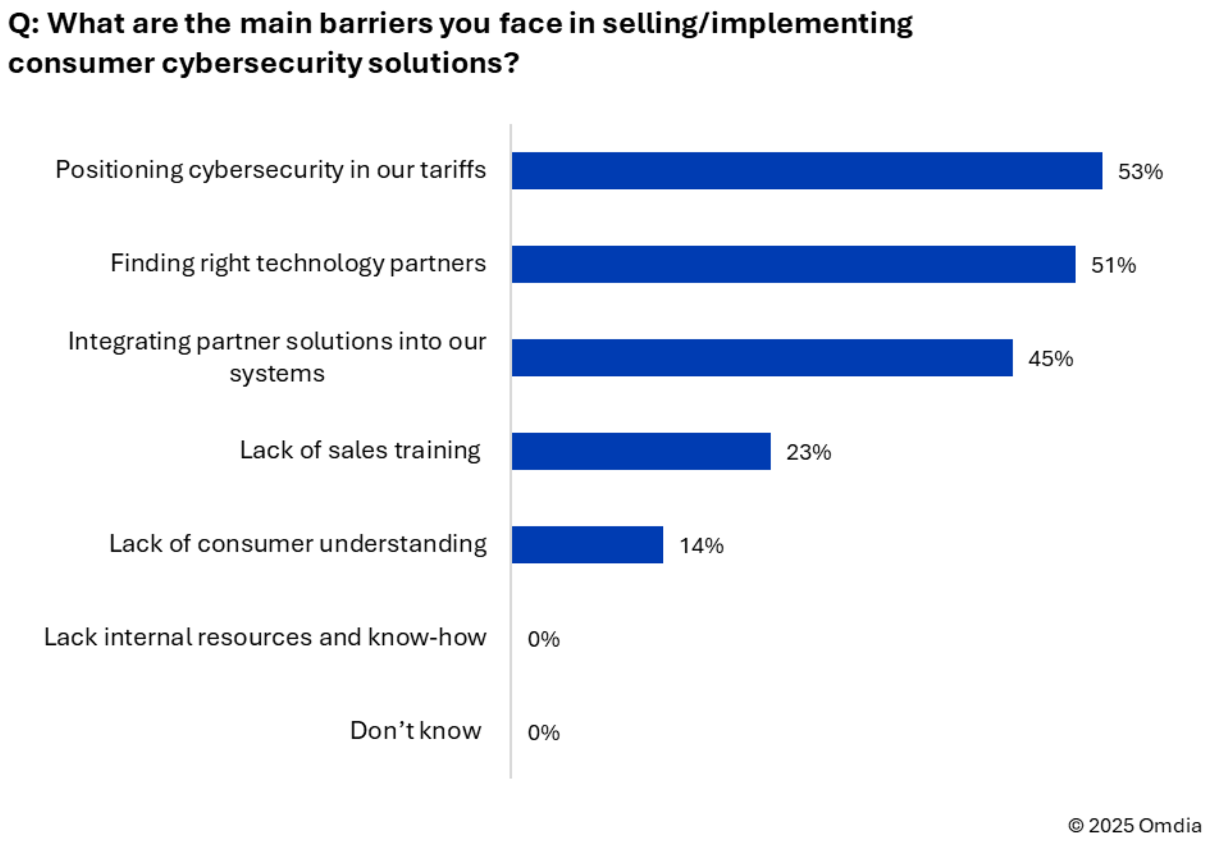
Additionally, CSPs have extensive data handling expertise, being able to handle massive amounts of customer data. This gives them a unique perspective on potential threats, while monitoring network activity. On top of this, CSPs often enjoy a good brand reputation, which can translate into greater consumer confidence in their cybersecurity portfolio. To illustrate this point, 61% of consumers would purchase security and privacy services from their ISP, according to F-Secure Consumer Market Research 2025 survey. This confidence can make CSPs more reliable and trustworthy partners when compared to other, less established players that also provide cybersecurity as part of their service proposition.

However, trust as such is not guaranteed and can be influenced by various factors. This include the CSPs reputation, the adoption of robust security measures, and the overall consumer perception of safety. For example, any significant security breach can severely damage consumer trust and lead to churn. Therefore, CSPs must regularly invest in cybersecurity and stay ahead of potential attacks.

From barriers to breakthroughs: How CSPs are cracking the consumer cybersecurity code

CSPs stand at a critical crossroads when offering consumer cybersecurity. While cybersecurity represents a significant revenue opportunity, numerous barriers prevent the effective monetization of these services as **Figure 6** shows. Understanding and addressing these challenges is essential for CSPs looking to expand beyond traditional connectivity offerings.

Figure 6: Product positioning is the main obstacle when offering cybersecurity solutions



Source: Omdia

Challenges to communicate value

Despite having robust technical capabilities, many CSPs struggle to effectively communicate the value of embedded security features in ways that resonate with consumers and drive adoption, as this is not their core product area. The challenge is that network cybersecurity as such offers invisible protection. It remains silent in the background, making value demonstration a difficult task for CSPs. To overcome this positioning challenge, CSPs should strengthen their focus on other type of solutions that drive greater visibility and engagement, such as end-point security that proactively notify users about threats. This approach can help CSPs to increase customer engagement levels, while making their consumer cybersecurity value proposition more noticeable.

Common positioning mistakes

Despite growing consumer awareness of online threats, a significant disconnect persists between this awareness and willingness to pay for protection. This gap is not being driven by consumer apathy, lack of understanding, or even the false sense of confidence they have when trying to identify scams by themselves, but rather by fundamental shortcomings in commercial positioning.

The most common failures include consumer cybersecurity solutions positioned by their technical features rather than their lifestyle benefits. Or the use of technical jargon rather than relatable outcomes when describing the benefits of digital protection. Another example refers to the case of benefits being framed around fear rather than empowerment. This is when the cybersecurity value proposition is being promoted as a solution designed to avoid bad things to happen rather than a strategic tool capable of enabling positive experiences.

Successful CSPs have learned to translate complex security concepts into everyday language that resonates with consumer priorities and experiences. Other CSPs have overcome these challenges by emphasizing their unique network-level visibility and positioning security as a natural extension of connectivity rather than a separate product category. Some CSPs have also been able to clearly communicate about blocked threats, not only preventing incidents but also reducing the growing volume of scam messages and calls that certainly generates annoyance among consumers.

Another important point is that effective scam prevention requires contextual intelligence. This means that successful scam prevention fundamentally relies on comprehensive contextual awareness. This necessitates establishing a robust data-sharing relationship built on mutual trust between consumers and their scam protection partners. When consumers willingly share relevant contextual information, protection systems can more accurately identify suspicious patterns, detect anomalies, and distinguish legitimate communications from fraudulent attempts. As a result, this collaborative intelligence framework can enhance the precision and effectiveness of scam detection mechanisms, creating a more secure digital environment through informed partnership rather than isolated protection efforts. Therefore, CSPs should position their cybersecurity offerings as intelligent protection partnerships that deliver superior scam prevention through collaborative contextual awareness rather than isolated technical solutions.

Implementation complexity

The internal implementation complexity is another important barrier for CSPs when offering consumer cybersecurity solutions. This includes challenges to identify the right security technology partner, integration difficulties when connecting partner solutions with existing systems, implementation hurdles due to multiple evolving platforms (like iOS, Android, Windows, MacOS), existing operational silos between network operations and security teams, and scalability concerns when deploying solutions across a large customer base. In most cases, this complexity often leads to delayed launches, compromised functionality, and higher-than-expected implementation costs. CSPs must develop clear integration roadmaps with realistic timelines and resource allocations to overcome these barriers.

Internal sales barriers

Even with a strong product portfolio, the existence of internal sales barriers can create hurdles in the commercial strategy. These limitations include awareness and knowledge gaps among frontline sales teams regarding security offerings, confidence issues when discussing technical security concepts with customers, incentive misalignment that prioritizes connectivity over security sales, resource limitations for specialized security sales training and support, and pressure on call handling times tied to representative compensation and staffing. These barriers result in missed sales opportunities and inconsistent customer experiences. Leading CSPs have addressed this through comprehensive sales enablement programs and specialized security sales teams.

Activation barriers

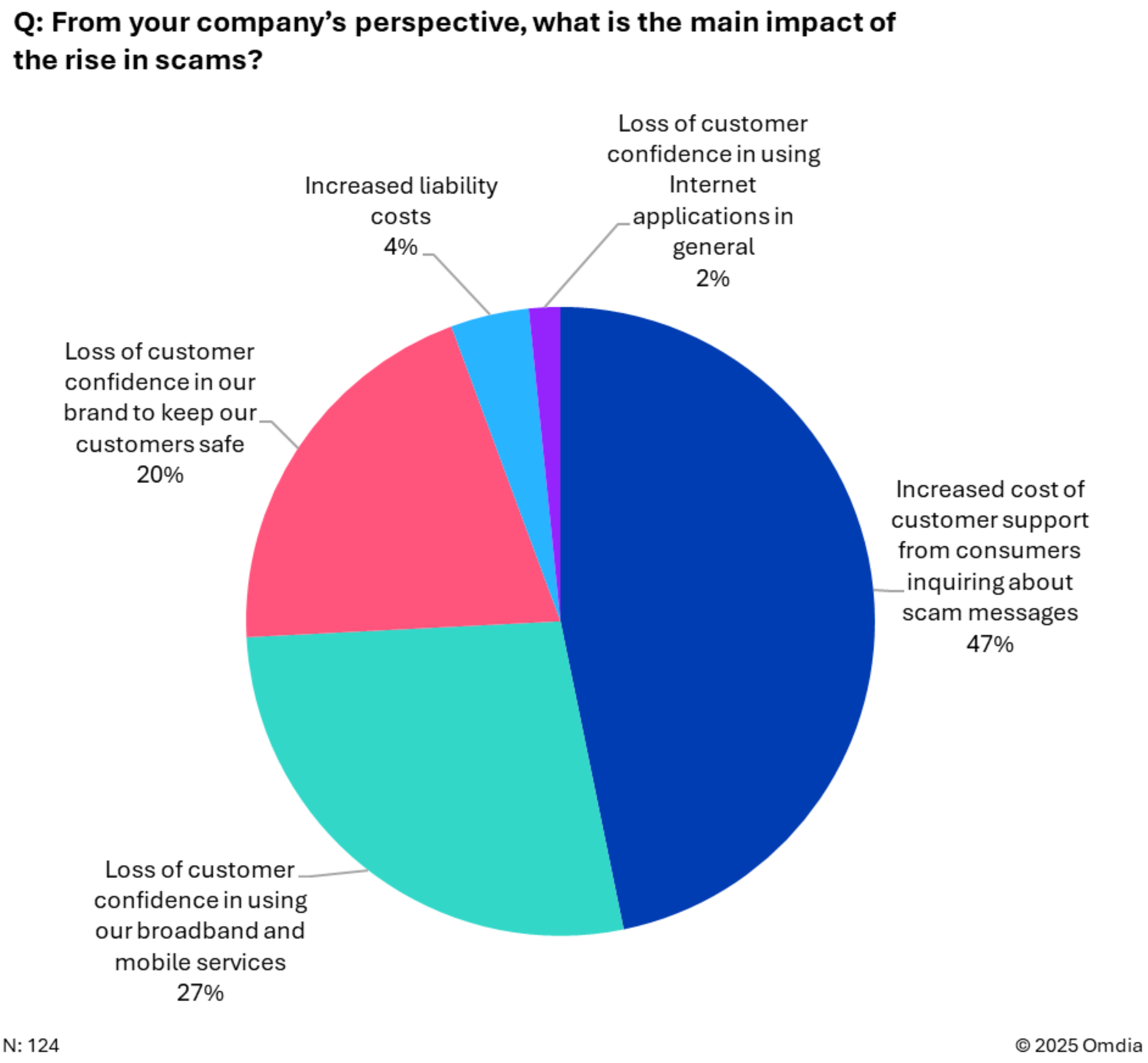
When looking at the customer journey, the path from purchase to active usage can contain numerous friction points. This includes issues such as setup complexity that exceeds customer technical capabilities, high upfront costs that create initial purchase resistance, confusing pricing structures with unclear value propositions, digital literacy requirements that exclude important customer segments, and information overload that can overwhelm potential customers.

These are some of the main customer activation barriers that CSPs face regularly when offering consumer cybersecurity services. As such, they have a negative impact on adoption and customer satisfaction rates, increasing churn and damaging brand perception at the same time. Successful cybersecurity offerings emphasize simplicity, clear onboarding processes, and tiered options that match customer technical capabilities.

Evolving consumer security expectations

Figure 7 shows how CSPs perceive the rise in scams and how it impacts them directly by reducing customer confidence and increasing operational costs.

Figure 7: CSPs believe investing in cybersecurity can offer significant operational cost benefits



Source: Omdia

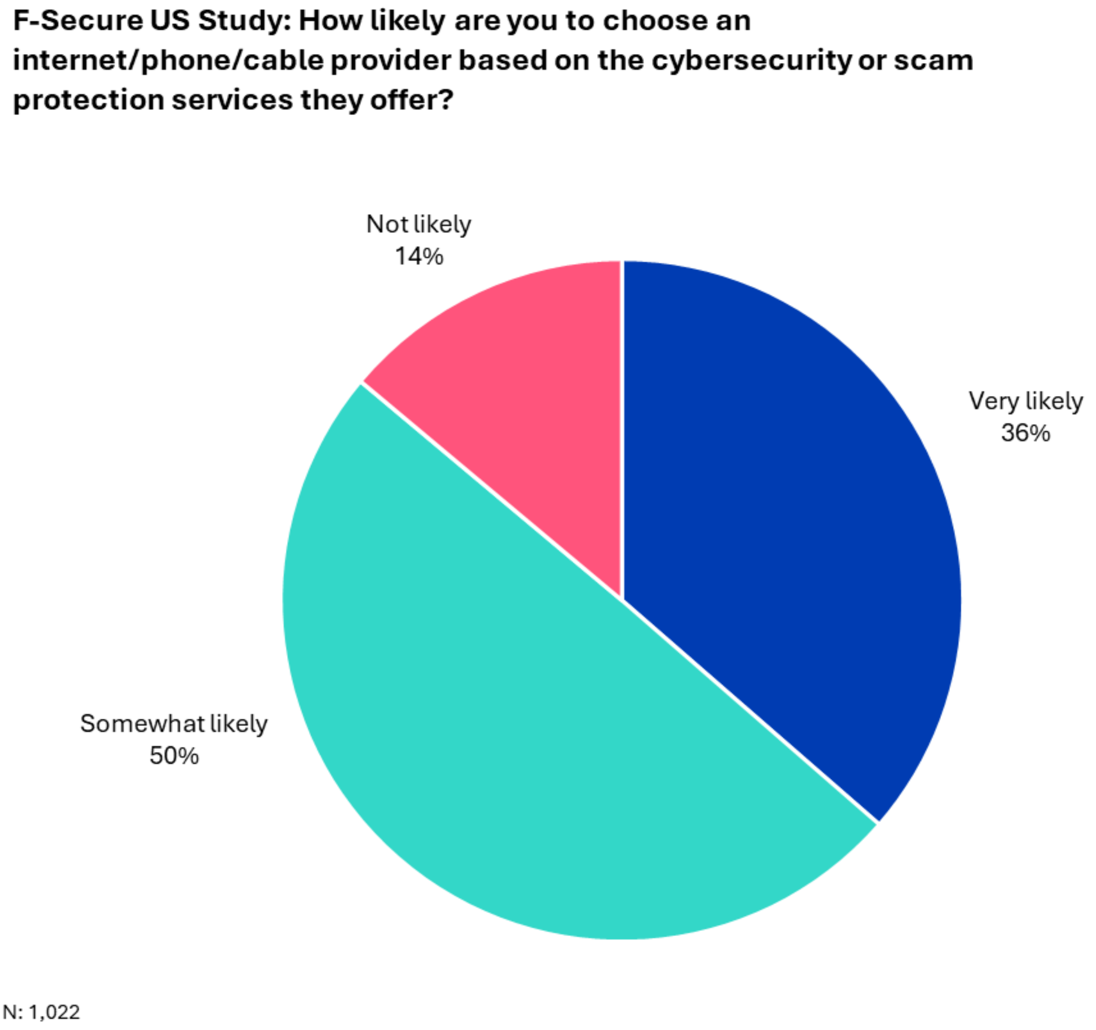
As analysed in the previous section, consumer cybersecurity expectations are rapidly changing. These expectations include the baseline safety assumption that connectivity should be inherently secure and that CSPs should bear significant responsibility for consumer safety online. Hence, the ongoing rise in scams not only damages consumer confidence in their broadband and mobile service provider but also increases their reliance on them for digital security, a situation that leads to a higher inflow of customer support calls to inquiry about online threats.

Omdia believes CSPs should prioritize consumer education as a key initiative for success. First, by helping consumers to identify devices that need greater protection as well as new potential threats. Second, by reminding them of all the different CSP initiatives that are taking place in the background to keep them safe.

The cost of inaction

Finally, the cost of inaction is another important barrier that CSPs can't afford to ignore. Failing to address cybersecurity effectively carries significant business consequences that could be catastrophic for the company's future. Besides the financial impact of direct breaches and potential regulatory penalties, not offering cybersecurity at all or at a basic level can reduce customer acquisition, especially as cybersecurity becomes a selection criterion (**see Figure 8**).

Figure 8: Cybersecurity as a driver of provider of choice



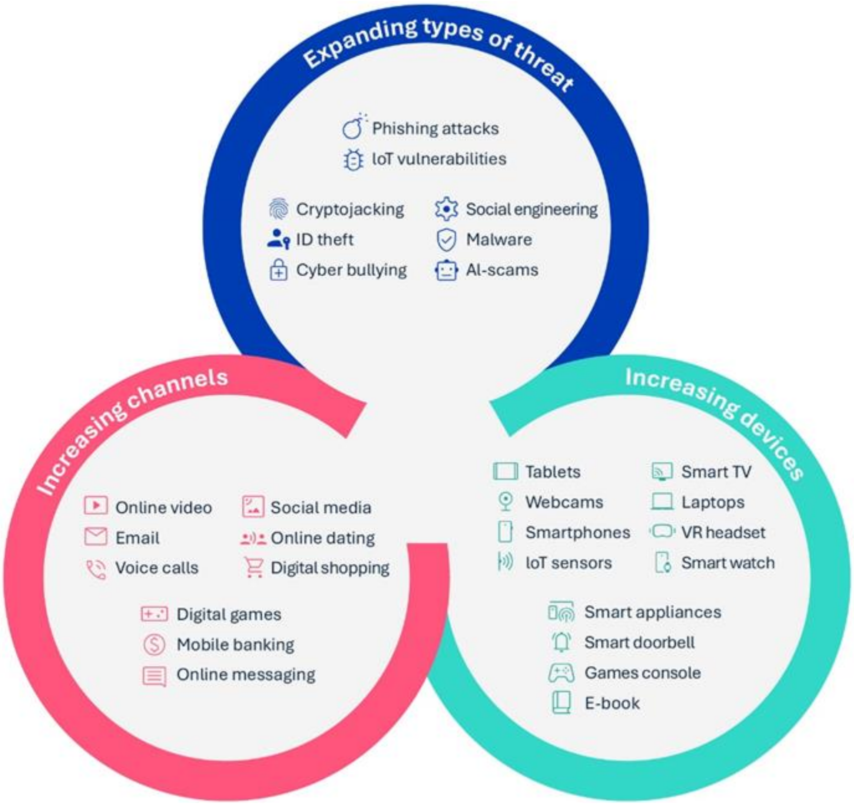
Source: F-Secure US Study, June 2025

Inaction also has important customer relationship costs as it can reduce potential cross-selling and upselling opportunities, while decreasing the customer lifetime value. In terms of brand and reputation, not addressing cybersecurity effectively can damage the company's image and overall attractiveness. Moreover, inaction represents a competitive disadvantage against providers proactively offering integrated security solutions. These forces create a compelling business case for addressing cybersecurity challenges proactively rather than reactively.

Embedded security: How CSPs are bridging the consumer cybersecurity gap through integration

The challenge for both consumers and the cybersecurity companies that protect them, is not merely the increasing number of cybersecurity threats, but also an expansion in the types of threats, and where and how those threats may arise. In addition, AI technology is enabling these threats to become increasingly sophisticated and harder to detect (**see Figure 9**).

Figure 9: The how, what, and where of consumer cyberattacks are changing rapidly



Source: Omdia

CSPs have offered their consumer customers cybersecurity solutions as part of their mobile and broadband offerings for many years. However, Omdia's research shows that many offerings today are based only on third-party, end-point cybersecurity solutions, typically protecting 5 to 10 devices such as smartphones, tablets, and PCs.

The drawback of such offers is twofold:

1. The solutions are limited in terms of the number and types of devices covered. The highest level of protection can only be achieved when all connected devices, including IoT and media devices such as smart TVs are protected.

2. The emphasis for installing and managing the solution normally resides solely on the end customer. Lack of knowledge and understanding on behalf of most consumers mean that the percentage of customers installing and activating the service can therefore be low - often into the single percentage digits. This lack of uptake can then be perceived by the CSPs as a lack of interest, effecting future investment decisions.

Other, more comprehensive, solutions are therefore required to help consumers become fully protected and for CSPs to maximise the cybersecurity monetization potential.

Network plus router-based solutions form the base of a comprehensive cyber service

To help provide a more complete cybersecurity offering, on top of providing end-point protection, it is important that service providers also invest in network and router-based cybersecurity solutions. These solutions provide complementary protection layers that work together. Network security offers essential baseline protection at scale without an app to install. Router security delivers a similar frictionless experience but provides advanced cyber-security features to identify and protect everything connected to the network, including IoT devices. These services allow service providers to reach and protect greater numbers of customers and devices more easily while endpoint security adds advanced threat detection capabilities for mobile phones and laptops that are often on-the-go.

The solutions consist of network-based cybersecurity providing a base-level protection such as DNS cybersecurity, network firewalls, and content filtering, together with a software client installed by the service provider on the router, to then protect all devices connected to that router, including IoT devices.

Network + router + endpoint provides total cyber cover

Cybersecurity protection is then maximized by the addition of end-point security on top of the network and router protection. Endpoint security adds two additional levels:

1. It protects devices when customers are ‘on-the-go’ and hence not connected to the home Wi-Fi network.
2. It provides more advanced security features that can only be attained through security installed directly on the devices, such as the virus removal, scam detection in digital moments, etc.

Although providing the maximum level of protection, this combination of network, plus router, plus endpoint security is not a ‘silver-bullet’, however, when it comes to successful service provider monetization.

Consumers may still not install the endpoint security applications, nor recognize or value the features provided through the network. Work still needs to be done therefore to ensure consumer engagement, which leads to successful monetization.

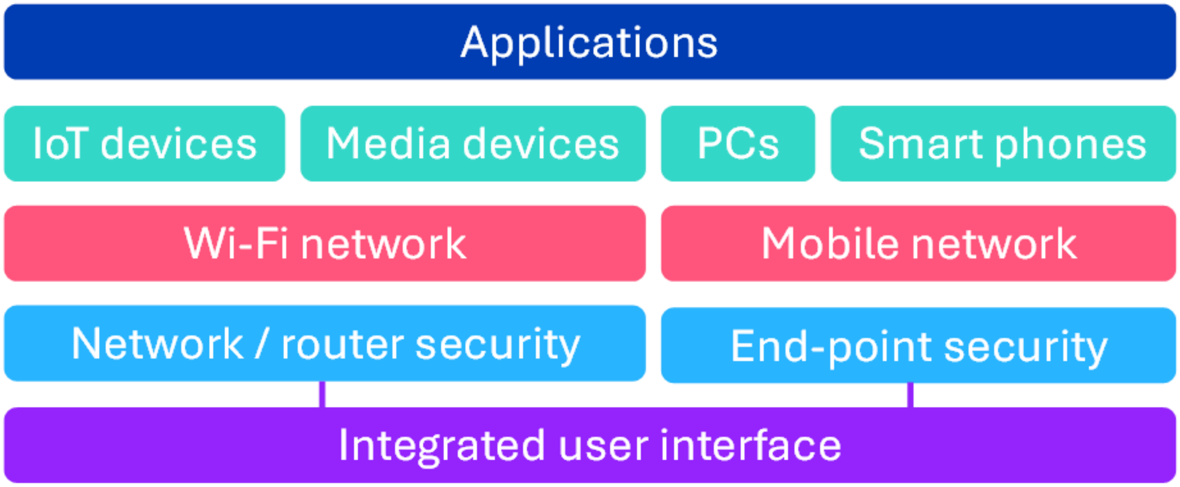
A large part of this comes down to greater consumer communication and education, as well as service promotion. Additionally, by embedding endpoint security capabilities into an existing CSP app with a wide user base, the challenge can be further mitigated.

The need for a single, end-user interface: Why fragmented security solutions are failing today's digital consumers

As discussed, cyber threats are becoming more sophisticated and the challenge for cybersecurity companies and service providers is to try and protect consumers across all applications, all devices, and across all networks. To achieve this level of protection you need multiple contact points (**see Figure 10**), however, in order to enable the user to control and monitor their security across all access points, setting out a common set of rules and parameters, then there must be a single user interface that controls all devices within that household ecosystem.

A simple use case of such an interface would be, for example, to allow the designated head of that household to set a range of controls for different individuals, regardless of what application, device or network they are accessing. Only by providing this single interface point can the solution not only be effective, but also simple enough for the every-day consumer to use. Failings on either of these parameters will only lead to customer frustration and disillusionment, reducing eventual take up.

Figure 10: A single interface to manage security measures across all devices and networks



Source: Omdia

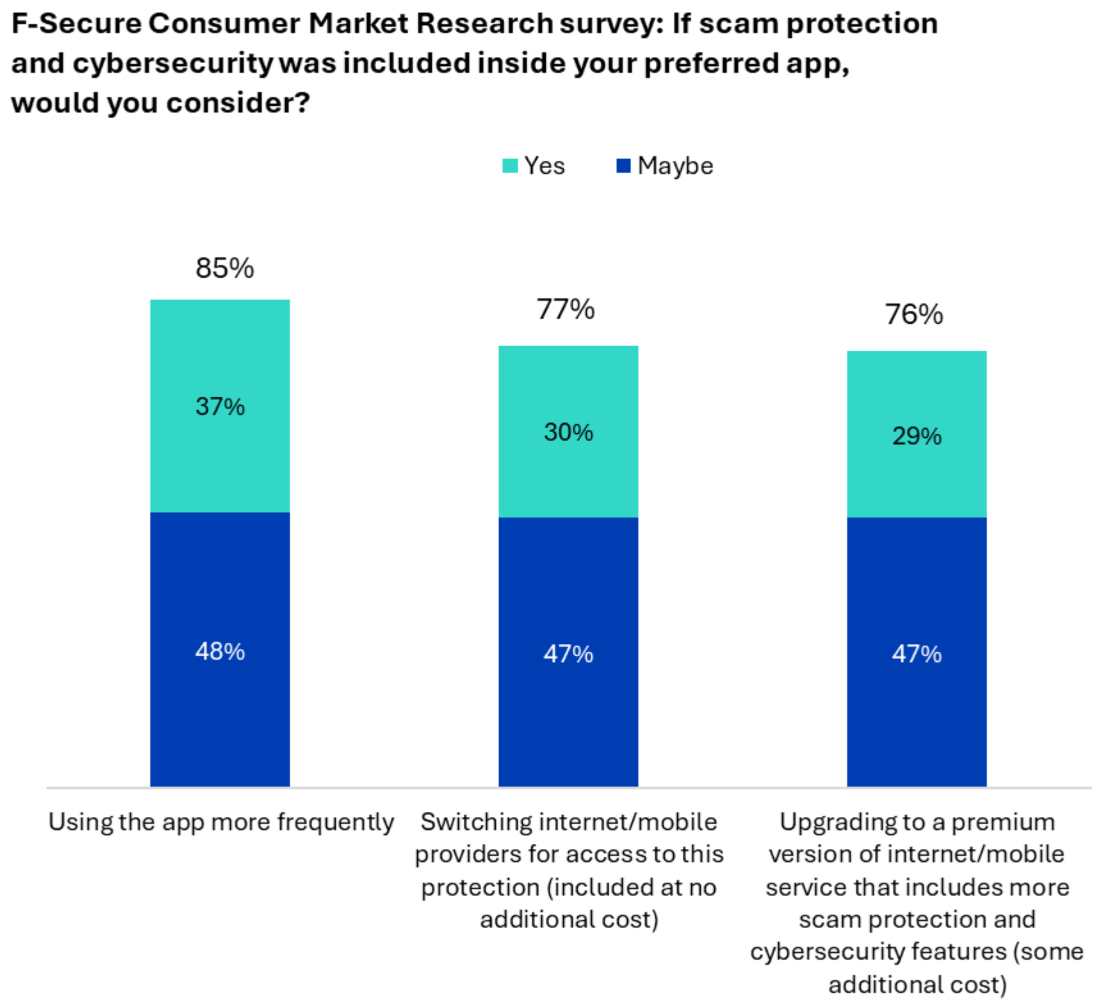
Integrating cybersecurity into the main CSP app is the secret to enhanced engagement

Given that installing end-point security provides the most effective protection for key devices such as smartphones, then logical conclusion would be that CSPs need to continue to offer specialised cybersecurity applications. However, as already discussed, specialised cybersecurity applications often fail to gain good levels of customer penetration and activation, and additionally, CSPs are in general looking to reduce the number of apps they must manage, in many cases down to a single, ‘super-app’.

Integrating cybersecurity features into an existing CSP application that already has a high penetration can therefore lead to greater efficiency and gets end-point cybersecurity onto more devices more quickly. Through greater consumer education and communication, CSPs can then look to help drive greater engagement of the cybersecurity features.

Survey data carried out by F-Secure shows that by embedding cybersecurity within the core CSP applications can not only increase the level of interaction with the cybersecurity features, but also greater engagement with the main CSPs application itself, which in turn increases the value of the CSP’s brand (**Figure 11**).

Figure 11: Integrating cybersecurity into the main CSP application leads to greater engagement

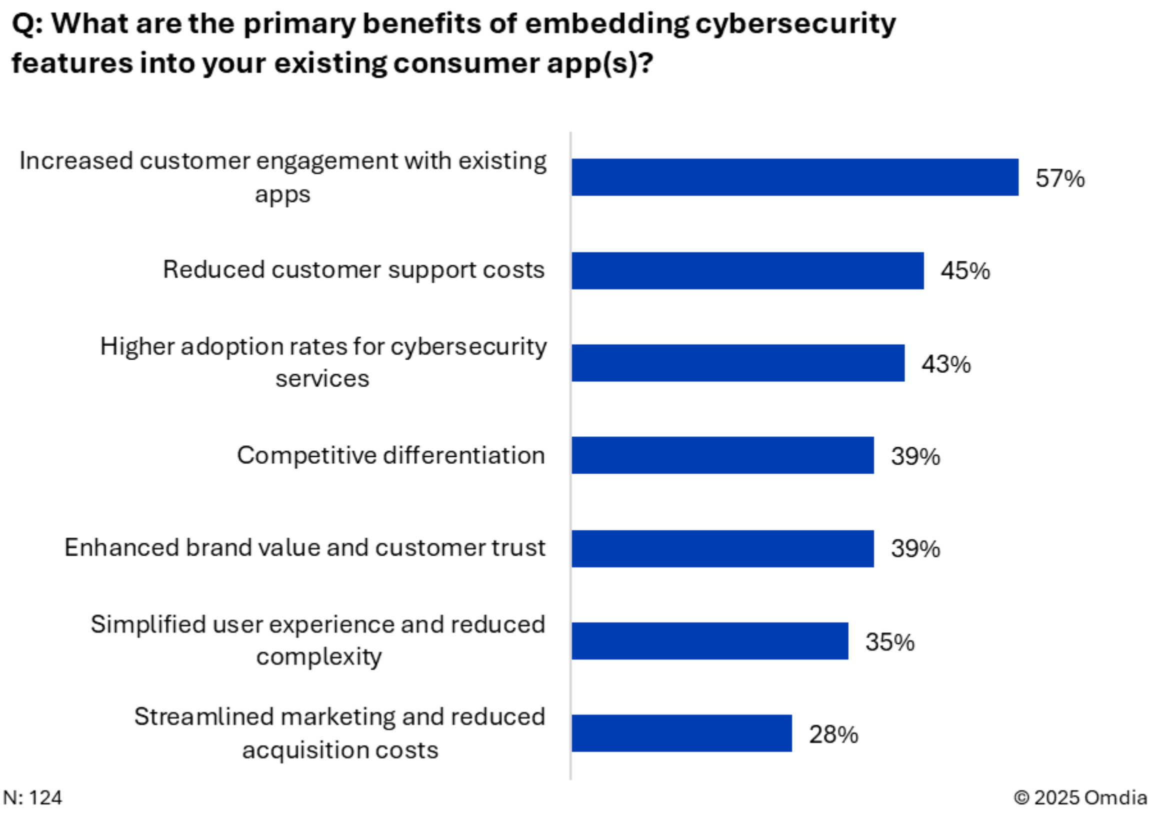


Source: F-Secure Consumer Market Research, January 2025

Embedding security into the core CSP app alone won't drive the engagement and monetization results that CSPs desire. As mentioned, a large part of the success also comes down to how the cybersecurity services are positioned in the mobile and broadband tiering system, as well as effective consumer communication.

Nonetheless, embedding security into the main app certainly has significant advantages, including aiding reduce these two barriers by enabling greater service flexibility and enablement, as well as an additional communications channel. When asked about the primary benefits of embedding cybersecurity features into the main CSP consumer app, 57% of CSP executives surveyed by Omdia agreed that it would help drive engagement of the overall app, with a further 43% stating that it would drive greater engagement with the cybersecurity features. In addition, 39% state that it would enhance their brand value and customer trust (**see Figure 12**).

Figure 12: Embedding cyber features into the CSP app is seen to drive greater engagement and efficiency



Source: Omdia

Not all CSPs so far have made a success out of consumer cybersecurity, but those that have can boast consumer activation of over 50% and direct revenues running into the millions of dollars. With greater investment in more comprehensive cybersecurity solutions, embedding cybersecurity features into existing core apps, and by driving more active consumer engagement, then the cybersecurity opportunity can be fully maximized.

Conclusions

CSPs occupy a privileged position in the consumer cybersecurity ecosystem due to their established network infrastructure, existing customer relationships, and natural trusted role as digital gatekeepers. This positioning creates opportunities that other security providers cannot easily replicate.

In parallel, the rapid evolution of cyber threats, particularly through AI advancement, has created security challenges that consumers struggle to address effectively. Therefore, the evolving threat landscape necessitates proactive CSP participation, especially as CSPs are expected to help customers to navigate the complex challenges that AI introduces.

This research study has also shown that consumer preference has shifted decisively toward simplified, integrated security solutions embedded into existing apps that can protect all devices without requiring technical expertise. CSPs' ability to implement network-level protection and offer end-point security solutions perfectly aligns with this preference, offering protection that works automatically across all digital moments – whether at home or on-the-go.

The convergence of technological capabilities, consumer preferences, and market dynamics has created a clear strategic imperative for CSPs to expand their role in consumer cybersecurity. By developing comprehensive security offerings that leverage their unique advantages, CSPs can simultaneously address consumer needs while creating sustainable new revenue streams. However, they also need to be successful in positioning and marketing these solutions as part of their core offering to consumers. Just offering an integrated complete protection solution with an enhanced user experience is not enough by itself anymore.

As cyber threats continue to proliferate and evolve, those CSPs capable of overcoming the obstacles and challenges listed in this research study will enjoy the success and reap the benefits of the evolving opportunities in the consumer cybersecurity space. As a result, CSPs that successfully execute on this opportunity will strengthen their market position, enhance customer relationships, and establish leadership in the increasingly critical domain of consumer digital protection.

Appendix

Methodology

This research study makes use of data from Omdia’s *Digital Consumer Service Provider Insights Survey 2025*, which was conducted in July 2025, covering 124 service providers across all regions.

Further reading

Digital consumer service provider insights survey - 2025 (July 2025)

Mariana Zamoszczyk, Principal Analyst, Digital Consumer Operator Strategy Services

Michael Philpott, Senior Research Director, Service Provider Consumer & Markets

askananalyst@omdia.com

Omdia
by informa techtarget

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.