OMDIA MARKET RADAR

Publication date:
15 Oct 2024

Author(s):
Michael Philpott, Research Director, Service Provider Consumer

Omdia Market Radar: Total consumer cybersecurity solutions for telcos

OMDIA
Brought to you by Informa Tech

Summary

Catalyst

Telcos are rapidly shifting their broadband marketing focus away from pure speed to broadband quality of experience (QoE). In this aim, the initial focus is on providing a high-quality, highly consistent, and reliable broadband service; however, after that, the focus turns to broadband value-added services (VAS) to further amplify the experience. Cybersecurity is one of the most important VAS. As one executive recently put it, "First we must provide a high-quality broadband experience, then we must ensure a safe one."

Telcos have provided consumer cybersecurity services alongside their broadband and mobile services for many years, but these tended to consist only of end-point security solutions—leaving some devices unprotected altogether and relying on the consumer to manage the security of the others. To ensure full protection, consumers need a solution that protects all their connected devices across all networks and all of the time—in this report, we refer to this as "Total consumer cybersecurity." Providing 100% protection is not easy, but this report explores the offerings from some of the leading vendors in this space who are looking to help telcos provide the most comprehensive solution possible.

Key messages

- To provide total consumer cybersecurity, it is necessary to provide three security layers: network, router, and end-point protection. Network security provides a base level of security, including DNS cybersecurity. Router-based protection then protects all devices in the home that are connected to the home Wi-Fi network. This includes IoT devices that often have no (or lower) built-in protection. The end-point security then protects devices, such as smartphones, tablets, and laptops, when they are connected to the mobile and third-party Wi-Fi networks.
- Most consumers look to their telco for protection. Technically, it is not the broadband service provider's responsibility to ensure their broadband customers are protected when online. However, over 50% of consumers in Omdia's consumer surveys state that the telco is their preferred supplier for cybersecurity, and therefore, it is an obvious VAS for them to provide. Additionally, in Omdia's view, providing a good level of cybersecurity service can help differentiate the broadband offering, help increase service stickiness, and help promote the broadband service provider as more of a "digital lifestyle service provider."
- Total cybersecurity is something many consumers are willing to pay for. Indeed, based again on Omdia's surveys, alongside broadband speed guarantees, it is the most likely broadband VAS that they would be willing to pay for. This is increasingly the case for consumers living with children, or those with installed IoT devices.
- It's not yet possible to protect all consumers all the time. Even with a combination of router and end-point protection, it is not possible for telcos to always protect their customers—telcos can't force the consumer to install and enable the proper security. However, telcos can help by flagging up to consumers when a certain device is not adequately protected, and by providing dashboards and management tools to help them manage this. It is critical that vendors provide the necessary tools to help telco clients enable this type of capability.

- Cyberthreats are becoming more complex, especially around online fraud. Online fraud is now the biggest form of cybercrime, and using new technology such as AI, attacks are becoming harder to detect, but also cheaper and easier for criminals to use. Helping consumers stay safe from these new threats will become increasingly challenging for telcos and their security vendors, but at the same time, it signifies a significant opportunity.
- Solutions must be able to adapt to external protection initiatives. Consumer security and privacy is, of course, becoming a bigger topic on the international stage. New regulations and technology standards designed to protect the consumer are, therefore, being released. However, sometimes these new initiatives can hamper a telco solution, for example, by hiding a device or information on that device from the telco's management or cybersecurity solution, thus disabling tools such as parental controls.
- Education must be a key part of the telco solution. Just providing a cybersecurity solution is not enough. Most consumers don't fully understand the threats posed to them, even when they hear about it in the media. Telcos must not scare their customers, but there is certainly a role for them to play in terms of supporting and educating them, and telcos increasingly have the right channel to do so through their stores, websites, and mobile and home broadband applications.

Recommendations for service providers

- Cybersecurity is a key VAS that all service providers should explore offering to their broadband subscribers. Without adequate protection, consumers are left vulnerable, and broadband service providers are in a key position to become trusted partners in this space.
- Service providers must look to provide total consumer cyber protection. Offering only end-point security means the service provider has less control over the end-user experience, limiting the monetization opportunities that cybersecurity can offer.
- Total cyber protection is something that consumers are willing to pay for, and this is likely to only increase as the number of connected devices in our homes continues to grow. Ensure, therefore, that pricing strategies maximize the monetization potential.
- A total cybersecurity solution can be modularized to create a number of different tariff and monetization strategies for the telco. Telcos must plan their strategy carefully to maximize the opportunity across all monetization levers, including customer experience, churn reduction, and ARPU uplift.
- Consumer education is a key element for success. Helping consumers identify devices that need greater protection and helping identify new potential threats, some of which will become increasingly sophisticated, will be both necessary and of high value to the consumer—assuming the messaging is done properly. Additionally, a lot of cybersecurity protection is done in the background and is, therefore, invisible to the everyday consumer. Reminding them now and again of the great work the telco cybersecurity system is doing in the background to keep them safe is not a bad thing.
- Ensure any cybersecurity strategy is future-proof. Digital threats, especially around fraud, are only set to increase in both number and sophistication. It is critical, therefore, that your vendor partners have a roadmap that can evolve to meet these new threats.

Recommendations for vendors

- **Ensure a futureproof roadmap.** Cybersecurity threats are quickly evolving. It is critical, therefore, that product roadmaps meet these new threats as well as enable telco partners to offer new types of consumer cybersecurity services.
- **Help telcos manage new regulations.** New regulations and standards are being passed to enable consumer privacy in this new digital world. If telcos are to continue to provide high-quality service across their portfolio—from connectivity to cybersecurity and parental controls to smart homes—then it is important that vendor solutions adapt to these new regulations while maintaining the privacy they were brought in to protect.
- **Provide an integrated end-user experience.** Total consumer protection means a layered cybersecurity solution that includes network, router, and end-point security. However, it is critical that the solution provides an integrated, single-user interface to maximize the end-user customer experience.
- **Provide the right tools to help with service provider messaging.** Communication will be a key part of the telcos' role in consumer cybersecurity. It is important that their vendors provide the right tools, both back and front-facing, to enable the telcos to provide this communication.
- **Help the telcos win success.** Telcos are likely to increasingly look to their cybersecurity partners to help them develop a successful go-to-market strategy. Vendors that have a complete end-to-end professional service solution are likely to have real differentiation.

Telco cybersecurity market landscape

The traditional telco cybersecurity market

Telcos have offered traditional antivirus software and parental control features for many years as a "value-add" to their broadband and mobile services. In terms of form factors, such services typically consist of a downloadable cybersecurity app that clients install on capable devices such as mobile handsets, tablet PCs, and PCs. It is standard for there to be a set maximum number of devices that are covered as part of the service, normally between 5 and 10.

This type of service is typically offered for free as part of the broader broadband/mobile bundle, or free for a certain amount of time (say for three months) and then charged at an additional fee, typically around $5–10 p/m. Another popular model is to offer a basic level of cover for free, and then premium upgrade options (perhaps to add more devices for example) for a fee.

A typical example of a traditional, client-based cybersecurity offering is shown in **Table 1**.

Table 1: Telstra's device security offering

Feature	Details
Number of devices covered	10
Cybersecurity protection	Blocks malicious email and SMS Antivirus protection Identity monitoring Secure VPN Password management
Pricing model	Free for the first three months, then AUD10 p/m

Source: Omdia

End-point only solutions have limitations

However, these more traditional, standalone end-point consumer cybersecurity applications can be limited both in terms of the range of security features they offer, and/or the number and range of connected devices they cover. Additionally, based only on an end-point software solution, the emphasis resides solely on the end customer to install the software (and on all required devices), set up the software adequately, and then manage it. This significantly reduces the telco's control of which devices end up being covered, as well as the overall customer experience received.

Lack of management potentially leaves customers vulnerable to cybersecurity attacks as:

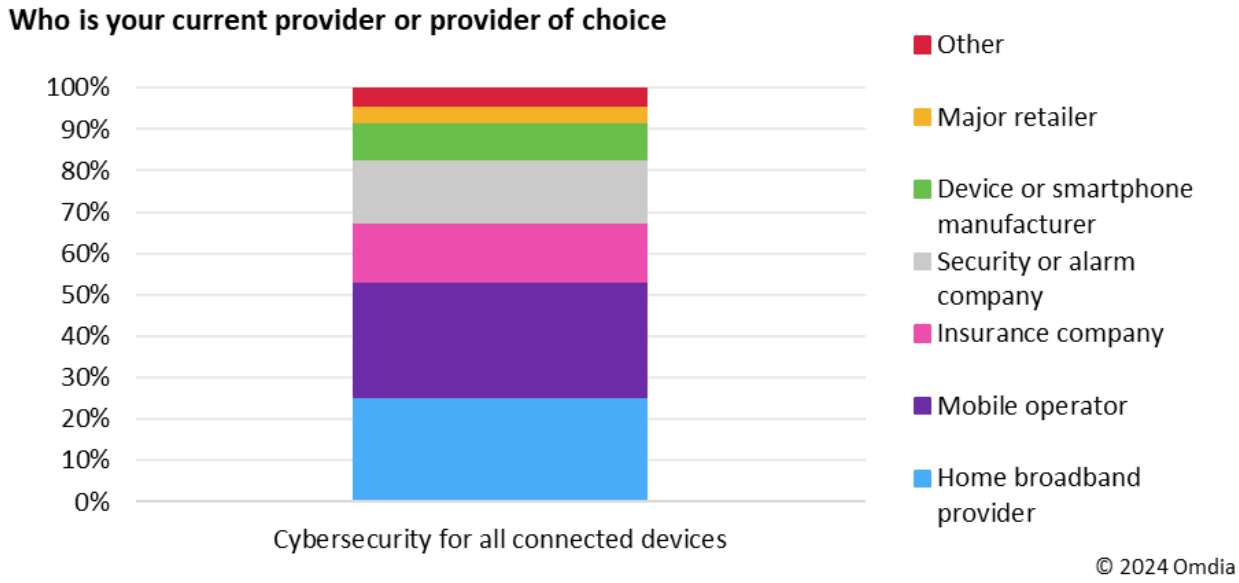
- Consumers may not install the software on all their mobile devices, therefore potentially leaving them exposed to attack.
- Even if installed, the cybersecurity software may not be set up or managed properly.
- Many connected devices, such as security cameras, smart door locks, etc., may remain unprotected altogether.

Inadequate protection can also harm the telco service provider

There is no legislative requirement for service providers to supply their broadband customers with cybersecurity protection. However, lack of adequate protection could come back to haunt service providers. As digital threats increase, leading to a rise in consumers' fear of being hacked, it could lead to a lack of consumer confidence that, in turn, could lead to customers becoming increasingly wary of using more connected devices and applications (smart home devices and apps, for example). This has a potential knock-on impact on future service provider business opportunities, especially those with ambitions of becoming "digital lifestyle service providers."

Additionally, as shown in **Figure 1**, based on Omdia's 2024 Digital Consumer Insights survey, nearly 50% of consumers see their broadband or mobile operator as their preferred channel for whole-home cybersecurity. Lack of adequate cybersecurity may, therefore, impact NPS scores if they are the ones who are blamed (rightly or wrongly) for not keeping customers safe.

Figure 1: Telcos' enjoy a great reputation in the cybersecurity service area



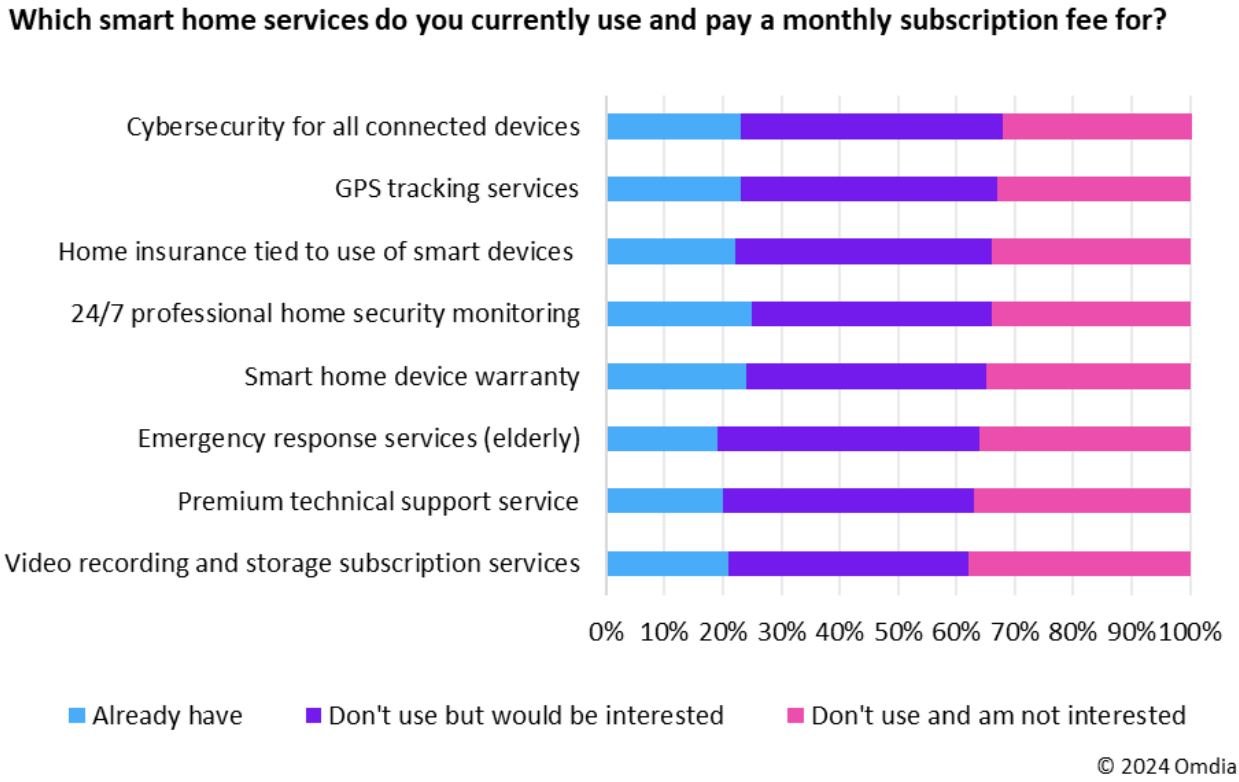
Source: Omdia

Moving to network/router-based platforms

To ensure greater control and provide a more complete home cybersecurity offering, some telcos have, therefore, invested in network/router-based cybersecurity solutions. These solutions consist of a software client that is installed on the router and has the advantage of then protecting all devices connected to that router—including IoT devices—without the need for the user to install any specific device software. As software is rolled out and controlled by the telco, it provides them with greater control of the level and the management of consumer cybersecurity protection—at least for all devices connected to the home broadband gateway.

This more "whole-home" cybersecurity solution is seen to be a more premium cybersecurity solution by telcos and, therefore, something they are likely to be able to monetize. Based on Omdia's Consumer Service Provider's survey of just under 200 service provider executives, 40% of respondents stated that a "whole home" cybersecurity solution would provide them with the biggest VAS opportunity for increasing broadband ARPU. This corresponds well with Omdia's 2024 Digital Consumer Insights survey of over 20,000 consumers, which concluded that 23% of respondents already use such a cybersecurity offering, with a further 45% stating an interest—the most promising of all smart home services included in the survey (**Figure 2**).

Figure 2: Whole home cybersecurity shows the most promise of all smart home services

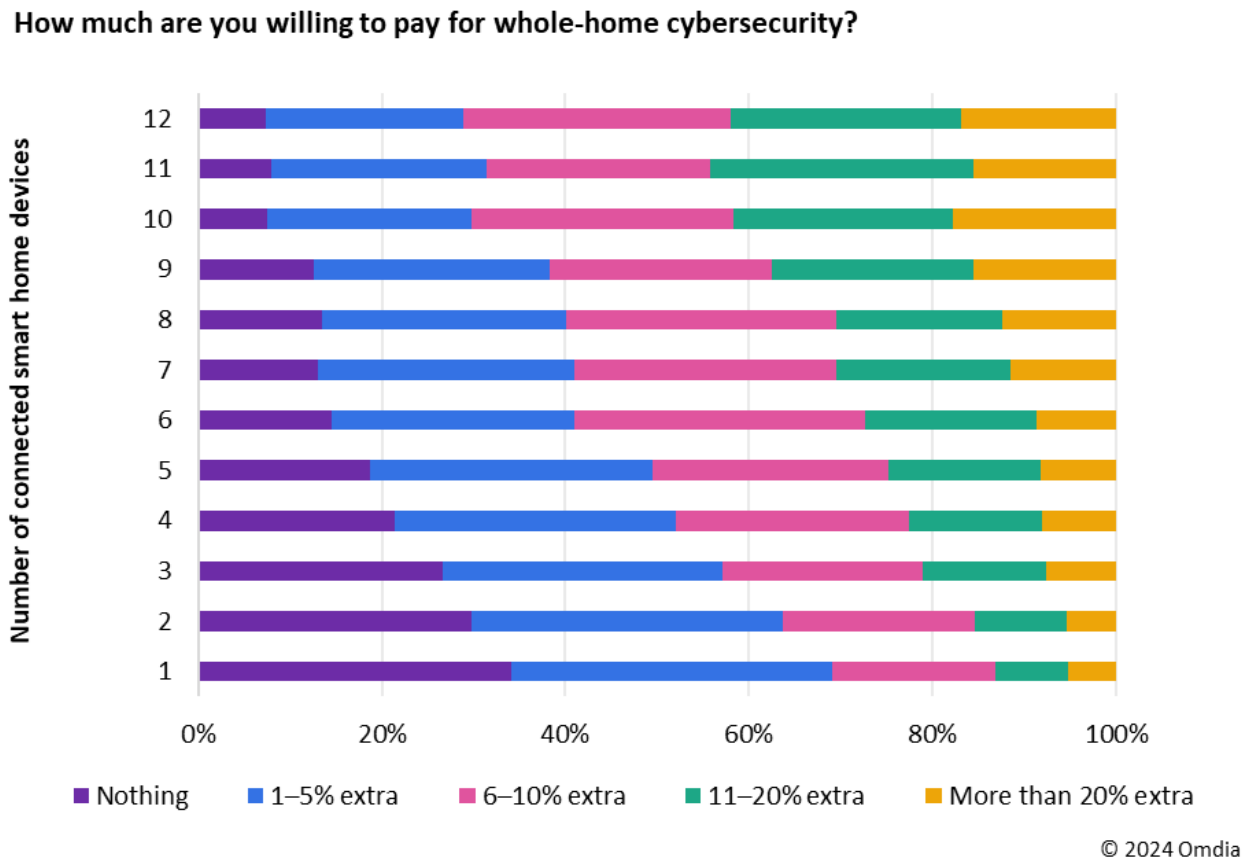


Source: Omdia

Based on Omdia's consumer survey, there is also a clear willingness to pay for high-quality, whole-home cybersecurity services. In terms of a broadband VAS, whole-home cybersecurity was the second most popular service that respondents stated that they would be willing to pay extra for, with 77% of respondents stating that they would be willing to pay. This percentage increased for respondents currently living with children (82%), and technology enthusiasts (80%).

Additionally, the percentage of respondents willing to pay increased with the number of connected smart devices they own, as well as broadly the amount they are willing to pay (**Figure 3**).

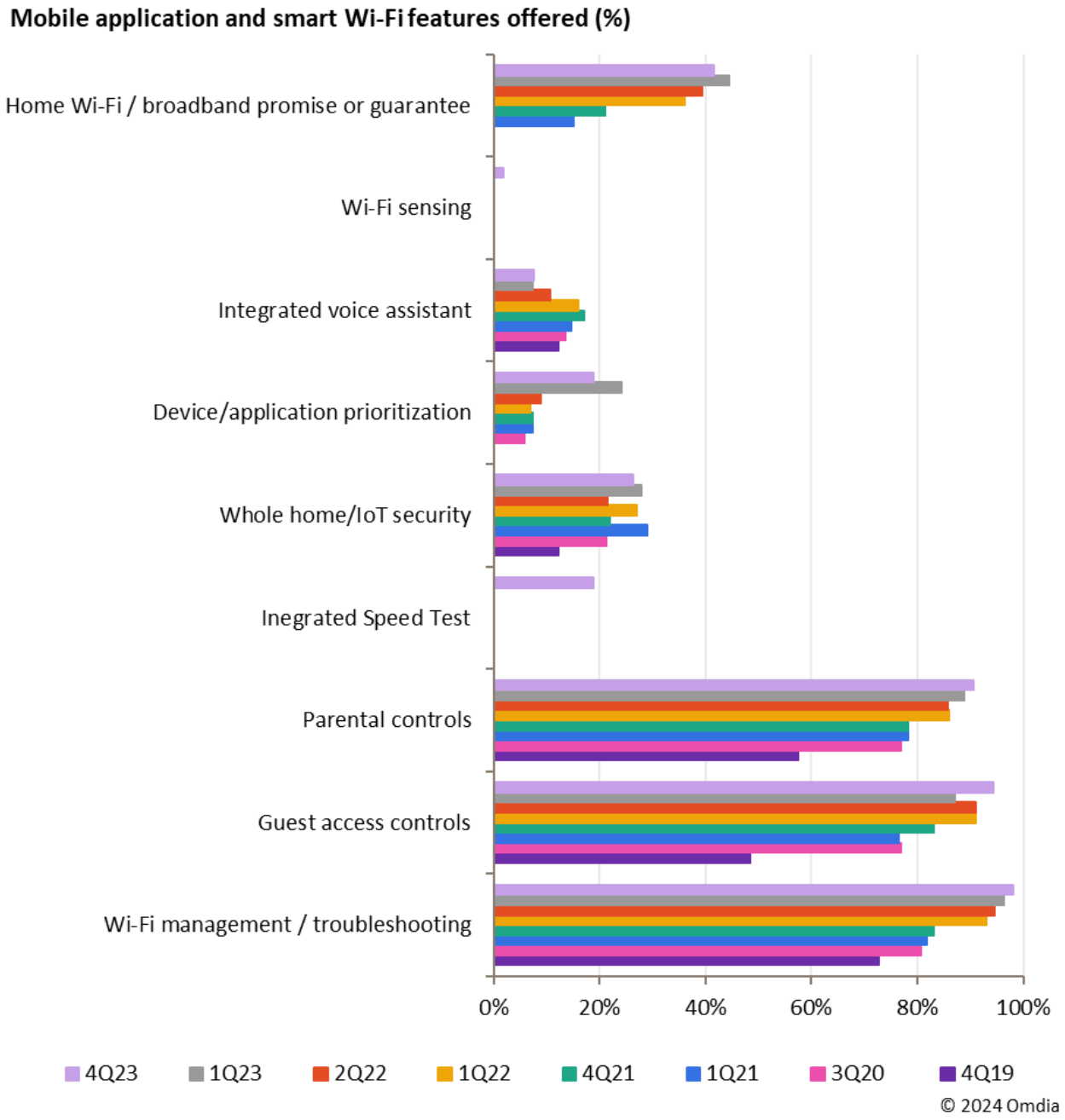
Figure 3: The greater the number of connected devices, the greater the willingness to pay for cybersecurity



Source: Omdia

However, as illustrated in **Figure 4**, only approximately 30% of telcos in Omdia's Smart Wi-Fi Service Provider Tracker currently offer such a solution. In Omdia's view, it is vital that all broadband service providers explore investing in such solutions, as they can help drive brand differentiation, reduce customer churn, and open new revenue opportunities.

Figure 4: The penetration of whole-home cybersecurity is gradually increasing



Source: Omdia

Total cyber cover is the holy grail

Of course, moving to a 100% router-based solution also falls short of a complete consumer cyber protection service. With a router-only solution, portable devices, such as smartphones, tablets, and laptops, will not be protected once they are not connected to that Wi-Fi network. A combination of router plus endpoint protection is therefore required to provide total cover. This still leaves the issue of how service providers properly manage the software installation on those end-point devices, but many of the vendors highlighted in this report look to provide a solution for that issue.

Total cyber cover leads to greater monetization potential

Offering total consumer cybersecurity enables the telco to explore a greater number of monetization options. As discussed earlier in this report, services that are limited to end-point-only solutions are really limited to either being bundled in for free or charged at a premium. However, as total consumer cybersecurity solutions are more modular in nature (network security, router security, and end-point security), then the different layers can be combined into the broadband Tiering system in multiple different ways. For example, network-only cybersecurity could be offered to all broadband customers as a base level of cyber protection, with router protection offered within more premium tiers and then end-point security offered as a premium add-on. This flexibility enables the telco to maximize the different monetization levers of customer experience, churn reduction, and ARPU growth, depending on their market situation and priorities.

Online threats are quickly evolving

Online fraud has quickly become the biggest threat

An increasing proportion of our daily lives is spent accessing digital applications, communications services, and content. Although such applications bring many advantages, the speed of technological development can also make the world a more confusing and dangerous place for the every-day consumer.

Online fraud is a rapidly growing issue that has now become the most common form of cybercrime. Data from CUJO AI, for example, indicates that phishing attacks are now affecting at least 56% of internet users, and, according to Interpol, online scammers stole over $1trn in financial fraud from its victims in 2023. The technology used to commit such crimes is also becoming increasingly sophisticated, and yet at the same time, less expensive and easier for criminals to access. The use of AI technology, specifically, enables scam attacks to become so sophisticated that even the most security-savvy individuals may fall victim. Increased public awareness and protection are therefore vital.

Yet, according to a survey by Bitdefender, 45% of respondents don't use any form of mobile security solution, even though such devices are becoming a central store of personal data and financial details. Another survey by F-Secure found that 54% of users don't know if their personal devices are secure. Helping keep their customers safe as they navigate this online world is, therefore, a significant and growing opportunity for broadband service providers of all types.

Advancements in connected devices also pose issues

The use of AI technology in personal devices, such as PCs, could potentially introduce new vulnerabilities. According to Trend Micro, AI applications that run locally mean that the application's AI models, and other critical files, are located directly on that device. This valuable data can then become a target for hackers to perform malicious tasks, or steal sensitive, personal data that can be used to further impact the user.

In addition, the sheer increase in connected IoT devices in the home has become an increasing focus for attack. With sometimes little in-built protection and an increasing number of IoT vulnerabilities, malicious actors can gain remote access to devices such as security cameras, home heating systems, and smart door locks. This alarming potential for cyberattacks within the sanctuary of one's home underscores the urgent need for robust security measures. Such is the potential threat that some governments have implemented manufacturing laws to ensure that smart home devices meet basic levels of cybersecurity protection. The UK, for example, introduced its "Product Security and Telecommunications Infrastructure Act (or PSTI Act)" law in April 2024.

Regardless of regulations, however, it is important that telcos work with their cybersecurity vendor partners to ensure that consumers continue to be adequately protected as technology innovations accelerate.

Telco solutions must adapt to new privacy-enhancing technology

Not all new regulations and standards help telcos in this fight though. There are some new privacy industry standards and initiatives that have been developed to advance the protection of consumers, but in turn, they can potentially limit service provider's ability to provide new services and features in the home. Encrypted Client Hello (ECH) and MAC randomization, for example, help protect the privacy of consumers, especially when connected to untrusted networks, but limit the service providers' visibility of the devices connected to the home Wi-Fi network.

Not being able to adequately identify certain devices on the home network can impact the service providers' ambitions to manage the quality of the home network and the applications running over them, as well as provide cloud-based cybersecurity and parental control services. Network-based security solutions must, therefore, evolve to work with these approaches to continue providing first-class protection while also, of course, preserving end-user privacy.

Telcos have a big role to play in consumer education

Not everything can be solved by technology. As discussed, cloud-based cybersecurity enables the telco to integrate security measures directly into their services without the consumer having do anything. However, it is not possible to guarantee coverage for every eventuality, especially when it comes to threats such as fraud. The consumer also has to take some responsibility, and for this, there needs to be more education. It is commonly recognized throughout the industry that most consumers have only a base level of understanding when it comes to cybersecurity protection, and they often neglect to properly secure devices, even ones that hold a significant amount of personal and sensitive data, such as the modern personal smartphone. Additionally, threats are getting more complex and more difficult, even for those more tech-savvy, to detect. As a trusted provider of broadband and mobile services, telcos are in a prime position to at least play a role in furthering consumer education.

This education can and should come in the form of awareness campaigns, but it also can be done "in-service" through the apps that telcos provide. Such apps could be used to provide messaging around:

- Updates around the latest security threats, new internet scams to monitor for, and any actions that should be taken.
- Notifications on new security features or practices being implemented.
- Alerts to notify customers if accounts or devices are potentially compromised or inadequately protected.

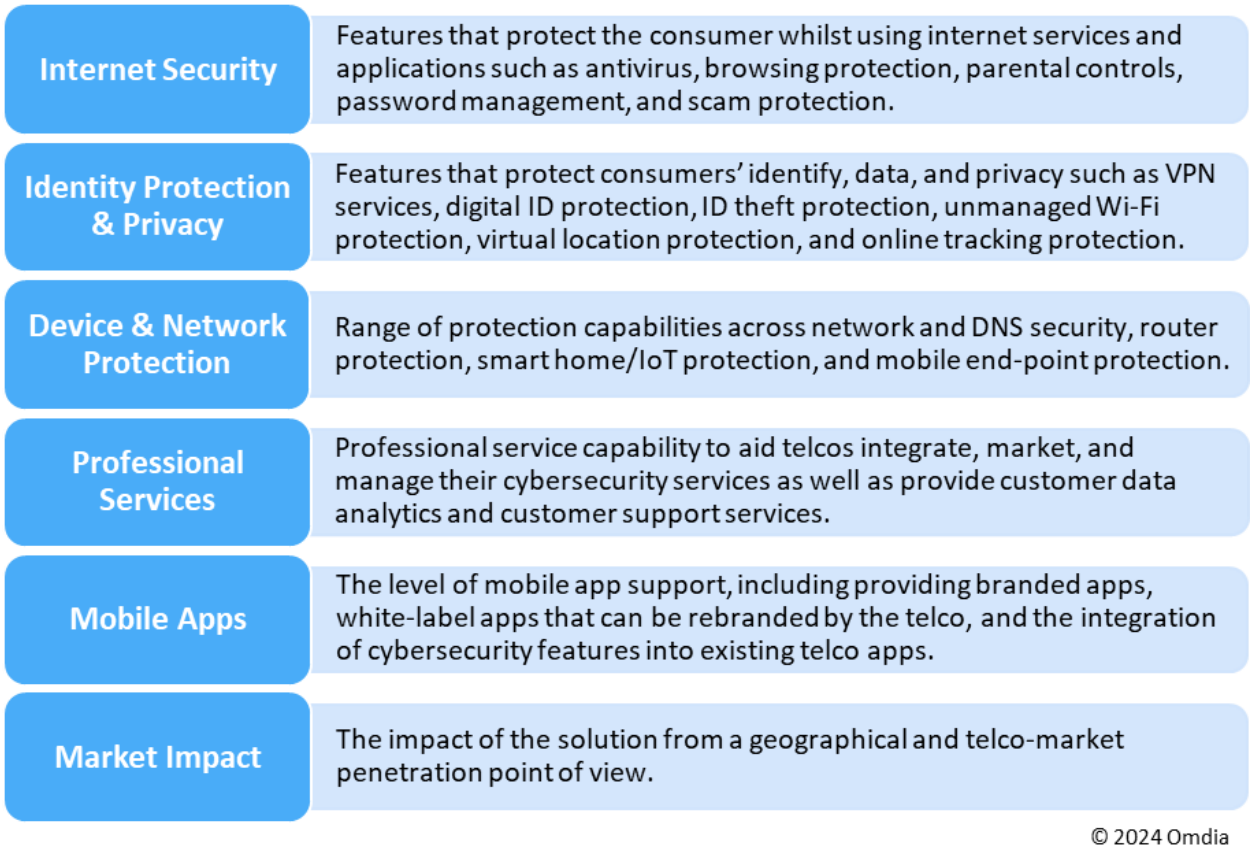
There is, of course, an important balance that telcos need to be careful to meet here. The objective is not to overtly scare the consumer but to support and educate. Therefore, getting the messaging right will be important, but if done properly the telco could become seen as an important and trusted partner in keeping consumers safe and increasing their service differentiation and brand strength in doing so.

Key capabilities and vendor landscape

To provide total consumer cybersecurity protection, telcos need to work with a vendor, or vendors, that enable them to cover all types of cybersecurity threats across all types of connected devices and across all environments. For some telcos, this will mean working with a single vendor that provides a complete off-the-shelf solution, but there are also others, especially larger Tier 1 players, that prefer a “best of breed” approach and are happy to piece together their own solution by working with a select group of vendors. For larger vendors, this will therefore require a complete solution, but one that is also modular in nature, and for smaller challenger companies, there is an opportunity to perhaps not provide all elements of the solution but to specialize as long as there is a willingness to then partner.

In developing this research, Omdia assessed different vendor solutions and capabilities across a range of six different criteria, as shown in **Figure 5**.

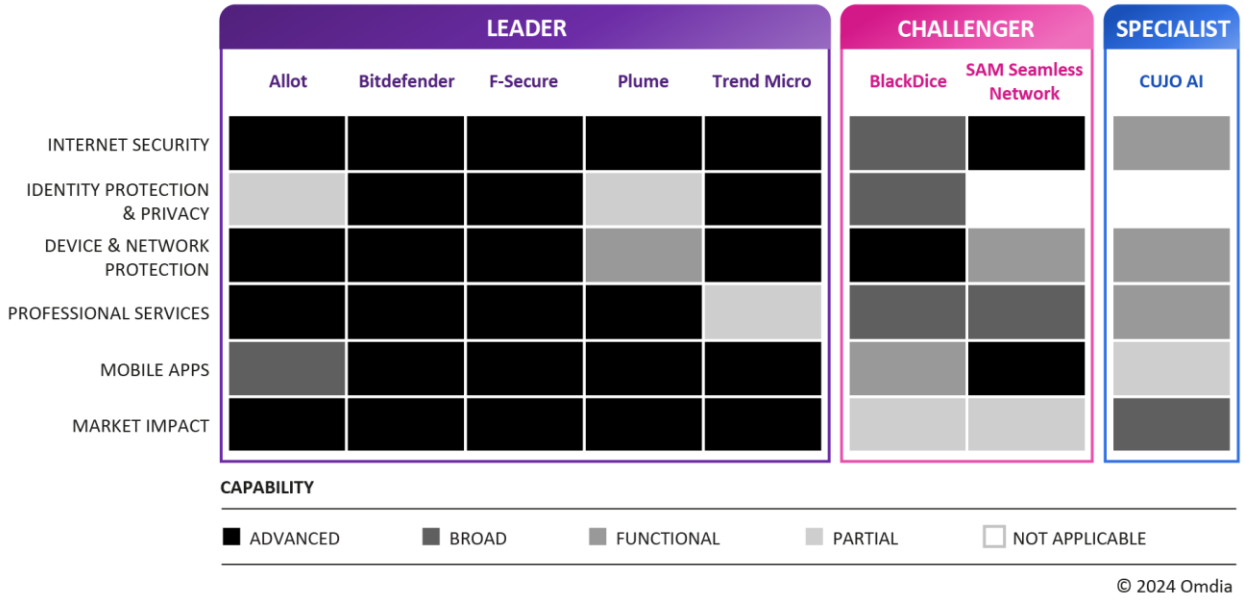
Figure 5: cybersecurity vendor market radar capabilities



Source: Omdia

All of the vendors covered in this report offer a robust set of features and a balanced portfolio of capabilities that can be customized to the requirements of the telco sector, and **Figure 6** illustrates the capabilities delivered by the competing vendor offerings that Omdia analyzed for this research. Additionally, the vendors we explored in this research offer solutions across all major geographies and have traction with and a strategy to target telco organizations.

Figure 6: Omdia heatmap for vendor consumer cybersecurity solutions



Source: Omdia

The Omdia Heatmap for cybersecurity solutions is colored as follows:

- **Advanced capability:** The vendor demonstrates a full set of expected features/support in this area.
- **Broad capability:** The vendor offers most of the expected features/support in this area.
- **Functional capability:** The vendor offers some of the features/support in this area.
- **Partial capability:** The vendor provides only limited features/support in this area.

The categorization of each vendor is as follows:

- **Market leader:** Vendor with significant market impact in terms of geographical coverage, total number of end customers protected, and number of telco partners.
- **Specialist:** Vendor with smaller geographical reach and overall market presence but recognized as a specialist and already working with [ten plus] Tier 1 telco customers.
- **Market challenger:** Vendors that are newer to the market but have gained good market presence are already working with some Tier 1 telcos.

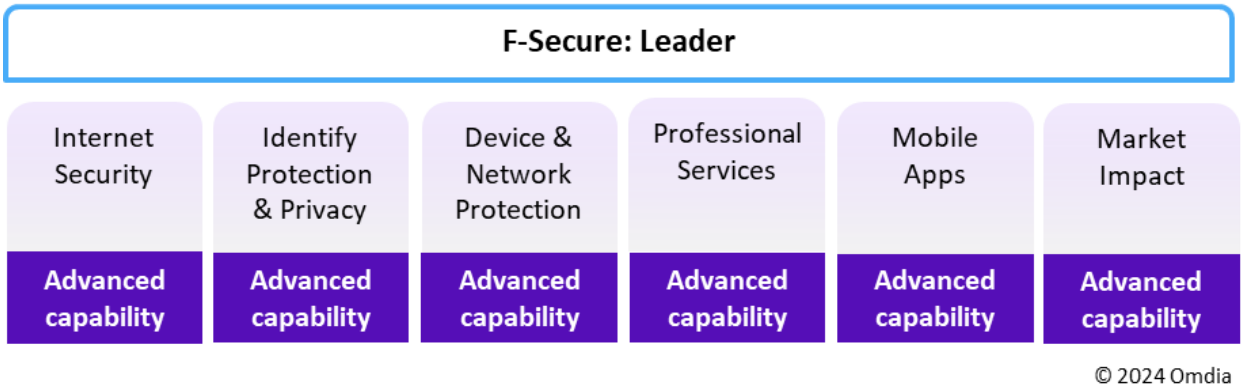
F-Secure

Omdia view

F-Secure is a leading cybersecurity company with over 200 clients in more than 100 countries, the majority of which are telco service providers. While F-Secure's focus is on selling through the partner channel, it also has a direct-to-consumer cybersecurity business. F-Secure is 100% focused on cybersecurity and provides a comprehensive solution encompassing router-based protection for the home, endpoint protection for devices on the move, and network security.

With a flexible, modular solution, F-Secure can tailor its products to each telco client's requirements. It then provides a service management platform—Security Business Platform—that provides insights and business KPIs to be used in marketing functions and customer support, as well as helping telcos in driving greater customer cybersecurity engagement with local dedicated account & partner success teams.

Figure 7: F-Secure's cybersecurity portfolio overview



Source: Omdia

Background and market impact

F-Secure is a leading vendor in the cybersecurity industry with over 30 years of experience. Headquartered in Helsinki, Finland, the company was founded by Petri Allas and Risto Siilasmaa in 1988 and currently employs more than 500 people with offices in Europe, North America, and Asia & Oceania. In 2022, F-Secure separated from the WithSecure group and is now 100% focused on the consumer market. In April 2023, F-Secure also announced the acquisition of Lookout consumer security business, which helped the company expand and strengthen its business in the US and Tier 1 telco clients.

To date, it has over 200 clients in more than 100 countries, the majority of which are telco service providers, but also include retailers, banks, and insurance companies. The company protects over 30 million people, and through its client partners, it makes consumer cybersecurity available to hundreds of millions of fixed and mobile network subscribers. As well as selling through partners, F-Secure has a direct-to-consumer business.

In terms of future expansion, the focus on its partner business will continue, and the company will look to drive new growth through:

- The accelerated growth of its F-Secure Total product, increasing revenue through its client partners as well as its direct B2C ARPU.
- Developing its current offerings and new products around growth areas such as scam protection.
- Expansion into new channels and partnerships.

Portfolio and key features

F-Secure's portfolio consists of five protection areas:

- **Internet Security:** Internet security service including antivirus/malware protection, parental controls, browsing, ransomware protection, phishing protection, system & privacy advisor, and banking protection.

- **Scam Protection:** AI-enabled message protection, shopping protection, social media protection, and Wi-Fi protection.
- **ID Protection:** Protects end-user passwords and online identity through 24/7 online identity monitoring (tailored to different types of personal information), real-time alerts, password generation, and identity theft prevention and personal assistance.
- **VPN:** Online privacy via an unlimited VPN service.
- **Connected home security:** Device detection, browsing & phishing protection, parental controls, ML anomaly detection, and management APIs/SDKs.

All of the security capabilities are available for partners as a fully modular co-branded app or embedded into the partner's own app via a portfolio of SDK, API, and browser extension capabilities. In addition, for F-Secure's co-branded Total app, it is possible to sell Total as a complete protection offering, or as a flexible up-sell solution. For example, telcos could initially offer internet security as standard and then offer ID Protection and VPN as additional premium services.

Total protection capability

F-Secure acknowledges that it is impossible to promise 100% protection all of the time. However, it believes that a comprehensive solution can be provided through a three-layered approach:

- Endpoint protection with internet security, scam protection, Identity Protection & Privacy, etc.
- Connected home/IoT security via a router-based security solution protecting all connected devices in the household
- A base level of protection when connected to telco mobile and fixed network through network-based security.

In addition, F-Secure's portfolio offers detection and response capabilities, such as breach detection or anomaly detection, complemented by its cyber help service.

Use of AI

F-Secure has spent the last two decades using ML and AI technology to enrich its cybersecurity offering. Cybersecurity, in general, is very data-sensitive, and massive amounts of data samples need to be analyzed to identify malicious content. Below are some key ways in which AI is utilized at F-Secure:

- **Malware Detection and Prevention:** AI can analyze files and code to identify malware signatures and behaviors. This helps real-time detection and blocking of malicious software.
- **Behavioral Analysis:** AI can establish a baseline of normal behavior for users, systems, and networks. It can then detect deviations from this baseline, helping to identify potential insider threats, compromised accounts, or abnormal activities.
- **Threat Detection and Analysis:** AI-powered systems can analyze massive amounts of data to identify patterns and anomalies that might indicate a cyberattack. ML algorithms can learn from historical data and recognize new attack vectors, even those previously unseen.
- **Anomaly Detection:** AI algorithms can identify unusual patterns or behaviors that might signify a breach or unauthorized access. This includes detecting abnormal network traffic, unusual login times, and unexpected file access.

- **Scam Detection:** AI-powered systems can analyze emails and messages to identify phishing attempts. They can do this by spotting patterns in content, sender behavior, and attachments that indicate malicious intent.
- **Predictive Analytics:** AI can predict potential security breaches by analyzing historical data and identifying patterns that might lead to an attack. This allows organizations to proactively strengthen their defenses.

As a security company, F-Secure claims that assessing risks and privacy impacts is at the heart of everything it develops. It has robust processes and tools to ensure that all tools, systems, and software it develops comply with industry standards for security and privacy, as well as F-Secure's own code of conduct. These same processes are used to analyze AI tools.

In addition, its cybersecurity and legal teams collaborate to ensure that the use of AI is consistent with applicable regulations (including national and EU law), frameworks, and best practices on AI development.

Unique selling point

F-Secure believes its value proposition consists of two levels:

- Becoming the trusted companion online for consumers and delivering security business as-a-service for partners serving their end customers. For partners, this means F-Secure does not only offer products but also helps its partners create proven business outcomes through comprehensive security solutions. F-Secure offers flexible solutions with a holistic and modular consumer cybersecurity portfolio, from ready-made to tailor-made, matching partner's needs as the right fit for their strategy.
- Providing partners with in-depth business data and metrics through its Security Business Platform. This platform consists of a single partner portal offering insights via data dashboards on business KPIs and threats, marketing best practices, and customer support, as well as customer engagement services to help drive uptake and lifecycle messaging to increase usage.

Appendix

Methodology

This report is based on in-depth vendor interviews, supplemented by Omdia's market analysis and 2024's *Digital Consumer Insights* survey.

Further reading

2024 Digital Consumer Insights: Digital Consumer Services (September 2024)

Service Provider Smart Wi–Fi Tracker and Benchmark – 1Q24 (April 2024)

Smart Home Broadband Service Provider Benchmark – 2023 (October 2023)

Author

Michael Philpott, Research Director, Service Provider, Consumer

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

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 you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com