

5 Essential Cybersecurity Trends Telcos Can't Ignore in 2025



Trusted. Always.

Contents

EXECUTIVE SUMMARY3

INTRODUCTION3

CYBERSECURITY TRENDS3

 USERS EXPECT CYBERSECURITY FROM THEIR PROVIDERS3

 CYBERSECURITY IS THE TOP VALUE-ADDED SERVICE4

 USERS ARE LOOKING FOR MORE THAN JUST BASIC CYBERSECURITY5

 USERS PREFER BUNDLES6

 USER EXPERIENCE CAN MAKE A DIFFERENCE6

CONCLUSION7

 OFFER COMPREHENSIVE DIGITAL LIFE PROTECTION7

 CAPITALIZE ON REVENUE OPPORTUNITIES7

 EDUCATE AND ENGAGE CONSUMERS7

 FOCUS ON USER EXPERIENCE8

 TARGET KEY DEMOGRAPHICS8

 COLLABORATE WITH CYBERSECURITY VENDORS8

Executive Summary

As markets grow more competitive, telcos struggle to go beyond speed and pricing to meet rising consumer demands for comprehensive cybersecurity. Users are increasingly valuing cybersecurity and online privacy and expect their providers to safeguard their digital lives, with 79% considering protection against cyberthreats essential and 45% believing it's the telco's responsibility. In this context, cybersecurity has become the most sought-after value-added service, surpassing entertainment options, as consumers are increasingly interested in complex cybersecurity solutions like digital identity protection and router-based security. A preference for bundled services (favored by 67% users) underscores the need for intuitive, seamless offerings. By integrating all-inclusive cybersecurity solutions, prioritizing user experience, and leveraging bundled packages, telcos can boost customer satisfaction, drive loyalty, and unlock new revenue streams, positioning themselves as trusted leaders in the digital age.

Introduction

In today's saturated and highly competitive broadband market, expanding the client base and maintaining customer loyalty is increasingly difficult for ISPs looking to maintain their competitive edge.

While pricing and network speed remain important factors in a customer's decision-making process, they're no longer sufficient to differentiate one provider from another. Modern users have higher expectations from their providers—they demand more than just fast and reliable connections. They're looking for a seamless, enriched experience that caters to their growing digital needs. From enhanced security and personalized services to innovative solutions that simplify their online lives, users want providers who go beyond the basics.

For broadband providers, however, these challenges also present important opportunities. By strategically offering meaningful, value-added services that address real user pain points and enhance the overall experience, ISPs can drive customer satisfaction and loyalty while also unlocking new revenue streams. This approach positions providers as leaders in a crowded, constantly evolving market.

At the same time, as cyberthreats expand at an unprecedented rate and our lives become increasingly digital, users are more aware than ever of the critical need for cybersecurity. Surrounded by a growing ecosystem of connected devices—from smartphones and laptops to smart home systems and IoT devices—consumers are turning to their network providers for comprehensive protection. They are not just looking for basic safeguards; they want holistic solutions that secure every aspect of their digital lives, from devices and privacy to smart home security, secure transactions, and digital identity.

What's more, users are willing to pay extra for this peace of mind, recognizing the value of robust, all-encompassing cybersecurity in today's high-risk digital landscape. Above all, they prioritize convenience—solutions must not only deliver powerful security but also integrate seamlessly into their lives, providing a smooth and hassle-free experience. For ISPs, this represents an enormous opportunity to become trusted partners in cybersecurity, driving revenue growth while enhancing customer trust and satisfaction.

The purpose of this paper is to guide telcos in effectively understanding and integrating cybersecurity into their strategies, enabling them to boost revenue, reduce churn, and gain a competitive edge.

Cybersecurity trends

Users expect cybersecurity from their providers

It's clear that, in recent years, cybersecurity has become more than just a simple want. Users increasingly expect their network providers to take responsibility for their online safety. According to recent surveys a significant 79% users consider protection against cyberthreats very important¹, while 45% believe it's the duty of telcos to safeguard them¹.

1 Cybersecurity Trends Among Telco Customers in the U.S., Bitdefender Survey, 2024

Additionally, 49% view the availability of cybersecurity solutions from telcos as highly important¹, emphasizing the growing demand for wide-ranging protection as a standard offering.

Key Drivers:

- ↳ Most subscribers are aware of cyberthreats, and know it's important to protect themselves, but lack the technical expertise to address them effectively.
- ↳ Many users experience analysis paralysis, unsure of which cybersecurity solution is best for them
- ↳ Subscribers expect help from their providers to manage their cybersecurity and are willing to pay extra for comprehensive protection (on average +\$6-\$10)¹

Implications:

- ↳ **For Subscribers:** Many are willing to pay a premium for better protection. Additionally, enhanced cybersecurity can influence their decision to switch providers.
- ↳ **For Telcos:** This represents a significant opportunity to increase revenue while boosting customer satisfaction and loyalty.

Cybersecurity is the Top Value-Added Service

Value-Added Services are the best way telcos can boost revenue and in today's landscape, cybersecurity emerges as the most in-demand value-added service (VAS) for broadband users. According to recent customer surveys across major markets, 20–30% of users rank cybersecurity above other VAS options, including music streaming, video streaming, gaming, and smart home bundles¹.

Key Drivers:

- ↳ **Consumer Demand:** Comprehensive whole-home cybersecurity is the VAS that consumers are most willing to pay for, as highlighted by Omdia Research².
- ↳ **Target Segments:** Certain demographics, such as parents with young children, exhibit even greater willingness to invest in enhanced security measures.
- ↳ **Connected Devices:** There is a clear correlation between the number of connected devices in a household and the demand for robust cybersecurity solutions.



Implications:

- ↳ **For Subscribers:** Cybersecurity has become a key factor in their purchasing decisions, with many willing to pay a premium for better protection tailored to their household needs.
- ↳ **For Telcos:** This presents a substantial opportunity to capitalize on consumer demand by offering comprehensive cybersecurity services, thereby driving revenue growth and strengthening customer loyalty.

Users are looking for more than just basic cybersecurity

Cyberthreats continue to evolve at an alarming pace which means users are demanding more than just basic endpoint protection to secure their increasingly complex digital lives. Moreover, telcos that rely solely on basic cybersecurity solutions risk losing control over the end-user experience and missing out on significant monetization opportunities according to Omdia research². To meet these demands, service providers must shift toward offering “total consumer cybersecurity” solutions that protect users across all devices, networks, and threat types.

Comprehensive cybersecurity solutions go beyond endpoint protection, addressing the growing vulnerabilities created by factors like the rise of smart home devices (up to 21 per household³, 32BN in the world by 2030⁴) and the increasing number of daily cyberattacks on smart homes (an average of 10 per home⁵).

Moreover, cybercriminals are leveraging advancements in AI to create increasingly sophisticated and convincing scams, making it harder than ever for users to distinguish between legitimate and malicious interactions. For example, Americans lost over \$108 million to scams involving AI in 2023⁵.

At the same time 78.3% of users admit to conducting sensitive transactions on mobile devices⁶, and 25% remain unaware that mobile security is even available⁴.

A rich **Digital Life Protection portfolio** is essential to address all these challenges. Such a portfolio ensures holistic protection for both families and businesses, covering everything from safeguarding personal data and online privacy to defending against emerging threats with advanced AI-driven threat detection. By utilizing network-level, device-level, and cloud-based sensors these solutions can quickly identify and mitigate even the newest, most sophisticated attacks.

Moreover, the rapid growth of AI has further shifted the threat landscape, enabling more sophisticated scams that require minimal technical expertise. To combat these challenges, telcos must incorporate AI models capable of detecting new scam waves in real time and deploy solutions based on large language models (LLMs) to enhance scam prevention capabilities.

Key Drivers:

- ↳ **Growing Demand for Comprehensive Solutions:** Up to 24% of users are willing to adopt additional cybersecurity services such as digital identity protection, VPNs, and password managers in the next six months¹.
- ↳ **Smart Home Vulnerabilities:** 35% of users want router-based security⁷, the surge in connected devices per home has amplified vulnerabilities, increasing the demand for holistic protection.
- ↳ **AI-Driven Innovation:** Leveraging AI and LLM-based technologies enables faster detection of sophisticated attacks, offering peace of mind to users while reducing response times.

Implications:

- ↳ **For Subscribers:** Consumers are willing to pay for comprehensive cybersecurity that safeguards all aspects of their digital lives, from online transactions to smart home devices. Total cybersecurity solutions can also influence their choice of provider.
- ↳ **For Telcos:** Offering an advanced Digital Life Protection portfolio tailored to different segments (e.g., families, small businesses) presents a unique opportunity to expand service offerings, enhance customer satisfaction, and generate new revenue streams. Moreover, Investing in AI-driven innovation and collaborative partnerships further positions telcos as leaders in delivering cutting-edge cybersecurity solutions.

3 The 2024 Iot Security Landscape Report, Bitdefender

4 IoT Connections Worldwide, Statista

5 FTC reporting

6 2024 Consumer Cybersecurity Assessment Report, Bitdefender

7 2024 Wi-Fi Router Assessment Internet Connected Users United States, Bitdefender

Users prefer bundles

As the demand for cybersecurity grows, users increasingly prefer receiving these services as part of a convenient package. Up to 67% of consumers express a preference for bundled cybersecurity offerings, recognizing the value and simplicity these packages provide⁸. Bundles not only simplify the decision-making process but also alleviate the confusion experienced by the 31% of users who are unsure about which cybersecurity solutions best suit their needs⁶.

By packaging cybersecurity with other services—such as smart home or entertainment solutions—telcos can deliver a seamless experience while addressing users' growing security concerns. Bundled offerings also enhance customer loyalty by providing an integrated solution that meets multiple needs in a single package.

Key Drivers:

- ↳ **Convenience:** Users value the simplicity of having cybersecurity integrated into a broader service bundle.
- ↳ **Analysis Paralysis:** With 31% of users unsure about their cybersecurity needs, bundles offer clarity and ease of adoption.
- ↳ **Perceived Value:** Bundled services present a cost-effective and comprehensive solution, increasing their appeal to a broad consumer base.

Implications:

- ↳ **For Subscribers:** Bundled cybersecurity services reduce the complexity of choosing protection while offering greater perceived value. This can enhance satisfaction and encourage long-term loyalty.
- ↳ **For Telcos:** Bundles present an opportunity to differentiate service offerings, drive revenue, and increase customer retention by delivering an all-in-one solution tailored to modern user expectations.

User Experience can Make a Difference

In the world of cybersecurity, convenience is king. Performance is influenced by usage and subscribers usually expect seamless, intuitive solutions that need minimal effort while offering maximum protection. This means telcos have to



prioritize user experience as a core element of their cybersecurity offerings to meet these expectations and stand out in the competitive market.

Tools like smart home security or DNS security are designed to deliver automatic, blanket protection for connected devices, requiring little to no input from users. This hands-off approach is particularly appealing to consumers who value convenience and peace of mind. Additionally, advancements in AI are making cybersecurity more efficient and convenient by promoting smarter, automated security that adapts to evolving threats, providing users with an enhanced sense of security without any added complexity.

In parallel, the rise of super apps is also revolutionizing the way users interact with cybersecurity services. By consolidating management tools into a single, easy-to-navigate platform, these apps improve the overall experience, making it easier than ever for users to monitor and control their digital safety. For example, the Bitdefender OneApp centralizes digital life protection in one place with a consistent experience across devices. It also adapts the user experience to different roles and segments, such as adults, children, teenagers, and assisted adults, ensuring relevance and clarity for every user type. Fast and streamlined onboarding processes further enhance usability, reducing friction and improving service adoption.

Key Drivers:

- ↳ **Convenience:** Automatic solutions like DNS security and smart home protection eliminate the need for user intervention, ensuring ease of use.
- ↳ **Automation Through AI:** Advanced AI capabilities enhance cybersecurity by providing smarter, adaptive protection without overwhelming users.
- ↳ **Tailored Experiences:** Unified apps, such as Bitdefender OneApp, adapt to various user roles and segments, ensuring personalized interactions for families, businesses, and individual users. They also simplify management and improve accessibility, creating a streamlined experience for consumers across all devices.

Implications:

- ↳ **For Subscribers:** A frictionless user experience enhances satisfaction and trust, encouraging continued adoption of cybersecurity solutions. Tailored interfaces for different roles within families or organizations further improve user engagement.
- ↳ **For Telcos:** By focusing on user experience and adopting tools like super apps with role-based personalization, telcos can differentiate their offerings, drive adoption, and increase customer retention. Integrating AI-driven automation will further position telcos as leaders in delivering innovative, user-centric cybersecurity solutions.

Conclusion

Recommendations for Telcos Aiming to Better Integrate Cybersecurity into Their Strategies

Offer Comprehensive Digital Life Protection

- ↳ Move beyond basic endpoint protection to provide “total consumer cybersecurity”, or Digital Life Protection solutions, that protect users across all devices, networks, and threat types.
- ↳ Don't ignore the growing vulnerabilities created by smart home devices and the surge in mobile transactions.

Capitalize on Revenue Opportunities

- ↳ Position cybersecurity as the top value-added service, supported by research indicating its ranking above entertainment services like video and music streaming.
- ↳ Use bundled and advanced offerings to differentiate your brand and secure customer loyalty, reducing churn and opening new revenue streams.

Educate and Engage Consumers

- ↳ Develop marketing campaigns that clearly communicate the importance of comprehensive cybersecurity and its added value.
- ↳ Offer educational resources to demystify cybersecurity, helping users overcome analysis paralysis and make informed decisions.

Focus on User Experience

- ↳ Prioritize convenience by offering intuitive solutions that require minimal user input, such as DNS security and smart home security.
- ↳ Explore super apps to consolidate management tools into a single, easy-to-use platform, simplifying user interaction and enhancing satisfaction.

Target Key Demographics

- ↳ Tailor solutions to specific segments, such as parents with young children and households with a high number of connected devices, who are more willing to invest in advanced security.

Collaborate with Cybersecurity Vendors

- ↳ Work with trusted technology partners that offer a full digital life protection portfolio to stay ahead of evolving cyberthreats and ensure your product roadmap meets new challenges.

For more information on Bitdefender products and services tailored specifically for telcos, please visit [The Subscriber Protection Platform](#) or Book a Consultation with our team of experts directly from the website.