No.82
February 2025

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/ SPONSORED

Telco Strategies for Consumer Security

Sponsored by Bitdefender

During Q4 2024, HardenStance took research inputs from leading telcos, vendors and regulators around the world about the 'what?', 'how?' and 'why?' of leading telcos bringing better cybersecurity to consumer households, devices and online experiences.

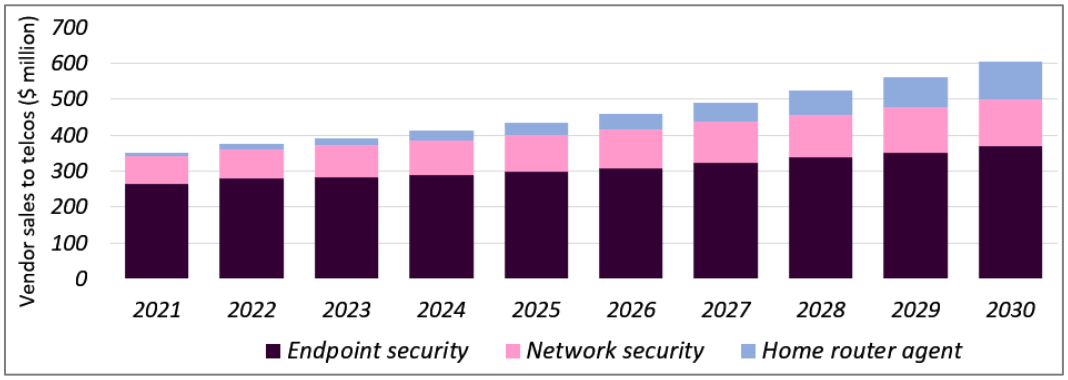
- The growth in high impact scams, including multi-platform scams, is the single most important trend in the consumer cyber threat landscape over the last 18 months.
- Telco spending on consumer security software will grow at a CAGR of 6.6% over the next six years - from $412 million in 2024 to $606 million in 2030.
- 70% of telco security spending on consumer software still goes on endpoint security. Widely deployed in North America, RDK-B open source home routers began rolling out in Europe in 2024. Routers using prpl are going live in 2025. These open source ecosystems will drive higher penetration of security agents on home routers. Annual telco investment in DNS or DPI-based network security will also continue growing.
- POCs of security models converging home LAN and telco network domains – possibly including GSMA's Open Gateway Exposure Platform - are likely in 2025 or 2026.
- The unprecedented destruction of 600,000 of Windstream's SOHO routers by malware in the U.S in October 2023 is a call to arms to better protect home routers. U.S legislators have already responded with the new ROUTERS Act bill.

Telco spending on consumer security is growing

HardenStance forecasts that total telco spending on consumer security will grow at a CAGR of 6.6%, reaching $606 million by 2030.

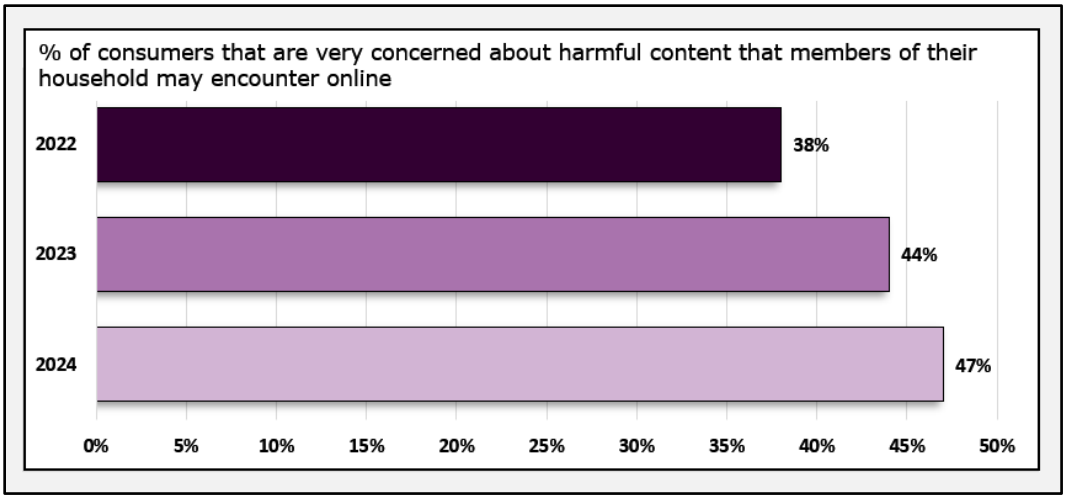
HardenStance estimates that telcos around the world spent around $412 million on consumer security software in 2024. 70% of this spending ($289 million) went on endpoint security software. Of the remainder, 23% ($96 million) went on network (mainly DNS-based) security that allows telcos to block customer access to malicious sites. The nascent home router security agent model that protects all connected 'things' in a household accounted for just 7% ($27 million). Total spending during 2024 was up 5% compared to 2023. HardenStance forecasts that total telco spending on consumer security software will grow at a CAGR of 6.6%, reaching $606 million by 2030.

Figure 1: Worldwide annual telco spending on consumer security software



Source: HardenStance

Figure 2: Consumer concern about harmful content is growing



Source: EY "Decoding the Digital Home" survey of 20,000 households world-wide, October 2024

Consumers are menaced by the threat from online scams

The single most important trend driving growth in aggregate telco spending on consumer security software is the heightened threat from online scams. Consider the following evidence:

- The newly formed Global Anti Scam Alliance, which defines its mission as "to protect consumers worldwide from scams", includes Amazon, Bitdefender, Capital One, F-Secure, Google, Mastercard, Meta, and Trend Micro among its Foundation members. GASA estimates consumers worldwide lost $1.026 trillion to scams in 2023 alone.

The single most important trend in the consumer cyber threat landscape is the heightened threat from online scams.

- In a November 2024 article in The Times, titled "Police this Epidemic", Lutz Schüler, CEO of Virgin Media O2, stated that fraud accounts for 40% of all UK crime and that "a quarter of people are targeted each week." Despite what he called "this tidal wave of criminality", Schüler said that there were 10% fewer fraud prosecutions in the UK in 2023 than in 2022. The terms "epidemic" and "pandemic" are now routinely used to describe the scale of the threat from scams.
- Credible survey data points to growing awareness of this heightened risk among consumers worldwide. As shown in **Figure 2**, 47% of those surveyed by EY in 2024 were "very concerned" about online risk compared to just 38% two years earlier.

Highly effective combinations of new and well-established techniques

Generative AI is an increasingly important factor driving the growth in scams – and the success rates scammers are enjoying. Scammers are integrating Gen AI to improve the efficacy of their Tactics, Techniques and Procedures (TTPs). They're using it to lower their costs and make their engagement with targets appear more trustworthy. The most common uses of Gen AI by scammers are creating more convincing lure content and faking the identities of individuals and organizations more convincingly.

- **More convincing lure content**. If you're not a native English speaker, Gen AI can create a far better written, much more convincing, English language phishing email or smishing text than you can yourself. That better quality composition can convince a target that a message is legitimate where inferior quality might trigger suspicion. AI can also create it a lot faster.
- **More convincing AI-driven identity spoofing**. The best AI-generated fake audio and video representations of peoples' voice and face are very convincing now. They don't even have to be that good to be effective. A target who is put under pressure may miss flaws that they would normally see or hear. Scammers don't need fakes to be interactive, either; 10-second fake audio messages can be very effective.

A new lease of life for SMS and Caller ID spoofing

The scam ecosystem isn't being driven by AI alone. By creating new options and new possibilities for scammers, AI is also giving a new lease of life to the use of well-established techniques like text and caller ID spoofing.

Spoofing allows the falsification of the number that that you see on your display when you receive a call or text. On seeing a bona fide number, many consumers trust that they are indeed being called from the phone of someone they know. And if a scammer says they represent the called party's employer, their bank, or their software provider, a quick online search will often verify that that number is indeed associated with that organization (most consumers don't know that the call centre number an organization publishes to invite incoming calls is typically not used for outgoing calls).

The introduction of new AI-based techniques is serving as a force multiplier, driving scammer usage of older techniques too.

In other words the introduction of new AI-based techniques is serving as a force multiplier, driving the use of older techniques too. If a scammer can use a new fake voice message to win a target's trust, the target is more likely to trust the malicious link the scammer sends them next via good old SMS. Or if they can gain initial trust with a phone call using old-fashioned caller ID spoofing, the chances are higher that the target will click on a well-written AI-assisted phishing email that is the next phase of the scam.

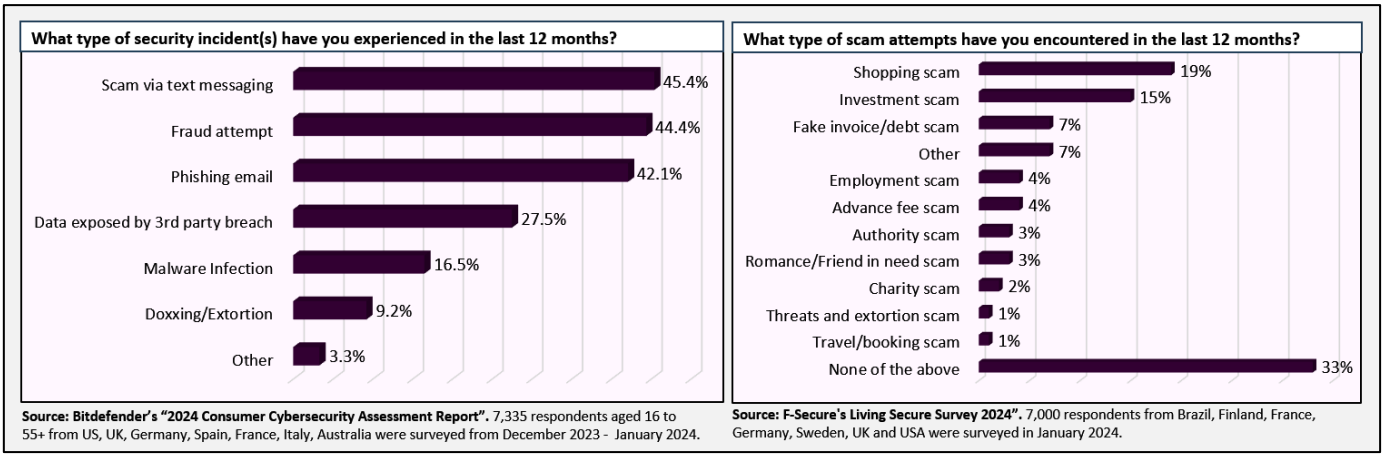
Persistent, intelligent pursuit of a target across multiple platforms

Legacy generations of online scams are scatter-gun efforts. Scammers launch huge volumes of lures into what is an internet void. They count on a fraction of anonymous targets responding to an email, clicking on a URL, or making a call to trigger a payment. Most are still single platform – a victim falls for a single phone call, email or SMS.

The most striking feature of some latest scams is how scammers are able to track and pursue a target across multiple platforms. They are investing time in building or obtaining a detailed profile of a single target individual. They are then pursuing them relentlessly and intelligently, across legacy platforms like telephony, SMS and email as well as newer messaging apps like WhatsApp and collaboration platforms like Teams.

In other words, the kinds of techniques that cybercriminals have been using for years to target prominent business leaders, employees and politicians are increasingly being used to target ordinary consumers. Moreover, high profile or wealthy individuals aren't necessarily the preferred targets. In many cases, low income or more vulnerable citizens are just as, or more, likely to be targeted. As shown in **Figure 3**, the most common scams now are online shopping, investment, and fake invoice or debts scams.

Figure 3: The prevalence of scams among threats and the frequency of different types of scams



Source: Bitdefender's "2024 Consumer Cybersecurity Assessment Report". 7,335 respondents aged 16 to 55+ from US, UK, Germany, Spain, France, Italy, Australia were surveyed from December 2023 - January 2024.

Source: F-Secure's Living Secure Survey 2024". 7,000 respondents from Brazil, Finland, France, Germany, Sweden, UK and USA were surveyed in January 2024.

And it isn't just phones and PCs that are entry points for scammers. A lot of so-called 'smart home' devices expose data that identifies the location of someone's home. Consumers don't yet understand that theirs and their loved one's physical safety is not separate from their virtual or digital environment. As well as using multiple virtual platforms, scammers are adding physical world phases. A scam that starts online can conclude with a gang member showing up on your doorstep posing as a courier.

Gaining full access to a bank account rather than merely abusing a credit card is exposing some victims to larger financial losses too. Depending on the country and the banks and telcos involved, not all victims recover all their losses. Among those that do, some suffer high, even devastating, stress until all their funds are reimbursed. Even after recovering all their funds, some victims suffer serious long-term psychological effects. Examples include elderly people being reluctant or completely unwilling to answer their phones or use their PCs again after they've been scammed.

Bitdefender partners telcos to bring cybersecurity to a mass market

Being among the leaders in endpoint security for businesses and consumers, Bitdefender is increasingly turning to telco channel partners to grow a mass market in consumer security. The company's Subscriber Protection Platform is tailored to a telco's unique requirements. It boasts one of the broadest portfolios on the market, spanning endpoint security, home router agent, privacy and identity, and network security. These can all be seamlessly managed by a telco's customers using Bitdefender's 'OneApp' unified app. Bitdefender also offers telcos go-to-market support via its Partner Success Portal. Live since the end of 2024, this provides access to strategy tutorials, pre-designed sales and marketing campaigns, and other supporting materials to help telco partners succeed.

At the start of 2024, Bitdefender already had more than 15 telco channel partners across different regions. As shown in **Figure 5**, Telefonica Tech and 3 UK were among 5 new telco account wins in Europe during 2024 for endpoint security along with two more in Latin America. As shown in **Figure 7**, two new North American telco accounts have also signed up for the company's home router security agent. For DNS security, Bitdefender works with partners, including one well-established DNS provider.

Consistent with trends in the threat landscape, Bitdefender's roadmap is focused on protecting against scams. In 2024, the company joined the Global Anti-Scam Alliance (GASA). It also launched Scam Copilot, an AI-powered, all-in-one scam prevention platform aimed at combating scams in real time over various digital environments. Among its main features are Scam Copilot Chatbot, which allows users to get a second opinion on suspicious interactions; Scam Wave Alerts, an alert system for regional scam outbreaks; and modules leveraging AI to secure email, chats, and messages.

Vulnerability research into smart homes and smart home products

One of the ways Bitdefender is looking to differentiate itself is via its vulnerability research into smart homes and smart home products. In April last year, the company's researchers identified 91,000 LG TVs that were vulnerable to being taken over via escalation of admin rights. Bitdefender sees a lot of opportunity in the open source home router agent market for protecting smart homes against their own IoT 'things'. Consistent with that, the company is one of the most active cybersecurity vendors in the prpl ecosystem. Its contributors have contributed a lot of the code that allows a security agent the kind of extensive and frequent access it needs to access the prpl stack, albeit with the necessary security controls built in to manage those access rights securely. Bitdefender's agent is also compatible with RDK-B. And a light version is compatible with older router generations.

Among prpl Working Groups, Bitdefender is especially active in Security, Life Cycle Management and High-Level APIs. Bitdefender contributors are working on augmenting the higher level APIs with new capabilities for more efficient functioning of security containers such as via fast path Packet Interception APIs, VPN management and DNS flow management. Bitdefender has demonstrated integrations of its prpl security agent with home router vendors like Kaon, Vantiva, Zyxel, ZTE. More are planned in 2025.

Big telcos are leaning in but many peers are holding back

The large majority of aggregate global telco spend on consumer security software has always been spent by around 30 of the world's largest, most well-resourced, telcos and telco groups. These companies have always driven – and continue to drive – this market. Investment in brand equity and subscriber churn management are secondary drivers. Growing revenues is by far the most important. As many telcos continue to struggle to grow revenues, selling consumer security offers a clear potential path to monetization.

Among the largest telcos, growth in security revenues is being driven by expanding premium security packages; converting value-driven subscribers to higher value fixed or mobile service packages with security built in; or signing up entirely new subscribers. Compared with reselling a service like Spotify, profit margins selling additional security to consumers can be much higher. Some endpoint security vendors reckon telcos can achieve 75% profit margins reselling their products. Monetization can be by charging for security directly; charging indirectly by bundling security into higher priced service packages; or indirectly via across-the-broad price increases.

The commitments big customers are making nowadays are less opportunistic and more strategic than they were, even just a couple of years ago.

Many big telcos are thinking more strategically now…

Vendors serving telcos in this market report that the commitments big customers are making nowadays are less opportunistic and more strategic than they were, even just a couple of years ago. They cite the following examples:

- fewer instances of a 'lone wolf' product manager or value added services leader advancing resale of nothing but endpoint security - but with only half-hearted support from upper management.
- more instances of management making long term commitments to consumer security at every layer as key to the telco's core value proposition. These days, delays in telco spending are more likely to arise from delays in technology maturity or solution deployment than from management hesitation to commit to this space.
- big telco RFPs that address just one of the three layers of consumer security have become the exception not the rule. Most RFPs tend to address all three now.

…but total sales don't just reflect commitments by the largest telcos

The modest overall growth in total worldwide sales depicted in **Figure 1** reflects relatively strong spending growth by a subset of large telcos being offset by flat spending among smaller peers, and a few nuanced variations on these themes. The main factors exerting downward pressure on aggregate global telco spending are the following:

- **Less well-resourced telcos and ISPs tend to spend little or nothing on additional layers of security beyond what is already embedded in the network by mandatory or optional standards.** That's because they tend to have fewer of the high ARPU subscribers that allow a good ROI on endpoint security or home router security. They also lack the scale and skillsets needed to justify the complex end to end integrations that some consumer security solutions require. Historically, such spending as these companies have done has tended to focus on one-off sales of premium, stand-alone, cybersecurity opt-ins for premium subscribers rather than bundling it across service packages.

  That said, as discussed in the network security section on page 8, there is evidence of smaller ISPs and some telcos in developing markets starting to invest in network-based security. Another factor that could move the needle among smaller players is if vendors can bring compelling SaaS solutions to them to reduce the resource and operations challenges associated with current models. One or two leading vendors have this in development and first releases may hit the market in 2025.

- **It only takes a couple of big telcos losing large numbers of subscribers to exert a significant downward drag on aggregate spending.** As F-Secure has shown with its experience during 2024, the loss by one of its big telco customers of what F-Secure's CFO, Sari Somerkallio, called "many millions" of subscribers translates into lost vendor revenue for every one of those lost subscribers. At the end of last year, Somerkallio told investors that the resulting loss of revenue for F-Secure had been "very significant". This impact comes straight off a vendor's top line. Hence it also comes straight off global aggregate telco spending, even though that telco's commitment to consumer security may not have faltered in any way.
- **There are comparable trends at play among consumers – some are opting in to better security, but others are opting out**. As shown in **Figure 2**, at an aggregate level, consumer concern about cyber risk is clearly increasing. Understandably, vendors and telcos tend to focus on the many consumers that are following through on that concern by spending more. But high concern doesn't always drive more spending. In the lived reality of today's cost of living challenges, some people are making the opposite choice. They are foregoing security and downgrading to a service with little or no added security. Each of these personal decisions felt by a telco also nudges their vendor's sales up or down accordingly.

Endpoint security 3.0 adds a layer of user experience software above the core security functions, with the goal of applying it consistently across all the security apps.

Endpoint security 3.0 – driven by scam prevention

HardenStance estimates that telco spending on endpoint security will grow from $289 million in 2024 to $368 million in 2030. The impact of online scams, and the role AI has in both driving them and defending against them, is driving profound change in the endpoint security product market. As HardenStance defines it, some but not all of the latest releases by vendors amount to a 3.0 generation of endpoint security products:

- **Endpoint security 1.0** was antivirus running on PCs and MACs.
- **Endpoint security 2.0** added additional applications alongside AV or malware protection like VPN, password management and identity monitoring. Vendors also extended their software to run on other devices, especially smartphones.
- **Endpoint security 3.0** adds a layer of user experience software above the core security functions of the apps themselves, with the goal of applying it consistently across all security apps and ultimately across all platforms. This aims to simplify the user experience; flag potential risks in real time; and give users simple, real-time, guidance on how to avoid being scammed.

Figure 4: Endpoint security vendors add new features and 'scam protection' branding

Vendor	Date	New endpoint security releases of 2024
Bitdefender	October 2024	**Scam Copilot** is an AI-powered platform that helps detect and prevent scams across web, email, SMS, chat apps, push notifications, and calendar invites. It offers **Scam Wave Alerts** – alerts about regional scam outbreaks, chatbot guidance, and protection to block evolving threats and remote access scams.
ESET	October 2024	**'ESET Home Security':** Addition of dark web monitoring; folder guard (Windows); improved anti-phishing (Android); better MAC firewalling; new password manager options.
F-Secure	October 2024	**'TOTAL'** endpoint security suite: 7 new AI-driven scam protection features added: shopping protection; SMS scam protection; banking protection; browsing & phishing protection; Wi-Fi protection; cookie popup blocker and ad blocker.
McAfee	August 2024	AI-powered **'Deep Fake Detector'** launched (for Lenovo PCs).

Source: HardenStance

Telco positioning of endpoint security in consumer value propositions

The way some leading telcos are integrating and positioning endpoint security in their consumer portfolios is evolving. Extending endpoint security from premium tier service packages to mid-range packages is one trend that vendors report seeing from the telcos they serve. A couple of other trends are also noteworthy.

The first is the proliferation of so called 'super apps', whereby telcos are consolidating and white labelling multiple third party apps, including cybersecurity apps, under their own-branded unified user interface and service ecosystem. These super apps started in Asia but big telcos around the world have picked up on the idea. For example:

- EE in the UK is targeting the smart home services space with a new consumer services platform accessible via a new EE app and 'EE ID'.
- Having only launched it in February 2024, T-Mobile was expecting to see 40 million downloads of its 'T-Life' super-app by the end of 2024. John Freier, President of T-Mobile's Consumer Group, told the December 3rd Wells Frago 8th annual 'TMT summit' in December 2024 that T-Life "is going to increasingly be the epicentre of how we do business. "[it is] promoting empowerment for customers to be able to take care of things when they want to versus when they must in terms of when a store is open or when a call center is available. [It is] helping them be able to manage their full suite of connections to the network, whether that be their smartphone connection, tablet, watches, high speed Internet from their home. Being able to do all of that within T-Life is our dream."
- A more narrowly-focused approach to this is telcos bundling a number of third party security solutions under their own unified and branded consumer security app. An example of this is 'ActiveArmor'. This is AT&T's mobile security app which comes in free and premium versions promising to "block spam calls and texts, get data breach alerts and more". Look under the hood of ActiveArmor and you'll find cybersecurity vendors F-Secure, Lookout (part of F-Secure); Neustar and Hiya.

Having only launched it in February 2024, T-Mobile was expecting to see 40 million downloads of its 'T-Life' super-app by the end of 2024.

F-Secure still leads the market in telco wins for endpoint security…

F-Secure is the incumbent endpoint security vendor in the telco market. Around 80% of its annual revenue of around €130 million comes from more than 200 channel partners, of which most are telecom operators. The company claims a share of around 40% of telco spending on endpoint security software.

As a public company, F-Secure can share more detail about its sales than rival endpoint security vendors that are privately held (which is a lot of them). During the company's 'Investor Day' in November 2024, F-Secure shared that 42% of its channel partners were using its multi-module 'TOTAL' product that provides access to its full suite of endpoint security apps. The company also shared that 24% of all users (across all direct and indirect channels) were using 'TOTAL', up from 9% in November 2023. The company said that in the last year it has increased the annualized ARPU by 9% among TOTAL users among its partners, most of which are telcos.

…while Bitdefender has the strongest momentum among challengers

The momentum behind cybersecurity starting to become more of a mass market is encouraging other endpoint security vendors to recognize the unique opportunity that telcos present for reaching consumers. A vendor can go direct to reach technically adept consumers who are able and willing to choose, download and manage an endpoint security client themselves. But to reach segments of a larger mass market that will pay for security if it can be made simpler, more intuitive, and more reassuring to use, endpoint security vendors need simplified solutions as well as trusted channel partners.

Figure 5: Recent vendor wins for endpoint security with telco customers

Vendor	Date	Operator	Country/Region
Bitdefender	2024	Telefonica	Group/Worldwide
Bitdefender	2024	3 UK	Europe
Bitdefender	2024	Three more telco contracts	Europe
Bitdefender	2024	Two telco contracts	Latin America
F-Secure	2024	Tier 2 telco	Middle East
F-Secure	2024	2 telco contracts	Europe (one in Italy)
F-Secure	2024	Mobile operator	Asia
F-Secure	2024	MobiFone	Vietnam
F-Secure	2024	SaskTel	Canada
F-Secure	2024	Tier 2 Telco	USA
F-Secure	2024	Tier 1 Telco	Global

Source: HardenStance
(McAfee, Symantec and Trend Micro were invited to share telco contract wins but didn't respond)

With more than 15 telco customers, Bitdefender seems to have the best market momentum among challengers in the endpoint security segment.

With more than 15 telco customers, including some new wins in 2024 shown in **Figure 5**, Bitdefender seems to have the best market momentum among challengers in the endpoint security segment. Despite landing wins with Telstra and Telefonica in the 2020 – 2022 timeframe, McAfee's momentum in the telco sector appears to have stalled somewhat. Some other endpoint security vendors are showing either new or renewed interest in the telco channel opportunity, and some are undertaking Proof of Concept (PoC) trials. HardenStance reached out to other relevant endpoint security vendors asking for their telco account win momentum during 2024 and received no responses. If other vendors are making significant strides in this market space then they're either keeping very, very quiet about it or HardenStance inadvertently missed them.

Network-based security may be seeing the fastest growth

HardenStance estimates that telco spending on network-based consumer security software grew from $96 million in 2024 and will grow to $133 million in 2030. Most of this market consists of DNS security software driven from a telco's DNS servers. This either blocks or advises users against accessing phishing websites and websites that deliver malware.

Many telcos find it relatively easy to extend this additional online network security as a baseline to all customers across fixed and mobile services free or with an added charge. Others provide it as an add-on which users need to opt in to. The limitation of network-based security is that it doesn't offer the depth of protection that endpoint security provides nor the breadth of protection against threats in the home from IoT 'things' that comes with a home router security agent. Leading vendors in this market space are Akamai, Infoblox, Efficient IP, PowerDNS, Whalebone and Allot. Allot competes in DNS security at the margins but centers its network security offer around a differentiated DPI-based solution.

The dynamics of the network security market as defined in this report are the most complex of the three consumer security segments telcos are spending on. The dominant trends in play are pulling this market segment in three contradictory directions:

1: A bearish sales outlook among established telco customers

Going back several years, incumbent vendors like Akamai and Infoblox drove early adoption of DNS-based network security by mostly large telcos in North America and Europe. These vendors continue serving those customers. However the spending trend on network-based security among this group of telcos is generally pretty flat. This market segment is largely saturated and pricing typically has to be lower to reach other telcos in other regions. In the last couple of years, the vendors serving these customers have been focusing on bigger market opportunities. DNS sales haven't been a key priority for Akamai; telcos haven't been a key priority for Infoblox. Hence, some of these vendors have come to have a limited scope or limited appetite for growing their telco DNS security footprint much within or beyond these core regions.

2: Whalebone – the first of two positive forces driving this market

The first of two contrary positive forces in play is the very aggressive targeting of this market by Czech Republic-based start-up Whalebone. During 2022 and 2023 Whalebone landed several sizable and named telco account wins for DNS security in Central Europe. It also won Telefonica O2 in Germany. Many of these telcos have provided compelling customer testimonials. Whalebone's core business focuses on sales and marketing hand-holding and peer-group information sharing around deploying and monetizing DNS security for telco customers. Small operators in price-sensitive markets tend to be heavily dependent on this kind of support for standing up the business case.

Whalebone claims a remarkable 17 new telco contract wins during 2024. Half these wins are in regions as far afield as Asia Pacific, Latin America and Africa.

As shown in **Figure 6**, Whalebone claims a remarkable 17 new telco contract wins during 2024 alone. Half these wins are outside the company's core European market, in regions as far afield as Asia Pacific, Latin America and Africa. Even if there may be a little 'stretching' of the definition of a fully closed account win in claiming these account references, Whalebone is clearly out on its own in terms of its commitment to growing the global footprint of consumers that are protected by telcos via DNS security.

If Whalebone can scale upwards as successfully as it seems to be scaling outwards, the impact on total market sales of DNS security software to telcos could be very positive. At around €10 million, however, the company's 2024 revenues didn't quite double compared with 2023. This suggests there may be something in the gripes of some competitors that the company is pricing very aggressively to win these deals.

Whalebone counters that it is persuading a high proportion of its telco customers to agree to revenue sharing models rather than more basic price-per-subscriber terms. This has potential to push its own sales sharply upwards – and total market sales up with it. For this year, HardenStance's market forecast assumes that Whalebone's impact on total market sales will be subdued for the next year or two. A sharp spike in 2025 revenues, as the company seems to be expecting, would cause HardenStance to revise the market forecast for this segment upwards.

Telco spending on DNS security driven by regulators (and banks too)

The other positive trend in play is that DNS security vendors – not just Whalebone, some others too – report new telco sales opportunities arising from the growth in the number of regulators around the world that are mandating better online security protections for consumers. In some cases it's only parental controls; in others it's more far-reaching requirements to better protect all users. In some cases, but not all, this is off the back of the launch of Protective DNS (PDNS) services for analyzing DNS querying and mitigating threats. A lot of these are being initiated by governments and their cybersecurity agencies like the National Cyber Security Centre (NCSC) in the UK.

In June 2024 Infoblox released a blog and webinar on PDNS security targeting the telco sector. The company declared that "for broadband operators, the call to action is clear and present. Your networks are the highways of the digital world, and with PDNS, you have the power to make these highways safer for every traveller." This suggests that even some incumbent DNS vendors may see new security sales opportunities from partnering telcos to be PDNS providers across enterprise as well as consumer markets.

An important aspect of DNS security is that it is relatively easy and low cost for a telco to deploy with universal reach. Hence from the perspective of a telco – arguably from the perspective of a regulator too – network security like this is 'low-hanging fruit' or a 'quick win'. It's a measure that 'ticks a box' showing that both regulator and regulated are acting to provide at least some basic cybersecurity protection to citizens. Faced with newly emerging requirements from regulators, the smart way for telco management to respond is to get ahead of these requirements rather than just waiting for them to land.

DNS security is relatively easy and low cost for a telco to deploy with universal reach. It's 'low-hanging fruit' or a 'quick win'.

DNS security software - used by telcos but paid for by someone else.

Some variants of the regulator-led use cases cited above have potential to complicate the market sizing challenge. Specifically, some governments are buying DNS threat feeds and making them available to all telcos and ISPs in their market. This can count as a vendor's sales for telco use cases, albeit the actual buyer is the regulator.

Another emerging use case sees telcos serving as the agents of DNS security enforcement on consumer transactions for banks. Where they are required to refund consumers that have been scammed and absorb losses to fraudsters themselves, banks can be highly motivated to pay for fraudulent, so-called 'lookalike' variants of their own websites to be identified and blocked by telco partners. Again, a telco can grow its DNS security revenues with this model, but here it may be the bank paying for the software.

Figure 6: New vendor wins for DNS-based network security

Vendor	Date	Country/Region	Telco
Akamai	2023	Germany	Tier 1 telco
Akamai	2023	USA	Tier 2 telco
Allot	2024	Czech Rep/Slovakia (with PowerDNS)	Tier 1 telco
Bitdefender	2024	Europe (with partner)	Tier 1 telco
F-Secure	2024	Netherlands (with partner)	Tier 2 telco
F-Secure	2024	Holland (with partner)	Tier 1 telco
F-Secure	2024	Poland (with partner)	2 telco contracts
PowerDNS	2024	Europe (with partner)	Tier 1 telco
PowerDNS	2024	Czech Rep/Slovakia (with Allot)	Tier 1 telco
PowerDNS	2024	Norway	Tier 2 telco
PowerDNS	2024	Turkey	Tier 1 telco
Whalebone	2024	APAC	5 telco contracts
Whalebone	2024	Europe	8 telco contracts
Whalebone	2024	Latin America	2 telco contracts
Whalebone	2024	Africa and MENA	2 telco contracts

Source: HardenStance **Allot also counts wins using its DPI-based 'Network Secure' solutions.*

DPI-based network security that competes with DNS security continues to be challenged by the growth in encryption. Last year, Allot introduced a new release of its DPI-based 'Network Secure' product for getting around the challenge posed by the growth in Encrypted Client Hello (ECH), which prevents networks from being able to see which websites its users are visiting. Allot stated at the time that AI/ML is being used in conjunction with what it called "other inputs" to ascertain whether the website a user is trying to reach is malicious or not.

Allot cites more than 30 network security customers, most of which are for its DPI-based 'Network-Native' branded approach. One value proposition Allot is increasingly trying to differentiate with is the commonality it offers across Network Secure and its home router agent. Allot claims, quite plausibly, that the integration across the two, at home and while on the move, is tighter and more seamless than any other integration of those two layers. As well as competing in network security with Network Secure, Allot also partners vendors in the DNS security space such as PowerDNS.

Sandvine, Allot's main competitor in the DPI-based space, had a highly disrupted 2024. In February, the company was put on the U.S government's 'Entity List', which subjects companies to export restrictions on grounds of national security. It was taken off again in October, following changes to its corporate governance and business practices.

Leading telcos in EMEA are starting to catch up with North America by finally starting to transition away from selling home routers that run on proprietary software.

Prpl launches planned as RDK-B routers roll out in Europe

HardenStance estimates that telco spending on home router security agents will grow from $27 million in 2024 to $105 million in 2030. Providing full visibility into all the good and bad traffic on a home network, with the ability to detect and block bad traffic, large telcos are uniquely placed to deploy and manage cybersecurity agents on home routers.

This market segment is seeing leading telcos in EMEA start to catch up with North America by finally starting to transition away from selling home routers that run on proprietary software with all the exhaustive integration effort that requires. They're increasingly deploying open source home routers that standards-compliant cybersecurity and other apps can run on. Some telco contracts signed with security agent vendors in 2024 assume initial deployments on traditional, proprietary home routers. But they also provide for those agents to run on open source platforms in later deployment phases.

The two open source home router OSs at the heart of these multi-year migration plans are Reference Design Kit (RDK-B) and prpl. The goal is that they should serve as the 'Android' of the home network, driving consumption of a variety of home networking applications like cybersecurity at scale. 2024 was a critical year for both ecosystems. Each made substantial progress in their own right. Some large operators are also taking advantage of opportunities to mix and match different features from each.

Security is key to monetizing some home network apps

There are multiple different direct and indirect ways for telcos to monetize consumer security. One that is starting to feature more prominently among some of the largest telcos is the recognition that their most compelling among new home network applications will not sell unless they are underpinned by really strong cybersecurity within the home network.

This was nicely captured by Sanjay Ahuja, Verizon's Senior Director, Software Development and Cloud Technologies at the October 2024 Global Summit held by prpl. "We are looking to build security, privacy and ease of use as key factors in our routers", Ahuja said. "We feel that without having consumer data within the home, the next generation of use cases, whether they are energy management or healthcare, are going to be a tough sell."

RDK-B has significant momentum in Europe now

RDK-B was once the preserve of North American cable operators who use DOCSIS such as Comcast, Charter, Shaw and Rogers Communications. Going back a number of years now, these operators have deployed a footprint of RDK-B home routers with Cujo AI's security software running on them to more than 60 million North American households.

Now several operators have started rolling out RDK-B products in Europe:

- In 2023, Sky rolled out RDK-B routers running Cujo AI software in the UK and Italy.
- In 2023, Deutsche Telekom started rolling out RDK-B across several European affiliates – also running Cujo AI software. Croatia was first to launch in 2023. Poland, North Macedonia, Montenegro and Greece followed last year. Cujo AI software is integrated on DT's RDK-B routers providing internet security, digital parenting and device intelligence.
- Virgin Media and Ziggo are selling RDK-B routers in the UK and the Netherlands respectively, with Sam Seamless Network security agents running on some of them.
- Vodafone announced last September that it too will use RDK-B for some of its open source home router deployments starting in April 2025. This may be in Germany where Vodafone also has DOCSIS-based cable networks.

Virgin Media and Ziggo are both selling RDK-B in the UK and the Netherlands respectively, with Sam Seamless Network security agents running on a subset of their products.

From a commercialization standpoint, the prpl ecosystem is catching up with RDK-B. It has strong support from AT&T, Verizon and Orange, all of whom are looking to leverage prpl home routers with their Fibre to the Home (FTTH) rollouts. At the Global prpl Summit in Paris in October 2024 these three big telcos that are driving prpl all committed to their first commercial deployments beginning either at the end of 2024 or in 2025.

Here are the respective commitments these leading operators made:

- **AT&T:** Jason Savard, Associate Vice President of Technology: "We have about six and a half million fibre gateways that we have started prpl deployment on. This is a kind of mix of our old proprietary software with new prpl modules added – and that's expected to complete by the end of 2025. Along with that, we also have new CPE that we're launching in 2026, or potentially earlier. That will launch with prpl software on day one.
- **Verizon**: Desirae Dolphin, Product Manager, Consumer Home Products: "We will be launching our first prpl router this later this year, and we will be rolling it out to all of our customers next year [2025]. This is our first, but we definitely plan to have all of our routers on the prpl stack."
- **Orange:** Koen Vermeulen, Group CIO & Senior Vice President, Innovation IT & Services: "we are committed to launch some of these gateways in some of our regions at scale very soon. We will be having real live productions with real people at large scale."

Orange went one step further in January 2025, announcing the "imminent deployment" by Orange Jordan of the world's first fully prpl-based broadband solution powered by prplWare and complementary SoftAtHome products. The rate at which prpl continues to scale up in the world of commercial services will be determined by at least three factors:

Operational challenges: At the level of home network CPE as much as in their own networks, telco development and operations teams don't just adapt effortlessly to open source models. Change is always challenging. The home environment itself brings its own challenges too. Migrating an installed base of proprietary home router CPE can't be done overnight. But managing parallel proprietary and open source operating models concurrently over a prolonged period can also be very messy and costly. Moreover, when you swap out a propriety home router with a purpl product, you're probably going to want to upgrade any extender or repeater product too.

Figure 7: Recent vendor contracts for home router agent based security

Vendor	Date	Country/Region	Operator
Allot	2024	Vodafone	UK
Allot	2024	MEO	Portugal
Bitdefender	2024	North America	Tier 1 telco
Bitdefender	2024	North Africa	Tier 2 telco
CUJO AI	2023	Italy and UK	Sky
CUJO AI	2024	North Macedonia, Croatia Montenegro, Poland, Greece	Deutsche Telekom
F-Secure	2024	Netherlands	Odido
F-Secure	2024	Japan	Tier 2 Telco
F-Secure	2024	Europe	Tier 2 Telco
SAM Seamless Network	2024	UK	Virgin Media
SAM Seamless Network	2024	Netherlands	Ziggo
SAM Seamless Network	2024	Europe	2 contracts
SAM Seamless Network	2024	Israel	2 Tier 2 telcos
SAM Seamless Network	2024	Latin America	Tier 2 telcos

Source: HardenStance

Those driving RDK-B and prpl are trying their level best to at least align, if not quite converge, the two as much as possible.

The impact of two open source home router ecosystems: Competing open source ecosystems can drive investment and innovation - but they can also hinder it. Pointing to either prpl or RDK-B as the 'Android' of the home networking market is a good analogy. But pointing to competition between the two as beneficial the way competition between Android and iOS is beneficial is less convincing. For one thing, prpl and RDK-B target a market that's worth a few billion dollars a year in sales; Android and iOS drive a market worth annual sales in the hundreds of billions. Moreover, prpl and RDK-B are both open source operating systems; in the mobile OS world there is only one big open source ecosystem – Android; iOS is proprietary.

As mentioned, prpl and RDK-B do originate from cable operator and telco ecosystems that use different technologies. In terms of duplication between the two, it's a fact of life that has to be dealt with. Fortunately, those driving the two ecosystems are doing their level best to at least align, if not quite converge, the two as much as possible.

For example, the Life Cycle Management (LCM) project is a key element of prpl's value proposition, providing telco customers with common high-level APIs for managing applications. Going back some time, the RDK-B and prpl communities have been working on aligning with one another on LCM's code so that a security or other application need only be developed once to be able to run in both environments. It already works well enough that Vodafone has prpl LCM integrated into its RDK-B rollout plans. Those working on the LCM project nevertheless recognize that still tighter alignment is needed.

The commitments of other big telcos: Other big telco players like BT, Telefonica, Telenor, NTT, Singtel, Telstra and Bharti Airtel have yet to go public with their choice of open source home router migration path.

Will home LAN and telco network security converge?

Ultimately, every department and every team in a telco has a stake in the security of their customers' online experience. At the sharp end of making the business case or delivering it, the number of stakeholders is fewer but there are still quite a few of them. The consumer sales and marketing teams are focused on the right-hand side of the graphic depicted in **Figure 8**. They work with endpoint security vendors and with home router and home router application vendors to deliver services, typically according to a B2B2C shared revenue model. They also work with their internal signaling security and DNS or other network security teams to integrate their value proposition into service tiers. Whether they charge for that, hence whether the underlying vendor is engaged in a B2B2C model or just serves as a B2B supplier, is more variable.

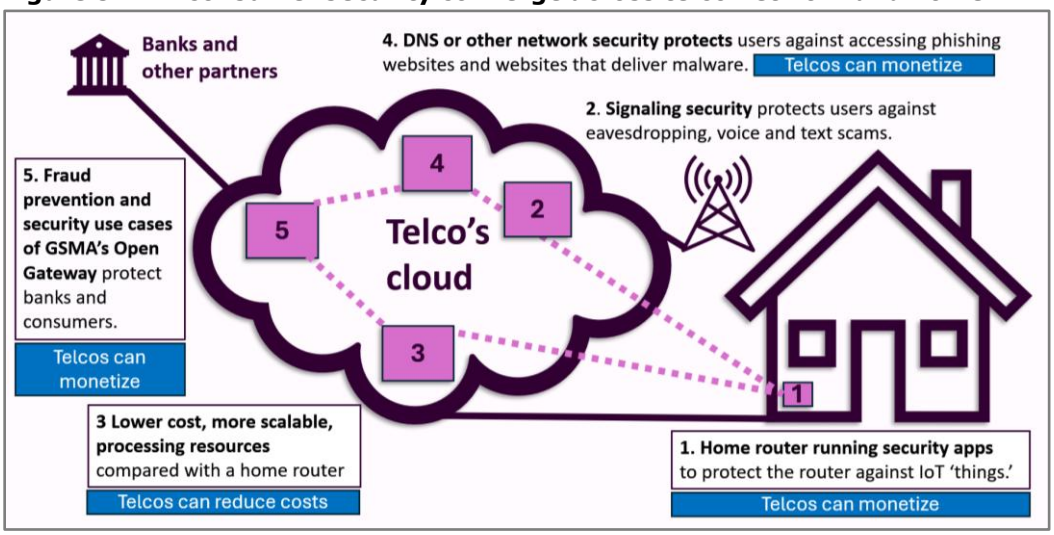
What's interesting about the future evolution of this market is the potential for convergence between the left and right sides of **Figure 8**. The telecom sector is always looking for new ways of doing the same thing at lower cost. The industry has started coalescing around the merits of using the home router in the home LAN as "the platform" for delivering new services like cybersecurity in the home. Historical precedent suggests that as these deployments begin to scale, at some point telcos and their vendors will inevitably cast their eye back into the network again. When they do they will wonder aloud whether all, or at least some, of the processing might be done more efficiently out there than on a piece of household CPE, no matter how high the spec.

At some point telcos and their vendors will inevitably cast their eye back into the network again.

Someone, somewhere, is bound to get budget approval to go and look into that. One might even speculate that approval may already have been granted. That doesn't mean it will happen; it just means the potential is quite likely to be explored. There's an additional layer to this that makes it still more interesting. Leading operators like Telefonica and Vodafone are rolling out GSMA Open Gateway's APIs. Among the lead use cases are fraud and security. This is a simple B2B model. As an example, a telco exposes its fraud-related APIs to a bank and the bank pays for access to that information. This gives the bank's customers greater confidence in the calls and other messages it sends them. By extension it also makes users more suspicious of other outreach claiming to be the bank.

This activity and monetization take place out of sight and out of mind from the telco teams working the right hand side of consumer security in **Figure 8.** But thanks to the B2B business being done over on the left, those among the telco's consumer customers that use that specific bank do nevertheless enjoy a marked improvement in the security of probably their single most critical service - and all without paying for it.

Figure 8: Will consumer security converge across telco network and home LAN?



Source: HardenStance

To flourish, any application ecosystem needs to grow and grow and grow – and then grow some more. Today the Open Gateway Initiative and both the open source home router ecosystems serve different markets and interests, according to different business models. Even allowing for the relative maturity of RDK-B, from a global perspective they are also in their formative stages in terms of becoming the 'Android in the home'.

Longer term, it's easy to see how the open source router and open gateway ecosystems are likely to start to extend out towards one another. Another relevant enabler here is the Linux Foundation's CAMARA project which refers to itself as the Telco Global API Alliance. Working very closely with the GSM Association, CAMARA has come up with APIs like the Quality on Demand (QoD) Wi-Fi API for managing downstream traffic from residential access points to a Wi-Fi connected device.

Longer term, it's easy to see how the open source router and open gateway ecosystems are likely to start to extend out towards one another.

There's certainly a debate to be had about the extent to which these different ecosystems will end up collaborating or competing (or both). But the idea that over time they continue to serve their own silos in splendid isolation from one another isn't very plausible. One or more forms of convergence looks a lot more likely.

The threat actors that want societal disruption not money

This report has primarily addressed telcos investing in – and monetizing – the protection of consumers against cybercrime and scams in particular. But there's another type of cyber threat to consumers that has – or should have – an increasingly high profile among telcos. This is the threat posed by large scale cyber-attacks. These come from threat actors – usually hacktivists or nation state threat actors - that are motivated less by financial gain and more by provoking disruption or even chaos in an adversary country.

As described below, the October 2023 cyber-attack on Windstream Communications in the U.S. was unprecedented in its impact. Back in 2016, Deutsche Telekom suffered a major outage of 900,000 home routers during the WannaCry outbreak. But in the case of Windstream, the ISP was not even able to update the impacted devices and get them back online as DT was able to do. All 600,000 SOHO routers used by Windstream customers were completely destroyed and had to be replaced.

The Windstream attack should serve as a call to arms to better protect consumer routers from a cybersecurity perspective, not just manage them from an asset management perspective. Cybersecurity software agents that can run on top are the icing on the cake of a layered approach to home router security. But there are a lot of basic fundamentals at the telco management layer that should also be in place. Shared credentials shouldn't be allowed. The opening and closing of ports should take full account of cybersecurity risk. Executing a remote reboot across a fleet of managed routers can rid devices of memory-resident malware.

Malware destroyed 600,000 SOHO routers in October 2023

A U.S. ISP – cited by Reuters and Recorded Future as Little Rock, Arkansas-based Windstream Communications – saw 600,000 Small Office Home Office (SOHO) routers destroyed by malware in October 2023. This was the most serious, large scale, attack on SOHO routers to date According to the originating research report from Lumen Technologies' Black Lotus Labs, the source of the attack was a malicious firmware update that deleted some of the routers' operational code, rendering the devices inoperable. There was no way of fixing them. They all had to be replaced.

The researchers identified "Chalubo", a commodity remote access trojan (RAT), as the primary payload behind the attack. They stated that it "employed savvy tradecraft to obfuscate its activity; it removed all files from disk to run in-memory, assumed a random process name already present in the device; and encrypted all communications with the command and control (C2) server."

Hardening security policy at the network level helps but this still leaves telcos and their customers vulnerable to flaws in the fundamental design of home router CPE itself. Arguably the biggest risk is the legacy of home router firmware that is only updated infrequently, at high cost, or not at all.

Telco requirements for a more frequent cadence of application software updates, and the full stack testing that goes with it, can pose increased risk to the stability of home router firmware. That's where open source home routers can help via the decoupling of application software from the rest of the stack. They allow more frequent application software updates. Crucially, they also allow home router vendors to focus on their core functionality and release fewer times a year than the legacy proprietary model would require them to.

Vendors interviewed for this report shared that by and large, home router vendors themselves are becoming more software-oriented now. That promises progress, albeit not necessarily at a fast enough pace. The open source RDK-B and prpl models are accelerating this positive trend. Every new application or service runs in its own container and work is ongoing in both communities to control access to sensitive system resources via APIs.

The attack on Windstream invites greater government engagement in ensuring consumers' homes are protected from cyber threats.

Silent stakeholders have additional resources to tap into

Only a small minority of telcos provide 100% coverage of network-based security across their subscriber base. Only a small minority are at more than a few percent user adoption of endpoint security offerings. And while RDK-B has driven very high adoption in North America, adoption of home router security agents elsewhere is very low.

As is implied by telcos spending less than half a billion dollars a year on augmenting consumer security, the investment going into this market is more of a trickle than it is a flood. Employers and governments are motivated to spend on improving consumer security but they are currently too removed from the way investment decisions are made to have much impact. As outlined below, more could potentially be done to engage them and tap into those potential sources of funding.

Tapping into funding from government

The attack on Windstream invites greater government engagement in ensuring consumers' homes are protected from cyber threats. Up until this point, and as shown throughout this report, most regulatory mandates to protect consumers have been at the network layer to protect against things like exposure to age inappropriate content or malicious websites. But it's not inevitable that government regulation ends here – especially if other telcos experience attacks like the one Windstream suffered.

In recent years telcos have come under increased pressure to improve cybersecurity because they are a key element of critical infrastructure, at the heart of the digital economy and society. Not unreasonably, what goes with that is a tendency to prioritize the core of the network first and the edges of the network like home routers second.

An attack of the kind Windstream suffered just over a year ago asks an important question: just how 'secondary' should the prioritization of home networks be? To put hypothetical numbers to it, suppose that just 3 people per device are dependent on 600,000 SOHO routers that get wiped out like that. That's 1.8 million users whose access to healthcare or other critical services is suspended. Suppose the cost of replacing all those routers is just $100 per unit. With 600,000 devices, that's a total replacement cost of $60 million. These are numbers that gain the attention of a telco CEO and CFO. Where an attack like this is carried out by a nation state threat actor – and a nation state threat actor was a prime suspect in the Windstream attack judging by the quality of the tradecraft used – these are numbers that also gain the attention of a country's national security and law enforcement authorities.

Signs of a new trend beginning to form – the proposed ROUTERS Act

There are signs of this trend beginning to form. Unsurprisingly, it is starting in the U.S. On Monday January 27th 2025, Senators Marsha Blackburn (Republican-Tennessee) and Ben Ray Luján (Democrat - New Mexico) introduced a new bipartisan bill. The Removing Our Unsecure Technologies to Ensure Reliability and Security (ROUTERS) Act has as its objective better protection for "tens of millions of families and small businesses across the country [who] use wireless routers as their primary access point to the internet."

The Routers Act would require the Department of Commerce to conduct a study of the national security risks posed by routers, modems, or other devices that are designed, developed, manufactured, or supplied by persons owned, controlled, or subject to the jurisdiction of U.S. adversaries. One might reasonably contest aspects of the bill. For example, any such study should address the need for better security of all SOHO products, irrespective of whether or not they meet the potentially malign foreign influence criteria specified. But at least it's a start – and an indication of the potential direction of travel that some legislators and governments are likely to want to take.

Employers and governments are obvious potential sources for driving additional investment.

Tapping into funding from employers

An enterprise security team can protect its organization's own assets in its own network and on an employee's company-issued devices. But a CISO would rest easier if they could rely on another layer of home router security to protect an employee's laptop against cyber threats emanating from their fridge, TV, and doorbell when they're working from home. Crucially there is bound to be some amount of willingness to contribute funding to that on the part of employers.

We don't yet have a workable brokerage model that a business can go to and pay for an employee's cybersecurity upgrade at home, irrespective of which telco in the local market that employee happens to subscribe to. Maybe it's time to find one.

Certainly, if stakeholders in consumer security want to see an acceleration of investment, employers and governments are obvious potential sources for driving additional investment beyond what telcos and consumers themselves are currently willing to spend.■

About Bitdefender

Bitdefender is a global cybersecurity leader specialized in providing best-in-class threat prevention, detection, and response solutions. With over 20 years of experience, the company has built its reputation as an expert in the field by safeguarding millions of consumers as well as enterprise and government environments.

Bitdefender is a trusted partner for telcos worldwide, providing comprehensive subscriber protection solutions. These include versatile router and IoT protection, advanced network security and award-winning endpoint protection designed to secure every aspect of customers' digital lives. By providing all-inclusive tailored solutions that enhance user experience, and integrate AI to combat evolving cyberthreats, Bitdefender helps telcos strengthen their competitive advantage and drive business growth.

For more information about Bitdefender's solutions for telcos and manufacturers please visit: https://www.bitdefender.com/partners/subscriber-protection-platform.html

Additional Reference Materials

- Bitdefender's "2024 Consumer Cybersecurity Assessment Report"
- Bitdefender's "Cybersecurity Trends Among Telco Customers in the U.S (Sept 2023)"

- HardenStance's "Telco Strategies for Consumer Security (January 2024 edition)

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.