No.88
February 2026

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/ SPONSORED

Telco Strategies for Consumer Security

Sponsored by Bitdefender, Cujo AI, Enea, Infoblox and PowerDNS

For the third year running, HardenStance spent the 4th quarter of last year researching the 'what?', 'how?' and 'why?' of telecom operators around the world bringing better cybersecurity to consumer online experiences, devices and households. The vendors interviewed were sponsors Bitdefender, Cujo AI, Enea, Infoblox and PowerDNS and non-sponsors Akamai, Allot, Efficient IP, F-Secure, Gen Digital, SAM Seamless Network and Whalebone. As last year, McAfee and ESET were invited to contribute but declined.

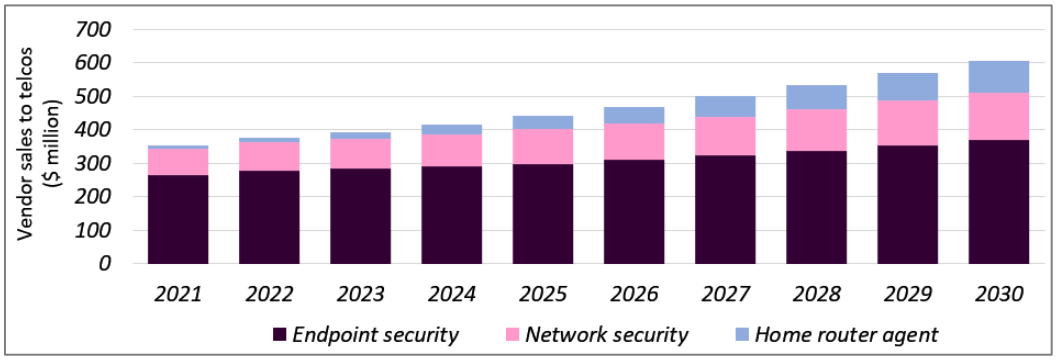
- The Global Anti Scam Alliance (GASA) estimates the global annual cost of scams at $442 billion. In 2025, HardenStance estimates that telcos around the world spent $441 million on consumer security software spanning endpoint security, home router security agents and network-based security.
- Vendors reported 38 new telco contracts for DNS security, 16 for endpoint security and eight for home router security agents during 2025. Half the DNS security contracts were awarded by telcos in Africa, the Middle East, Latin America and Asia.
- In 2026, we should finally see open source prpl home routers being commercially deployed at scale, most of them with security agents. In the meantime, the alternative, more mature, RDK-B ecosystem is extending its commercial footprint from North America into Europe, driven by Deutsche Telekom and Vodafone.
- Future evolutions of telco consumer security strategy will be driven by tighter integration and orchestration across today's security product silos. Telco network firewalls should be included in discussion around these future architectures.

In 2025, vendors reported 38 new telco contracts for network-based security, 13 for endpoint security and eight for home router security agents.

Telco spending on consumer security is growing

HardenStance estimates that telcos around the world spent around $441 million on consumer security software in 2025. 68% of this spending ($298 million) went on endpoint security software. Of the total spend, 23% ($102 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 9% ($40 million).

Figure 1: Worldwide annual telco spending on consumer security software



Source: HardenStance

Total spending in 2025 was up 6% compared to 2024. HardenStance forecasts that total telco spending on consumer security software will grow at a CAGR of 6.5%, reaching $604 million by 2030. The positive take is that telco spending in this market space is set to continue growing. The less flattering perspective is that annual spending of $441 million amounts to less than 5 cents per year per person on the planet. To put it another way, this $441 million amounts to 0.1% of the $442 billion which the Global Anti-Scam Alliance (GASA) identifies as the total amount people lose to scams every year.

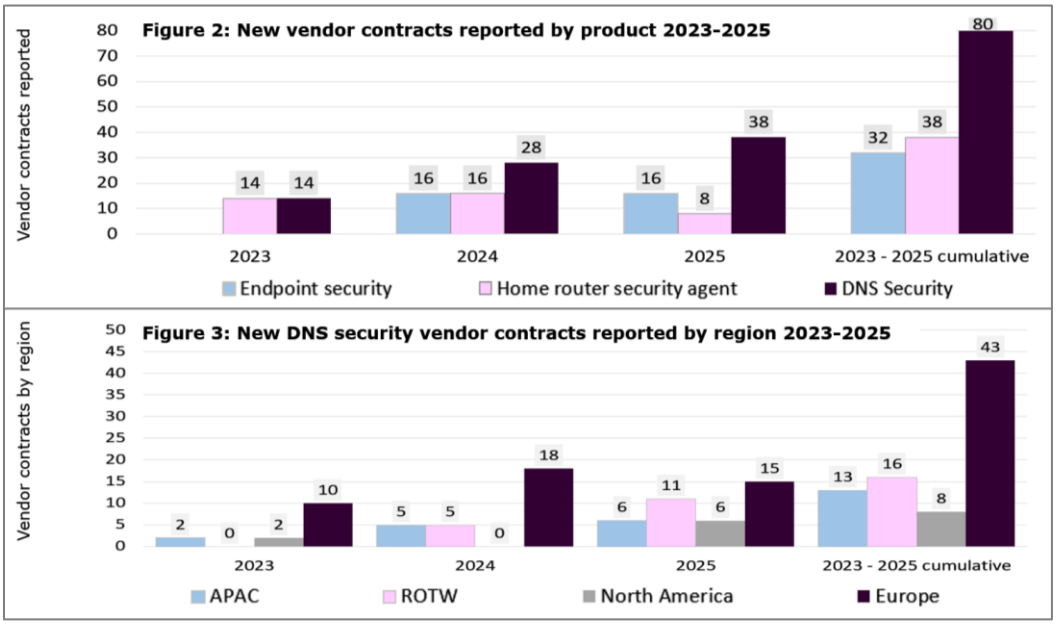
Figure 2 and **Figure 3** below show two separate cuts of the data on new contract wins that participating vendors shared with HardenStance for the previous February 2024 and February 2025 editions of this report as well as this year's edition. The data has some limitations which are set out in the Appendix on page 22. Taking full account of those limitations, the data still holds two significant and related insights about the direction of aggregate telco spending on consumer security worldwide.

The positive take is that telco spending in this market space is set to continue growing. The less flattering perspective is that $441 million amounts to less than 5 cents per year per person on the planet.

- **Figure 2** demonstrates that many more telcos are making new spending commitments to DNS or network-based security than are making new commitments to endpoint security or home router security agents. Cumulatively over the last 3 years, telcos have signed more contracts for DNS security than they have for endpoint security and home router based security agents put together.
- **Figure 3** demonstrates the marked acceleration in spending commitments to network-based security spending by telcos across Africa, the Middle East and Latin America (grouped in the single 'Rest of the World' category) as well as in Asia Pacific. Telcos across all these regions accounted for 17 new contracts for DNS security reported during 2025 – compared with 21 reported for European and North American telcos.

These datapoints are discussed in a lot more detail in the network-based security section that starts on page 12.

Figures 2 & 3: Cumulative data spanning the 2004-2026 editions of this report



Source: HardenStance

Scams are top of mind among consumer threats…

Scams continue to be the type of cyber threat that consumers are most aware of and most concerned about. **Figure 4** provides some important new data on how consumers around the world are actually experiencing, dealing with, and recovering from scams and scam attempts. The data is from a global survey of consumers commissioned by the Global Anti-Scam Alliance.

The GASA survey findings point clearly to consumers throughout the world continuing to be highly vulnerable to scams. It's clear from the findings that industry, regulators and law enforcement need to do much better at protecting consumers at every layer of the ecosystem. The telecom sector represents just one of those layers, albeit the one with unique reach and touch points into the consumer market.

…but there's a lot more to consumer threats than scams

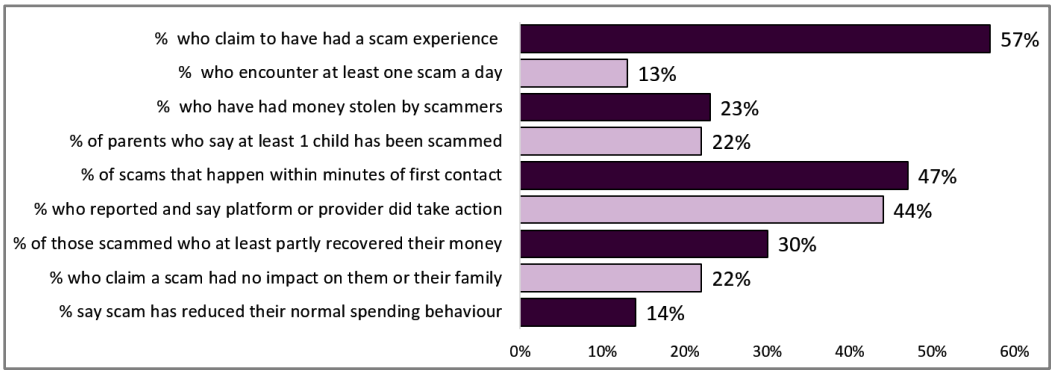
As disproportionately important as they undoubtedly are, the high profile of what is now routinely called a 'global epidemic' in scams can risk overshadowing the other types of cyber threats consumers face. The left hand side of **Figure 5** on page 4 depicts the primary types of threats and the types of individuals that carry them out. These include:

The voyeurism-as a-service criminals were charged for live streaming the private moments of Italians in retail fitting rooms, swimming pools and at home.

Targeted surveillance: In some countries, high-profile business leaders, politicians, journalists, and NGO workers have been at risk from foreign as well as domestic law enforcement and national security agencies for many years. But people from all walks of life – especially women – are also vulnerable to cyber stalking. This can be from current or former romantic partners, acquaintances, or even people they don't know. Determined cyber stalkers don't need to have the skills to carry out the surveillance themselves – they can hire these services from the darknet. Importantly, cyber-based surveillance techniques also enable real-world physical attacks, not just cyber-attacks.

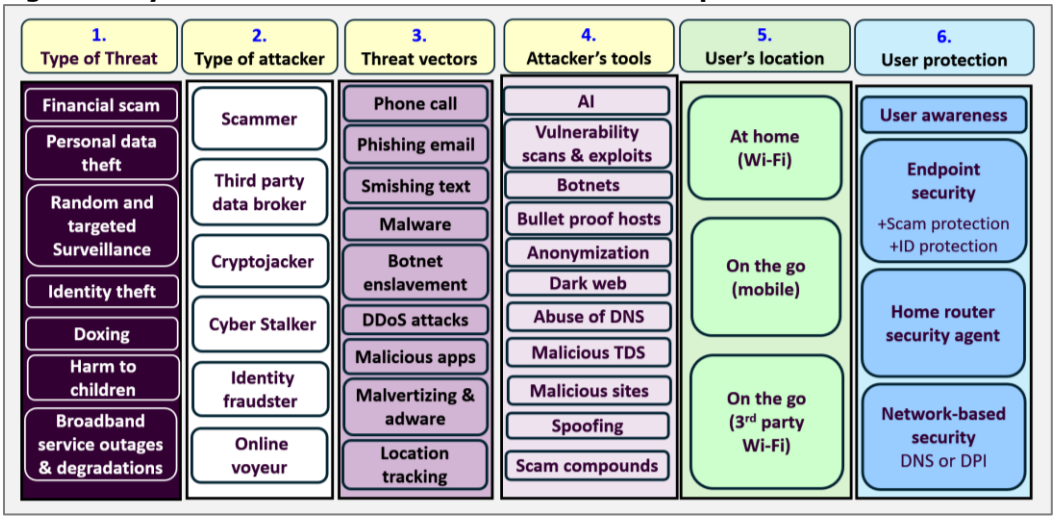
In their own homes, consumers can also be exposed to random surveillance, without even being aware of it. The risk of the angle of a home camera surveying the comings and goings at a neighbour's property is a relatively well known example of home cameras being misused or abused to violate peoples' privacy. But there are greater risks than this. In June 2025, a Milan court sentenced five men to prison for running a 'voyeurism as-a-service' business. They scanned the Internet and obtained access to tens of thousands of live video camera feeds throughout Italy. These cameras all had factory default credentials or other weaknesses. The criminals were charged for live streaming the private moments of Italians in retail fitting rooms, swimming pools and at home. Subscribers shared clips on social media with degrading comments and location tags.

Figure 4: The User's Experience of Scams in 2025



Source: Global Anti Scam Alliance (GASA), Global State of the Scams, 2025 based on a survey of 46,000 consumers across 42 markets between March 7 and March 20, 2025.

Figure 5: Cyber threats to consumers and available protections from telcos



Source: HardenStance

Doxing: This is the release of private images or other information about someone online without their consent with intent to humiliate them or otherwise harm their reputation. A doxing victim may have willingly shared their private information without consenting to share it. But doxxers can also steal a victim's private information by accessing their devices or accounts without their authorization or from a third-party source.

Many of the world's largest botnets are comprised mainly of infected smart home devices.

Cryptojacking: this entails vulnerable devices being exploited and enslaved in botnets so that the device's processing power is 'hijacked' for cryptocurrency mining. Many of the world's largest botnets are comprised mainly of infected smart home devices. Certainly some consumers don't notice this. But even though they typically don't know they're the victim of a cyber-attack, many users do notice the impact in terms of degraded quality of service on their home LAN. This can drive customer churn, especially among advanced users such as video game players.

Latest trends in threat actor TTPs

The middle two columns of **Figure 5** depict the main Tactics, Techniques and Procedures (TTPs) that are used by threat actors to target consumers. The cybercrime ecosystem that operates on the dark web is remarkably complex and sophisticated. It can now be considered a highly optimized ecosystem or value chain featuring specialized providers of different cybercrime services. The barrier to entry has been markedly lowered by this specialization among cybercriminals. Instead of building all the components of an attack themselves, scammers and others who actually launch the campaigns can buy in each of the modules they need. They buy them from specialist dark web providers operating at scale, lowering the cost and ease-of-use of each service.

This section provides the latest on four key components of the modern cybercrime ecosystem, how scammers and other threat actors are weaponizing them, and some of the challenges of defending against them. They come under these four headings:

- Scam compounds drive scam income to as much as 68% of GDP
- Beyond 'cyberslop' – weaponization of AI against consumers
- Despite major takedowns, botnet activity is still increasing
- Abuse of DNS and Traffic Distribution Systems (TDS) models

Scam compounds drive scam income to as much as 68% of GDP

Scam compounds, where operatives are often lured with the promise of legitimate work only to be effectively enslaved by gangsters, have become a major feature of the threat landscape in recent years. Cited in The Guardian, on December 2 last year, Jacob Sims, visiting fellow at Harvard University's Asia Centre and an expert on transnational and cybercrime, stated that in the past five years scamming has mutated from "small online fraud rings into an industrial-scale political economy."

Citing data from the U.S. Institute of Peace, UNODC and the World Bank, the same article estimates that at $15.3 billion, scams accounted for 23% of Myanmar's GDP of $66.8 billion. Cambodia's $12.8 billion in scam income is reckoned to be worth 30.2% of its GDP of $42.3 billion. And at $10.9 billion of a total of $15.8 billion Laos' income from scams is estimated at 68.5% of GDP.

High-profile crackdowns have a mixed record. Much of the reporting of last year's supposed crackdown by Myanmar's military junta on the notorious KK Park scam compound on the Thai/Myanmar border was highly sceptical. The performative-looking release of film footage showing compound buildings being blown up is one reason. There has also been very little evidence of any subsequent action taken. It remains unclear who exactly has been running and profiting from KK Park. Besides the Junta itself, speculation points to Buddhist militia, Chinese Triads and other South-East Asian organized crime gangs. Since scam compounds are so lucrative, corrupt governments in poor countries will always be tempted to turn a blind eye to them. And they will always have the option to outsource their operation to proxies.

Cambodia's $12.8 billion in scam income is reckoned to be worth 30.2% of its GDP of $42.3 billion.

Beyond 'cyberslop' – weaponization of AI against consumers

Last year Kevin Beaumont, a leading cybersecurity practitioner and influencer, coined the term 'cyberslop' to describe how some vendor marketing and media reporting on the use of AI by cybercriminals is breathless and exaggerated, even misleading. The following three examples are not cyberslop. They align with the UK National Cyber Security Centre's (NCSC's) AI risk assessment published last year (see page 23). These examples also reflect specific cyber threats targeting consumers.

1. **More convincing phishing campaigns at scale**: Gen AI is being used to improve the quality of language and phrasing of phishing messages; embed it into scraping workflows that search and combine the personal information of individuals to target them with spear-phishing; and to augment polymorphic phishing for even faster automation in the creation and distribution of phishing messages.
2. **Convincing and complex deepfakes**: According to an estimate by Deep Media, cited by the UK government's Accelerated Capability Environment (ACE) in February 2025 and a European Parliament Briefing in July 2025, the number of AI-generated deepfakes shared online was expected to grow from half a million in 2023 to 8 million in 2025. Determining whether to block these or not is increasingly challenging. Some deep fakes are malicious; others are harmless fun. But some now combine minutes of real footage with just a few seconds of fake footage spliced in.
3. **More effective vulnerability research and exploit development**: As shown at the top of the next page, the NCSC assesses that AI's greatest impact on cyber threats will be augmenting vulnerability research and exploit development. This directly affects consumers. Cheap consumer IoT devices, including many home routers, are the devices most exposed to software vulnerabilities. Moreover, householders can't reasonably be expected to keep up with patching these vulnerabilities themselves.

The UK NCSC's assessment of AI's impact on cyber threats

In its May 2025 report, "Impact of AI on cyber threat from now to 2027," the UK's National Cyber Security Centre (NCSC) shared its assessment of the impact of AI on cyber security to date and the most significant uses of AI threat actors will make in 2026 and 2027. Specifically the reported stated:

- "Cyber threat actors are almost certainly already using AI to enhance existing tactics, techniques and procedures in victim reconnaissance, vulnerability research and exploit development, access to systems through social engineering, basic malware generation and processing exfiltrated data."
- "The most significant AI cyber development will highly likely come from AI-assisted vulnerability research and exploit development that enables access to systems through the discovery and exploitation of flaws in the underlying code or configuration."
- "AI will almost certainly continue to make elements of cyber intrusion operations more effective and efficient, leading to an increase in frequency and intensity of cyber threats."

Despite major takedowns, botnet activity is still increasing

Consumers suffer from malicious botnet activity in many ways. The malicious messages they receive, and the cryptojacking malware that makes its way onto their home networks, are often launched by botnets. At the same time, botnets are themselves made up of millions of compromised devices – and the majority of those compromised devices are often infected smart devices in the home. So as well as being a target of threats, consumers are also the enablers of cyber-attacks on other people due to their own smart home devices being part of a botnet, usually without them even realizing.

Once the enslaved devices were disconnected from RapperBot, Aisuru and other botnets re-compromised those devices almost immediately.

There have been high-profile takedowns of botnets and arrests of criminals operating them. However, the evidence suggests these takedowns may be doing nothing more than capping their growth rates. That's in part because some botnets are engineered for redundancy, making them very resilient at recovering after a temporary pause in activity. Once a botnet is disrupted and devices are disconnected, devices that were compromised may still be insecure and exposed to enslavement by another botnet. As an example, the Aisuru botnet expanded its footprint immediately following the takedown of another large botnet, RapperBot last summer. Once the enslaved devices were disconnected from RapperBot following intervention by law enforcement, Aisuru and other botnets re-compromised those devices almost immediately.

Available evidence points to sharp peaks and troughs in indicators of botnet activity. But the overall trend over time still seems to be upwards:

- **Spamhaus spots a spike in botnet activity during 2025.** Spamhaus, the non-profit global provider of anti-spam blocklists, researches and publishes its botnet threat report at six-month intervals. For each of the three six-month periods covering July 2023 to December 2024, Spamhaus reported declines in the total number of botnet command and control servers or botnet controllers it counted worldwide. These six-monthly declines amounted to 9%, 6% and 4%, respectively. More recently, however, this encouraging trend went into reverse. For the six months to June 2025, Spamhaus reported a count of 17,258 botnet controllers. This was up 26% from 13,720 in the six months to December 2024.
- **Botnet scanning events increased in 2024 compared with 2023.** In its Sensor Intel survey conducted in partnership with Efflux, F5 Labs observed that scanning events probing for open ports, misconfigurations and Common Vulnerability Exploits (CVEs) were down 7% to 5.1 million in 2023 compared with 5.5 million in 2022. However, this then spiked sharply upwards to 8.7 million scanning events in 2024.

Abuse of DNS and Traffic Distribution Systems (TDS) models

According to CISA, 90% of cyberattacks involve DNS interactions. Most registrars carry out little if any scrutiny of who wants to register domains and why. Its versatility allows DNS to be abused for a variety of attacks like phishing and malware distribution and for C2 communications for continuous updates and control over assets under an attacker's control. This makes DNS a key tool for threat actors as well as a key intelligence source. In its recent threat intelligence reports, Infoblox, a sponsor of this report, put numbers on the automation of malicious DNS domains at scale and the use of other malicious infrastructure. Examples include:

- **Specialized infrastructure-focused threat groups cycle through huge numbers of DNS domains to meet growing demand from their clients.** These groups continuously register, activate, and deploy massive numbers of new domains so that their clients' attack campaigns can overwhelm and evade detection controls.
    - During Q4 2025, Infoblox discovered 7.6 million new malicious domains. Of these, 119,000 – anywhere from 3,000 to 10,000 per day – were zero day DNS domains. These are new domains that have never been queried before. None of these persisted for longer than 72 hours. During Q4, Infoblox also reported an average of 11,000 new domains per day that are bulk registered by threat actors using Random Domain Generation Algorithms (RDGAs) to manage command and control servers. Its threat research team also saw an average of 245 new lookalike domains per day. These are used to impersonate real brands. In its 2025 threat intel report, Infoblox said it had identified 100.8 million newly observed domains (second-level domains) in the previous 12 months.

Specialized infrastructure-focused threat groups cycle through huge numbers of DNS domains to meet growing demand from their clients.

- **Malicious actors are building their own Traffic Distribution Systems (TDS) on a greater scale - and for more malicious activities - than previously understood**. As well as the legitimate use of TDS to leverage contextual user data and intelligently route traffic for load balancing, content delivery and ad tracking, the same types of systems have long been used to drive 'nuisance ware' like advertising pop ups. Infoblox research has found that threat actors are building TDS-like infrastructures to drive users to malicious sites at scale. In its 2025 threat report, Infoblox said it had discovered over 1 million domains used by 168 malicious adtech operators within their TDS infrastructure. 82% of all Infoblox's customer networks queried domains that were part of TDS. The company states that much of this is "operated by malicious adtech operators known for concealing harmful content, such as tailored phishing sites, scareware, scams, and infostealers."

Three user contexts to protect – and three security solutions

The two columns on the right of **Figure 5** are the core focus of this report. Column 5 highlights a telco's perspective on the three main networking contexts in which a consumer needs protection:

- at home, on their home Wi-Fi network;
- on the move, on the mobile network;
- and on the move, on third-party Wi-Fi networks.

Column 6 highlights the three product types that telcos have at their disposal for protecting consumers across these three contexts - endpoint security, network-based security and home router security agents. The next three sections share the findings of this year's report. These arise from discussions with vendors that are selling into each of these market spaces. These next sections provide the market forecast for each product segment and new telco contract wins in 2025 as reported by participating vendors. Each section also provides analysis and insight into the key market and technology trends that are in play with respect to each segment.

A low growth outlook for endpoint security

HardenStance's forecast for telco spending on endpoint security is unchanged. We expect the market will grow from $298 million in 2025 to $368 million in 2030. Our forecast continues to be heavily influenced by F-Secure's consistent mid-single digit CAGR forecast for consumer security in the mid-to long-term. F-Secure has many more telco accounts than any other endpoint security vendor and reaffirmed in February 2026 that it expects growth amongst its partners (primarily telcos) to drive that growth. HardenStance has not seen any other public financial information or received any informal vendor guidance that would justify a more bullish outlook. HardenStance expects the share of total spending on consumer security software that telcos allocate to endpoint security will decline from 67% in 2025 to 61% by 2030. This share will go to increasing spend on home router security agents.

While large tier 1 telcos continue to generate good revenue and margins from reselling endpoint security and embedding it in their own consumer apps, many others are still finding it challenging to make the business case stand up. In many markets, cost is still a barrier for most consumers. Having to download, install and pay attention to an endpoint security client is another barrier. Built-in endpoint security from big providers like Microsoft and Apple is often considered 'good enough' too. And endpoint security doesn't protect against the growing risk from IoT 'things' in the home.

F-Secure and Bitdefender reported nine endpoint security contracts with European telcos between them, while Gen Digital reported another two.

The overwhelming majority of telco spending on endpoint security continues to be in North America and Europe as well as a subset of choice markets in Asia Pacific. Europe remains easily the most dynamic region, by virtue of its maturity and the sheer number of operators. **Figure 6** captures the state of the market quite well. F-Secure and Bitdefender reported 9 endpoint security contracts with European telcos between them, while Gen Digital reported another two. F-Secure also reported 3 new deals in Asia.

Figure 6: Telco contracts for endpoint security in 2025

Date	Date	Operator	Country/Region
2025	Allot	1 telco	Europe
2025	Bitdefender	SIA TET	Latvia
2025	Bitdefender	Three UK	UK
2025	Bitdefender	Drei Austria	Austria
2025	Bitdefender	IPKO	Kosovo
2025	F-Secure	Softbank	Japan
2025	F-Secure	Orange Group	France
2025	F-Secure	Lyse Tele	Norway
2025	F-Secure	Valoo	Finland
2025	F-Secure	CelcomDigi	Malaysia
2025	F-Secure	VNPT	Vietnam
2025	F-Secure	2 Tier 2 contracts	Europe
2025	Gen Digital	A1	Austria
2025	Gen Digital	Sky	UK
2025	Gen Digital	Omantel	Oman

Source: HardenStance
(McAfee & ESET were invited to share telco contract but didn't respond)

The North American market appears to be pretty stable with most operators seemingly sticking with their current vendors. Participating vendors reported no new endpoint security wins at all in Latin America or Africa. Just one was reported in the Middle East (Oman). For endpoint security vendors there's clearly more money in displacing one another in mature European markets than in targeting developing markets. This year's research leads us to conclude that after F-Secure, the other two leading players by market share with telco customers are Bitdefender and Gen Digital. As last year, ESET and McAfee both declined to be included in this research.

These days endpoint security comprises much more than traditional antivirus and VPNs. It also includes other modules. Most important among these is scam protection. Endpoint security vendors now look to differentiate around user experience notification and alerting or blocking against social engineering patterns that follow users across SMS, email, social media, voice and other platforms and applications. Vendors are increasingly centring their value propositions on this at least as much as on malware detection. They are also seeking to differentiate on ease of use.

Self-interest is driving the financial services sector to mount an increasingly credible challenge to telcos as the provider of choice for consumers buying endpoint security.

A good example of the R&D effort that typifies this direction in vendor roadmaps is Bitdefender's use of AI honeypots to lure scammers into engaging with fake AI individuals. This is to lure them into sharing their tactics, techniques and procedures (TTPs). This could be a more valuable AI use case for protecting consumers than just wasting a scammer's time such as with 'Daisy', the very confused 'AI-generated Grandma' that O2 developed and subsequently promoted awareness of during 2024.

Can scam protection features drive faster adoption?

The pivot towards scam protection is undoubtedly the right one for endpoint security vendors. There is ARPU upside for telcos if they can persuade existing endpoint security users to pay extra for new scam protection features. But there is as yet little evidence that scam protection features can drive faster adoption rates among users that aren't already endpoint security customers. What is perhaps more likely to move the needle here is the marked acceleration in commitments to deploy DNS security by telcos outside Europe and North America (see **Figure 9**). If it can be shown to drive tangible consumer security improvements via a good communications campaign, a good baseline DNS security service can be a foundational first phase of a consumer security strategy in these markets. Done well, this can then make consumers more receptive to a telco's endpoint security solution when it's offered as a premium add-on further down the line.

Meanwhile, self-interest is also driving the financial services sector to mount an increasingly significant challenge to telcos as the provider of choice for consumers buying endpoint security. Many banks have to refund consumers that have been scammed and absorb those losses themselves. F-Secure and Bitdefender are both pursuing the opportunity with the financial services channel. But the vendor that is making the biggest bet in this space is Gen Digital, including via its $1 billion acquisition of mobile banking platform, MoneyLion, which was completed in April 2025.

Home router security is set to split three ways

HardenStance estimates that telcos spent $40 million on home router security agents during 2025. Users in advanced markets want protection against IoT threats arising from what is often twenty, thirty or more smart devices in the home. We expect telco spending to grow to $93 million in 2030. Whereas home router security agents accounted for 9% of global telco spending on consumer security software across the three different product types covered in this report, we expect its share to grow to 15% by 2030.

Over the three year period spanning January 2023 to December 2025, Allot, Bitdefender, Cujo AI, F-Secure, and Sam Seamless Network have reported a total of 38 telco contract wins for their home router security agents. The actual total is likely a little higher as Bitdefender did not contribute to the February 2024 edition of this research.

North America is by far the most advanced market

By any measure, North America is by far the world's largest and most advanced market. This arises from the roll-out of home routers using the opensource RDK-B home router standard dating back many years by a number of U.S and Canadian cable MSOs such as Comcast and Charter, and more recently by T-Mobile. Cujo AI is the sole supplier of security agent software to all these deployments. As of the end of 2025, Cujo AI states that its software is deployed in over 60 million households worldwide, over 90% of them in North America. The security agent isn't universally deployed in all these routers – some telcos prefer to make it optional for users rather than a default feature. Cujo AI indicates that the penetration is nevertheless very high.

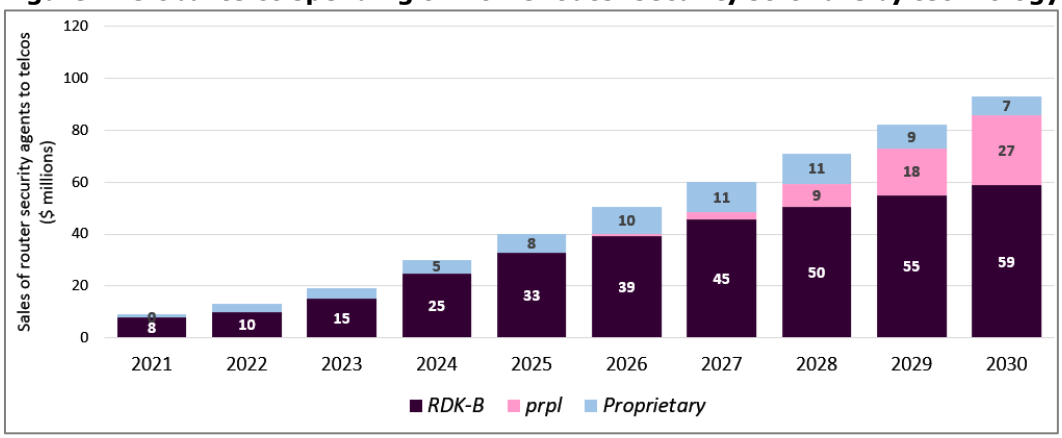
We expect 2026 will be the first year that vendors start recognizing revenue from software deployed on home routers that support prpl.

European telcos account for 20 of all the 38 new contracts for home router security agents reported over the last three years. North America and the rest of the world markets account for nine each. Vendors have only reported three contracts in Asia Pacific over the least three years. None were reported in 2025. As shown in **Figure 7**, we have segmented the home router security agent market by technology for the first time. In 2025, we estimate that 81% of home router security agent software was spent on RDK-B products, with 19% spend on proprietary platforms. We expect annual spending on RDK-B to reach $60 million in 2030. Driven by AT&T, Verizon and Orange, we expect 2026 will be the first year that vendors start recognizing revenue from software deployed on home routers that support prpl, the other open source home router software suite.

RDK-B – recent momentum and outlook

The last 18 months have witnessed deepening penetration of RDK-B in North America. T-Mobile's aggressive new roll out of RDK-B home routers serves its 5G Fixed Wireless Access (FWA) customers. Just as significantly, RDK-B is seeing significant adoption and rollout in Europe now, led by Deutsche Telekom and Vodafone.

Figure 7: Global telco spending on home router security software by technology



Source: HardenStance

Figure 8: Telco contracts for home router agent based security in 2025

Date	Vendor	Tech	Country/Region	Operator
2025	Allot	Proprietary	Europe	Tier 1
2025	Allot	Proprietary	Europe	Tier 1
2025	Bitdefender	Proprietary & prpl	United States	Tier 1
2025	CUJO AI	RDK-B	Germany	Deutsche Telekom
2025	CUJO AI	RDK-B	United States	T-Mobile
2025	SAM	Proprietary	EMEA	Tier 3
2025	SAM	Proprietary	Latin America	Tier 2
2025	SAM	Proprietary	EMEA	Tier 2

Source: HardenStance

HardenStance has seen DT's ambitious targets for the number of households covered across its European footprint, including with security agents. However it declines to share these publicly. Vodafone is rolling out commercially in the UK, Germany and other affiliates. As well as being sole supplier to Deutsche Telekom, Cujo AI is also the supplier to Sky in the UK and Italy. Other vendors in this space position around being able to support RDK-B, but for now Cujo AI seems to be the only vendor delivering security agents into telcos operating RDK-B in commercial service. Due to RDK-B's dominance among all types of commercial deployments, we conclude Cujo AI is inevitably, and by far, the global market leader by revenue in home router security agents.

At this very early stage of prpl's commercial deployment in live networks, the hierarchy in terms of best placed vendors is very different from the RDK-B ecosystem.

prpl – recent momentum and outlook

In terms of commercial rollouts, the prpl ecosystem is some way behind RDK-B. While we expect the first $1 million of sales to be registered for security agents running on prpl home routers during 2026, we expect $39 million for agents running on RDK-B. The prpl ecosystem is nevertheless moving forward. Roll outs this year will be driven by original founders AT&T, Verizon and Orange. Encouragingly, the prpl Summit in Paris in October 2025 saw KPN, TIM, Telenor and Turk Telecom announced as new members.

prpl Life Cycle Management (LCM) is already running on 12 million AT&T home gateways. Verizon is aiming to upgrade 10 million home gateways to prpl by the end of this year. Having launched prpl in Jordan last year with home gateway and Wi-Fi repeater products from SoftatHome, MediaTek and Nokia, Orange's second launch is imminent in Morocco.

At this very early stage of prpl's commercial deployment in live networks, the hierarchy in terms of best placed vendors is very different from the RDK-B ecosystem. As the supplier to Orange in Morocco, Bitdefender is set to be the first vendor to see its home router security agent deployed in a live prpl deployment anywhere in the world. As indicated in **Figure 8**, Bitdefender is also the only vendor citing a contract with one of the large Tier 1 telcos in the U.S. This is for delivering home router security agents for that telco customer's prpl deployments as well as its proprietary deployments.

There are five other vendors in this market, giving telcos deploying prpl a choice of six potential security agent vendors to choose from. Three of these other five are F-Secure, SAM Seamless Network and Allot, all of which have been active in prpl for many years. F-Secure did not have any new contracts to report for 2025. Cujo AI has announced that its prpl solution became Generally Available (GA) at the end of 2025. Nagravision, the media and entertainment technology division of the Kudelski Group that serves content creators, providers, and operators worldwide, is also entering this space with its NAGRA Scout home router security agent.

Apart from Cujo AI, other vendors supporting commercial deployments in this market space have been delivering proprietary solutions until now. The complexity and cost of this model was the driver for telcos investing in RDK-B and prpl in the first place. As shown by our forecast in **Figure 7**, we expect sales of proprietary solutions to level off and decline as RDK-B and prpl continue scaling up. In the meantime the RDK-B and prpl communities continue to seek alignment wherever possible to reduce total costs across their two ecosystems. For example, Vodafone's Wi-Fi 7-powered Ultra Hub 7 home gateway that the company launched in 2025 uses prpl's Life Cycle Management (LCM) software integrated with an RDK-B OS. T-Mobile USA also integrates LCM with RDK-B.

Accelerating growth in network-based security

HardenStance has slightly raised its forecast for telco spending on network-based consumer security software. We now think it will grow from $102 million in 2025 to $143 million in 2030. Nearly all this market consists of DNS security software driven from a telco's DNS servers to either block or advise users against accessing malicious sites. Incumbent DNS vendors typically upsell their telco customers to their security service. Some challenger vendors deploy a dedicated overlay DNS security filtering infrastructure alongside the installed base to help minimize disruption.

HardenStance has slightly raised its forecast for telco spending on network-based consumer security software.

Figure 9: New vendor wins for DNS-based network security

Date	Vendor	Country/Region	Telco
2025	Akamai	North America	2 Tier 1 telcos
2025	Akamai	Eastern Europe	2 Tier 1 telcos
2025	Akamai	Latin America	1 Tier 1 telco
2025	Allot	North America*	Tier 1 telco
2025	Allot	Panama*	Mas Movil
2025	Allot	Poland	Play
2025	Allot	Czech Republic	O2
2025	Allot	Europe*	Tier-2
2025	PowerDNS	Northern Europe	2 telcos
2025	PowerDNS	Middle East	Tier 1 telco
2025	PowerDNS	North America	2 telcos (one a Tier 1)
2025	Infoblox	United States	Tier 1 mobile operator
2025	Infoblox	Europe	Tier 1 mobile operator
2025	Infoblox	Middle East	National operator
2025	Infoblox	Africa	Mobile operator
2025	Infoblox	Southeast Asia	Mobile operator
2025	Whalebone	Africa	4 Tier 1 telcos, 1 Tier 2
2025	Whalebone	Europe	4 Tier 1 telcos, 3 Tier 2
2025	Whalebone	Asia Pacific	4 Tier 1 telcos, 1 Tier 2
2025	Whalebone	Latin America	1 Tier 1 telco

Source: HardenStance **Wins using Allot's DPI-based 'Network Secure' solutions.*

The increase in our forecast is explained by the remarkable haul of 38 new telco contracts that were signed in 2025 as shown in **Figure 9**. These were reported by Akamai, Infoblox, Whalebone, PowerDNS and Allot. Allot's 'Network Secure' solution uses entirely its own DPI or Deep Network Intelligence (DNI) while 'Allot DNS Secure' includes PowerDNS technology. **Figure 3** shows that vendors reported a cumulative total of 80 network-based security contracts over the three years from January 2023 – December 2025. This is more than the combined total of 70 contracts reported for endpoint security and home router security agents over the same period.

Historically, there have been three main issues that have made telcos hesitate to spend on DNS security. These are their own indifference to consumer security in general; the political challenges of navigating thorny net neutrality, censorship and child protection issues; and lack of confidence in detection and blocking efficacy. As the data shows, these barriers are evidently breaking down – and for the following reasons:

- **The impact of today's industrialized cybercrime ecosystem has made it harder for telcos to ignore the need - or the opportunity - to do more to protect their customers**. Whether it be in the interests of brand building, churn reduction or monetization, security has moved up the agenda of telco management.
- **Governments are becoming more engaged in finding and directing solutions as a matter of national policy**. Legislatures and governments such as in the Philippines, Japan, Singapore are at various stages of wanting to impose some form of regulatory mandate around telcos to do more. One idea being pursued is that new Protective DNS (PDNS) services should be built and dedicated to citizens rather than to the public sector or private sector businesses (as most PDNS services tend to be today). Higher prioritization by regulators tends to mean more weight is attached to cybersecurity relative to net neutrality and censorship concerns now.

It's likely that there is a correlation of some kind between strong momentum in these regions and GASA data showing developing nations losing a much higher proportion of their GDP to scams.

Of all a telco's options, network-based security is best suited to quickly meeting baseline consumer security requirements, including those stipulated by regulatory mandates. Irrespective of the relative security efficacy of other approaches, network-based security has a unique advantage in terms of rapid deployment and scalability. It allows telcos to offer some level of protection to every one of their fixed or mobile users at relatively low cost. This can be implemented either with the smallest of efforts on the part of subscribers (like opting in to an SMS prompt) or just by switching on DNS security filtering without an opt-in. Other approaches can't achieve anything like the same reach, anything like as quickly. With other approaches, a user has to buy, upload and manage endpoint security software or buy and install a new home router. Network-based security can just 'tick a box'. Both regulator and regulated can act – and be seen to be acting – to give all citizens at least some basic cybersecurity protection.

Strong contract momentum outside North America and Europe

It's noteworthy that almost half the total of 38 new telco contracts for network based security reported in 2025 were from telcos outside North America and Europe. This differentiates this product space from endpoint security and home router security agents, whose vendors report far more limited win momentum outside those two core regions. It's likely that there is a correlation of some kind between strong momentum in these regions and GASA data showing developing nations losing a much higher proportion of their GDP to scams. GASA data shows that for the U.S, Switzerland, Hong Kong, Ireland and Sweden the sums lost to scams amount to 0.2% or less of GDP. At the other end of the scale, scams account for 11.3% of GDP in Nigeria, 10.9% in Kenya, 2.5% in Pakistan, 2.1% in Malaysia and 1.7% in Saudi Arabia.

Among vendors, the disruptor in DNS security is the Czech company, Whalebone, which focuses on overlay security solutions. As shown in **Figure 9** Whalebone added another 18 telco contracts in 2025 to the 18 it reported in 2024. Half of its 18 wins were with telcos in Asia Pacific, Africa and Latin America. There is no denying Whalebone's

achievement in extending its telco account footprint as widely and rapidly as it has. That said, its competitive positioning is more nuanced than its list of contracts suggest:

- **Volume of contract wins is not an accurate proxy for market share by revenue**. A large tier 1 telco can have tens of millions of subscribers whereas a tier 2 or tier 3 ISP may only have a few million or even a few hundred thousand. This is further compounded by the fact that any one telco contract can provide for protecting 100% of an operator's end users; or it can serve a premium subset of just 10% percent of them, for example.
- **Whalebone's annual revenues are still quite small.** Whalebone has shared approximate guidance on its annual revenues for this research for the last three years. In last year's report, HardenStance estimated the company's 2024 revenues at around €10 million. Whalebone did not contest that estimate. For calendar year 2025, Whalebone states that its annual revenues grew by 41%.

Leveraging the billions of security events it sees in its AI-driven threat cloud, Cujo AI commercialized a DNS security plug-in the first half of 2025.

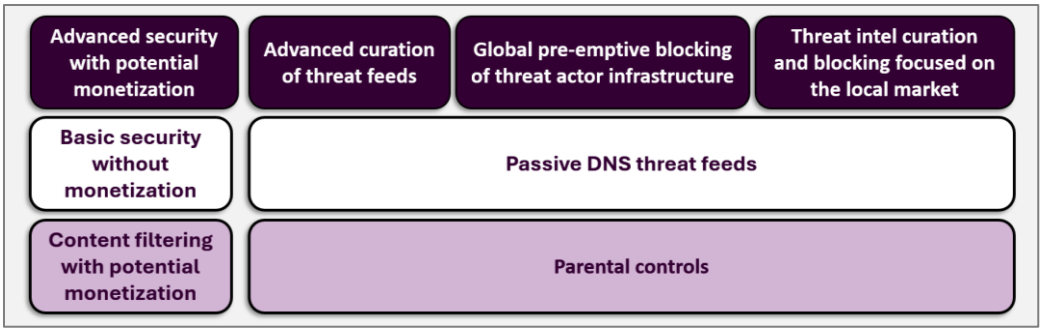
- **Incumbent DNS vendors are signing new telco deals too.** PowerDNS contributed to the February 2025 edition of this report as a non-sponsor but is a sponsor this year. Infoblox chose not to participate in the 2024 and 2025 editions but also chose to sponsor this year's report. As shown in **Figure 9**, PowerDNS and Infoblox reported five new telco account wins each for their security solutions in 2025. Having contributed to the February 2024 report, Akamai chose not to contribute to the February 2025 report but chose to contribute again for this year's report. Efficient IP also contributed to this year's report for the first time.
- **Incumbent vendors are also paying more attention to opportunities outside North America and Europe**. During 2025, Akamai and Allot each reported new contract wins in Latin America. PowerDNS and Infoblox each reported wins in the Middle East, while Infoblox also reported new wins in Africa and South-East Asia.

Other vendors in adjacent market spaces also recognize the potential of DNS security. Leveraging the billions of security events it sees in its AI-driven threat cloud, Cujo AI commercialized a DNS security plug-in the first half of 2025. This is a DNS threat feed that allows telcos and ISPs to provide a basic layer of DNS-level threat blocking to some or all of their subscribers. The DNS plug-in can be delivered independent of, or as well as, home router-based security software solutions. It can be plugged in to any telco or ISP's existing DNS infrastructure, irrespective of the DNS vendor.

Demonstrating DNS blocking efficacy can still be challenging

DNS vendors selling security filtering need to show detection and blocking capabilities that deliver superior outcomes to those enabled by baseline DNS threat feeds. These can block access to some known malicious sites but if they're not continuously updated and curated, they can allow a lot of threats to get through. That can make it difficult for telcos to justify the investment, and especially difficult to charge for it. As shown in **Figure 10** on the next page, differentiation and monetization can be achieved via three approaches to augmenting baseline DNS threat feeds. These are complementary rather than competitive. No one vendor has strong differentiation across all three.

Figure 10: Different approaches to using DNS threat intelligence



Source: HardenStance

Here's how PowerDNS and Infoblox position their treat intel offerings:

- **PowerDNS leverages raw threat intel feeds from more than 70 sources, including multiple leading security vendors and crowdsourced tools**. These represent a wide range of detection technologies such as antivirus, domain scanning, file characterization, as well as behavioural and predictive analytics. By adding proprietary intelligence rules and manually enriching them with additional context, PowerDNS targets threat detection accuracy that substantially exceeds what is available from baseline threat feeds. The weighting, configuration and composition of threat feeds can also be customized to each operator's unique requirements and those of its local regulator.

Leading telcos are considering a number of new directions in how consumer security is architected and operationalized.

- **Infoblox focuses on pre-emptively blocking access to DNS infrastructure when it sees it is owned by threat actors**, even if the infrastructure has yet to demonstrate any malicious behaviours. The company cites the specific example of a tier 1 mobile operator in Europe to whom it sold a pre-emptive security upgrade (see **Figure 9**). Infoblox states that this operator saw a 20% - 30% increase in blocking events per hour across all its subscribers after rolling out the premium service last year. The company also claims the activation saw very low false positives and no issues with customer complaints.

New directions in consumer security architecture

A subset of the world's leading telcos in advanced markets are considering a number of new directions in how future iterations of consumer security strategy could or should be architected and operationalized. This section looks at three of those potential directions:

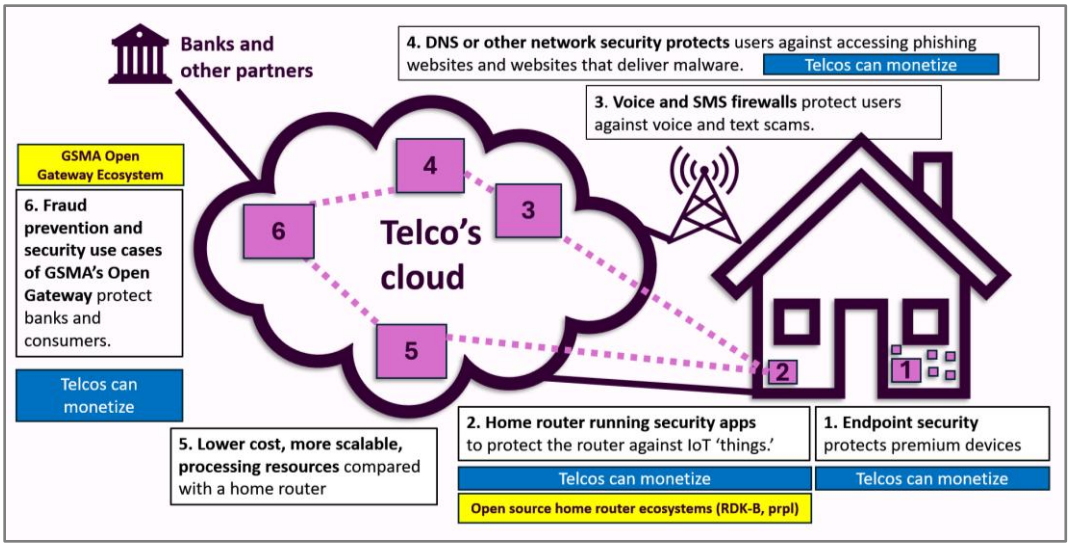
- rebalancing of processing across LAN, data center and cloud.
- seamless integration of existing siloed product offerings.
- data orchestration for user-centric security.

The three approaches are complementary rather than competitive and none are new in terms of ideas. Implementing any of them at scale would nevertheless represent a milestone in telco strategies for consumer security.

1) Rebalancing of processing across LAN, data centre and cloud

In last year's report, as depicted in **Figure 11**, we speculated that telcos would take an increasingly close look at the potential for recalibration of the balance of processing of security software across telco cloud, public cloud and home router domains. We floated the idea that telcos should look into rebalancing the share of processing away from the home router towards centralized and distributed private or public clouds. Ultimately this question comes down to control and cost of computing. The feedback from this year's research is that what is currently determined to be the optimal balance between the domains isn't shifting much. The reasons cited include greater freedom to inspect the individual user's traffic on the home LAN; higher than expected public cloud bills; the

Figure 11: Security convergence across telco network and home LAN?



Source: HardenStance

ramping up in processing power that's available in newer generations of home routers; and offloading energy costs onto the household. We do nevertheless continue to see potential for new models to evolve here. In particular, we continue to see opportunities arising from what will be a hybrid of competition and collaboration in the relationship between open source home gateways running on prpl or RDK-B and network-based solutions hosting security and fraud prevention applications running on the GSMA's Open Gateway specifications.

Such handover as there is between security products and user contexts or locations tends to be hard or indeed non-existent rather than soft.

2) Seamless integration of existing products

Today, the primary consumer security solutions that are the subject of this report are typically sold by vendors to telco customers as dedicated stand-alone products. In turn, telcos typically sell them on to their consumers as stand-alone products. At a commercial level, there is certainly some amount of integration. For example, many telcos are selling premium broadband packages that include endpoint security bundled together with network-based DNS or a home router security agent. But today there isn't much technical integration between these different products. For the most part, telcos aren't yet providing users with the assurance that they are protected seamlessly, irrespective of the device they are using and irrespective of the location, environment or context they happen to be in. Such handover as there is between security products and user contexts or locations tends to be hard or indeed non-existent rather than seamless.

This is a gap in their consumer portfolios that advanced telcos will increasingly turn their attention to. Most consumers want to understand their cybersecurity in terms that are binary rather than nuanced. They prefer to know that they either have a secure online experience or that they don't. And siloed solutions don't allow for that.

There are two main ways this could be put right.

- **Investment by individual vendors in adjacent product spaces and in integrating them.** There are examples of vendors building products in adjacent market spaces and enabling handover between the two. Last year Cujo AI launched a mobile SDK. This integrates into a telco's own customer app. This extends the security and parental controls of Cujo AI's home router security agent in the home to a household's mobile devices when connected to the mobile network. Bitdefender offers something similar that can be enabled via its own OneApp solution or embedded into a telco's customer app. PowerDNS has a DNS proxy which can intercept and filter traffic on home CPE and connect to the network service. It also

has a CPE-based collaboration with another vendor. More telcos need to buy two products from one vendor if the vendor R&D incentives are to improve here.

- **Tighter integration between partner vendors.** Some vendors featured in this report cite go-to-market partnerships with one another. For example, vendors of home router security agents tend to partner network based security vendors to give breadth of coverage in and outside the home. One or two vendors speak of strategic partnerships, but most engagements seem to be opportunistic engagements targeting just one telco account. As reflected in this report, most telco deals are for a single security product. There may be a small subset of deals that embrace two products. Even that small number likely breaks down into further subsets involving simple resale on the one hand and some amount of integration on the other. But deep integrations that resolve issues arising from each vendor's own approach to things like content characterization, error and blocking messages – not to mention commercial incentives spanning a telco and two different vendors – seem to be pretty few and far between today.

3) Data orchestration for user-centric security

For the third successive year, this report has focused on the same three product silos – endpoint security, home router security agents and network-based security for blocking access to malicious websites. In this year's report we make a start on questioning the rationale for this conventional framing. We give some initial answers, with a view to providing more informed answers next year. The initial questions are as follows:

One or two vendors speak of strategic partnerships, but most engagements seem to be opportunistic engagements targeting just one telco account.

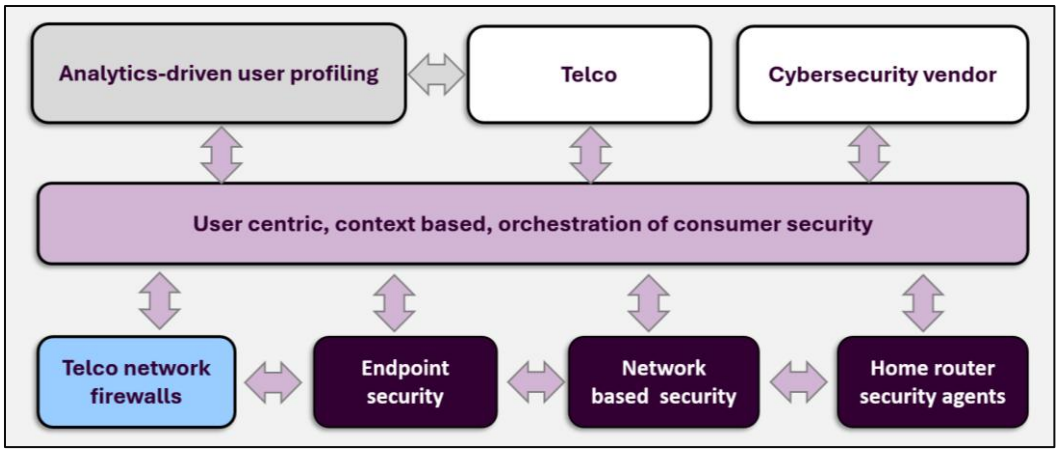
- Many telcos, typically the more advanced ones, use signaling firewalls, voice firewalls and SMS firewalls provided by vendors like Enea, Hiya and Mobileum. For the sake of simplification, let's group these products under the name 'telco network firewalls." These products can help telcos significantly reduce the risk to consumers from cyber threats and scams. So why does the market typically view these product types as separate from the other three and isolate them accordingly?
- Is there a case for tighter integration of telco network firewalls with the other three product categories? Is there a case for a new outlook around these four to supercede today's 'three plus one' outlook? And if so, what might the driver or drivers for that be, and what might such an approach look like?

Why are telco network firewalls largely ostracized today?

There are three related reasons why telco network firewalls are currently separate from the other product types. They all have to do with the legacy of telecoms as a sector that was originally exclusively dedicated to telephony to one that evolved to support data and SMS and then went on to converge with IP and the Internet.

1. This legacy is why many telcos deploy signaling firewalls to block unauthorized location tracking and espionage, nuisance or malicious voice calls and nuisance or malicious SMS texts - either because they choose to or because regulators force them to. These threats arise from flaws in the original design of legacy telecom networks. Hence the traditional expectation which survives to this day tends to be that telcos themselves should bear the cost of mitigating that risk.
2. The second reason is that the traditional use cases underpinning telco network firewalls protected the operator first and the consumer second. The first use case for SMS firewalls was to protect the operator against fraud arising from the use of 'grey routes' to bypass chargeable international routes. From a user perspective these firewalls primarily blocked SMS spam, which is more nuisance than threat. Originally, SMS firewalls didn't block messages with malicious urls embedded in them. This has changed – SMS firewall vendors block malicious urls and other

Figure 12: User-centric security orchestration for telecom operators



Source: HardenStance

threats now. This explains why SMS firewalls have traditionally been isolated from the three core product types covered by this report – but the direction their roadmaps have taken makes the case for them to be integrated more tightly now.

Telcos are already making increasing use of their own analytics around consumer contexts. For security use cases, however, they typically lack the relevant threat detection algorithms.

3. The third reason for the isolation of telco network firewalls is that due to the factors already cited, it's typically harder for telcos to charge users for the protection they provide. Whether it's by selling them as standalone add-ons or embedding them in premium service packages, the monetization path with endpoint security and home router security agents is clear. Some operators can also charge for DNS security. Thus far, however, telcos have found it a lot more difficult to charge for the protection extended by voice and SMS firewalls - either due to regulatory requirements, user expectations or competitive dynamics that make it prohibitive.

"4" beats "3+1" for more predictive, user-centric security

There are two main ways telco network firewalls can be integrated alongside the other three product types as one among four products in a telco consumer security portfolio. The first is through security orchestration at the telco level. The layered integration described on page 17 merely stitches together and extends the coverage footprint of the three primary products. Better security orchestration across all three product types as well as telco network firewalls has potential to take this a step further.

Taking account of the broadest possible range of relevant threat intelligence to drive security decisions can generate deeper, more accurate insights to protect consumers according to the sort of model that the banking sector already uses. Adopting that model can deliver better threat detection by allowing telcos to be more predictive about risks, spanning malicious social engineering patterns as well as malicious software. Key to this is user-centric security orchestration that embraces an individual or family across all the devices they use, all the contexts they are active in, and all the security tools that monitor their activity at any given moment. Telcos are already making increasing use of their own analytics around consumer contexts. For security use cases, however, they typically lack the relevant threat detection algorithms to run on that data.

Although the early uses cases for the GSMA's Open Gateway initiative centre on telcos protecting banks against fraud, open APIs allowing network data to be queried and shared by third parties can be applied to enabling user-centric consumer security too. The alternative to the telco doing the security orchestration itself in this model is for a vendor to do it – potentially one or more from among the vendors cited in this report. For the best possible orchestrated, user-centric solution, any vendor pursuing that would need to consider ingesting telco network firewall threat intelligence as well as that from any one of the three core consumer security product vendors.

Sponsor profiles

The following five companies sponsored this year's report according to a multi-sponsorship model – Bitdefender, Cujo AI Enea, Infoblox, PowerDNS. HardenStance's profiles of these companies follow below:

Bitdefender

Bitdefender is a privately held company, headquartered in Bucharest, Romania. Its heritage is in endpoint security for consumer and enterprise markets. The company has leveraged the endpoint security heritage and its threat intelligence cloud to build a home router security agent portfolio. Bitdefender has a strong direct go to market model but has accelerated its commitment to telco channel partnerships in the last couple of years in conjunction with accelerated investment in the home router security agent space.

At the start of 2024, Bitdefender already had more than 15 telco channel partners across different regions for its endpoint security portfolio. During 2025 the company announced four new endpoint security contracts, all of them with European telcos. These were with SIA TET (Latvia); Three (UK); Drei (Austria); and IPKO (Kosovo).

Bitdefender has established itself as the early market leader with a security agent for the open source prpl ecosystem.

Having scored some wins deploying security agents with home router partners like Netgear on proprietary router products, Bitdefender has established itself as the early market leader with a security agent for the open source prpl ecosystem. It has demonstrated integrations of its prpl security agent with home router vendors like Kaon, Vantiva, Zyxel and ZTE. More are planned. Marquee wins delivering security agents to a Tier 1 service provider in the U.S and those of Orange in Morocco are strong customer references. Bitdefender is also engaged in prpl's Working Groups, notably the Security, Life Cycle Management and High-Level API Working Groups. Bitdefender states that its home router security software is compatible with RDK-B and is pursuing these opportunities as well, but it has yet to break into Cujo AI's monopoly in this space.

Scam protection is at the heart of Bitdefender's roadmap investment across both its endpoint security and home router security agent portfolios. The company is investing further in its AI assisted Bitdefender Scam Protection Platform. This detects and prevents scams across web, email, SMS, chat apps, push notifications, and calendar invites. It views cross-channel correlation on threat and scam detection algorithms as essential but within that it has seen social media become a primary scam distribution vector during 2025. Hence protecting users against malicious ads on Facebook, Instagram, and TikTok that drive users to phishing pages and fake investment schemes is a particular focus area. In the case of messaging apps, Bitdefender expects that SMS will peak as an attack vector as a result of greater RCS adoption and improved carrier filtering. As scams shift to other messaging platforms like WhatsApp, this will become another key focus area. Detection and defence capabilities for voice scams including the use of voice honeypots, deepfake-enabled scams and better detection of 'fake-shops' that scam users by posing as legitimate online shopping stores will also feature.

Cujo AI

Cujo AI, headquartered in Covina, CA, USA, is a provider of cybersecurity and granular network and device intelligence software for telcos, MSOs and ISPs. The company is privately owned by Comcast and Charter Communications.

Cujo AI's core business is delivering device intelligence and cybersecurity software agents to run on routers deployed in the home as well as for businesses. The company has established itself as the world leader in home router security agents by revenue by virtue of the dominance it has established in the RDK-B market. This footprint was initially built out several years ago in North America, delivering device intelligence and then security software onto RDK-B deployments for Comcast, Charter Communications and Shaw.

It now reaches over 62 million households. During 2025 the company announced T-Mobile as an additional RDK-B customer in the U.S. Cujo AI is being deployed with T-Mobile's roll out of its 5G Fixed Wireless Access (FWA) products. Through to the end of 2025, HardenStance assumes that Cujo AI accounted for 100% global market share in RDK-B cybersecurity software agents which we estimate at $32.7 million.

The last couple of years have seen Cujo AI expand its RDK-B footprint with new telco and ISP customers in Europe. Sky, a Comcast subsidiary, has rolled out in the UK and Italy. Deutsche Telekom affiliates are selling RDK-B routers running Cujo AI software in Croatia, Germany, Poland, North Macedonia, Montenegro and Greece. As well as growing its RDK-B footprint, Cujo AI's three main growth areas centre on prpl, a mobile SDK to augment its core product and a new DNS plug-in. First and foremost, the company launched a Generally Available (GA) prpl security app at the end of 2025, enabling it to compete for business with big backers of prpl like Orange, AT&T and Verizon.

Cujo AI's three main growth areas centre on prpl, a mobile SDK to augment its core product and a new DNS plug-in.

CUJO AI has a significant footprint of OpenWRT-based platforms, including in large tier 1 operator environments. While RDK-B has been a major driver of the company's market leadership, a substantial portion of CUJO AI's deployments is built on OpenWRT-derived platforms that sit beneath proprietary, non-RDK and non-prpl management layers. This enables it to deliver device intelligence and home router security across diverse CPE software stacks.

Cujo AI recognizes emerging opportunities in the DNS security space of the kind also reported by DNS and DNS security specialists Akamai, Efficient IP, Infoblox, PowerDNS and Whalebone for this report. As described on page 14, Cujo AI offers a DNS security plug-in. This is a DNS threat feed that allows telcos and ISPs to provide a basic layer of DNS-level threat blocking. It is vendor-independent so it can be plugged in to any telco or ISP's existing DNS infrastructure.

The Mobile SDK was also launched in the first half of 2025 and integrates into a telco customer's own customer app. It extends the protection provided by Cujo AI's home router security agent in the home to a user's mobile devices when connected to the mobile network or third party Wi-Fi networks. It supports parental controls as well as cybersecurity options and is available across both iOS and Android environments.

There doesn't appear to be any interest in entering the endpoint security market. Among all the vendors selling consumer security software into telcos, Cujo AI has been a bit behind the curve in terms of looking to grow its footprint outside of Europe and North America. The momentum the company has in its core business suggests 2026 should be the year to get bolder.

Enea

Enea describes itself as a leading provider of signaling firewalls and SMS firewalls. Its voice firewall that protects against malicious CLI spoofing, Flash and Wangiri calls, is built on the company's core signaling and messaging security platform. This allows for correlation of voice and signaling traffic for threat detection in the same platform.

In the context of this report, Enea can be considered a leading provider in the telco network firewall category. As such the company is in a position to capture the opportunities presented by trends that evolve in the direction of user centric telco security orchestration as set out on pages 17-18.

Infoblox

Infoblox is a privately held company. Moodys estimates its recorded revenues were $938 million for the year to July 2025. Infoblox is the world's largest pure-play provider of DDI (DNS, DHCP and IP address management) hardware and software solutions. It counts the majority of Fortune 100 companies among its 13,000 customers world-wide, of which 2,000 are cloud customers.

Infoblox has a differentiated approach to threat research and intelligence with security sales into all customer segments. The company's global footprint gives it access to more DNS-related threat data than any comparable DDI or DNS focused solutions vendor. That's not sufficient to assure high quality outcomes but it is a good starting point.

Use of threat intelligence to pre-emptively block access to malicious domains before they are even activated for use in a campaign is central to Infoblox's approach. Once Infoblox identifies that a given set of assets is owned or controlled by a cybercrime group it can exercise the option of blocking access - even if those assets are not yet behaving maliciously. If this is done well, taking full account of the risk of disruption to legitimate services if the intelligence turns out to be wrong, risk can be reduced further compared to traditional approaches that rely on blocking sites that have already acted maliciously.

Infoblox is looking to drive synergies between its service provider channel and its government business.

When it comes to targeting opportunities to help telcos leverage DNS security for consumers, Infoblox is looking to drive synergies between its service provider channel and its government business. The company is working with telco customers that are preparing to comply with regulatory mandates and encouraging them get ahead of those impending or potential mandates. The goal is to enable telcos to execute on premium, monetizable business models at the same time as meeting minimum requirements (whether those are set by the telco itself or imposed by the regulator).

As discussed on page 15, Infoblox upgraded an existing telco customer in Europe to its pre-emptive threat feed last year. The company states that this operator saw a 20% - 30% increase in blocking events per hour across all its subscribers after rolling out the new service. The company also claims the activation saw very low false positives and no issues with customer complaints.

In the case of telco customers that are afraid of violating local censorship laws with this same universal approach, Infoblox encourages them to position pre-emptive security as a premium opt-in service requiring the user's explicit consent instead. As well as existing customers, Infoblox's pre-emptive approach to DNS security is driving its engagements into telco accounts that have only recently started to pay close attention to consumer security and the opportunity associated with it.

PowerDNS

PowerDNS is a leading provider of secure open source and commercial DNS software to telcos and enterprises around the world. While its commercial solutions power the Internet for more than 400 million telco subscribers, the community editions are used by many more. Since 2015 PowerDNS has been merged with Open-Xchange, a provider of secure email and collaboration tools. The business is privately held, sharing R&D and business support systems while nevertheless supporting two distinct brands.

PowerDNS delivers on-premises solutions for high performance DNS. It offers a complete suite of DNS solutions for telcos, including recursive and authoritative DNS, infrastructure solutions, DNS encryption, security filtering and parental controls. It offers cloud automation for a cloud-native DNS architecture, including cloud-native malware filtering and parental controls. Its cloud-native solution has been validated and certified by Broadcom VMware and the Sylva project. A new Single Pane of Glass for monitoring and orchestrating cloud-native DNS was demonstrated to customers at the end of last year and is due to be released soon.

To meet the requirements of dedicated RFPs for delivering cybersecurity, the company can deploy a DNS filtering overlay in parallel to existing core DNS infrastructure. In the telco space the company's core focus has traditionally been on large, incumbent, telcos in North America and Europe. It cites sizeable telco customers in these regions, including BT. In one case, PowerDNS provides security filtering for over 40 million subscribers.

As shown in **Figure 9**, the company reports growing demand for DNS security, citing two more wins in each of its two core regions during 2025, at least one of which involved displacing the incumbent DNS vendor. A fifth win during the year in the Middle East captures the company's regional focus quite well – a concentration on the two largest regions, tempered by a commitment to targeting select opportunities elsewhere.

In the telco space PowerDNS' core focus has traditionally been on large, incumbent, telcos in North America and Europe.

For its security and Protective DNS (PDNS) solutions, PowerDNS leverages raw threat intel feeds from more than 70 sources, including multiple leading security vendors and crowdsourced tools. These represent a wide range of detection technologies such as antivirus, domain scanning, file characterization, as well as behavioural and predictive analytics. By adding proprietary intelligence rules and manually enriching them with additional context, the company positions around achieving threat detection accuracy that substantially exceeds what is available from baseline threat feeds. The weighting, configuration and composition of threat feeds is customized to each operator's unique requirements and those of its local regulator.

In the home router space, PowerDNS has a DNS proxy which can deal with encrypted DNS traffic on the CPE and connect to the network service. This protects the confidentiality and integrity of traffic in the first mile of internet access and provides the ability to filter and block malicious content, whether or not the traffic is encrypted.

PowerDNS also has a partnership with Allot. In one joint collaboration, PowerDNS supported Allot in its development of Allot DNS Secure, a PowerDNS-based mass-market cybersecurity solution delivered to telco customers. DNS Secure is deployed at the network level and provides protection against a broad range of cyber threats, including malware and phishing, and offers content filtering, along with parental control options.

Appendix

Flaws in the data used in Figure 2 and Figure 3

A couple of flaws and limitations in the cumulative data used in **Figure 2** and **Figure 3** should be noted:

- Endpoint security wins were not counted in the February 2024 edition. Also Gen Digital is a significant player in the telco channel but did not contribute to this report until this year's edition.
- Akamai contributed to the 2024 and 2026 editions but not to the 2025 edition. PowerDNS contributed to the February 2025 and 2026 editions but not in 2024. Infoblox contributed for the first time this year.

While there are gaps in the 2023-2025 coverage of the endpoint security and DNS security markets, coverage of the home router security agent market is comprehensive. Here the only significant omission among major players over the last three years is the absence of Bitdefender's contribution to the first report in February 2024.

Additional Reference Materials

- The Global Anti Scam Alliance's "Global State of the Scams, 2025"
- "The Bitdefender and NETGEAR 2025 IoT Security Landscape Report"
- ENEA's "Key Insights from the Global Signaling Threat Landscape" (December 2025)
- "The Infoblox 2025 DNS Threat Landscape Report"
- The Guardian: "Age of the scam state: how an illicit, multibillion-dollar industry has taken root in south-east Asia" (December 2nd, 2025)
- The UK NCSC's "Impact of AI on cyber threats from now to 2027" (May 2025)
- HardenStance's "Telco Strategies for Consumer Security (February 2025 edition)
- HardenStance's "Telco Strategies for Consumer Security (February 2024 edition)
- HardenStance's "Proven Ways to Stop CLI Spoofing Scams" (March 2025)
- HardenStance's "Smart Home Security at Scale using prpl" (November 2025)

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. To Register for HardenStance's online Telecom Threat Intelligence Summit taking place on June 9th and 10th 2026, you can register here:

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.