No.73
January 2024

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security PUBLIC/UN-SPONSORED

Telco Strategies for Consumer Security

During Q4 2023, HardenStance spoke with Akamai, Allot, CUJO AI, F-Secure, SAM Seamless Network, and Whalebone about the 'what?', 'how?' and 'why?' of their telco customers' approach to augmenting cybersecurity for consumers. This report summarizes how telcos around the world are addressing this market.

- Considering the downturn in the sector, telco spending on consumer security software is holding up well. Some leading telcos are upping their commitment, extending better cybersecurity to many more users and growing incremental sales.
- More than two thirds of spending is still going on endpoint security but network-based security seems to be growing faster. Home router-based security is rolling out more slowly but there is near term as well as longer term interest in this model.
- In 2024, more leading telcos will commit to a multi-layered approach, investing in two, or even all three, ways of delivering consumer security. Hopes of fundamentally altering the playing field rest on open source projects like prpl and RDK-B.

Telco spending on consumer security edges up

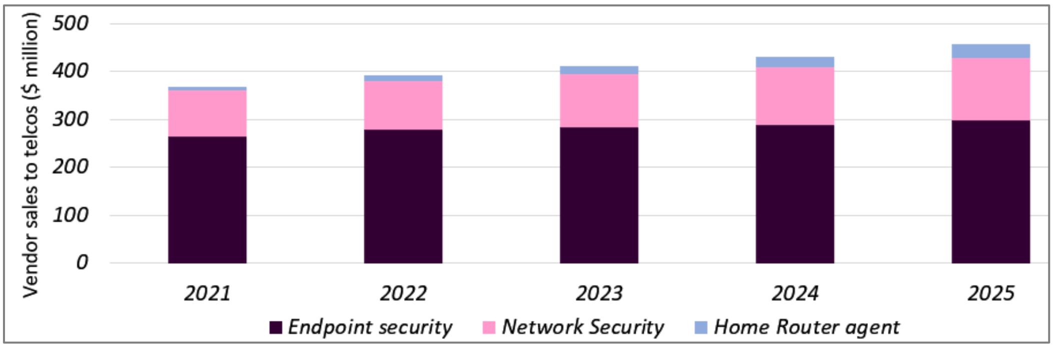
HardenStance estimates that telcos around the world spent around $411 million on consumer security software in 2023*. Some large operators are spending several million or more per year. Small ones are spending in units of $100,000 or $10,000 a year.

Considering the overall tech downturn in 2023, telco spending on consumer security software is holding up well.

During 2023, 69% of telco spending (around $284 million) went on endpoint security software. Of the remainder, 27% (around $111 million) went to network-based security, enabling telcos to block customer access to malicious sites. The nascent home router agent security model that provides protection for all connected 'things' in the household accounted for just 4% ($16 million) of this spending.

Total spend during 2023 was around 5% up on 2022. Considering the overall tech downturn, including major profit warnings and redundancies announced by leading telecom vendors like Cisco, Ericsson and Nokia towards the end of the year, telco spending on consumer security software is holding up well. Although there is downside potential if the economic outlook deteriorates, HardenStance estimates that the market will grow by 5% and 6% in 2024 and 2025, driven by growth in network-based security.*

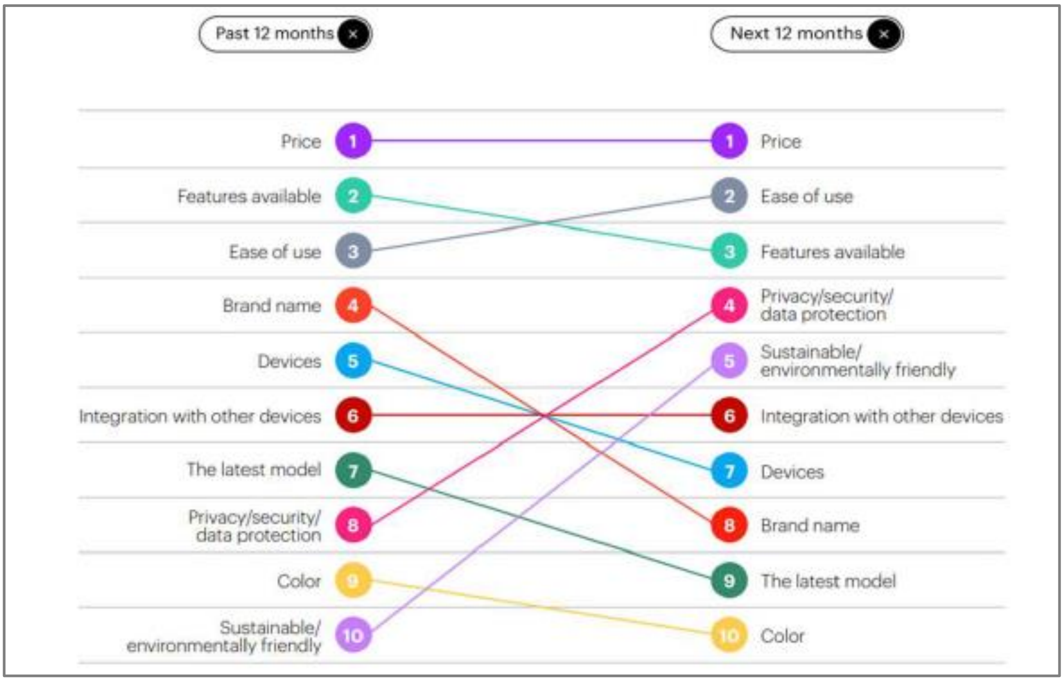
Figure 1: Worldwide Telco Spending on Consumer Security Software



Source: HardenStance

** See Appendix on page 11 for assumptions underlying these market size estimates and forecasts*

Figure 2: Past and Future Drivers of Consumer Electronics Product Purchasing



Source: 2022/2023 Global GSMA survey of 22,000 consumers in 11 markets

The big challenge for telcos in the home environment is to be able to charge for anything more than just basic connectivity.

Heightened relevance for the telecom sector's 'code-red moment'

Telco demand for consumer security software is holding up despite weakness in overall consumer demand. In its October 2023 Interim report for the first nine months of the year, the market bellwether, F-Secure, referred to "strong price sensitivity among consumers in the face of a challenging operating environment."

As reflected throughout this Briefing, what seems to be underpinning the market is a doubling down on the part of some telcos to embed consumer security as fundamental to their core business. This is rooted in what Nik Willets, CEO of TM Forum, called the telecom sector's 'code red moment' at the organisation's Digital Transformation World (DTW) last September. Pointing to telcos having spent over $1 trillion in the previous 5 years for a return of less than 1%, Willets said telcos risk "getting left behind by the very revolution we've created." They need "to find a path that recognizes that our customer needs are changing faster than we can," he said.

In the consumer segment of the communications services market, customer spending on Internet-connected products and services in the home has grown strongly in recent years. However, telcos have captured very little of that new spend. In the home market, competition to deliver just basic connectivity is increasing, such as via 5G Fixed Wireless Access (FWA) solutions. The bigger challenge for telcos is to be able to charge for anything more than just the basic connectivity.

Cybersecurity remains highly relevant for consumers

Cybersecurity remains highly relevant for consumers. **Figure 2** shows that price is still the number one consideration when people buy consumer electronics products. But it also shows that security has become a much more important buying criteria for consumer electronics products than it used to be. Yes, consumers hesitate to pay extra for security (especially when, as now, budgets are tight). But in many cases, they also hesitate because the options available to them are too complicated and they lack the confidence to make a smart choice. It's really not the case that consumers don't care.

Increased volumes of familiar threats are one reason cybersecurity remains so relevant. As of October 2023, BT reported seeing 17 million SMS phishing and spam messages (+97% compared to 2022) and 700 million phishing emails and links every month. But threat actors are also finding new ways to wreck consumer's online experiences.

We are vulnerable to hearing a fake audio of a distraught loved one

Nowadays not many of us are likely to fall for a random email from an African Prince offering to share their $25 million inheritance. But we are vulnerable to a high quality fake video or audio of a distraught loved one begging to be released from their kidnapper – especially when we're panicked into believing that the link for paying a ransom expires in 5 minutes (and our loved one isn't immediately picking up their phone). We're also vulnerable to relatively new QR code scams. A woman in the UK was recently defrauded of £13,000 using her phone to pay for parking at a train station. Fraudsters had covered the official payment app QR code with a fake one that was displayed on the payment instructions in the car park and directed her to a fraudulent site.

Leading telcos are raising revenue targets for security services, in some cases quite sharply.

It's in this context that vendors interviewed for this report point to examples of some telcos increasing their commitments to securing the consumer's experience. They report that leading telcos are raising revenue targets for security services, in some cases quite sharply. These leaders are doubling down on delivering layered security to attract new customers, reduce churn, and grow revenue more aggressively than in the past.

They're looking to do that by getting 30% - 40% or more of their customers to pay directly or indirectly for one or more layers of security. Speaking to the challenge of meeting these ambitious goals, F-Secure CEO Timo Laaksonen told the company's Investor Day in September 2023: "It's not enough to secure 15-20% of customers. How do we get to secure 100% of customers? That's the exam question for us."

An initial trickle rather than a flood of 'three layered' commitments

Allot says it has upsold several telco customers on a second service. One example is a Tier 1 in Europe that opted to buy home router-based security, having had a good experience with its NetworkSecure network-based security offer. In August 2023, F-Secure announced that a major European telco was the first to buy into all three layers of its extended portfolio spanning endpoint, network-based and home router agent-based security.

Nevertheless, the slow growth in sales of consumer security software to telcos depicted in **Figure 1** indicates that, for now at least, such examples of telcos stepping up their commitments are more of trickle than a flood. Other factors that are keeping the lid on stronger growth in vendor sales include the following:

- As discussed on page 7, some operators implement their own network-based security for consumers, avoiding the cost of commercial vendor software altogether.
- Some operators have been committed to increased spending for some time. However, they are still inching their way through all the complex integrations, optimizations and alignments across marketing, sales, customer support, legal and billing environments that are needed to launch and manage a value-added security service successfully. These customers aren't contributing much to vendor sales yet.
- Some are reviewing their options and are open-minded rather than committed.
- Some operators have concluded that investing in consumer security isn't for them.

Where telcos are committed to investing more, vendors report that the drive is coming from upper management. This marks a change because, traditionally, consumer security strategy has been driven by middle layers of management like individual product managers leading value-added service initiatives. Without upper management's support, these efforts have often delivered underwhelming results. Where stronger support is coming from management, telco organizations are more likely to deliver the necessary end-to-end process integration and optimization.

Security included in sweeping brand promises

Incremental revenue and churn management are still the key drivers of strategy – sharpened, in some cases, by wanting to respond to the industry's quite widely felt 'code red' moment. Alignment with security-infused brand promises is becoming more important too. This is shown by these examples that were current as of December 2023:

> *"We accompany our customers, as a trustworthy partner and ensure no one gets left behind. That is what Deutsche Telekom's brand stands for."*
>
> *"AT&T 5G. Fast. Reliable. Secure."*
>
> *"As a trusted partner, Orange gives everyone the keys to a responsible digital world."*

A premium security offer aimed at just a small subset of customers is nowhere near good enough to underpin brand promises like these. Although telcos are also under strong pressure to meet increasingly stringent new cybersecurity regulations, these are generally focused on hardening a telco's overall cybersecurity posture and the security of key business customers. Hence new regulations don't seem to be materially impacting consumer security strategy for now. As discussed on page 5, however, this could potentially start to change over the next couple of years.

The next three sections of this Briefing summarize the state of demand and deployment, with examples, across the three segments of telco-delivered consumer security services – endpoint-based; network-based; and home router agent-based.

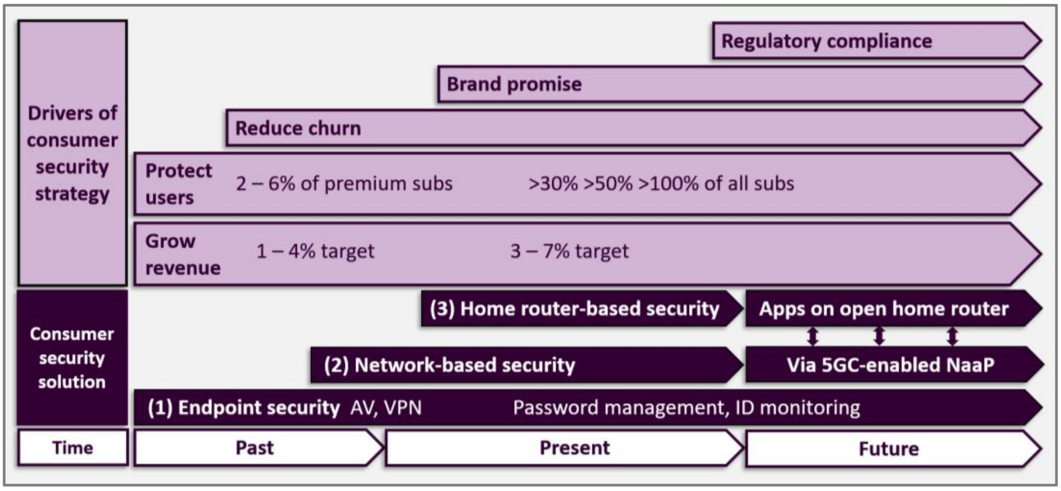
HardenStance estimates that telco spending on endpoint security will grow from $284 million in 2023 to $289 million in 2024 and $298 million in 2025.

There's additional revenue in endpoint security – but not enough

HardenStance estimates that telco spending on endpoint security will grow from $284 million in 2023 to $289 million in 2024 and $298 million in 2025. F-Secure, now a stand-alone consumer security business following the demerger of WithSecure, is the widely recognized endpoint security leader for the telco channel. Its partner channel, which telcos dominate, accounts for 80% of F-Secure's sales. Other prominent vendors in this segment are McAfee, Bitdefender, Norton and ESET.

Where consumer endpoint security is concerned, the big opportunity for telcos is to scale out rather than scale up. Endpoint security vendors are augmenting traditional apps like antivirus or malware detection and VPN with new features like password management and identity monitoring. This is enabling telcos to scale out their endpoint security offer and yield a cut of incremental revenue from the additional services sold.

Figure 3: A 'Telco's Eye' View of Consumer Security: Past, Present and Future



Drivers of consumer security strategy
Regulatory compliance
Brand promise
Reduce churn
Protect users
2 – 6% of premium subs
>30% >50% >100% of all subs
Grow revenue
1 – 4% target
3 – 7% target
Consumer security solution
(3) Home router-based security
Apps on open home router
(2) Network-based security
Via 5GC-enabled NaaP
(1) Endpoint security AV, VPN
Password management, ID monitoring
Time
Past
Present
Future

Source: HardenStance

Some of the newer endpoint security features also offer more effective ways of communicating value to consumers. Not that many consumers are impressed by reams of historical data detailing all the threats to their devices that have been blocked. But the green light around the perimeter of a computer screen that's triggered whenever an F-Secure-protected user opens an online banking session nowadays is much more compelling. The value isn't "here's some dry data about what we did last month." It's "hello again, it's us. We're right here, not interfering with anything; we're just letting you know we have your back - right at this moment when you're especially vulnerable."

Bundled as well as standalone endpoint security apps

At its Investor Day in September 2023, F-Secure pointed to how scaling out new endpoint security features via its new 'Total' app will drive its revenues, and those of its customers. While many of F-Secure's security apps are each available as standalone products, they're also now available together as part of a comprehensive suite via its 'Total' protection option.

New cybersecurity laws aren't affecting strategy much – for now

Whilst a worldwide wave of new cybersecurity laws and regulations is being imposed on critical industry sectors in general, or even targeting the telecom sector in particular, these new regulations aren't explicitly prescribing measures to protect the consumer user experience.

However, this doesn't mean they're having no impact at all on how telcos determine consumer security strategies. The general trend of government regulations raising the bar on what's expected, and invoking stiffer penalties for non-compliance, means telcos should expect that governments may get round to being more prescriptive regarding consumer security over time. In the near term, some regulators may even interpret some of the generic language of current and imminent legislation as allowing them to assert their right to intervene more directly in the consumer security space.

Several vendors interviewed agreed that while it has not been a key factor driving telco consumer security strategies in the last year, it's not entirely absent from considerations either. There is also evidence of governments actively preparing to do more to protect consumers as well as business users.

- **Singapore**: a new joint consultation from the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) floats the idea that telcos and banks should be required to compensate victims of SMS phishing scams (**November 2023**).
- **France:** Article 6 of the 'Securing and Regulating the Digital Space' bill brought before the National Assembly would grant the regulator powers to demand the deletion of phishing and other scam sites by their owners and the display of alerts by notified browser vendors. Telcos would be required to block domain names where publisher/site owner can't be reached. (**October 2023**). Orange is among the operators looking to bring this to the 2025 review of the European Electronic Communications Code (EECC).
- **UK:** The National Cyber Security Centre (NCSC) announced that from 2024 it is extending terms of eligibility for free access to its Protective Domain Name Service (PDNS) throughout the national school system to protect children's online experience on campus. How big a leap would it be for the NCSC to consider options for protecting learning from home? (**October 2023**)
- **Worldwide:** Many governments and regulators are engaging more in efforts to combat the scourge of rogue and unwanted voice calls. There isn't much to show for it so far in terms of materially reducing volumes of such calls or deterring spammers and fraudsters. And there is a particular lack of commitment to resourcing the enforcement aspect of regulation in this area. But it can at least be said that regulatory engagement with the problem does seem to be increasing.

Adoption rates for F-Secure 'Total', current as of last September, were:

- 18% of sales were coming from channel partners that were already selling 'Total'. These customers were seeing additional sales driving Average Revenue Per User (ARPU) increases of anywhere from 20% to 100%.
- 64% of sales were coming from partners that had upgraded to the 'Total' platform but had yet to start selling the full service suite.
- The remaining 18% of sales were coming from channel partners that had yet to upgrade to 'Total'.
- The company is targeting 76% of channel partners selling 'Total' by 2026.

Much as they are valued as channel partners, telcos also face increasing competition from alternative channels to market for endpoint security products. In Malaysia, for example, 21 million users of Touch and Go Digital's contactless smart card E-Wallet have F-Secure's ID Monitoring and Cyber Help embedded in it. Users don't have to download it themselves. This forms part of the growing popularity in parts of Asia of so-called

'Super Apps' that consolidate multiple apps under a unified service ecosystem and user interface. The financial services sector and others such as health and wellness providers offer other ways endpoint security vendors are reaching consumers besides telcos now.

HardenStance estimates that telco spending on network based consumer security software will grow from 111 million in 2023 to $120 million in 2024 and $129 million in 2025.

While there's clearly more revenue to be extracted from it, telcos can't achieve ambitious revenue, customer protection or churn management targets by scaling out with endpoint security alone. Reaching consumer penetration rates measured in units of ten percent requires investing in network-based security or home router-based security solutions.

Network-based security may be seeing the fastest growth

HardenStance estimates that telco spending on network-based consumer security software will grow from $111 million in 2023 to $120 million in 2024 and $129 million in 2025. 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. Leading vendors in this market space are Akamai, Infoblox, Whalebone and Allot. Allot competes in DNS security as well as with a differentiated inline solution where it competes with HiveFlow, a solution delivered by NetHive and Fortinet.

Network-based security is an unusual market segment. Some vendors provide DNS and DNS security solutions to businesses, but they don't serve the telco channel with DNS security for consumers. Quite a lot of telecom operators use open source BIND in their DNS operations, thereby avoiding the cost of commercial software altogether. Norway's Telenor provides an interesting example. It buys commercial DNS and DNS security software from vendor partners to serve business customers. But it drives its 'Nettvern' consumer DNS security service entirely from an internally developed solution.

The key differentiator for network-based security is that 100% of subscribers can be reached, independent of what end devices or home router they each have, and without them having to go to the trouble of downloading anything. It also provides the exact same level of protection to fixed and mobile connections. A network based security service can be enabled automatically for all subscribers or with a premium-priced service tier. It can also be made available for any user to opt in at the point of sale, online or in store, by simply ticking a box that they want the additional protection. Alternatively they can reply 'Yes' to a text inviting them to opt in. Akamai points to its telco customers being able to generate additional ARPU of anywhere from 5% – 10% per month.

Having acquired DNS vendor, Nominum, back in 2017, numbers provided by Akamai make it look like the leader by revenue in this segment. Half of Akamai's almost 120 telco and ISP customers for DNS use its 'Secure Internet Access' security features. These 60 telcos and ISPs reach almost 600 million subscribers. Of those, around a third are fixed broadband connections into households, and two thirds are mobile connections.

A lot of very positive testimonials

Whalebone, based in the Czech Republic, is a scrappy challenger in this space. The company says it has been enabling new telco customer launches at the rate of one a week since the summer of 2023. In this market space, and at this point in time, that seems like an unusually high win rate. As shown in **Figure 4**, Whalebone's customers are mostly Tier 1 operators concentrated in Central and Eastern Europe. It points out that there are other current customers besides the ones shown and promises "many more to come". A large number have agreed to feature in very positive testimonial interviews, many of which started appearing on the company's website in the second half of 2023. Up until recently, Whalebone committed to telco customers that it could show them a path to 5% overall revenue growth with its 'Aura' software and services suite. Based on recent experiences, it has upgraded that target to 7% now.

Whalebone says it has been enabling new telco customer launches at the rate of one a week since the summer of 2023. In this market, that's a high win rate.

Operational complexities slow down home router security momentum

HardenStance estimates that telco spending on home router security agent software will grow from $16 million in 2023 to $22 million in 2024 and $30 million in 2025. Specialists CUJO AI and SAM Seamless Network, as well as Allot and F-Secure, are the leading vendors. The home router security agent model consists of a telco investing in a vendor's cyber security agent deployed on a home router. In conjunction with a continuously updated threat intelligence cloud, the agent then prescribes and enforces robust security

Figure 4: Recent vendor wins for network security (DNS security unless stated)

Vendor	Date	Operator	Country/Region
Akamai	2023	Tier 1	Germany
Akamai	2023	Tier 2	USA
Allot	2022	Far EasTone*	Taiwan
Allot	2022	Mobile operator*	North America
Allot	2023	Yettel	Bulgaria, Hungary
F-Secure	2023	Tier 1 operator**	Europe
Whalebone	2023	A1	Austria, Bulgaria, Croatia, Serbia
Whalebone	2023	Elisa	Estonia
Whalebone	2023	LMT	Latvia
Whalebone	2023	m:tel	Montenegro, Bosnia, Herzegovina
Whalebone	2023	O2	Czech Republic
Whalebone	2023	O2 Telefonica	Germany
Whalebone	2023	Tele2	Estonia, Latvia, Lithuania
Whalebone	2023	Vietnamobile	Vietnam

Source: HardenStance ** Allot's NetworkSecure* *** Leveraging a DNS partner*

Figure 5: Recent Vendor contracts for home router agent based security

Vendor	Date	Country/Region	Operator
Allot	2021	Europe	Tier 1
Allot	2022	Asia Pac	Tier 1
Allot	2022	Latin America	Tier 1
CUJO AI	Footprint put down in 2016-20. Cybersecurity features activated subsequently	North America	Comcast
CUJO AI		North America	Charter
CUJO AI		North America	Shaw
CUJO AI		North America	Rogers
CUJO AI	2023	UK & Italy	Sky
F-Secure	2022	Finland	Elisa
F-Secure	2021	Vietnam	FPT
F-Secure	2020	U.S	Windstream
SAM	2019	Belgium	Telnet
SAM	2022	U.S	Verizon
SAM	2023	Belgium	Orange

Source: HardenStance

policies from within the home router. It also leverages visibility into all the LAN traffic to block malicious connections to, from and between every device and IoT 'thing' in the household that is connected to the router.

In October last year, SAM Seamless Network announced Orange Belgium as a new customer.

The pace of commercial rollouts relying on this model has been slower than the momentum behind endpoint and network-based security. This relatively slow overall momentum nevertheless conceals a very important regional discrepancy. The vast majority of CUJO AI's revenues come from North America, where it began rolling out several years ago. The company has now accumulated a footprint spanning more than 50 million households served by cable MSO providers (see **Figure 5**).

Up until recently, CUJO AI was generating most of its revenue from its 'Explorer' privacy and tracking protection software deployed in its customer footprint. In the last couple of years, however, the company reports good progress in overlaying sales of its 'Sentry' network security and device protection software onto that. CUJO AI says it is also seeing significant momentum with some big telco operator groups in Europe, although the only accounts it publicly cites for now are Sky (UK and Italy) and EE (UK).

SAM Seamless Network cites 8 customers, including Bezeq. In October last year it announced Orange Belgium and is also engaged with Tier 1 customers in the UK and the Netherlands and a Tier 2 in Switzerland. SAM doesn't provide a breakout of which customers are using SAM Cybersecurity (home network security) as compared with those using SAM Intelligence (telco insights into customers' home and small business networks) and SAM Enablers (device awareness and fingerprinting insights).

A key reason for slower adoption of the home router agent model is the strong dependency it has on the security software vendor having to integrate its agent with a myriad of different proprietary home router vendor products that different telcos around the world expect to have supported. The integration effort costs time and money and is inherently inflexible for rapid service innovation at scale. Added to this, CUJO AI reports

Europe being behind the curve compared with North America because of the amount of operational and marketing autonomy each national affiliate of a big European telco group typically has. It’s often a lot more compared to the more uniform approach a North American operator has to rolling out across its North, South, East and Western regions.

Security is a lead application for fulfilling prpl and RDK hopes

In the spirit of breaking out of the telecom sector’s ‘code red’ moment, many telcos want to go beyond merely augmenting revenues with cybersecurity and value-added services. Instead they’re seeking to ignite a fundamental step change in their positioning to grow their share of spending on consumer electronics products and services for the home. Cybersecurity features typically form a central element in these strategies.

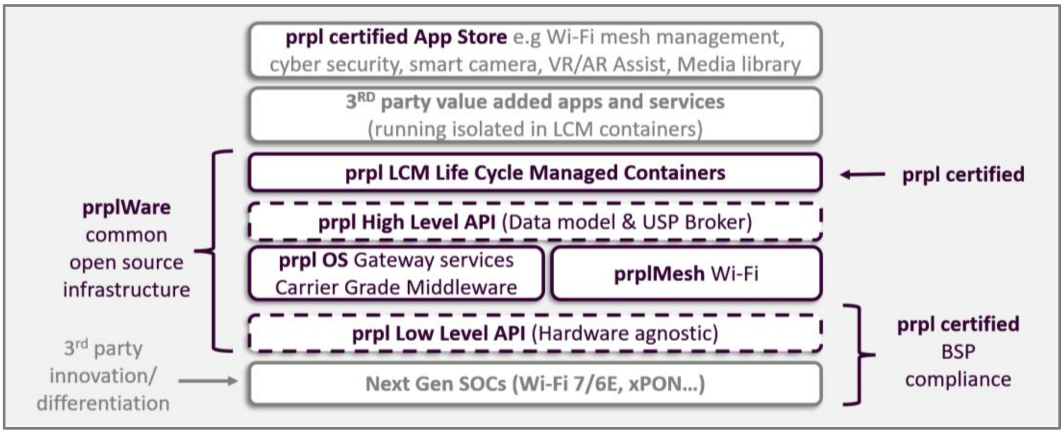
EE, part of BT, is one telco that is intent on revolution rather than evolution. In a December 5th 2023 article in “This is Money”, the Head of EE, Marc Allera spoke of EE aiming to be “one of the top three retailers for consumer electronics” and “a viable alternative” to the big online shopping giants and high street players. “Customers tell us they have so many apps and subscriptions they don't know where to put them,” Alera stated. “They have devices in their homes that they can't find or don't know if they're connected. We can play a really good role in helping them navigate all that.” The goal, which borrows heavily from the ‘super app’ model, is that “when people see our app on their smartphone, they will want to come back every day and every week to buy products and services from us.” CUJO AI and Netduma are in the mix among EE’s vendor partners.

In October 2023, Orange hosted 270 attendees at the prpl Summit in Paris. Supporting vendors gave 23 different demos over the two days.

Regardless of whether their consumer security services roadmap assumes a revolution of the kind EE is targeting, or even just an evolution, some amount of telco strategy around the world is starting to coalesce around the idea that transforming the capabilities of the humble home router is a key step in the roadmap. Specifically, hopes rest on a new generation of open source home routers becoming an open global platform on which telcos can work with value-added service partners to innovate and grow revenues at something approaching web scale. The first of the two open source communities they’re looking to is Reference Design Kit (RDK). Initially focused on cable video devices, and driven out of North America by the likes of Comcast and Charter Communications, RDK has since developed RDK- Broadband (RDK-B) for the home router market. CUJO AI, for example, states that its agent is deployed on 30 million RDK- compliant devices in North America.

The second is the prpl Foundation, which has a larger following among telcos around the world. Among its 70 member companies are telcos including Verizon, AT&T, Dish, TeliaCompany, TIM, Orange and BT. Perhaps because it has large consumer market footprints in both the U.S. and Europe, Deutsche Telekom appears to be one of the few telcos to be backing both RDK-B and prpl.

Figure 6: The prplWare Service-Delivery Platform Stack


prpl certified App Store e.g Wi-Fi mesh management, cyber security, smart camera, VR/AR Assist, Media library
3RD party value added apps and services (running isolated in LCM containers)
prpl LCM Life Cycle Managed Containers
prpl certified
prplWare common open source infrastructure
prpl High Level API (Data model & USP Broker)
prpl OS Gateway services Carrier Grade Middleware
prplMesh Wi-Fi
prpl Low Level API (Hardware agnostic)
prpl certified BSP compliance
3rd party innovation/ differentiation
Next Gen SOCs (Wi-Fi 7/6E, xPON...)

Source: Hardenstance/prpl Foundation

A goal of high velocity, service-driven innovation

Driven by its service provider steering committee, prpl defines its mission as "to enable high velocity, service-driven innovation on CPE by harmonizing interfaces in open APIs and delivering open source reference implementations of common infrastructure." In this model, cybersecurity is just one of many value-added services or apps that telcos can deliver from an open home outer. Examples of other apps include Wi-Fi network optimization, speed tests, smart camera management, VR/AR assistants and media libraries. The vision allows for apps to run on a home router or in the cloud, depending on how latency tolerant the application is.

By removing the dependency on dozens of different proprietary home router operating systems, telcos hope to slash integration costs and incentivize developers in areas like cybersecurity, network performance, home security, gaming experience optimization and others, to commit to developing for the prpl App store. The aim is to greatly reduce time to market with new telco-delivered services that improve and augment the consumer experience.

The level of participation by telco software engineering leaders in prpl and RDK suggests that these open source home router projects do have some chance of succeeding.

In October 2023, Orange hosted 270 attendees at the prpl Summit in Paris. Supporting vendors gave 23 different demos over the two days. Among cybersecurity vendors, SAM Seamless Network and Bitdefender distinguished themselves as the only ones to feature as premium sponsors of last October's prpl Summit. BitDefender demonstrated its IoT security agent. SAM Seamless Network can already run as a container in the prpl Life Cycle Management (LCM) framework as well as run some things through the high level API. The company demonstrated CPE observability and security for homes as well as businesses at the Summit. Cyber AdApt, a start-up, also showed a demo on threat detection in the home network. Among other cybersecurity vendors, Allot and F-Secure are also members and participants in prpl.

The outlook for open source home router projects

The telecom sector's heritage of collaborating to create inter-operability through common standards is a fine one. But it has nothing like that track record when it comes to collaborating to direct the building of highly competitive open source solutions, let alone ones that can drive highly competitive consumer product spaces.

The level of participation by telco software engineering leaders in prpl and RDK suggests that these open source home router projects do have some chance of succeeding. Three main stakeholders hold the keys to determining how far they can go:

- **Application developers need to be incentivized to commit at scale**. That requires that the open source ecosystem itself and the code that arises from it is exquisite to work with rather than just ‵good enough'. It also requires that unique telco customers commit to both buying at scale and ensuring that whatever layers of differentiation they want to add on top are easy for developers to execute on.
- **Peers among the telco's product management and sales leaders need to be convinced.** They will need to be convinced if they are to switch their allegiance from proprietary to open home router ecosystems. Upper telco management can help with setting and supporting top level targets but it will need solid support from commercial stakeholders throughout the organization if it is to make a truly big bet on something like prpl or RDK.
- **Consumers need to believe in the telco – trust isn't enough.** Ultimately, the idea of a telco-delivered open source home router service platform can only succeed if consumers themselves invest in it. That requires more than trust as it relates to privacy where telcos have an advantage relative to the webscalers. It also requires confidence as it relates to the ease of the user experience. Consumer confidence in the ability of Google, Microsoft and Amazon to deliver on that key requirement tends to be quite a bit higher than it is in their local telco. That gap has to be closed.

There is also potential to augment open service innovation on the home router with more open access to information from within the operator's network. Specifically, major telcos like Vodafone and AT&T are ramping up their marketing machineries to talk up the Network as a Platform (NaaP) capabilities of the 5G Core (5GC). At the 10th Brooklyn 6G Summit in November 2023, AT&T Network's President, Chris Sambar, outlined the company's NaaP vision. Stating that "the network is the killer app," he said that cybersecurity is "the earliest application that we're seeing" for an increasingly disaggregated network in which network functions run as applications on a server in the network. While AT&T already has enterprise customers in beta for NaaP-delivered cybersecurity services, Sambar also stated that AT&T sees the model as extendable "even for consumers on their home gateways."

Appendix: The data behind market size estimates

The global market sizing assumptions for endpoint security, network-based security and home router agent based security that are shown in **Figure 1** were extrapolated from the following available data points:

Endpoint security ($284 million in 2023)

- **F-Secure** is the widely recognized market leader as a provider of endpoint security solutions to telecom operators. It is now a stand-alone consumer security business following the demerger of WithSecure as a dedicated enterprise security business in June 2022.

  In September 2023, the company gave revised guidance of total revenues for the year in the range of €128 – €132 million. According to F-Secure, telco channel business accounts for 80% of its sales. The company's sales into telcos for 2023 were around $113.5 million.

  By its own reckoning, F-Secure has more than 40% market share of the worldwide telco market, citing more than 130 telco customer partners (to which the Lookout acquisition has added another 20). That points to telcos spending a global total of around $284 million on endpoint security software in 2023.

  For the nine months to September 2023, F-Secure reported organic revenue growth (excluding Lookout) of just 2.3%. In Q3 2023, that shrank to just 0.3%.

Network-based security: ($111 million in 2023)

As stated in the report, this category is comprised primarily of DNS security software features with the addition of Allot's own inline solution.

- **Open source BIND:** Quite a lot of telecom operators use BIND in their DNS operations. From the perspective of this report, this inevitably exerts downward pressure on what vendors are able to charge for managed DNS security software.
- **Akamai** acquired DNS market leader, Nominum, back in 2017. Akamai's annual report for that year shows that the price paid was $180 million. As stated in this Briefing, today half of Akamai's almost 120 telco and ISP customers leverage the company's 'Secure Internet Access' DNS security features. These 60 telcos and ISPs reach almost 600 million subscribers. HardenStance estimates that Akamai's annual revenue from DNS security software amounts to somewhere in the range of $55 - $85 million.
- **Allot's** earnings statement for first nine months of the year to September 2023, stated that the company's Security as a Service (SECaaS) recorded sales of $7.5 million. This was up 11% on the nine months to September 2022. A large majority of all Allot's SECaaS revenues come from network-based security.

- **Whalebone** earns substantially all of its revenues from DNS-based network security. Whalebone shared with HardenStance that its annual revenues are in the $5 – $10 million range.

Home router agent based security: ($16 million in 2023)

- There are no public domain numbers of any kind in this market.
- SAM Seamless Network has 4 paying tier one telco customers in the home router security space currently: Bezeq (Israel); Telnet and Orange (Belgium) and Verizon (U.S).
- Only a small share of Allot's total SECaaS revenues of a little over $10 million comes from the home router agent based segment. ■

More Information

- HardenStance blog: "Do telcos care about consumer cybersecurity? Do consumers?" (January 2024)
- Register for HardenStance's "Telecom Threat Intelligence Summit 2024"

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.

Register for HardenStance's virtual/online Telecom Threat Intelligence Summit, taking place on June 11th and 12th free of charge here.

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.