White Paper

HardenStance

Smart Home Security at Scale using prpl

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

Bitdefender

November 2025

Executive Summary

- 2025 saw Orange, Verizon and AT&T all make progress deploying home routers that use the prpl Foundation's open source software. Along with new members, KPN, Telenor, Turk Telecom and Bell Canada, these Tier 1 telcos all view prplWare as a key enabler for growing revenues in smart home applications and services.
- When it rolls out with Orange Morocco, Bitdefender is set to be the first of six vendors to see its prpl security app commercially deployed. Weaknesses in home routers and connected IoT 'things' can be used to attack home networks. The same devices can also attack other customers and clog up telco networks with DDoS traffic or malware distribution. Millions of home routers at a time can even be taken offline.
- prplWare is a critical enabler for protecting smart homes against cyber threats. The first prpl-certified home router products were released earlier this year. The first prpl-based routers are rolling out with prpl-compatible security apps.
- Householders themselves have most to gain from prpl security apps. So too do telco consumer product teams who can monetize them. But telco network and security operations, as well as law enforcement and national security agencies, have a lot to gain from using prpl to help harden home routers against cyber threats as well.

The global prpl Summit held in Paris on October 13th 2025 saw TIM, Turk Telecom, Telenor and Bell Canada announced as new members of the prpl Foundation.

New tier 1 members give prpl new momentum

The global prpl Summit, attended by 435 delegates in Paris on October 13th 2025, saw KPN, Telenor, Turk Telecom and Bell Canada celebrated as new members of the prpl Foundation. They join Verizon, AT&T and Orange driving prpl as a key part of their smart home strategies. The prpl Foundation defines its role as "developing open source software for carrier-grade CPE." The smart home market space is still hotly contested by consumer electronics vendors, public cloud providers and telecom operators. Bandwidth is no longer a differentiator. What stands out comparing future Wi-Fi 8 and current Wi-Fi 7 specs is how the differences relate to reliability, efficiency and quality of experience. Maximum speeds and the core building blocks behind them don't change.

Android for the home network

The telcos backing prpl want it to be an operator-controlled 'Android for home networks.' They want home gateways to be open source application delivery platforms for the home that they are uniquely positioned to deploy, manage and generate new ARPU from at scale. They want prpl to deliver home networking apps that can be developed once and deployed on any prpl-compliant router anywhere in the world, according to an agile development model. Telcos expect to see prpl apps in their own as well as other app stores. They want prpl to tip the market in smart home services decisively in their favour.

Figure 1: prpl commercial milestones in 2025

Operator	Country	prpl deployment milestone
Orange	Jordan	Launched in Q1 2025 with prpl home gateway and Wi-Fi repeater products from SoftatHome, MediaTek and Nokia.
Orange	Morocco	Launch imminent with ZTE prpl home gateways and Bitdefender security apps.
Orange	France	Planning underway for the roll out of prpl throughout France.
Verizon	U.S.	Upgrades for up to 10 million prpl-compatible home gateways planned for 2026.
AT&T	U.S.	12 million home gateways already support prpl LCM. Further upgrades planned.
Vodafone	UK	Wi-Fi 7-powered Ultra Hub 7 home gateway launched during 2025. It uses prpl's Life Cycle Management (LCM) software integrated with an RDK-B OS.
Vodafone	Germany	

Source: HardenStance

As shown in **Figure 1**, Orange, Verizon and AT&T all reached new prpl deployment milestones during 2025. Vodafone has deployed using the alternative RDK-B OS, albeit it has nevertheless integrated prpl's Life Cycle Management (LCM) module with that.

Cybersecurity and Wi-Fi optimization are the top two apps

Consumer surveys around the world consistently show that cyber security and Wi-Fi optimization are the two home router apps householders are initially most willing to spend on to enhance their user experience. From when it first embarked on a roadmap for delivering more open home broadband services, AT&T has made cybersecurity apps its first priority (see 'More Information'). When Orange launches its first prpl routers in Morocco, the first app it will launch with will be Bitdefender's cybersecurity app. This will likely be the first prpl security app to be commercially deployed anywhere in the world. Five other vendors – Allot, Cujo AI, F-Secure, Nagravision and SAM Seamless Network – either have or will soon have commercially available prpl security apps. Telcos also hope to sell a variety of other apps such as app integration and QoE optimization; VR/AR Assist, home security; and Wi-Fi sensing applications like detecting falls of elderly people and household comings and goings for energy efficiency or as a home security feature.

When Orange launches its first prpl routers in Morocco, the first app it will launch with will be Bitdefender's cybersecurity app.

Good cybersecurity ensures secure access to basic broadband services. But it's also a key requirement for advanced home network services. Householders can be open to spending on health and wellness, energy management, or personal security apps. But many won't if a service doesn't come with a compelling cybersecurity service wrapper. This White Paper addresses cybersecurity risk in the home network and the contribution prpl makes to reducing cyber risk while growing telco revenues. It addresses:

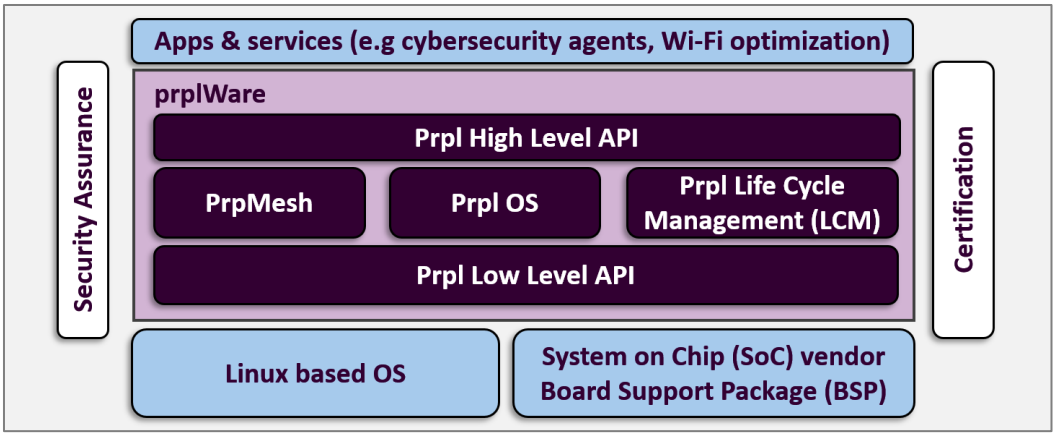
- The nature of cyber threats in the home.
- The role of prpl and prpl cybersecurity apps in securing home networks and growing telco revenues.
- Key selection criteria for telco buyers evaluating prpl security app products.
- The security hardening that prplWare provides via the decoupling of hardware and software, the adoption of agile development principles, and additional security features embedded in various parts of the stack.
- Why other stakeholders – specifically telco network and security – should be investing resources in supporting the prpl ecosystem.
- The contribution that more active law enforcement and IoT security regulation is making to reducing cyber threats from IoT devices.

Goodbye to integrated routers and waterfall development

Prpl is disrupting the legacy model by which telcos deploy applications on home routers. That model depends on products built largely on proprietary software so it's complex, expensive and slow. Application software vendors invest 6 to 12 months integrating with the proprietary middleware of each home router or home gateway partner. It's more waterfall than agile and it encourages vendor lock-in.

Diverse firmware and hardware drives fragmentation and impacts stability. Even minor updates have to be tested comprehensively with each party, including for forward and backward compatibility. The legacy model is nowhere near efficient and agile enough for telcos to deploy and maintain compelling smart home services with the velocity and scale they want. The different stakeholders cited above are all represented in prpl because they recognize the advantages it brings to telcos. But they are continuing to fulfil commitments to the legacy model while also investing in prpl's power to disrupt and replace it.

Figure 2: prplWare: The complete suite of prpl software



Source: the prpl Foundation/HardenStance

The prplWare suite for home gateways

The prplWare roadmap and feature set has achieved Minimum Viable Product (MVP) status. Release 4.10 was confirmed on October 12, 2025. The complete suite of prplWare is set out graphically in **Figure 2**, and described below:

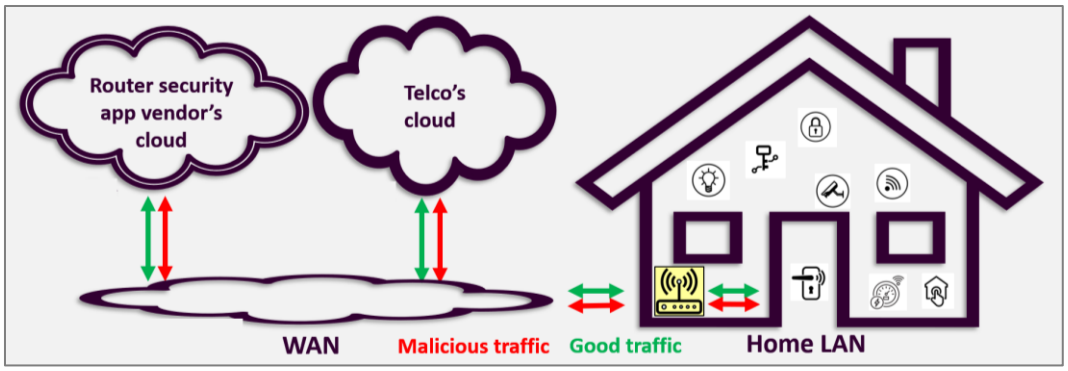
The prplWare roadmap and feature set has achieved Minimum Viable Product (MVP) status. Release 4.10 was confirmed on October 12, 2025.

- **prpl High Level API:** allows applications and services to interact with and manage router functions (like Wi-Fi, devices, and security) in a consistent, vendor-agnostic way within the prpl ecosystem.
- **prplMesh**: the Wi-Fi mesh network implementation allows Wi-Fi access points in the home to talk to one another with carrier-grade management for local and cloud-based Wi-Fi applications.
- **prplOS:** the OS uses the Linux-based OpenWRT specification which is specifically designed for embedded networking devices.
- **prplLCM:** the platform-independent life cycle management module allows operators to securely manage the individual life cycles of containerized applications independently of a home router's firmware. prplLCM uses the Broadband Forum's TR-369 User Services Platform (USP) specification, the successor to the widely deployed TR-069. Where TR-369 instructs a home router to download and install a prpl application; prpl LCM then manages that app. AT&T is using LCM even on home gateways that ultimately will not be upgraded to prplware. AWS also uses prpl LCM to manage apps on its IoT GreenGrass service. Vodafone's proof-points for prplLCM integrations with the RDK-B home router ecosystem are shown in **Figure 1.**
- **prpl Low Level API**: standardizes access to lower level components, including SoC vendor BSP and Linux-based OS.

Threats to smart homes come from two directions

Whether it is based on mostly proprietary software or an open source framework like prpl, any home router is vulnerable to cyber threats. At one end of the scale, unskilled 'script kiddies' use off-the-shelf malicious tools to exploit them while more advanced criminals combine third-party tools with their own. At the other end of the scale, botnet operators infect and enslave vulnerable smart devices by the hundreds of thousands to carry out much larger scale attacks. The 'Aisuru' botnet which compromises 700,000 enslaved IoT devices is one of many examples (see **Figure 5**). Some botnet operators hire out their assets to other criminals according to an 'as a service' model; others make exclusive use of them themselves.

Figure 3: The home router faces cyber threats from the WAN and the LAN



Source: HardenStance

As shown in **Figure 3** there are two primary routes by which cyber attackers can access and compromise a home network remotely – from the WAN or from within the home.

- **On the WAN-facing side**, home routers themselves are permanently exposed to malicious hackers scanning for open ports. For ports that are closed but poorly secured, such as with weak passwords, attackers use brute force and other techniques to bypass those controls and gain access to the home network.
- **From within the home** poorly secured smart devices or IoT 'things' pose three types of risk. A compromised device can be abused. Once exploited, a compromised device can also enable access to the other devices on the home network. If it's enslaved into a botnet, that device can also be weaponized to attack other individuals, householders and businesses that might be on the next street or could be located in another country altogether.

As proven by the many malicious botnets that have comprised hundreds of thousands of devices, hacking into a lot of home routers and connected things in the home is not all that hard.

Home routers and smart IoT devices tend to have a lot of vulnerabilities

As proven by the many malicious botnets that comprise hundreds of thousands of devices, hacking into a lot of home routers and connected things in the home is not all that hard. These are relatively low-cost consumer electronics products, after all. Many have very poor security such as default passwords. Their software tends to have a high number of common vulnerability exploits (CVEs). This remains true of many of the latest generations of home routers but it's especially true of legacy products. That includes many that are still in operation years after they have reached end of life and are no longer supported. Connected devices tend to have especially weak security but some models of low-cost router aren't much better.

It's certainly true that some leading countries are legislating to mandate better security on the part of consumer IoT product manufacturers as well as cracking down on botnet operators. But as the analysis of recent data on page 10 suggests, the impact of these measures on the global threat landscape will only be felt incrementally over many years.

The main cybersecurity threats to householders

Comprised devices in the home can drive a variety of impacts including the following:

- Exposure of personally identifiable information (PII) of household members.
- Financial fraud.
- Deterioration in quality of experience, arising from bandwidth consumption by breached devices on the home network misbehaving.
- Temporary or sustained outages arising from malicious updates to the home router requiring a reset or bricking the device altogether.
- Children being able to access inappropriate content or hackers finding ways to communicate with children directly by remote takeover of toys or other devices.

As well as familiar cyber threats, many users may not be familiar with the cyber risks that the connected home also presents to householders' physical security. These include:

- Remote takeover of connected indoor or outdoor cameras allowing remote surveillance of household members within the home or comings and goings to and from the home.
- Remote takeover of connected door or window locks, heating or lighting systems, garage doors or air conditioning systems.

Cybersecurity apps in the prpl ecosystem

A cybersecurity app running on the home router is the best way to protect any smart home. Endpoint security is great for a PC, smartphone or TV but most other connected devices can't support it. If it's offered with rich, dynamic features, network based security leveraging DNS or DPI can provide a good basic security layer for all devices in the home. As depicted on page 7, however, a security app on the router provides the richest feature set for protecting each and every device on the home network.

A prpl security app should initially observe all the devices attached to the network, and fingerprint and register each one with key technical data.

As shown in **Figure 1**, leading telcos driving prpl are transitioning from pre-commercial trials to commercial deployment at scale. Consistent with that, the prpl Foundation's product certification programme is up and running. Gemtek, using MaxLinear technology, became the first home gateway vendor to get its products prpl-certified in April this year. As shown in **Figure 4**, certification of 10 platforms from seven companies has either been achieved or was pending as of October 2025.

What a prpl cybersecurity app does

Within the prpl ecosystem, a security app is differentiated according to the accuracy of its detections and blocking decisions, and the extent to which it does or does not disrupt the user experience. When it's uploaded onto the router, a prpl security app should initially observe all the devices attached to the network, and then fingerprint and register each one with key technical data about each product (this information has value in itself, independent of the cybersecurity use case - some operators currently buy this information on their own customers from third parties). Devices should be scanned for known vulnerabilities and weak passwords. Traffic to and from those that are identified as insecure should be continuously scanned for threats. Those that are identified as secure should be periodically scanned for vulnerabilities.

Figure 4: Platforms certified for prplWare as of the prpl Summit, October 13, 2025

Company	Product	Certification date	Hardware	Software	prplWare
Arcadyan	Mozart*	Pending	2.3	2509	4.0.1
Gemtek	OSPv2**	April 2025	MB: VO2	GTK OS prpl3.1-2.1	3.1
Gemtek	TB-372	April 2025	HW: V02	GTK 1.0.1.66	3.1
Nokia	Beacon19	Pending	00	M1.2	3.2
MaxLinear/Gemtek	OSPv2	Cert by definition	V2	9.1.100	4.1
Qualcomm/WMC	Freedom	Cert by definition	V1	ath13.0	4.1
Sagemcom	Fast 5598 GW	May 2025	V1.0	***	3.2
Sagemcom	F5598	Pending			4.0
Sagemcom	F5298	Pending			4.0
Zyxel	EE4600	Pending			3.1

Source: HardenStance/prpl Foundation **Regular track ** WGRTD-159BE *** SG_PRPLOS_v3.2.0_20250515_F5598*

As with all cybersecurity, layers of protection are needed

A good prpl cybersecurity app should provide different layers of protection against the various different types of cyber threats. These are some of the capabilities to look for:

A good prpl cybersecurity app should provide different layers of protection against the various different types of attack.

- Brute force protection, such as temporarily suspending access to a device following a given number of failed password attempts.
- DDoS protection to detect and block recognized patterns of DDoS traffic.
- URL filtering
- Deep packet inspection (DPI) to detect and block malware.
- A VPN layer that encrypts outbound traffic for specific devices or services.
- Anomaly detection – for example to flag when a Samsung fridge that routinely connects to a South Korean server tries to connect to a server in North Korea.
- A sensitive data protection layer that automatically prevents a device from sending sensitive information like credit card details, GPS coordinates or username and password combinations out over the Internet without encrypting them.
- Parental controls.

DevOps with prplWare also helps harden router security

As well as enabling a direct reduction in cybersecurity risk in the home via prpl security apps, prplWare also provides core hardening of home router security independent of any cybersecurity app. The scale of this contribution should not be exaggerated. Embedded programming is specialized and hard. Firmware vulnerabilities can be very hard to patch. That's just one example of many security exposures in the way home router products are built and managed that is out of prpl's current scope.

That said, prpl's indirect contribution to home network security should not be underestimated either. The whole smart home ecosystem benefits from the way prpl allows each app access to only the specific resources it needs and from the way the cadence of container updates is de-coupled from the periodic firmware releases of a router vendor.

Prpl allows security updates to be released as soon as they're available

Most of the framing of prpl's value tends to be around faster time to revenue with new service innovation. But there are disproportionately big cybersecurity gains that arise with this model too. That's because security updates need to be released more frequently than other updates in order to keep up with the discovery of new vulnerabilities and the new Tactics Techniques and Procedures (TTPs) of malicious hackers. prpl enables security updates to be released as soon as they're available. They don't have to be held back until the next firmware release. This helps reduce the home network's attack surface. Reducing the frequency of firmware updates also reduces the pressure on router vendor or telco development teams to cut corners on security processes, including firmware security testing.

There are other ways prplWare improves home router security. Sandboxing within prpl isolates individual containers from one another. The low level APIs ensure that a malicious or misbehaving container does not impact others in two main ways. The APIs ensure that a container can't directly infect another container with malware. They also control each container's access to system resources. They limit each container's access to the specific resources it needs. This avoids indirect impacts from memory leaks, crashes and reboots that can arise when OS resources are shared, and those shared resources are then abused. The prpl Security Working Group is led by industry leaders from Vodafone and Verizon. Requirements documents already published by the group include those on device security requirements; secure manufacturing data standard; standard flash layout; secure boot requirements; packet inspection requirements; multi-subsystem firmware management and security APIs.

A significant subset of end users views notifications from a security product as important proof that the solution is actually working and providing value for money. For these users, notifications need to be delivered in a compelling way. It's one thing just to provide user notifications but vendor roadmaps need to evolve so that they point users to easily understandable and readily available fixes. That said, the large majority of users ignore security notifications. They need to be able to 'set it and forget it'. Where users ignore notifications, protections nevertheless need to be applied automatically.

Key security features must not be considered in isolation from a vendor's alignment with more basic technical and commercial requirements, however. These include:

Technical compliance for a prpl security app

- **Deployment proof points,** including stand-alone deployments as well as integrations with prpl-compliant experience management software that optimize whole suites of prpl applications relative to the unique profile of a specific household.
- **Efficient use of resources**. An outstanding-looking feature may not be very useable if it has to draw too heavily on router hardware resources.
- **Future Application certification**. For now, the prpl certification programme only certifies hardware (see **Figure 4**). However, a new work item is underway to extend certification over time to application software. There is a big job to be done to define and meet the requirements of the telco community here and it will take time. Ultimately application certification will assure that a prpl-certified app is secure, portable and interoperable across multiple CPE devices and providers.

Telco network and security operations has a very strong interest in blocking malicious outbound traffic from compromised smart home devices reaching the telco's own network.

Attractive commercial terms for a prpl security app

- **Flexible, modular pricing**. Within the same app, many telcos want to be able to offer customers a basic set of features and upsell them on premium features. An app vendor needs to support flexible pricing so telcos can position those which are best suited to their customer segmentation strategies – and at the right price points.
- **Strong after sales support** so that telco customers can learn from and implement best practise in marketing and selling router-based security to householders.

prpl's value for network and security operations

As stated throughout this paper, monetization is the driving force behind prpl. The core aim is to enable telcos to grow their revenues with faster time to market. In that context, cybersecurity is just another value-added service or app to be monetized. But the capabilities of prpl can also be leveraged for potential opex savings for telcos and for achieving critical societal goals in terms of reducing cybersecurity risk.

Telco network and security operations has a very strong interest in blocking malicious outbound traffic from compromised smart home devices reaching the telco's own network. This malicious traffic risks causing network congestion and gets handed off to peer telcos and ISPs, typically destined for malicious command and control (C2) servers. This damages a telco's IP reputation among its peers. Enough malicious traffic can even trigger a DDoS outage in a telco's own network or that of a peer telco or ISP to which malicious traffic is handed off.

Network and security operations teams running fixed broadband networks are already familiar with managing the risk from smart homes. But the risk is relatively new to 4G and 5G Fixed Wireless Access (FWA) networks. In this case, it is limited and often expensive spectrum resources in the last mile that are at risk of congestion from malicious traffic rather than almost unlimited fixed broadband capacity. U.S. operators deploying FWA services are committed to deploying open source home routers. For example, Verizon is committed to prpl-based routers for 5G FWA. Today, the network and security operations side of the telco organization isn't yet putting its shoulder to the wheel to help drive the prpl ecosystem, but there's a strong case for it to do so.

Figure 5: When home router vulnerabilities become a large-scale security operations challenge

Year	Market	Telco	Attack & Impact
2023	U.S.	Windstream	A malicious firmware update bricked 600,000 SOHO routers by deleting their operational code. The commodity remote access trojan (RAT) hid itself by encrypting C2 comms. Even if the replacement cost was only $100 per unit that's a $60 million cost.
2024	U.S.	Multiple	The FBI disrupted KV botnet, operated by Volt Typhoon, a Chinese nation state threat actor, which was targeting end of life Cisco and Netgear home routers with malware.
2024	Global	Multiple	Vulnerabilities in 157,000 botnet enslaved Asus home routers were a primary driver of a world-wide, month-long, L3/4 DDoS attack campaign, peaking at 3.8 Tbps. Telcos and financial firms targeted according to Cloudflare.
2025	Asia	Major Asian telco	China-linked 'Weaver Ant' APT found to have been spying within the telco's network for four years. Used operational relay box of compromised Zyxel home routers to proxy traffic and conceal infrastructure. Multiple eviction attempts were unsuccessful.
2025	Global	Multiple	During 2025 the 'Aisuru' botnet of 700,000 compromised IoT devices launched several 20 Tbit/s DDoS attacks. Most recently, compromised IoT devices in the homes of AT&T, Charter, Verizon and other customers were exploited in attacks on telcos and ISPs hosting gaming communities but other telcos were also impacted.

Source: HardenStance

Figure 5 features a number of large-scale incidents in which hundreds of thousands of smart home devices have either been impacted or alternatively have been used for cyberattacks on other targets. **Figure 5** demonstrates not just that any one telco's network and security operations has an interest in more secure smart home networks to protect itself. It also points to how telco operations teams need to collaborate with one another to better protect each other at the national, regional and global level.

Large scale cyber threats that exploit compromised smart home devices can be a national security risk, provoking civil disruption and unrest.

Government intervention is helping – a bit

Telcos and their customers aside, government also has a major stake in averting the impacts of the attacks cited in **Figure 5**. Legislators, regulators, law enforcement and national security agencies all want home routers to be secured at scale. As well as enabling criminality, large scale cyber threats that exploit compromised smart home devices can be a national security risk, provoking civil disruption and unrest. That's especially the case where outages are timed to support phases of a full-scale military campaign. This is the strategic intent that the U.S. and its 'Five Eyes' partners have attributed to the Chinese state threat actor, Volt Typhoon, cited in **Figure 5**.

This concluding section assesses the impact government intervention has started having on reducing cyber threats to home networks. This intervention is taking two main forms:

- Legislators and regulators are mandating higher standards of cybersecurity for consumer IoT products including home routers.
- Law enforcement agencies are ramping up their efforts to take down malicious botnets that exploit smart home devices as well as prosecute those operating them.

The latest evidence suggests these efforts are having some positive effect. At minimum they are helping contain the rate at which these cyber threats escalate. So far, however, the evidence suggests that while these efforts could materially reduce cyber risk in the long term, their short-to-medium term impact will mostly be marginal.

The impact of new legislation and regulation

The following examples show how some well-crafted government interventions are helping to make it harder for malicious hackers to succeed and points to flaws in some less well-crafted government interventions.

1. IoT security regulation in the UK, Germany, Japan and Singapore

In the last two to three years, the UK, Germany, Japan and Singapore have all introduced new regulations mandating better cybersecurity practice by consumer IoT product vendors. Their different initiatives all leverage ETSI standard ETSI EN 303 645 which provides guidance according to 13 core security principles.

The regulations introduced by all four leading countries mandate that consumer IoT vendors must initially adhere to a minimum of the first three principles – no universal default passwords; implementation of a vulnerability disclosure policy (VDP); and commitment to keeping software updated. Taken together, these countries' new regulations form a big enough market to directly influence the roadmaps of global consumer IoT vendors. Two recently published datasets show the positive impact these new regulations are having:

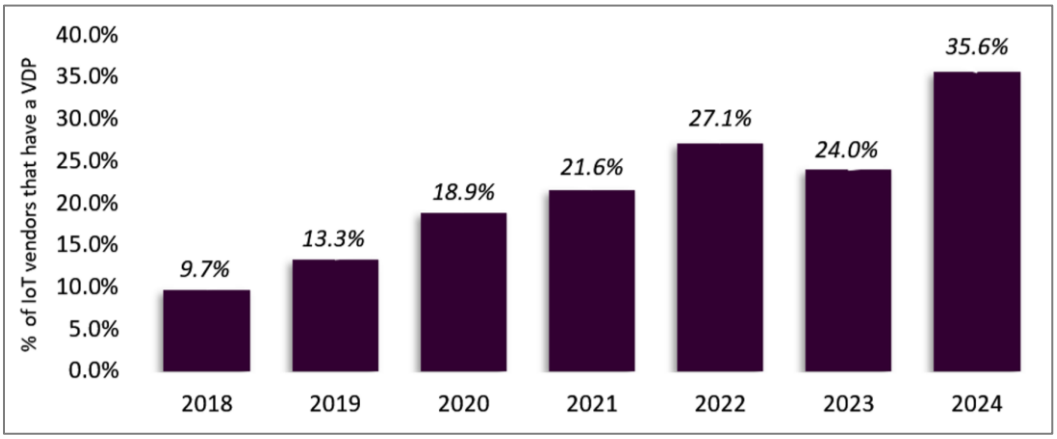
27% of vendors claimed compliance in terms of security updates but survey researchers could only find evidence of that for 19% of them.

- **A UK Department for Science Innovation and Technology (DSIT) survey of consumer IoT manufacturers offers some encouragement**. Published in December 2024, it found that 52% of manufacturers of consumer IoT devices reported being fully compliant with the requirement to implement unique passwords as set out in the UK's new Product Security and Telecommunications Infrastructure (PSTI) Act. 27% of vendors reported compliance with the requirement to provide information on the minimum length of time for which security updates are available.

  These numbers are bound to represent a year on year improvement (and probably a significant one) compared to before the Act came into effect. There is a rider to this, though. The survey highlighted a variance between the compliance claimed by vendors and publicly available evidence of that compliance. For example, 27% of vendors claimed compliance in terms of security updates but survey researchers could only find evidence of that for 19% of them.

- **Copper Horse's "The state of vulnerability disclosure policy usage in global consumer IoT in 2024" provides perhaps the most encouraging data point.** The main reason is the combination of a positive trend and the global scope of the survey. As shown in **Figure 6**, the number of global IoT manufacturers that serve consumer markets and have a vulnerability disclosure policy (VDP) grew to 35.6% at the end of 2024. The trend shows good progress. However this does still mean

Figure 6: Most IoT manufacturers have no vulnerability disclosure policy (VDP)



Source: Copper Horse Ltd: "The State of VDP Usage in Global Consumer IoT in 2024"

that two thirds of these vendors still had no way for security researchers to even contact them about vulnerabilities in their products. Moreover, assuming the positive trend is maintained, it will likely still be years before a large majority of vendors have a VDP.

2. The House of Representatives and Federal agencies in the U.S.

From their recent activities there can be no doubt that legislators and federal agencies in the U.S. recognize the threat that compromised home routers present to America's economy and national security:

- **The Removing Our Unsecure Technologies to Ensure Reliability and Security (ROUTERS) Act**, addressing telco network, enterprise network and home network routers, was passed by the U.S. House of Representatives in April 2025 (though it has yet to be passed by the Senate).
- **The Washington Post reported in October 2025 that at least 6 U.S federal departments and agencies support a ban on future sales of TP-Link**, one of the most popular home routers. According to the newspaper, this is "on the grounds that the vendor's ties to China make them a national security risk."

Though well intentioned, both these efforts take insufficient account of the risk from benign vulnerabilities in the products of trusted vendors.

So far, high profile takedowns aren't turning the overall tide on malicious botnet activity.

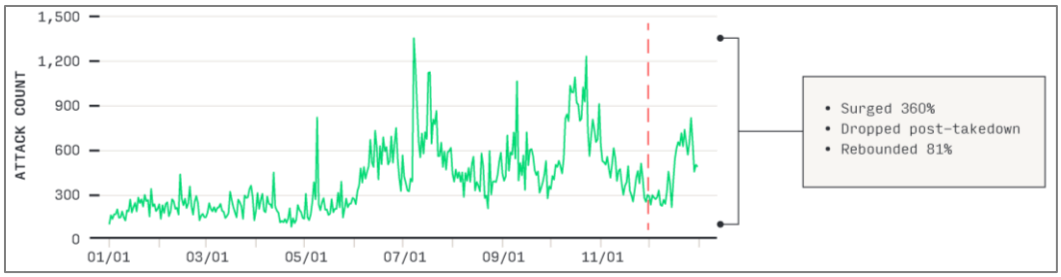
Despite big takedowns, malicious botnets are thriving

Besides regulation on IoT products, the other way governments are acting is by disrupting malicious botnets. Especially in collaboration with international partners, governments can point to some recent high-profile successes. One example is the take down by the FBI and international partners of the 911 S5 botnet in May 2024 and the arrest of its administrators. The 911 S5 botnet comprised 19 million compromised IP addresses. At the time it was widely considered the world's largest botnet.

So far, though, high profile takedowns aren't turning the overall tide on malicious botnet activity. That's in part because the way malicious botnets are engineered for redundancy makes them very resilient at recovering after a temporary pause in activity. This is evident from recent data shown below. It points to sharp peaks and troughs in indicators of botnet activity. To date there is no clear trend of malicious botnet activity declining:

- **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 positive 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 in 2023 that scanning events probing for open ports, misconfigurations and Common Vulnerability Exploits (CVEs) were down 7% to 5.1 million compared with 5.5 million in 2022. However, this then spiked sharply by 71% to 8.7 million scanning events in 2024. Normalizing the count for variable factors from one year to the next, the year-on-year growth figure for 2024 was put even higher at 94%. In the case of scans for Common Vulnerability Exploits (CVEs), the 2024 survey found that 42% of them targeted IoT devices and consumer routers.

Figure 7: MIRAI-involved attacks on telco networks (2024)



Source: NETSCOUT's DDoS Threat Intelligence Report (2H 2024)

Governments have started to take action, but they still need to do more (and in some cases better).

- **Netscout data points to very sharp spikes in botnet-driven DDoS attacks targeting telecom operators.** As shown in **Figure 7**, Netscout reports very sharp spikes in volumes of DDoS attacks targeting telcos originating from the MIRAI botnet, which remains extremely active almost 10 years after it first brought huge disruption to the Internet in the U.S and Europe in late 2016.

Multiple layers of security and collaboration across all of them

As this concluding section demonstrates, government intervention is important in a multi-layered approach to securing smart homes against cyber risk that threatens other targets as well as individual householders themselves.

As also shown, governments have started to take action but they still need to do more (and in some cases better). As with any layer of cybersecurity, government intervention doesn't represent any kind of silver bullet. All parts of the ecosystem – including both the sales and operational sides of telco organizations – must intensify their collaboration efforts within partner ecosystems like prpl. That's how to accelerate the speed at which home routers and connected devices can be hardened at scale.

"Telco Strategies for Consumer Security 2026"

HardenStance is hosting its "Telco Strategies for Consumer Security 2026" report and webinar programme on February 10th. To receive the report and attend the webinar you can **REGISTER HERE**

More Information

- "The Bitdefender and NETGEAR IoT Security Landscape Report (2025)"
- AT&T White Paper: "AT&Ts Container to prpl Foundation Life Cycle Management (LCM) Transition" (May 2025)
- UK Department of Science, Innovation & Technology (DSIT) Survey: "Cybersecurity of Consumer IoT - Manufacturer Survey (December 2024)
- prpl Foundation video: "Building Secure Broadband CPE & Wi-Fi Devices with prpl, featuring security working group leaders from Verizon and Vodafone (2024)"
- HardenStance Briefing: "Telco Strategies for Consumer Security 2025"

About Bitdefender

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

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

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

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. 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, ETSI and TM Forum. To learn more visit www.hardenstance.com

HardenStance Disclaimer