White Paper

HardenStance

Two-Sided Security for 5G Fixed Wireless Access

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

Bitdefender NETSCOUT

June 2024

Executive Summary

- 4G and 5G Fixed Wireless Access (FWA) are highly disruptive of mobile network engineering and operating models. To succeed in this market, telcos need to mitigate some of the effects of this disruption at the same time as they embrace it.
- Protection against cyber threats and scams is a key part of a FWA value proposition for end users. It's also key to profitable FWA growth for mobile operators.
- Better visibility into both the mobile network itself and the FWA customer's LAN is needed for optimal detection and mitigation of malicious and unauthorized traffic.

FWA can look like 'low hanging fruit'

These are challenging times for telecom operators. At its 'Digital Transform World' event last September, Nik Willets, CEO of TM Forum, an 800 member strong telecom sector industry association, invoked a 'code red moment' for his telco members. Pointing to sector spending of 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."

According to Ericsson, FWA data traffic had already reached 19% of global mobile network data traffic by the end of 2023.

Amid ongoing challenges generating incremental revenues, one of the clear bright spots in the sector is the Fixed Wireless Access (FWA) market. According to the GSM Association (GSMA), more than 120 telcos with mobile operating licences around the world had launched FWA services as of the end of 2023. Originally rolled out using 4G and a variety of proprietary wireless access technologies, the market momentum behind FWA has additional impetus now, arising from large and diverse spectrum allocations; the extensive 5G New Radio (5G NR) coverage that many operators now have, and the additional operating efficiencies promised by 5G Standalone (5G SA).

According to its Fixed Wireless Access Handbook 'Insights' published earlier this year, Ericsson estimates that a little over 30 million of the total 130 million FWA subscriptions in service worldwide at the end of 2023 were connected with 5G. This amounts to around 25% of the global total but this number conceals huge regional variations. According to Ericsson, 5G already accounts for the overwhelming majority of FWA subscriptions in North America, Western Europe and Asia Pacific. In contrast, there are many more FWA subscribers using 4G and proprietary wireless access technologies than there are using 5G in the Middle East, Africa and Latin America, as well as some parts of Asia.

Figure 1: 5G FWA momentum and Targets of Leading Telcos

Country	Telco/ISP	Actual or target number of FWA subscribers
Denmark	Telia	79,000 5G FWA subscribers as of December 2023.
India	Reliance Jio	Commercial service available in 514 cities in 25 Indian states as of December 2023. Targeting 100 million 5G FWA customers.
Norway	Telenor	Having launched FWA in Q4 2020, Telenor had 125,000 FWA subscribers as of December 2023.
Saudi Arabia	Zain	Mobile and FWA services available at launch of 5G in October 2019 across 2,600 sites in 27 cities. 800,000 5G FWA subscribers at the end of 2023.
USA	AT&T	Having launched 5G FWA services in August 2023, AT&T reached 200,000 customers at the end of March 2024.
USA	T-Mobile	Launched 5G FWA at the end of 2021, reached 5 million customers at the end of 2023. In its Q1 earnings, management reaffirmed its original target of 7 – 8 million subscribers and continues to evaluate potential to go beyond that.
USA	Verizon	3.4 million FWA subscribers as of end March 2024 (+84% vs March 2023).

Source: HardenStance

Figure 1 on page 2 shows the numbers of FWA subscriptions that leading mobile operators around the world have already sold or have publicly stated they are targeting. Due to the economies of scale and performance it offers, it stands to reason that 5G's share of the global FWA market will grow rapidly. The GSM Suppliers Association (GSA) reports that 307 different 5G FWA devices were available from 83 different vendors as of November 2023. 5G CPE costs curves should see cost points approaching those of 4G CPE in the second half of 2025. Ericsson reckons 5G will grow its share from 25% of all FWA connections worldwide at the end of 2023 to 85% by the end of 2029.

5G CPE costs curves should see cost points approaching those of 4G CPE in the second half of 2025.

FWA User segmentation and network engineering

For telco marketing professionals, arriving at a suite of FWA service packages to meet the needs of different customer segments is at least as hard as defining mobile service packages. In some ways it's even more complex. Many FWA users will pay a premium to assure they have access to a guaranteed speed tier. Most users should be able to self-install their CPE but a subset may not be able to. And for some high-speed tiers the use of millimetre wave radios requires a professional on-site installation to get the customer up and running.

For a mobile operator's CTO and their team, planning and engineering for FWA creates a lot more complexity than fixed telephony, fixed broadband Internet, or any generation of mobile services has ever done. To the user, FWA is just a variant of fixed broadband. But to a telco CTO, it's a completely different way of exploiting mobile network resources. And to serve new FWA endpoints, those resources have to be used in a way that marks a significant break with tradition.

Verizon's FWA Business and Strategy Update (May 2024)

Where the use of 4G and 5G technologies is concerned, the U.S. is probably the world's most competitive FWA market. T-Mobile has established an early lead in customer acquisitions. It claimed in March 2024 to still be on track to reach 7-8 million subscribers by 2025. AT&T has made a more cautious start, citing 200,000 subscribers in Q1 2024. Verizon is currently positioned between them in terms of subscriber count. Here are some key indicators for Verizon's FWA business as of May 2024:

- Verizon reported net adds of 354,000 in Q1 2024 to give a total of 3.42 million FWA subscribers, of which 2.07 million (61%) were consumers and 1.35 million (39%) were businesses. The company is targeting 4 - 5 million consumer and business customers over the next year. Both 4G and 5G FWA services continue to be sold to consumers and businesses
- Verizon reported FWA revenues of $452 million for Q1 2024, up nearly $200 million year-on-year.
- Verizon's '5G Business Internet' is now available to 2 million businesses in 900 cities. It will be available to two-thirds of businesses by the end of this year. The overwhelming majority of '5G Business Internet' customers use self-install FWA routers leveraging C-Band (3.7–4 GHz) spectrum for speeds up to 200 Mbit/s. So far, only a small subset use professionally installed CPE supporting millimetre wave spectrum for speeds up to 400 Mbit/s. A millimetre wave product for multiple dwelling units (MDUs) or apartments is on the roadmap to be launched by the end of this year.
- Verizon stresses that FWA sales to businesses are not centred on 'fill-in' use cases where there is no fibre or cable footprint. In fact, the majority of sales to businesses are in urban or suburban markets. Small and Medium Businesses (SMBs) account for the largest share of business customers, but public sector organizations and enterprise customers account for one in three sales.
- Verizon will update investors on its plans for the next phase of FWA rollout (likely before year end).

Nevertheless, the disruption of the mobile network model that FWA introduces has to be done in a way that also allows all the smartphones and other devices that connect directly to the mobile network to continue to be supported as before. That's because mobile services tend to generate more than half – often a lot more than half of a telco's total revenues. To put some numbers on it, in Q1 2024 Verizon generated $452 million in FWA services revenues compared to $19.4 billion in total mobile services revenues.

The co-existence of FWA and mobile broadband services

What are some of the challenges and risks involved in supporting these two very different models from the same mobile network platform?

- **Very high bandwidth consumption and the revenue and margin impact**: FWA users typically use anywhere from 20 to 50 times more bandwidth than mobile users. According to Ericsson, FWA data traffic had already reached 19% of global mobile network data traffic by the end of 2023. The company reckons this will reach almost 30% by the end of 2029.

  There are so many different FWA use cases, and so many different regional and local market dynamics, that it's impossible to generalize accurately about how FWA ARPUs compared with mobile ARPUs. For example, where adjacent services like security, TV, streaming and gaming can be sold to consumers, or SD-WAN, SASE or other enterprise security services can be sold to businesses, then FWA ARPU can be significantly higher. In terms of profitability, however, the gulf between the two in terms of data consumption does means that FWA connections do typically tend to yield lower revenue per bit, hence lower profitability than mobile connections.

FWA connections expose a mobile network to subscriber-driven malicious and fraudulent traffic at scale for the first time.

- **Malicious and fraudulent traffic**. FWA connections expose a mobile network to subscriber-driven malicious and fraudulent traffic at scale for the first time. Insecure IoT 'things' at home or on a business premises are just as likely to generate malicious traffic over a mobile operator's FWA connection as an ISP's fibre connection. Increased gaming activity also attracts a significantly higher risk of DDoS activity. Some operators allow some kinds of tethering like using a smartphone as a connectivity hub for other devices. But operators have to rigorously police and act on unauthorized tethering. This includes users abusing fair usage terms and starving other users of bandwidth by hosting an unauthorized high-speed server in their spare room or basement; neighbouring households sharing the same connection; or users leveraging WiFi extenders or repeaters to resell access to a single broadband connection to multiple tenants in an apartment block. Mobile networks are spared these risks – until FWA routers start connecting to them.
- **Pressure on spectral efficiency**. Acquiring radio spectrum is one of the biggest costs many telcos face. Abuse of that spectrum by malicious and fraudulent traffic is a barrier to profitable growth of a FWA business. The same is also true of abuse of a mobile operator's core and transport network resources; albeit it's usually on a lesser scale.
- **Planning for capacity and performance.** The dedication of spectrum to FWA use cases is necessarily a function of whatever excess capacity there is beyond the forecasted requirements for growth in mobile broadband traffic. Operators have to devise, apply and monitor new engineering rules that allow alignment with KPIs and subscriber QoS profiles. This requires specifying metrics such as the limits on how many FWA users (or how many among different types of FWA user) can be provisioned in any one cell site or cell site sector. These rules build on the metrics used for mobile broadband, albeit with some adaption for FWA use cases.

  At this early point in the market's development, most operators are borrowing from the fixed-line ISP world in terms of using fair usage policies as well as speed tiering to manage the relationship between bandwidth allocation and revenue per FWA subscription. 5G SA is designed to bring end-to-end efficiency gains in operating the

600,000 of a U.S. ISP's SOHO routers destroyed in October

As widely reported in May this year, a U.S. ISP suffered a huge cyber attack-induced outage across its customer base last October. The attack destroyed more than 600,000 of the ISP's Small Office Home Office (SOHO) routers. This was arguably the most serious attack on SOHO routers of recent years because of the number of customers impacted and the scale of the damage done.

According to the originating research report from Lumen Technologies' Black Lotus Labs, the destruction took place over three days in October last year. The source of the attack was a malicious firmware update that deleted some of the routers' operational code, rendering the devices inoperable. There was no way of updating them – hardware upgrades were required.

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

As the researchers pointedly noted, "a sizeable portion of this ISP's service area covers rural or underserved communities; places where residents may have lost critical information; farming concerns may have lost critical information from remote monitoring of crops during the harvest; and health care providers cut off from health or patients records."

Having researched the background to the attack for its reporting of the attack, Reuters concluded that the impacted telecom operator was Little Rock, Arkansas-based Windstream Communications.

mobile network. With that, many operators also plan to dedicate one or more network slices to FWA users. While it can be a useful tool, network slicing has so far proved operationally complex to implement, adding to the challenge of using it for FWA (as much as any other use case). Despite adding some complexity to the mobile network operating model, FWA does nevertheless offer the distinct advantage to network planners of the endpoint being stationary. That greatly reduces the statistical uncertainties as to where traffic originates that have to be contended with in managing mobile broadband networks.

Despite adding some complexity to the mobile network operating model, FWA does nevertheless offer the distinct advantage to network planners of the endpoint being stationary.

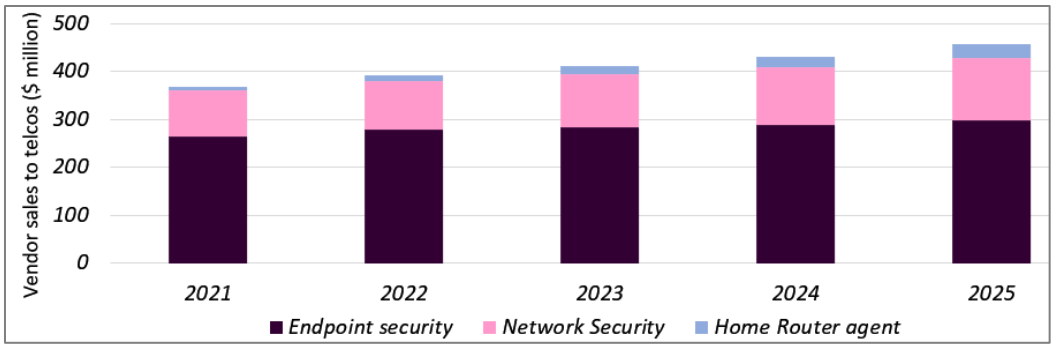
Augmenting security to better protect the end user and the network

The rest of this White Paper looks at measures that operators can use to arrive at better end-to-end network visibility, as well as better threat and anomaly detection and mitigation capabilities, spanning both the operator's mobile network and the FWA customer's LAN environment. Because of their dependencies on one another, these approaches must aim at achieving revenue and profitability targets across both mobile broadband and FWA lines of business as FWA connections scale up.

Beginning with the end user side of the equation, this White Paper directly addresses the home networks and small business LANs that make up the large majority of FWA environments. It doesn't directly address the subset of FWA connections that are enterprise or outdoor deployments in field operations where visibility and security may be managed internally or by specialist providers other than the telco.

Mobile operators inevitably spend heavily on baseline network security. They spend on network security architecture, interfaces and specifications as mandated by 3GPP. They also spend on operational security focused on threats to their entire customer base like DDoS attacks. In addition to those baseline investments, telcos also invest to a more varying degree in cybersecurity software that augments end user security.

Figure 2: Worldwide Telco Spending on Consumer Security Software



Source: HardenStance

As shown in **Figure 3**, despite stiff cutbacks in several areas of expenditure over the last year or two, telco spending on additional end user security software for mobile broadband and home broadband services has been holding up well:

- **Network security**: telco spending is growing in additional network security – typically DNS security – which protects users against malicious websites and URLs.
- **Home router security**: spending is also growing on cybersecurity agents deployed on home and small office routers. These protect every single device connected to the router, whether they're PCs and smart TV's or dumb IoT 'things' like doorbells and garage doors.
- **Endpoint security:** spending has been roughly flat on endpoint security software that protects the subset of PCs and other higher end devices in a household or office that are capable of supporting it.

Unlike endpoint security, a security agent running on a home or small business router can monitor and protect against threats to and from each and every device on the home network or business premises.

As shown in HardenStance's January 2024 report – Telco Strategies for Consumer Security – leaders in this market are investing across all three of these security layers. Many of these telcos are showing tangible results in terms of charging for these security services to grow incremental revenues – they're not just bundling them in for free, without charging any premium. As well as being distinct growth opportunities in their own right, there is an opportunity for telcos to bring FWA and cybersecurity together to bolster the FWA value proposition with compelling end user security features. This is a potential 'win-win' for an operator's customers as well as for the operator itself.

For FWA, home router security is front and centre

Augmenting an FWA proposition with advanced security should certainly feature network based security as well as endpoint based security options. However, the third of the three layers – router-based security - should feature front and centre. Here's why:

- Unlike endpoint security, a security agent running on a home or small business router can monitor and protect against threats to and from each and every device on the home network or business premises. Router-based security also provides far deeper protection than the thin layer of protection against web-based threats that network security provides. It needn't require active engagement by the user either.
- FWA is a relatively new market. Most FWA routers are relatively new products. Hence substantially all these FWA routers – and certainly all 5G FWA routers – have enough processing resources for a cybersecurity agent to run on them. That is not the case in the fixed broadband market which is characterized by a wide variety of routers. Many of these can support a cybersecurity agent but many others can't.
- As shown, FWA connections – and all the devices connected to them – pose a potentially greater risk to efficient telco operations and the achievement of network, service and application level KPIs than fixed-line connections do.

- Open source home and small business router operating systems promise a solution to the age-old cost and complexity of getting cybersecurity agents (and other value added service apps) to work on the proprietary OSes of many dozens of different routers built by many dozens of different vendors. For years, this has inhibited telcos and security vendors from partnering well for home router-based security.

  RDK-B is an open source OS that is already widely deployed in North America, driven by the big cable operators. Worldwide, there's more momentum behind prpl, which has backing from AT&T, Verizon and Orange. All three of these leading telcos have prpl-based home routers in their roadmaps. Verizon Business confirmed in a May 2024 analyst webinar that a prpl-based FWA router is on its roadmap.

- Decisions on whether to charge FWA customers for the security agent on their router or to provide it as bundled part of the service should be independent of a decision to require that the agent be embedded as a default build requirement in FWA router products. Telcos should ensure that both options remain open to them.

Some home router security agents can block anomalous or malicious traffic from a connected device without having to engage the user and without affecting the device's useability.

Key features of a robust home router security solution

Here are the sorts of capabilities that a FWA router running a security agent can provide to protect the end user as well as protect the mobile operator's network against abuse.

- **Block anomalous or malicious traffic from a connected device without having to engage the user and without affecting the device's useability.** For the user, this ensures that a misbehaving garage door opener or doorbell can still work. It also reduces any risk of their service being temporarily suspended due to a device participating in a botnet. This also keeps malicious traffic out of the mobile operator's network according to what amounts to the 'holy grail' of telco network security, i.e. blocking bad traffic at source rather than deeper in the network once network resources have already been consumed. This can include LAN-level DDoS protection against incoming attacks (by blocking attacker's known IPs) as well as outgoing attacks (preventing connected devices from participating in DDoS attacks)

- **Best in class security patching throughout the router's lifecycle.** Some telcos are dependent on their home or small business router vendors carrying out security patches for them. That leaves those devices highly vulnerable when they reach end of life and security updates are no longer supported. Also, firmware deployments tend to be slow and complex. Patching and fixing these vulnerabilities can take weeks or months. In the interim, router agents should be able to at least monitor for signatures of known vulnerabilities and block that traffic with immediate effect.

- **Protection against brute force attacks**. Security agents can protect routers themselves as well as individual connected devices against brute force attacks that use trial and error to crack passwords, log in credentials and encryption keys across those multiple protocols like FTP, SSH, Telnet, HTTP or HTTPS.

- **Device fingerprinting and updating.** Each and every device that's connected to the network can be identified, together with core information about the manufacturer and model name, OS and version. Devices that establish a new connection to the network – as well as disconnections of currently connected devices – can be flagged in a user app. Metadata and packet level data across multiple protocols can be continuously monitored and analyzed to identify when a device has been updated and ensure the device definition is updated.

  There are both cybersecurity and monetization use cases for this. Knowing whether a device is used by a human or not establishes whether to expect deterministic or non-deterministic behaviour. Anomaly detection can be used to spot potentially malicious changes in deterministic behaviours. On the monetization side, granular information about the installed base of specific devices connected to the router can be used to create customized upgrade packages.

The two use cases come together where telcos can identify that nine out a user's 24 connected devices can support an endpoint security client but only three are currently doing so. That user can be advised that two of their five paid licences are currently unused and an additional five licences can be offered at a steep discount.

- **Formats that can run on open source OSes.** The best home and small business security software vendors make their solutions available so that they can run on open RDK-B and prpl OSes as well as on proprietary vendor OSes.
- **Actionable information.** There's no doubt at all that only a small subset of users will act on any alerts or advisory information that's made available to them. The idea that this information therefore has little value is nevertheless misplaced. It certainly has value to the subset of small business users and advanced home users that are willing and able to act on it. Just as importantly, a telco that has access to that information can act on it on the user's behalf. As well as the use cases already discussed, others include making this detailed information to customer care centre employees when customers call to complain that they've been hacked.

5G SA introduces a host of new vulnerabilities into day to day mobile network operations at the same time as it introduces new efficiencies.

Security monitoring within the mobile network

As far as the FWA customer's premise is concerned, the only factor driving new security requirements is the introduction of the new FWA service. On the mobile operator's side there are two factors driving these same requirements:

- The first is, similarly, the new challenges to the mobile network posed by having a FWA router connected to it that is serving a myriad of devices, some or many of which have inadequate security (or no security at all).
- The second is the rollout of 5G SA. That's because 5G SA introduces a host of new vulnerabilities into day to day mobile network operations at the same time as it introduces new efficiencies.

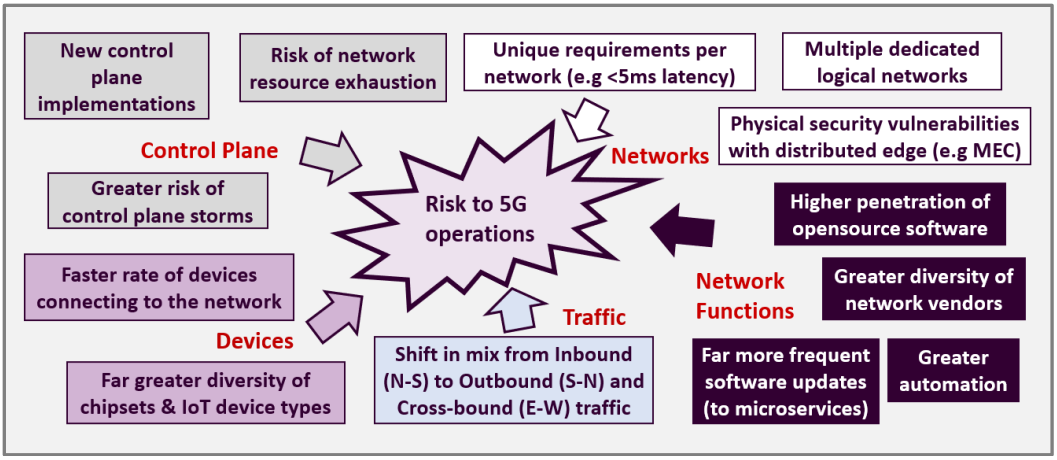
As depicted in **Figure 3**, the dynamism of a much more open cloud native network composed of microservices is an unforgiving environment for meeting stringent KPIs and business customer SLAs, including in relation to delivering network slices. The use of open APIs based on the HTTP/2 protocol is an environment which is also much more familiar to hackers than the closed telco industry protocols of 4G, 3G and 2G.

The two lines of business must be considered together

Attempting to isolate which of the two services – mobile broadband or FWA - is the greater driver of new security requirements tends not to yield a compelling answer. If visibility, threat detection and mitigation is inadequate, then in revenue terms the greatest business risk is clearly posed to mobile broadband revenues as users are migrated to the 5G SA core. However, on a per connection basis, as shown, a single FWA connection misbehaving in terms of things like DDoS threats and aggressive scanning tends to create a lot more disruption than a single mobile broadband connection. So long as an operator is intent on supporting both mobile broadband and FWA, both are important for different reasons. Investment must take both into account.

The baseline requirement for ensuring FWA and mobile broadband service types can co-exist so that profit and revenue targets are aligned is comprehensive end-to-end insight into both user and control plane traffic across core, transport and RAN domains. Granular insight into user traffic is needed so that operators can classify specific inbound and outbound traffic types. Control plane visibility is needed to attribute individual subscriber and device identities to user traffic as it traverses the network. Correlation is needed to allow the operator to map specific behaviours to specific devices. Making those classifications and correlations is key to operators being able to attribute fraudulent or malicious traffic to specific accounts so that they can take action to mitigate and/or remediate it.

Figure 3: An Unforgiving 5G SA Environment for Mobile Network Operations



Source: HardenStance

There's a large body of industry knowledge of how to do this kind of threat detection and mitigation in fixed broadband networks. However, it's new to mobile networks because deploying FWA at scale in mobile networks is relatively new. The compounding effect of 5G SA on network complexity and the introduction of new risk is new too. There are some fundamental differences in the workings of any mobile network, whether it's 4G, 5G NR using the 4G core, or 5G SA. These mean that while the same high level threat detection and mitigation principles can be ported from the fixed-line world into mobile network operations, some of the detail has to be different.

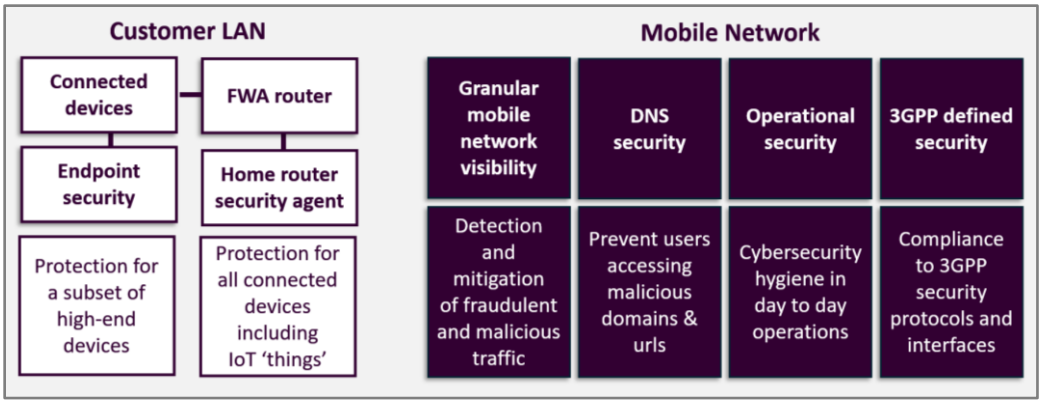
Mobile user traffic in 4G and in 5G NR is in GTP-U tunnels so rather than relying on flow as is typically be done in a fixed network, different methods are needed to extract user plane telemetry.

- Within a mobile network, user traffic in 4G and in 5G is in GTP-U tunnels. Telemetry from within the mobile network gives a complete view of user activity, in, out and cross-bound. Rather than relying on the flow-based technologies typically used to get user traffic visibility in fixed networks, different methods are needed to extract user plane telemetry and expose it to detection and mitigation engines.
- In order to identify a specific subscriber's devices and make use of policy control for mitigation in the mobile network, the identity of the FWA or mobile endpoint must be known. The control plane provides this data, and can be correlated with the user plane so that traffic can be mapped to a given user by the 3GPP-specified International Mobile Subscriber Identity (IMSI), to a device type, cell location etc.

Using fine-grained security analytics then allows the mobile network's blocking, re-direction and rate-limiting capabilities to be exploited with confidence through inter-working with the 4G Policy and Charging Rules Function (PCRF) or 5G's Policy Control Function (PCF). Depending on what types of network security solutions an operator already has deployed across its fixed infrastructure – and from which vendor – operators may be able to deploy the required security monitoring, detection and mitigation capabilities in the mobile network by augmenting their existing wireline network security solution with additional capabilities.

The obvious motivation for operators deploying these security monitoring capabilities in the mobile network is a commercial one - it's critical to enabling them to prevent and stop bad traffic from consuming expensive capacity, maintaining KPIs, and assuring a high quality of service across the two types of FWA and mobile broadband services in alignment with business goals. There's also another less obvious reason. In a lot of countries, there are strict consumer protection laws a telco must comply with in order to justify suspending a broadband service for abusive behaviour. Hence telcos can also leverage this information to create the supporting legal documentation they are required to present.

Figure 4: Two-sided security within a layered approach to FWA security



Source: HardenStance

FWA deployments need to harden cybersecurity on both the customer LAN side and on the mobile network side.

Two-sided security for FWA

This paper has addressed the new opportunity presented by leveraging the mobile network at scale for FWA and the new challenges of managing that line of business alongside mobile broadband services. From a cybersecurity perspective the case that is made is also rooted in the very well established principle of layered security.

As shown in **Figure 4**, some of these layers are already in place. But as FWA is rolled out, the new ones pointed to in this paper need to be added in. To scale successfully and without negatively impacting mobile broadband services, FWA deployments need to harden cybersecurity on both the customer LAN side and on the mobile network side as outlined. Without this hardening on both sides, telcos run the risk of leaving themselves exposed to significant subscriber experience and network performance problems. Either of these, or both combined, pose a risk to any mobile operator's FWA revenue and margin targets, and potentially to its mobile broadband business too. ■

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 consumer, enterprise, and government environments. Bitdefender is trusted by telco partners all over the world, for which it delivers comprehensive protection solutions such as router and IoT protection, network protection, device protection, and privacy. As a pioneer in CPE protection, the company has been at the forefront of innovation, constantly improving its IoT security agent over the last decade. This mature security solution leverages AI and machine learning to provide robust protection to millions of routers worldwide.

The proliferation of 5G Fixed Wireless Access (FWA) introduces new challenges and security risks for both end users and telcos. Because this type of equipment typically serves remote or rural areas, any service outage could have disastrous consequences for users. At the same time, mobile operators cannot tolerate malicious traffic that chokes the network and cannot afford service disruptions.

Bitdefender's router-based security components are designed to protect FWAs both from a user and a telco perspective thus safeguarding smooth and uninterrupted online access.

Bitdefender Router Protection protects the router against attacks coming from both within the home network, and from the open Internet. At its core, it uses the Bitdefender Global Protection Network to offer:

- **Exploit prevention** - intelligent Intrusion Detection and Prevention System (IDS/IPS) that protects its host against even the newest vulnerabilities.
- **Brute force protection** - Bitdefender Router Protection protects routers from brute force attacks and makes them less likely to become part of botnet armies.
- **DDoS protection** – Protects against both external attacks and potential attacks from "guest" devices.

Bitdefender Smart Home Security automatically protects all network connected devices, including WIFI connected IoT devices, against security and privacy threats:

- **Device fingerprinting –** Machine learning is used to identify each device connected to the home gateway, including information such as manufacturer and model name, operating system and version, network name, etc.
- **Vulnerability Assessment -** When a new device connects to the home network, it is automatically scanned for vulnerabilities. (open ports and services with default credentials or weak passwords, firmware or services with known vulnerabilities etc.)
- **Anomaly Detection -** Machine learning algorithms and cloud correlation are used to learn how home network devices behave. Users are notified of any anomalies in their devices' functionality.
- **Web Protection -** Checks outbound connections against the Bitdefender Global Protection Network, allowing users to browse the Internet safely and engage in any online activity without concern.

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

About NETSCOUT

NETSCOUT is a leading provider of service assurance, DDoS protection, cyber security, and business analytics solutions to the world's largest and most innovative service providers, enterprises, and government agencies. NETSCOUT has a 40-year heritage in highly scalable network packet acquisition and analysis for fixed, cloud, and mobile 4G/5G networks. Via its acquisition of Arbor Networks, NETSCOUT provides industry-leading DDoS attack research and Adaptive DDoS Defense solutions for fixed cloud, and mobile networks.

As 5G Fixed Wireless Access (FWA) increases mobile network traffic to levels previously associated with fixed-line networks, these networks will face the same service availability and quality risks that have plagued wireline networks for years. The performance of costly radio spectrum and resources will be adversely impacted by the presence of heavy users, unauthorized servers, and illegitimate traffic from compromised devices/bots executing DDoS attacks.

To fully understand what is happening, and to mitigate any threat, whether east-west or north-south, User Plane and Control Plane traffic must be correlated to establish the identity of the devices involved in suspicious activities.

NETSCOUT's Arbor Sightline Mobile and MobileStream products protect FWA infrastructure by identifying, anomalies and security threats before they consume network resources and adversely impact services. MobileStream utilizes scalable DPI technology from NETSCOUT's market-leading mobile service assurance solutions to monitor both user and control plane traffic within 4G and 5G networks. MobileStream

passively monitors this traffic, correlating user traffic to device identity, location and service, and streaming this telemetry to Arbor Sightline Mobile for:

- Network Visibility - Unprecedented subscriber-level and infrastructure-aware traffic visibility
- Detection - Detect threats and DDoS attacks within the 4G/5G network.
- Identification - Quickly identify impacted subscribers, devices, and infrastructure.
- Protection - Correlate control and user-plane traffic in real-time for surgical mitigation.

For more information about NETSCOUT Sightline Mobile and MobileStream products please visit: https://www.netscout.com/product/arbor-sightline-mobile

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 GSM Association, ETSI and TM Forum. HardenStance is also a Cyber Threat Alliance 'Champion'. To learn more visit www.hardenstance.com

HardenStance Disclaimer