No.84
March 19th 2025

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/ NOT SPONSORED

MWC25: Taking Stock of Telco Security

This review of telco security at MWC 2025 includes notes from meetings with Allot, Aeris, Bitdefender, Enea, Ericsson, F5, F-Secure, Fortinet, Gen Digital, Juniper, Mobileum, Netscout, Netnumber, Nokia, Palo Alto Networks, PowerDNS, Ribbon and Whalebone.

- At MWC 2025 earlier this month, the CTO of the UK's National Cyber Security Centre (NCSC) gave the telecom sector a "C+ at best" grade for its cybersecurity efforts. As if to prove his point, less than 400 of more than 100,000 MWC attendees heard his message. No media outlets appear to have even reported on the comment.
- Driven by regulation as well as telco monetization strategies, the single most encouraging theme of MWC 2025 was the number of vendors as well as some operators upping investment in protecting businesses and users from online scams.
- With only incremental features from incumbent vendors on offer, hopes of new vendors innovating in telco security operations solutions were dashed this year.

Telecoms merits a 'C+' grade for its cybersecurity

Ollie Whitehouse's grade might sound harsh if you haven't heard of 'Salt Typhoon' but it's generous if you have.

From a cybersecurity perspective, the most important statement of Mobile World Congress 2025 was served up by Ollie Whitehouse, CTO of the UK's National Cyber Security Centre (NCSC) on the Tuesday of the security conference sessions. When asked by GSMA's Technical Security Director, Alex Leadbeater, what grade he'd give the telecom sector for its cybersecurity posture, Whitehouse shot back with an uncompromising "C+ at best".

That sounds harsh if you haven't heard of 'Salt Typhoon' but it's generous if you have. As an industry, Whitehouse went on, we suffer from optimism bias: "we believe we are doing a good job – that we are keeping up with the threat landscape. That is not true. Telecommunications operators are being penetrated by default passwords and poor configurations. We know more about what's in our sausages than what's in our software. We need to be honest with ourselves and we need to demand honesty from others."

Source: GSMA

Much as cybersecurity professionals might have liked this to set the tone for MWC, Whitehouse's comment did no such thing. Rather it was an anomaly – one that was only detected by 400 or so security folks in the audience. It will have gone entirely undetected by MWC's 100,000 other attendees. A google search on March 19th shows that not one single news outlet had reported on the NCSC CTO's damning verdict.

One of the great clichés of cybersecurity is that it's a team sport that everyone needs to commit to in order to achieve the best results. In the spirt of Ollie Whitehouse's call for honesty, HardenStance can report back that MWC offered up plenty of proof of great telco security practitioners doing their best in very difficult conditions. There was also evidence of vendors investing to improve the tools that are their disposal.

For the first time in human history, we can't trust our own eyes and ears anymore.

But MWC did also serve up evidence, as it does every year, that the telecom sector is a very long way from properly embracing the team sport ethic that's needed if it is to start measuring cybersecurity progress in strides rather than footsteps. Among standalone presentations made during the GSMA's security sessions, three stood out:

1 **Deutsche Telekom's Chief Security Officer, Thomas Tschersich**, framed the risk from AI-driven fakes very well with another memorable one-liner: "for the first time in human history, we can't trust our own eyes and ears anymore."

2 **BT's Chief Security and Networks Officer, Howard Watson**, made the seemingly obvious but nonetheless poignant comment that in the case of telecom vendors the challenge for telcos is to diversify whereas in the case of cybersecurity vendors the challenge is to consolidate.

   No-one will have appreciated that more than Palo Alto Networks CEO for EMEA and LATAM, Helmut Reisinger, who preceded Watson on stage with yet another rendition of the company's relentless messaging around 'platformization'.

3 **Stuart Wiggins, Northern European Theatre Lead for CrowdStrike**, shared some compelling data from the company's latest threat report:

   - Even among the top three sectors China-nexus adversaries most commonly target — government, technology, and telecommunications — China-nexus activity increased 50% in 2024 compared to 2023.
   - Seven new China-based targeted intrusion adversaries were identified in 2024, five of which are unique in their specialization and sophistication. LIMINAL PANDA, LOCKSMITH PANDA, and OPERATOR PANDA are high-capability adversaries with unique telecom network targeting remits and toolsets.

Reflecting meetings with a variety of different networking, security and fraud protection vendors, this report on what HardenStance saw and heard throughout the week in Barcelona is organized into three sections:

- telco network protection;
- enterprise network protection;

  and

- user protection

1. Telco network protection

Exhibition pods that promote the efficiency and efficacy of telco SOC operations tend not to get that much footfall at MWC – mainly because there isn't much incremental revenue or 'monetization' in it. These are the solutions where one of the first questions telco management tends to ask is "yes, all well and good but can we do without this? Just how much do we risk losing if we postpone investing another year (or more)?"

As of MWC last year, HardenStance had been working on product and marketing strategies with two vendors – one a big American vendor, another a small startup. Both were targeting an out of the box AI-driven telco security operations platform tailored to a telco network's unique domains, protocols, attack surface and scaling needs. At the time, HardenStance was optimistic about telco-focused innovation in security operations. But in the subsequent 12 months leading up to this year's MWC, the big American vendor pulled its product development and the start-up also went very quiet.

Telcos may lament the limited choice of vendor partners but that won't change unless more of them are willing to commit more resources to this space.

Telco security operations platforms are still proving challenging

Telco security operations is a market space that is characterized by increasingly well-established products from very well-established vendors. At MWC, these vendors occasionally have new products to announce. More typically their pitches, as detailed below, are about new features that have been added in the last twelve months or are expected to be added in the next twelve.

This year HardenStance met with one large vendor at the Fira Barcelona. Their guy shared that they were working on – guess what? – a new out of the box, AI-driven telco security operations platform tailored to a telco network's unique requirements. He said they were targeting launch by the end of this year. Hope that there might be some new innovation here after all were soon dashed, however. As Hardenstance was preparing to release this report, that same large vendor – that same guy – reached out to say that the content of our conversation two weeks ago could not now be published. Why? Because a lead telco POC customer had pulled out, meaning the project is now on hold.

Depending on what you're trying to achieve, and what product you're targetting, the legal, data protection and scalability challenges associated with accessing, ingesting and processing telco traffic and telco logs for security ooperations can be decidely non-trivial. Telcos may lament the limited vendor innovation in this space but that won't change unless telcos are willing to commit more of their own R&D resources.

Ericsson

- Ericsson pointed to continued momentum with the Ericsson Security Manager (ESM), its security automation and orchestration platform for mobile networks. Somewhat behind Nokia, which demonstrated the application of Gen AI in its Cyberdome solution at MWC last year, Ericsson has recently made available a first version of a Gen AI Assistant for ESM. The main use cases are explaining gaps in configurations, as well as compliance and mitigation recommendations.

  Following a new partnership announcement last summer, Ericsson now uses Post Luxembourg's Telecom Intrusion Detection System (TIDS) for detecting roaming signaling threats in conjunction with Ericsson's own signaling firewall product together with integration into ESM.

- Nowadays, Ericsson is selling 'Premium RAN Security' solutions. What it calls 'Integrated Endpoint Detection and Response' or 'Integrated EDR' leverages threat monitoring and detection software. In contrast with enterprise IT-grade EDR or XDR solutions, Ericsson IEDR is customized to operate within the radio baseband without disrupting RAN service or application performance. Telcos will have to decide just how much risk this solution can buy down. Some sense of how much they are

spending on it might be inferred from whether Ericsson is invited to speak on EDR alongside CrowdStrike at MWC 2026.

Netscout

- Netscout is fortunate in so far as it occupies the premium end of the telco security operations solutions market – namely the DDoS protection segment where the need for a high and sustained level of spending isn't contested by any tier one telco worthy of the name.

  Having launched MobileStream and Arbor Sightline Mobile for mobile network security operations in the run up to MWC 2024, Netscout's pitches had more of an incremental augmentation feel to them this year.

  Examples include:

  - Improvements to the Sightline product line so that it can detect and classify traffic types based on their sources as well as their destination.
  - Progress on the roadmap to enabling cyber threat mitigation via the Policy Control Function (PCF) in mobile networks.
  - Leveraging Netscout's DPI portfolio so SOC operatives can access all the data they need to reduce time to threat mitigation and remediation. This includes providing new visibility into dropped as well as forwarded packets and being able to review traffic flows retrospectively. Examples include the following:
    - Enabling an automated mitigation template generated on a Saturday to be manually enhanced by a SOC operative reviewing the threat traffic on the Monday - and adjusting the mitigation template according to their findings.
    - Threat actors will often tweak attacks from one target to another. Rather than just providing high level statistics on this, Netscout is enabling SOC operatives to review what these changes look like at the level of individual packets. This can help defenders understand the evolution in attackers' Tactics Techniques and Procedures (TTPs).
    - For DORA compliance, some financial services customers that telcos serve with DDoS protection want to be able to review attack traffic that has targeted their organization even if didn't impact them at all.

Netscout pointed to progress on the roadmap to enabling cyber threat mitigation via the Policy Control Function in mobile networks.

Nokia

- The Netguard Cybersecurity Dome continues to be Nokia's core cybersecurity offer for the telecom sector. At MWC last year, Nokia showcased the application of Gen AI in Cyberdome to better support incident handlers. By enabling them to understand and process incidents faster, last year's demo showed how Gen AI can enable a SOC team to reduce Mean Time To Detection (MTTD) and Mean Time To Respond (MTTR) rates.

  This year's demo showed a different use case supporting proactive detection and threat hunting. Leveraging threat intelligence from other telco security vendors, Cyberdome can monitor for fraud or espionage threats on a telco network interface, like a signaling interface. Cyberdome's 'Hunt Assistant' maps the threat intelligence to the telemetry and then Open AI LLMs hosted in Microsoft Azure can code the entire attack playbook. SOC detection rules can then be rapidly updated so as to prevent incidents altogether.

  As in previous years, Nokia positioned this demo as a telco-network focused extension of SOC operations that complements and augments enterprise-level SIEM and SOAR solutions. By highlighting a single pane of glass across multiple network elements and multiple vendors, this year's demo also showed Cyberdome's potential

to leverage threat detection from other vendors' security tools and add value via better, more automated, mitigation options.

2. Enterprise network protection

As has become more pronounced in the last couple of years, the big NGFW vendors like Palo Alto Networks, Fortinet and Juniper all use MWC to focus their pitches more on selling through telcos to reach enterprise customers than on selling directly to them. The propensity for that balance to switch back at some point might come to serve as a lagging indicator for the rate at which 5G SA is rolling out at scale.

Aeris

- When Aeris acquired Ericsson's IoT business 3 years ago it was just one more example of a leading telecom sector player having tried and ultimately given up on adding value to an IoT business beyond just basic connectivity. Three years on, Aeris made one of the most interesting cybersecurity announcements of MWC 2025 with the launch of the aptly named Aeris IoT WatchTower. This is what the company calls the "world's first fully integrated security solution for cellular IoT."

Aeris IoT WatchTower certainly ticks a lot of boxes in terms of enterprise requirements for IoT security

- Aeris IoT Watchtower is a separate product from Aeris IoT Accelerator, its core IoT connectivity management platform. The software is nevertheless built in at the connectivity layer – no agent or custom SIM card required – so it's easily activated. Leveraging Aeris' own internally developed AI as well as known threat databases from partners, the description certainly ticks a lot of boxes in terms of enterprise requirements for IoT security: real time, inline security monitoring (tick box), visibility (tick box) and security policy enforcement to watch for and block anomalous behaviours and stop or quarantine active attacks (tick box).
- Swisscom Broadcast Service (SBS), which operates Switzerland's largest LoRaWAN, is among the first users of Aeris IoT WatchTower. SBS gains immediate visibility into the security posture of more than 8,000 existing customer gateways. Aeris operates the core network across 25 mobile operators around the world. That makes Aeris a very large global mobile network footprint to which real time IoT security monitoring and enforcement can now be introduced at the push of a button.

F5

- The largest part of F5's pitch in the Fira Barcelona was around its new AI Gateway to manage and secure AI traffic and applications on behalf of both users and providers of AI services. The AI Gateway can be deployed in any cloud or data center and will natively integrate with F5's NGINX and Big IP platforms

Fortinet:

- Fortinet was pushing its 'Sovereign SASE' solution direct to enterprises as well as via telco channel partners. This provides for all data plane traffic to be managed within a customer's own data centre while Fortinet provides the SASE management and orchestration from the AWS cloud. EMEA is the lead market. A single tenant solution is due to be GA in Q2 2025 with multi-tenant due in Q3.

Juniper Networks

- In the week running up to MWC, Juniper announced the new SRX 4700 Next Gen Firewall (NGFW) a 1 U device for telecom operators, cloud providers and large enterprises, claiming throughput of up to 1.4 Tbps throughput per rack.

Palo Alto Networks

- Having been heavily invested in the SASE and 5G security market spaces for many years, Palo Alto Networks chose MWC 2025 as the occasion to announce converging the two in a Generally Available (GA) 'Prisma SASE 5G' solution. With this extension

of the portfolio, telcos can integrate support for an enterprise customer's 5G connected devices to integrate and comply with its SASE-driven security policies.

When an employee uses a 5G connection, they are initially authenticated via their SIM. The traffic is then routed via high bandwidth, dynamically scalable, cross connects between the telco's network and the PRISMA SASE cloud. Here the organization's security policies can be applied per user, application or device based on one or more 5G identifiers like an IMSI or IMEI number.

- Palo Alto Networks pointed to a prestigious lead customer in the form of Singtel for its ability to embed security features into 5G network slices at scale. Although the acronym 'SECaaS' is quite widely used to mean 'Security as a Service' the company has decided to apply that term to its own 'SECurity as a Slice'.

  It is now available as part of Singtel's Mobile Protect for 5G customers. Since its launch six months ago, this has protected over 20,000 customers. It has filtered over 600,000 malicious URLs and blocked over 5,000 cyber threats – such as viruses, malware, spyware and phishing links – in real time, daily.

There is increasing market segmentation according to whether telcos want to lead in protecting against online scams or whether they prefer to be passive and await direction from the regulator.

3. User protection

The major MWC themes from a user protection perspective were:

- a marked increase in engagement and intervention by regulators to guide or direct the implementation of better consumer protection against scams;
- an equivalent ramping up of investment by vendors dedicated to meeting those same goals;

  and
- increasing market segmentation according to whether telcos want to lead in protecting against online scams (and position themselves for incremental revenue), or whether they prefer to be passive and await direction from the regulator.

Allot

- Allot's team at MWC was able to enjoy the context of having just posted positive financial results for the first time in a while. Fourth quarter revenues were up 2% year over year and 7% sequentially, representing a return to revenue growth. Security as a Service (SECaaS), which is at the heart of Allot's 'Security-first' turnaround strategy, continued to grow strongly, increasing 49% year-over-year.
- HardenStance has recently worked with Allot under NDA so has visibility into the company's roadmap for the remainder of this year. Suffice to say for now that the company is intent on applying its core traffic inspection, behavioural analytics and machine learning technologies in new ways as well as augmenting it with other technologies it hasn't previously used. In the case of at least one cybersecurity product line, this will result in a significant improvement in competitiveness.
- One new product line Allot was talking about at MWC was OffnetSecure. This is an additional feature of NetworkSecure, the company's network security solution that allows telcos to block customer access to malicious or inappropriate sites. As the name suggests, OffnetSecure allows a telco to extend coverage not just to the household and its cellular coverage map but also into W-Fi hotspots outside of the telco's own W-Fi coverage. Allot also plays in the home router security agent market segment where it recently announced new telco account wins with Vodafone (UK) and MEO (Portugal).

Bitdefender:

- Being among the leaders in endpoint security for businesses and consumers, Bitdefender is increasingly turning to telco channel partners to grow a mass market in consumer security. The company's Subscriber Protection Platform is tailored to a telco's unique requirements. It boasts one of the broadest portfolios on the market, spanning endpoint security, home router agent, privacy and identity, and network security.
- At the start of 2024, Bitdefender already had more than 15 telco channel partners across different regions. Telefonica Tech and 3 UK were among 5 new telco account wins in Europe during 2024 for endpoint security along with two more in Latin America. Two new North American telco accounts have also signed up for the company's home router security agent. For DNS security, Bitdefender works with partners, including one well-established DNS provider. Last year the company launched Scam Copilot, an AI-powered, all-in-one scam prevention platform aimed at combating scams in real time over various digital environments.

Enea:

- During MWC, Enea announced that its customer, Saudi Arabia's STC, has achieved 100% compliance with the signalling security controls recommended by the GSMA. That's a potentially important landmark that will hopefully encourage other telcos to aim for and publicise hitting that target. In June 2024, Enea also announced that Telecom Egypt, its first voice firewall customer, had seen a 90% drop in malicious CLI spoofing calls following deployment of its solution.

F-Secure's CEO, Timo Laaksonen, is liable to challenge any colleagues that are still tempted to use the term "value added service" to refer to what the company does.

- The new release of Enea's messaging firewall, launched in Q4 2024, supports AI-powered real-time URL analysis for blocking malicious links in messages and Restricted Image Detection (RID). This allows telcos to allow benign messages with embedded urls and images while blocking malicious-looking ones.
- Both Enea and Mobileum affirmed that with demand for 5G SA roaming still moving at a glacial pace, demand for Security Edge Protection Proxy (SEPP) solutions has pretty much stalled.

F-Secure:

- Among other endpoint security vendors, F-Secure is the incumbent market leader in the telco market. It continues to be laser focused on the partnership model with telcos, enabling them to embed, re-brand and differentiate with F-Secure's technology. The company's commitment to making security a core part of a telco's service and brand value proposition is the foundation of its portfolio and strategy. CEO, Timo Laaksonen, is liable to challenge any F-Secure colleagues that are still tempted to use the term "value added service" to refer to what the company does.
- Increasingly, F-Secure is evolving its portfolio to intervene across any one of various stages of a scam as it unfolds across multiple phases rather than just detect and block one specific type of threat. The October 2024 release of its 'TOTAL' endpoint security suite saw the addition of 7 new AI-driven scam protection features: shopping protection; SMS scam protection; banking protection; browsing & phishing protection; Wi-Fi protection; cookie popup blocker and ad blocker.
- As well as its core endpoint security products, F-Secure also competes in home router security software agents where it landed three new telco account wins last year. It works with partners in DNS network security, where it also landed 3 new telco wins last year.

Gen Digital:

- Gen Digital is a global cybersecurity company with a family of consumer brands, including Norton, Avast, LifeLock and Avira. The company is embedded as a partner with several leading telcos including Deutsche Telekom, BT/EE , Pelephone and Telus. Recent new account wins include T-Mobile (Czech Republic); Vox (South Africa) and A1 (Austria).
- LifeLock is a comparatively advanced identity protection service focused on the U.S., where incidents of identity theft leading to large scale financial and other fraud using stolen identities are among the highest in the world. One of LifeLock's best features is a dedicated team of 'Identity Restoration Specialists' who are standing by 24/7 to offer real, empathetic, knowledgeable, customer support. They are available to help identity victims of theft, who can sometimes be highly distressed. Gen Digital has started rolling out advanced identity protection in Europe too.
- Consistent with broader market trends, Gen Digital is driving its value proposition to protect users against a sequence of events associated with a scam as much, or more, than it protects against one single event. The company promises that its AI Assistant, 'Genie', which allows users to verify the authenticity of message content, is just the start of a roadmap of innovation in this critical area.

Gen Digital has started rolling out advanced identity protection in Europe too.

Mobileum:

- Mobileum emerged from Chapter 11 bankruptcy last September with $160 million in financing. Just before MWC, the company announced the release of RAID 9, the latest evolution of its telecom risk management platform.
- Mobileum pointed to a marked change in regulators allowing content inspection of SMS messages for fraud protection, citing new regulations coming into force in Germany as an example. The company anticipates a similar trend in new opportunities in voice fraud protection and has a POC underway for AI-based call analysis which it describes as signature-like detection. The company is well aware that it will need to demonstrate conclusively that its approach cannot be used to breach user privacy.
- Mobileum also noted an acceleration in back end information sharing, including real time information sharing, between telcos and regulators. In the case of the url scanning feature of its SMS firewall solution, Mobieum is now able to offer tight integration with a telco's DNS infrastructure. Both Mobileum and Enea affirmed that with demand for 5G SA roaming still moving at a glacial pace, demand for Security Edge Protection Proxy (SEPP) solutions has pretty much stalled.
- Mobileum also cited accelerated demand for GTP firewalls, albeit the company admitted not being entirely clear what is driving this. One possibility is the efficacy of signalling firewalls encouraging hackers to target GTP instead. Another is telcos looking to protect themselves against Chinese threat actors named by CrowdStrike as Light Basin and Liminal Panda. These have set up fake GTP nodes and GTP tunnels for data exfiltration.

Netnumber:

- Netnumber is a leader in Number Intelligence as a Service (NIaaS), providing up-to-date intelligence on the status of the world's 10 billion phone numbers. The company normalizes data formatting and provides real-time delivery over a unique global signaling infrastructure hosted on AWS.
- Netnumber's pedigree as the routing authority and sender ID registry for North America's messaging market is the background to its MWC 2025 announcement of a new Fraud Prevention Registry (FPR), developed in partnership with cyber threat intelligence firm WMC Global. The FPR enables the rapid exchange of fraud data

among industry stakeholders, including communication service providers, CPaaS providers and enterprises. Launching in North America and then rolling out worldwide, it tracks phone numbers linked to phishing and other fraudulent activities. Once a fraud attack is identified by one of the FPR's participating members, other members can react and prevent the attack from spreading further.

- The other new part of its NIaaS portfolio Netnumber was touting at MWC was its new "Dynamic DNO" service, launched last September. This constantly updates its list of phone numbers that are known to be used only for receiving calls. If a DNO-listed number ever presents as an incoming call, it is by definition maliciously spoofed and can therefore be blocked.

PowerDNS:

- PowerDNS is in the background of more telco DNS security solutions than is generally recognized. The company won another three telco accounts in Europe during 2024 in the Czech Republic (with Allot), Norway and another country, as well as a fourth in Turkey.
- DNS filtering is an important part of the company's overall value proposition. Power DNS for malware protection includes PowerDNS Recursor (reliable, fast and secure DNS resolving and caching server); PowerDNS Dist (load balancing and DDoS protection for DNS traffic); PowerDNS Protect (network based security for fixed and mobile networks); and PowerDNS Cloud Control (cloud native PowerDNS deployments).

The other new part of its NIaaS portfolio Netnumber was touting at MWC was its new "Dynamic DNO" service, launched last September.

Ribbon:

- Ribbon confirmed ongoing rollout of the STIR/SHAKEN components of its Ribbon Call Trust portfolio for caller ID authentication, signing and verification for a number of telcos in France where STIR/SHAKEN is mandated for all national SIP traffic. The company went as far as to specify that it has recently received a batch of new requirements including for better STIR/SHAKEN attestation features.

Whalebone:

- A few days before MWC, Whalebone, the Czech Republic based DNS security provider, was able to announce an additional €13.35 million in funding led by London-based Unbound. Having made good headway with Tier 1 account wins in Central Europe in the last couple of years, 2024 marked a big uptick in account win momentum for Whalebone. During the last year the company landed no less than 17 new telco account wins. Half of these were in regions as far afield as Asia Pacific, Latin America and Africa.
- These opportunities are being driven in significant part by regulators in these markets mandating DNS or other network based security as a universally accessible layer of security for all users. Besides a basic level of protection against malicious or inappropriate sites, the other key benefit is that these are services that can be provided without users having to do anything - or at most having to opt in to a service via a simple text or other tick-box type of response.
- Regulators may be driving this but at this point Whalebone is some way ahead of other DNS vendors in responding to the opportunity. Whalebone is ahead in terms of competitive cost points as well as with the kinds of sales, marketing and business development support that telcos in developing markets need.

GSMA's Open Gateway APIs

The use of GSMA's Open Gateway APIs to drive new revenues featured even more prominently throughout MWC this year than it did last year. Fraud prevention and security use cases that protect telcos, their enterprise customers, and those enterprise customers' end users again featured prominently among use cases.

They featured especially prominently in a presentation with partner guests by David del Val, Telefonica's Global Director, Open Gateway. David shared the following in his talk:

- Telefonica is now offering phone verification from Google Firebase, used by 3.5 million developers to build apps for Google platforms like YouTube and gmail. Telefonica responds to developer requests for verifying specific phone numbers.
- Abel Muino, VP of Engineering with Cabify, a large ride share app with more than 50 million users in Spain and Latin America, shared his company's experience of working with Telefonica. Munio noted the contrast with a manual sign-up process requiring manual inputs, reliance on third party data, and use of one-time SMS passcodes. Noting how this drives some users to disengage part way through the sign up phase, Cabify expects a 7.7% improvement in new user sign up completions by leveraging Telefonica's APIs.
- David Saidden, Global Head of Mobile at TikTok, stated the company is using Telefonica APIs among many data inputs for the purpose of age verification of users.
- BBVA, a large Spanish bank, leverages Telefonica's SIM swap API to verify whether a customer's SIM has been changed recently. The authorisation process is adjusted accordingly if it has.
- Albert Lang, Head of Telecom at Itau Unibanco, a large Brazilian bank, said his company has been using the SIM swap API for about a year connected to its own anti-fraud engine. This was seeing 2 million hits a month at the end of last year. Itau Unibanco is now looking to use addition APIs such as 'Know Your Customer' and device location. As well as reducing fraud, Lang pointed to a 30% improvement in call centre efficiency arising from this partnership with Telefonica.
- Lastly, David stated Telefonica is working with partners on two other use cases:
  - Point of Sale (PoS) provider, Getnet, which is part of Banco Santander, uses the SIM Swap API. This is in cases where a new customer, such as a market stall holder or other small retailer, wants to open a new POS account.
  - Brazilian debt collection and renegotiation companies, Millinium and Creditativos use phone calls among several means of reaching out to debtors who have not paid their bills. These companies use Telefonica's 'Know Your Customer' API to determine the level of confidence they should have that they will reach a specific debtor with a given phone number according to the closeness of the match with the telco's records. The telephone outreach to the debtor is then driven from a different script depending on the level of confidence that the API returns. ■

POS provider, Getnet, uses the SIM Swap API. This is in cases where a new customer, such as a market stall holder or other small retailer, wants to open a new POS account.

HardenStance's annual Telecom Threat Intelligence Summit

Register here for HardenStance's 2025 Telecom Threat Intelligence Summit

"MWC25: Taking Stock of Telco Security", Copyright: Patrick Donegan, HardenStance Ltd, 2025

More Information

- **Virtual Event**: Register for HardenStance's two-day "Telecom Threat Intelligence Summit 2025", taking place on June 10th and 11th 2025.
- **White Paper**: "Proven Ways to Block CLI Spoofing Scams" (March 2025)
- **Briefing**: "Telco Strategies for Consumer Security" (January 2025)
- **Briefing**: "Threat Intel in Telecoms (TTIS 2024)" (August 2024)
- **White Paper:** "Two-Sided Security for 5G FWA" (June 2024)
- **Briefing** "MWC 24: Taking Stock of Telco Security" (March 2024)
- **Briefing**: "A Quantum-Safe Roadmap for Telcos" (March 2024)
- **White Paper**: "Telco Security Takeaways from the NIS2 Directive" (Nov 2023)
- **White Paper:** "Aligning Spectrum Policy with Cybersecurity Goals" (May 2023)

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. HardenStance is also a formally recognized Cyber Threat Alliance 'Champion'. **www.hardenstance.com**.

To receive new public domain HardenStance reports as soon as they are released, register here (there are only five fields): **Registration Link**.

Contact: Founder & Principal Analyst patrick.donegan@hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, 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.