No.76
March 14th 2024

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/ NOT SPONSORED**

MWC24: Taking Stock of Telco Security

HardenStance absorbed the vibes within and beyond the Fira Barcelona at MWC at the end of February. This snapshot review of telco security includes notes from meetings with Allot, Bitdefender, CTOne, DigiCert, Enea, Ericsson, F5, F-Secure, Fortinet, Hiya, Juniper Networks, Mobileum, Napatech, Netscout, Netnumber, Nokia, Palo Alto Networks, SandboxAQ, Titanium Platform, Thales, VMware and Whalebone.

- Cybersecurity was well represented at MWC this year. The quantity and quality of security innovation promoted throughout the event was also better than last year.
- AI was everywhere but cybersecurity use cases had quite a low profile. Using GenAI to augment incident response had a higher profile than traditional AI for threat detection. There was too little emphasis on AI ethics and the security of AI.
- Quantum safety for telcos got a high profile. Raising awareness of requirements and challenges should be prioritized along with executive buy-in and an inventory of current cryptographic systems. The most pressing need is for direction and timelines from regulators. The EU Commissioner promised a recommendation "soon."
- Excluding investment in 3GPP-specified security, new investment by vendors in 5G security for telco networks would appear to be flatlining at best at this time.

Russia recently destroyed Kyivstar's core network

Just over 2 months before this year's Mobile World Congress, Russian state cyber operations executed Phase 2 of perhaps the most devastating cyber attack ever on a telecom operator. The core network of Kyivstar, Ukraine's largest mobile operator, was completely destroyed. Thousands of servers were wiped, leaving 24 million Ukrainians with little or no mobile service for up to two days. Phase 1 involved establishing a presence in the Kyivstar network several months previously for surveillance. Consider too that Kyivstar will have had some of the U.S and NATO's most advanced defensive cyber capabilities at its disposal since (or before) March 2022 when Russia invaded.

Cybersecurity was surprisingly well represented this year.

Then on February 7th – three weeks before MWC - the national cyber security agencies of the U.S, UK, New Zealand, Canada and Australia issued an advisory. They warned that Chinese state cyber operations is less interested in IP theft and espionage now. The focus now is on destructive attacks on telcos and other critical infrastructure of the kind Russia – China's 'partner with no limits' – hit Kyivstar and its 24 million customers with.

The New York AG is investigating AT&T's pre-MWC outage

Only partially related to these developments – the company stated that it was not caused by a cyber attack – the nationwide outages AT&T suffered the week before the Fira Barcelona opened its doors affected tens of thousands of mobile customers. Even emergency 911 services were impacted. Announcing a formal investigation into the incident by her office on the last day of MWC, New York Attorney General, Letitia James, stated that "nationwide outages are not just an inconvenience, they can be dangerous."

This year's security coverage at MWC was surprisingly proportionate

Even with that sort of background context to the event, the best that can reasonably be expected of any general telecom industry jamboree like Mobile World Congress is that cybersecurity should receive a share of coverage in talks and at exhibitor booths which is in some way 'proportionate'. Against that metric, cybersecurity was actually pretty well represented this year.

This was clear from a lot of the content presented by exhibitors but also in terms of the coverage of security topics in MWC conference talks and dedicated seminars. By way of contrast, there was just one single open session dedicated to cybersecurity at the previous MWC a year ago. To add insult to injury, telco security professionals may recall that last year GSMA also pushed that one event out to the last day, day 4.

This year was much better. The equivalent general security seminar was brought forward to the Tuesday (Day 2). Moreover, over the four days, this session was also augmented with three dedicated 2 - 3 hour seminars on AI in cybersecurity, smartphone security assurance, and quantum safe networks. HardenStance was only able to view the post quantum safe networks session but that was well attended and very informative.

Excluding Chinese vendors from the AI RAN Alliance is one less thing for telco security professionals outside China to worry about.

The key cybersecurity themes of MWC24

These were the primary cybersecurity themes HardenStance identified at MWC this year:

1. There's AI with everything - cybersecurity too.
2. Momentum around a quantum-safe roadmap for telcos is picking up steam.
3. There's new appetite for countering telecom fraud.
4. When selling consumer security software to telcos, marketing savvy is winning.
5. New investment in 5G security for telcos appears to be flatlining at best.

Each of these is now addressed in sequence in the next five subject headings. The last section of this Briefing provides a brief summary of each of the 1:1 meetings Hardenstance had with 22 vendors over the four days.

1. AI with everything – cybersecurity too

The AI boom was omnipresent throughout MWC. But while the need to embrace privacy and security imperatives of AI may have been well articulated in the more polished conference sessions, out on the exhibition floor the messaging was the sort of garden variety rough and ready fodder that can leave cybersecurity folks exasperated and fatalistic. There was plenty of blatant disregard for the privacy of customer data on view at booths championing AI use cases. There was next-to-no discussion of how AI algorithms should be defended against being hacked, either.

The impression this gave was that it's still far too easy for companies and individuals to be successful while not caring much – and being seen to not care much – about mitigating privacy and cybersecurity risk. Out on the show floor, privacy and security did still appear to be someone else's job, someone else's problem. There didn't seem to be much evidence at exhibition booths of the well-worn mantras that cybersecurity is a team sport and that it needs be baked in at the outset of everything we do now. Many or even most folks pitching AI didn't appear to have been copied on that memo.

Excluding Chinese players for the AI RAN Alliance is the easy part

The AI RAN Alliance was announced on the Monday of MWC. It made no bones about excluding Chinese participants on what can only be geopolitical, cybersecurity-related grounds. The initial partners are Nvidia; AWS; T-Mobile; Arm; DeepSig; Ericsson; Microsoft; Nokia; NorthEastern University; Samsung, and Softbank.

Excluding Chinese vendors from the AI RAN Alliance is one less thing for telco security professionals outside China to worry about. This will avoid the ongoing headaches that western and western-allied players in the Open RAN community have to contend with arising from the ongoing participation of Chinese companies in the ORAN Alliance. That said, excluding untrusted vendors is the easy part of ensuring high standards of ethics and cybersecurity in the governance and strategy of using AI in telco networks – whether it be in the RAN or any other domain. The ORAN Alliance has only - finally - started going through the gears with cyber security specifications in the last year or two. The new AI RAN alliance should move sooner and faster - on AI ethics, on cybersecurity use cases of AI in the RAN, as well as on the security of AI in the RAN.

HardenStance's experience of talking about AI with RAN architecture and operations leaders in telcos is that they are very enthusiastic – and are already seeing compelling proofpoints – on applying AI to RAN monitoring and network optimization. However, where cyber threat detection and mitigation are concerned, expectations of what AI can do in the RAN are generally lower.

Historically, there has been limited interest in any kind of threat detection in the RAN, whether AI driven or not, because the risk of a major impact arising from something that requires an AI to spot it has been perceived as low. More open interfaces arising with ORAN and the prospect of more remote edge deployments – especially the combination of the two – is nevertheless changing perceptions of cyber risk in the RAN. Change in the cyber threat landscape and mobile network architecture and technology models have heightened the perception of risk overall.

Cybersecurity use cases of may be less top of mind than other use cases of AI in the RAN but there is certainly still interest.

In addition, CTOs used to worry much less about the risk to software integrity in the RAN than they did about availability and confidentiality. Today the risk of the exploitation of ORAN interfaces to breach system integrity to remotely manipulate connected devices, especially in critical industries, has closed that gap. A lot of CTOs worry almost as much about threats to integrity as they do about threats to confidentiality and availability now. So cybersecurity use cases may be less top of mind than other use cases of AI in the RAN but there is certainly still interest.

Examples of AI use cases for cybersecurity at the Fira

Here are some examples of how exhibitors were positioning the use of AI in cybersecurity in telco environments on the exhibition floor:

- **IBM** pushed its portioflio of AI capabilities to the fore. The company insisted that cybersecurity is an important use case - it has been leveraging Watson in conjunction with IBM Security's portfolio for years. However security didn't feature prominently among AI use cases promoted for telcos. The most promising use cases – for which IBM showed a couple of dozen different telco customer logos – were pitched as customer care and sales; network; IT/code/AIOps; and back office.
- **Enea** reported seeing 98-99% accuracy in its new application of AI/ML to classifying A2P text messages. This is to better support variable and dynamic pricing regimes in the wholesale SMS market. There was nothing new as regards using AI/ML in network security or fraud use cases, though.
- **Nokia** announced the integration of a GenAI Assistant with Cybersecurity Dome, what the company calls its 'XDR' platform. Nokia has trained the OpenAI algorithms on telecom network topologies, as well as threat intelligence and attack and defensive playbooks derived from multiple sources. The use cases are centred on leveraging GenAI to present analysts in a telco's Security Operations Centre (SOC) with ready access to relevant data throughout the lifecycle of an incident. Where classical or traditional use of AI in cybersecurity aims at better detection of potential threats themselves, Nokia's integration of GenAI to Cybersecurity Dome targets enabling SOC analysts to understand and process them faster. Both can reduce Mean Time To Detection (MTTD) and Mean Time To Respond (MTTR).

- **Fortinet:** in a somewhat similar vein to Nokia's announcement, Fortinet promoted the recently-launched Fortinet Advisor, the company's GenAI assistant, with its FortiSIEM and FortiSOAR products. In common with Nokia's new capabilities, this enables security operations centre operatives to investigate and remediate threats faster. The big difference, though, is that Fortinet Advisor targets the general enterprise security market whereas Nokia's is tailored to securing telecom networks.

- **Ipoque, a Rohde & Schwarz company**, positioned its recently launched next generation DPI engines. The R&Space2 is optimized for compute stacks, the R&SvPace can be used with telco Virtual Network Functions (VNFs) and Cloud-native Native Functions (CNFs). The products themselves use machine learning and deep learning to extract relevant contextual data from payloads within encrypted traffic. R&S calls it Next Gen DPI with Encrypted Traffic Intelligence (ETI). Besides cyber threat detection, other use cases include identifying encrypted OTT video and audio traffic and distinguishing between on-demand streaming and downloading traffic.

Allot's new release of Network Secure will include AI/ML for managing Encrypted Client Hello (ECH).

- **F-Secure** presented a balanced view of how AI can augment consumer cybersecurity, with the aim of moving fast with adoption, but nevertheless being hypersenstive to the risk of breaking consumer trust. The company's philosophy is that "false positives have to be avoided at all costs."

  F-Secure says it has been using AI for some years. Its latest application of it is behind its 'Text Message Checker', a good use of an AI bot for detecting known anomalies amongst vast data sets. Text Message Checker allows Android and IoS users to verify suspected text messages including iMessage, WhatsApp, Facebook Messenger, Telegam etc as well as SMS. In addition to being bundled into F-Secure's portfolio, it's also a free service available to anyone via the F-Secure website.

- **Allot's** new release of Network Secure will include AI/ML for managing Encrypted Client Hello (ECH), the new standard that prevents networks from seeing which websites users are visiting. With metadata no longer in the clear, the Q2 release of Network Secure leverages AI/ML with what Allot will only call "other inputs" to ascertain whether the website the user is trying to access is malicious or not.

2. Post quantum safety is picking up steam

The threat posed by quantum computers to the integrity of all contemporary encryption standards is years away. And yet at the same time, the threat from Store Now Decrypt Later (SNDL) attacks carried out today is real in the here and now (see below). The migration of an organization's cryptographic assets to quantum safe algorithms will take place over many years. Assets leveraging contemporary protocols such as TLS, HTTPS, SSH and IPsec are going to need to be upgraded to Post Quantum Cryptography (PQC)

The Threat from Store Now Decrypt Later (SNDL) attacks

The threat quantum computers pose to the integrity of contemporary encryption standards is imminent at the same time as it is years away. The years we have left until "Q-Day", when a quantum computer can crack our current systems, is hotly debated. Estimates range from two years to more than twenty.

Nevertheless, rival nation state intelligence agencies are already working on – or executing on – Store Now Decrypt Later (SNDL) attacks, also called Harvest Now Decrypt Later (HNDL) attacks. These involve data being copied – potentially today – and then stored for many years without actually being decrypted. Come Q-Day, decryption of some of that old data, even at that point, will still retain the power to cause a lot of harm. For example, some personal medical data can remain sensitive for many years. From a national security perspective, examples include the layout of missile silos or other military or defence facilities, as well as the conversations of Presidents and Prime Ministers.

algorithms. In the interim, or in parallel, hybrid key distribution solutions with pre-shared keys that harden existing encryption standards or borrow from both current and post quantum encryption algorithms and architecture will need to be deployed. This segment focuses on the challenge this represents from the perspective of the telecom sector. However, the same core principles also apply to other sectors of industry, especially other industries that fall into the category of critical infrastructure.

A quantum-safe roadmap for telcos is going to be a vast undertaking:

- The scale and variety of cryptographic assets deployed across a telco's IT and telecom infrastructure estates is huge. Most telcos lack visibility into either a substantial or very large subset of those assets. Many, if not most, vendors don't have an inventory of the cryptography in their products and they have "lost" certificates hard coded into software. Telcos often don't know which of their vendors have certificate credentials deployed in their products – or they may know that they use them, but they don't know how they use them. Back in 2018, expired Ericsson certificates were the cause of substantial mobile services outages in the UK (O2) and Japan (Softbank).
- The challenge of undertaking a comprehensive asset inventory in a telco isn't just a technical one. It's a human, organizational and political one too. Hands up which head of department wants to cooperate in a crypto asset discovery exercise that might expose vulnerabilities that have left the organization exposed for years? If there is no executive buy-in behind a discovery exercise or audit – and with very few exceptions today, there isn't – what's the motive for supporting it?
- When it comes to prioritizing use cases for cryptographic upgrades, the telco context is unique. Customer data is potentially at its most vulnerable when it's in transit, which makes this a critical priority. But telecom sector regulators are becoming increasingly prescriptive about how telcos defend the network itself against being breached - to defend against national security-impacting attacks like Russia's devastating cyber attack on Kyivstar, for example. That makes investment in adequate protection for telco network management interfaces a much higher priority for upgrades than it was in the past.

The most striking example of this sector's relative immaturity is the way the SIKE PQC algorithm was hacked by Belgian researchers.

The development and selection of new PQC algorithms

Post quantum cryptography is a very new discipline. As such, the efficacy, maturity and operability of individual algorithms is still largely unproven. Each algorithm will have to undergo a long process of proving itself in live operations. The most striking example of this sector's relative immaturity is the speed and ease with which the SIKE PQC algorithm was hacked. SIKE was one of a second group of four additional candidate PQC algorithms selected by NIST for post quantum key establishment in the summer of 2022. It was hacked by Belgian researchers within four weeks of NIST selecting it.

More encouragingly, NIST's first group of four algorithms has so far proven resistant to attack. The first of these is CRYSTALS-Kyber for establishing asymmetric (public-private) encryption keys, which are then used to share a symmetric encryption key based on an algorithm such as AES. The other three are CRYSTALS-Dilithium, FALCON and SPHINCS+. These are for digital signatures – for example, when there is a need to verify identities for a digital transaction or remotely sign a document.

The expectation is that these first four will be ratified as standards following the fifth PQC standardization conference in Rockville, MD in the U.S next month (April 10th – 12th). This would then allow for vendors to start embedding the first PQC algorithms into protocols and products from the second half of this year.

Apple is among the early, pre-standardization, adopters of Kyber

Global cloud providers and applications ecosystem leaders have already started adopting pre-standard versions of the NIST algorithms. The week before Mobile World Congress, Apple announced that it has integrated a pre-standard version of the Kyber algorithm into iMessage. This is with effect from iOS 17.4 which was released on March 5th. This forms part of the privacy features arms race between the big messaging players. Apple follows Google Cloud Platform (GCP), Google Chrome, AWS and Cloudflare, all of which have implemented one or more pre-standard versions.

Crypto agility will extend beyond just reducing the cost of swapping out legacy cryptographic primitives to one that drives automated end-to-end cryptographic lifecycle management.

The NIST algorithms are pivotal but there are also other options

According to Annex A, Table 4, of the GSMA's "Post Quantum Cryptography: Guidelines for Telecom Use Cases" (see "More Information" at the end of this Briefing), so far only China and South Korea have formally committed to developing their own PQC algorithms. That said, a number of other countries are still considering other options at the same time as they are considering NIST's algorithms. The European Commission will shortly be publishing a recommendation on European policy (see page 5).

The costs of upgrading will be susbtantial

There will be costs to upgrade to PQC algorithms in software – and significantly higher costs for doing it in hardware. So-called 'crypto agility' is going to become an increasingly important requirement. The requirement here will extend beyond just reducing the cost of swapping out legacy cryptographic primitives to one that drives flexible, automated, end-to-end cryptographic lifecycle management.

There will be all manner of additional capex and opex implications to contend with too. The PQC algorithms will have an impact on CPU consumption, memory, latency and other end to end performance metrics across networks, services and applications. One example is that due to Google's early support of a pre-standard version of Kyber, one

Vendor solutions for making current crypto more quantum resistant

As well as planning to deploy new PQC algorithms, further hardening of existing encryption standards against quantum threats will also form a part of telecom sector roadmaps. Here are two examples:

- **Nokia**: From its IP/Optical portfolio, Nokia promoted an adapted and layered approach to quantum-safe networks. This uses a physics-based cryptographic offer, enabling IP, MPLS, Ethernet and Optical connectivity. This solution leverages Pre-Shared Keys, symmetric out of band distribution, and AES cipher block encryption techniques to harden engineered connectivity against the quantum threat today. To scale this solution, Nokia promotes its widely deployed, and NATO certified, 1830 SMS (Security Management Server) centralized key management platform. The solution works with Nokia's 1830 family of WDM optical line systems, as well as at L2, L2.5 and L3 with the Nokia 7750 Service Router portfolio.
- **Juniper**: Juniper has completed integration of its vSRX virtual firewall with the new Symmetric Key Agreement Platform (SKA) from Arqit Quantum Inc. Arqit's development of the SKA has been driven by President Biden's White House National Security Memorandum #10 of May 2022. This mandates that U.S government agencies must adopt symmetric key protections for National Security Systems (NSS) to meet the challenge of quantum computing.

  Arqit has found a way of augmenting the symmetric key exchanges in the establishment of IPsec tunnels to make them more quantum resistant. The SKA is designed to be both complimentary to and compliant with IPsec, as well as compliant to National Security Memorandum #10. Juniper supports IPsec across its telecom operator product and services portfolio across fixed and mobile networks, including the MX router series as well as the SRX firewall.

of NIST's four selected PQC algorithms, in Chrome, Allot is already working on having to adjust its software to accommodate the different packet flows triggered by Kyber. Moreover, each of the new algorithm's impact on performance will be unique. Vendors that have not taken adequate account of the impact of upgrades on the physical and mechanical side of their designs may find themselves having to respin hardware.

Hybrid solutions will form part of the roadmap but aren't yet defined

For now, there doesn't appear to be much agreement as to how "hybrid" solutions should be defined but they are going to be a key part of the roadmap. If precedent is anything to go by, vendors will decide for themselves whether or not to adopt the term, independent of any broader market sentiment.

In principle, though, the definition ought to involve the combination of contemporary and PQC algorithms together in such a way that you remain protected come "Q-Day". And if advances in cryptanalysis make it possible to break a PQC algorithm before Q-Day – which is certainly plausible as demonstrated by the vulnerability that was quickly discovered in SIKE– then you remain protected by the contemporary algorithm. This allows PQC algorithms to be phased in gradually - you deploy hybrid on a server, and any client that supports PQC uses both algorithms in hybrid mode, while any older client that doesn't have PQC just uses the classical one. Hence elegant support for hybrid deployments will be a critical component of crypto agility.

South Korea's SK Telecom has successfully trialled Thales 5G PQC SIM cards in its 5G SA network, which used a pre-standard version of Kyber.

Telco trials and supporting cryptographic management software

During Mobile World Congress, HardenStance spoke with Thales and SandboxAQ about their pre-standard PQC deployments with SKT Telecom and Vodafone, as well as with DigiCert and Ericsson about what they can offer by way of cryptographic management solutions. Profiles of all four companies and their value propositions follow below:

Thales

Thales can point to one of the strongest POC proof-points in partnering the telecom sector for quantum safety roadmaps. Last December, the company announced that South Korea's SK Telecom had successfully trialled Thales 5G PQC SIM cards in its 5G SA network. This used a pre-standard version of Kyber. The partners made progress in understanding some of the implications and requirements on the handset side for managing a PQC algorithm's larger key sizes.

The OS upgradeability feature of the Thales 5G SIM has potential to make an important long term contribution to crypto agility. The company reckons 99% of an OS can be upgraded over the air. That includes any crypto algorithms, whether they be contemporary or future PQC algorithms. The Hardware Subscriber Module (HSM) side of Thales, which counts big telecom names among its customers, including Ericsson, is also doing early work on quantum safety. In early trials, Thales has been renewing RSA or other contemporary certificates with PQC certificates. The same types of trials with pre-standard versions of all four of the NIST algorithms are underway with the company's extensive portfolio of high speed encryption products for protecting data in motion.

Thales observes that the banks are currently leading with preparation for the post-quantum era to protect themselves against financially motivated cyber attacks. Telcos, which are more likely to be targeted by nation state cyber operations, are behind.

SandboxAQ

SandboxAQ's Security Suite is a cryptographic management software platform that provides a full range of services for achieving cryptographic agility. Central to its' value proposition is saving time through automated discovery and management of cryptographic assets as well as the remediation of flaws such as obsolete certificates.

Across its portfolio, the company partners NVIDIA to simulate quantum mechanics using AI. The company has already published customer case studies with Vodafone and

Softbank. With Softbank, SandboxAQ has tested and compared the performance of contemporary elliptic curve-based encryption protocols against several pre-standard versions of the NIST PQC algorithms. To deliver Quantum Key Distribution (QKD) solutions, SandboxAQ is partnered with EvolutionQ. SandboxAQ promotes the company's BasejumpQDN, a software layer that manages and secures QKD delivery and optimizes QKD use for efficiency, what it calls 'adaptive network stability', and reduced latency.

DigiCert

DigiCert is one of the world's leading providers of high-assurance TLS/SSL, PKI, IoT and signing solutions. One of the company's core missions at MWC was to reinforce its credentials as an established player and partner as telcos prepare to undertake their migration to PQC cryptography. Its' value proposition comprises three core pillars.

> **Standards:** DigiCert has a deep understanding of the PQC algorithms themselves. It has worked closely with the NIST algorithm selection process and also has a rich pedigree of working with standards organizations like 3GPP on encryption and signing requirements for the telecom sector. DigiCert has deep understanding of how PQC cryptography differs from contemporary standards as well as how different NIST-selected algorithms compare to one another in terms of key sizes and how that impacts telecom networks.
>
> **Products:** DigiCert has a portfolio of crypto discovery and lifecycle management products. For discovery, the company can deploy its own product or integrate with existing discovery solutions. It leverages AI/ML as part of the process of determining which assets are most and least vulnerable to the quantum threat.
>
> DigiCert is a proven leader in automated lifecycle management and brings that portfolio to bear in the PQC era. The company points to how the cracking of the SIKE PQC algorithm demonstrates how important it is to be able to introduce and replace different algorithms in an organization's infrastructure with minimal disruption – a key component of crypto agility.
>
> **Advisory:** DigiCert's advisory service brings the human and organizational know-how to help leaders and their teams navigate the many internal challenges of creating and adhering to a quantum-safe roadmap. It can help align people, processes and technology to de-risk that migration plan.

DigiCert leverages AI/ML as part of the process of determining which assets are most and least vulnerable to the quantum threat.

Ericsson Security Manager (ESM)

While it's unlikely to be in any way fully competitive with specialist cryptographic management software platforms, Ericsson does position the Ericsson Security Manager (ESM) as capable of supporting cryptographic inventory for telcos. Among its crypto features, ESM can assure that the right encryption is being applied for each interface, whether it be an internal or external interface.

Regulatory impetus is urgently needed

As was shared in the GSMA's Post Quantum Networks seminar on the Monday of MWC, deliverables generated by the Post Quantum Telco Task Force are already demonstrating the critical importance of telcos collaborating to navigate this challenge. The most recent example of this is the "Post Quantum Cryptography – Guidelines for Telecom Use Cases" report which was released the week before MWC. In the case of 80 – 90% of the use cases identified, the Task Force has identified gaps in 3GPP and other standards that are going to need to be closed in order to align with operator requirements for optimally supporting post quantum cryptography.

Whether it be in terms of identifying and scoping out use cases, sharing best practice on internal organizational change, or generating requirements for vendors, no one telco can be an island. In any one country or region, telcos and their vendors urgently need guidelines and timelines from regulators to help ensure all players are pointing in the same direction, making common assumptions, leveraging the same toolsets, and sharing best practices in the same industry fora. Those charged with driving the necessary change are becoming impatient for regulatory intervention now.

In some cases, this may be an excuse for delay but in others it's a genuine recognition of the need for a common regulatory platform from which they can start building out a quantum safe roadmap on the right footing.

The European Commission will publish a recommendation "soon"

The EU Commissioner for the Internal Market, Thierry Breton, gave a surprisingly under-reported speech on the Monday of MWC entitled "Changing the DNA of our Connectivity Infrastructure." HardenStance found his comments singularly confusing, albeit they did at least contain the promise of greater clarity "soon".

According to the European Commission's own transcript of his speech, Commissioner Breton told the Mobile World Congress audience the following:

> *"To safeguard critical applications from the risk of potential attacks, we need to develop strategies to transition to quantum safe digital infrastructure.*
> ***The first step in this direction is developing European post-quantum standards and then deploy them across the whole of Europe****.*
> *We will soon present a recommendation to that effect."*

HardenStance found Commissioner Breton's comments singularly confusing, albeit they did at least contain the promise of greater clarity "soon"

Unfortunately, Commissioner Breton's words can legitimately be interpreted in at least three very different ways:

Possible interpretation #1: *The Commission doesn't want Europe to be reliant on NIST's post quantum algorithms because it doesn't trust that America's National Security Agency (NSA) won't have a backdoor into them*. At this point much of European industry, the telecom sector included, would appear to be assuming the adoption of the NIST algorithms. At this time, there is no evidence of any political mandate for European alternatives (and the Commissioner is nearing the end of his term anyway). It would take a lot of time to develop European alternatives, albeit the UK, Germany, Austria and Switzerland are all strong in cryptography. Such a scenario could conceivably allow for the initial introduction of the NIST algorithms in Europe, while also making the adoption of future European-developed algorithms optional or mandatory. It cannot be ruled out that this literal interpretation of the Commissioner's words may be the correct one.

Possible Interpretation #2: *The EU will soon make a recommendation on post quantum safety, but it will be on regulation - not standardization as stated.* This will provide regulatory guidelines that this, that or the other sector of industry must implement quantum safe encryption in a, b, c phases by this, that or the other date (with an implicit or explicit assumption that the NIST algorithms will be embraced).

Misleading language was used because poor speech writers didn't grasp that 'standardization' and 'regulation' are fundamentally different rather than interchangeable. While the first half of this interpretation could be correct, it's very unlikely that the second is. The Commission is surely too well-oiled a bureaucratic machine when it comes to speech writing and checking to make an error of this kind.

Possible Interpretation #3: *As above, the EU will soon make a recommendation on post quantum safety, but it will be on regulation - not standardization as stated.* The use of misleading language was deliberate – no more than political hi-jinx by the Commission. It was a dog whistle to fears of deepening dependence on U.S technology with post quantum crypto, albeit with no plan to actually do anything about it.

In this case, the inappropriate use of the term 'standardization' can (sort of) be justified because the European Telecommunications Standards Institute (ETSI) is, of course, developing what genuinely are "European post encryption standards". ETSI, however, is specifying the interfaces that will manage the operation of PQC algorithms in live networks; ETSI isn't specifying the PQC algorithms themselves.

It's good that the Commissioner committed to releasing a recommendation "soon" because European industry is poorly served by the current ambiguity.

Much more to come at MWC 2025

At the end of last year, BT, Fortinet and Arqit Quantum Inc announced the launch of an integrated product for quantum-safe VPN communications using Arqit's Symmetric Key Agreement (SKA). It followed the successful trial of quantum-safe tunnels between three BT sites in London, Exeter and Suffolk.

At MWC the week before last, BT's Chief Network Officer, Greg McCall, gave an interview to Telecom TV in which he said: "I predict that if it's not this year, then next year quantum will be a headline here in the same way that AI is going to be this year." This is a sound prediction. This year it felt as though the touchpaper was lit on the topic of quantum safe networks. Coverage is indeed likely to be greater still next year.

3. New appetite for countering telecom fraud

Historically, telcos have tended to view fraud as no more than a low-level nuisance. In the last 12 months there has been an upward spike in the problems themselves and an upward spike in the engagement of regulators to better address them.

We trust that an Uber driver that comes to collect us, has been vetted by the platform in some way. Plain old telephony hasn't caught up with this trust model.

- **During 2023, when Artificially Inflated Traffic (AIT) started surging, Elon Musk, CEO of X, did both a good and not-so-good job of raising the profile of fraudulent SMS traffic.** He did a good job in terms of highlighting the costs that bad actors in the messaging ecosystem are imposing on businesses like his. He did a not so good job by appearing to point the finger solely at the operators themselves. He didn't take proper account of how, in many cases, SMS fraud is perpetrated by aggregators, independent of the telcos. Nor did he take account of how social media platforms like his are instrumental in enabling artificial (bot-generated) traffic more generally. Vendors at MWC concurred that AIT is especially challenging to combat. Two of them pointed to business buyers of wholesale messaging services being best placed to bear down on it by authenticating requests to their own websites before allowing an SMS to be sent in response.
- **In trust terms, plain old telephony is still in the dark ages.** It's still by no means universally present, and it's not even 100% fail safe when it is, but we have come to assume some basic level of trust in many of the most popular apps and online services we use. We trust, for example, that an Uber driver that comes to collect us, or an Airbnb host that takes a payment from us, has been vetted by the platform in some way. Plain old telephony hasn't caught up with this trust model. If someone has your phone number, there's literally nothing to stop them calling (or texting) you. Hence the open invitation to criminal actors to leverage all manner of techniques to try and defraud consumers - and a commensurate souring in peoples' willingness to pick up their phones to anyone other than a known contact.
- **Telcos are feeling regulatory pressure – hence vendors are too.** During meetings at MWC, no-one would put a number on it but several vendors in the fraud prevention space spoke positively about the new pressure telcos are feeling to invest in fraud protection solutions arising from regulatory mandates – and how they stand to benefit from it in the form of new orders. While this can't help but be partially self-serving, it's also consistent with feedback from telcos, regulators and other vendors over the last year. Three different vendors HardenStance met with drew particular attention to Singapore's leadership in this area of regulation. Two of them cited the work of the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) to make telcos and banks share the costs of consumers being scammed by fraudsters using SMS as a vector in financial fraud.

- **While it’s good that regulators are demanding more technical interventions by telcos, more is also needed in terms of law enforcement.** To point to just one example – there are many others – the FCC in the U.S. makes hardly any use of the powers at its disposal under the Telephone Consumer Protection Act. The FCC also has a poor track record when it comes to enforcing fines for unwanted robocalls.

Specific examples of companies raising their profile and committing to do more to combat telecom fraud at MWC included the following:

- **Telefonica joined forces with Orange and Vodafone’s Spanish affiliates** leveraging the GSM Open Gateway Initiative to launch two network API services for intelligent layers of customer authentication, verification, and security in mobile networks. The two services will target number verification and SIM swap services at financial institutions and online retailers. Operators Cell C, MTN and Telkom announced a commitment to launch the exact same two services in South Africa. That said, their PR conveyed somewhat less substance and immediacy behind their commitment than that of the Spanish operators.
- **Enea** is not a name you would traditionally associate with solutions for preventing voice fraud but that’s changing. The rules engine of the former AdaptiveMobile Security platform – now part of Enea - is in the process of being refreshed to be able to block some fraudulent voice calls. This is the first step in a long term commitment to expanding Enea’s footprint in voice fraud prevention. Enea doesn’t see itself competing with existing voice fraud prevention solutions that use traditional rules engines. Rather it believes telcos are becoming more open than in the past to augmenting those with new real time blocking capabilities.

Consistent with market trends, Netnumber reported particular customer interest in helping them combat Artificially Inflated Traffic (AIT); CLI spoofing and account takeover.

- **Hiya** has been building momentum with its voice fraud protection solutions in the North American market. The company used the landing of big contracts with EE and Virgin Media O2 in the UK in recent months as a platform to project itself onto the world market at MWC this year. Hiya pitches Hiya Registration – which businesses can use to register bona fide numbers – as “the telecom industry’s first and only global SaaS-based phone number registration product that is free and provides full self-service number management and transparency.”
- **Titan.ium Platform** finds itself in the unusual position of being in a leadership position in terms of STIR/SHAKEN deployments outside the U.S. This is by virtue of being a supplier to SFR in France, where STIR/SHAKEN has been mandated for all national SIP traffic. That said, Ofcom has recently rejected STIR/SHAKEN for the domestic UK market so the standard’s future in Europe and throughout the rest of the world outside the U.S is uncertain.
- **Mobileum** reported increased demand for its SMS firewalls. Until recently, demand tended to be driven by grey-routing. These days, demand is increasingly driven by protecting users against phishing and smishing. A new URL scanner feature, announced in January, scores the reputation of URLs embedded in SMS messages in real time, allowing telcos to deploy filters to block malicious ones.
- **Netnumber:** Consistent with broader market trends, Netnumber reported particular customer interest in helping them combat Artificially Inflated Traffic; CLI spoofing and account takeover. One example of Netnumber repositioning its portfolio since its separation from Titani.ium Platform a year ago is the positioning of a new service called NumeriCheck. Launched last April, NumeriCheck allows phone numbers to be flagged as invalid when one or more checked indicators point to something suspicious. Netnumber sees customers using it for a number of use cases including user account verification, traffic routing and fraud prevention.

4. Marketing savvy wins in consumer security

It’s hard to overstate how much the market in selling consumer security services via the telco channel has changed in the last couple of years. Technology differentiation – higher detection accuracy, lower capex or opex – has receded in importance. Instead, telcos increasingly value the marketing savvy that a consumer security software partner can bring them as regards how to effectively target customers; how to persuade them to opt-in; how to delight them with easily understandable and engaging features; and how to persuade them to upgrade to spend more on additional services.

This theme arose in meetings with Bitdefender, F-Secure and Whalebone:

- **Bitdefender’s** Digital Identity Protection feature provides a potentially compelling and straightforward way for a consumer to exercise their right to require that a data broker delete the data they have on them. By clicking ‘Remove’ in the Bit Defender app, the specific data broker is legally obliged to delete your data and contact you to confirm that it has been done (though whether the data is immediately deleted in order to be legally compliant only to then be “reinstated” later may be another matter in some cases).
- In the evolution of **F-Secure’s** roadmap of “visible value” features, the company will be enabling users to do things like easily tailor the feedback their security app gives them according to their own personal appetite for information. This might include such things as their risk profile; how their risk profile compares with that of others; how it’s changed; and how to further reduce risk. F-Secure has a balanced view of how AI can augment consumer cybersecurity. It aims to move fast with adoption, but nevertheless be hypersenstive to the risk of breaking consumer trust. The company emphasizes that false positives must be avoided at all costs.
- A common theme in many among the remarkable number of **Whalebone’s** telco customer video testimonials it has up on its website is the extent to which these customers welcome persistent handholding, guidance, and progress review against targets. Whalebone supports them with this in conjunction with selling them network security software as a service.

In the evolution of F-Secure’s roadmap of “visible value” features, the company will be enabling users easily tailor the feedback their security app gives them.

5. Innovation in 5G security for telcos is flatlining

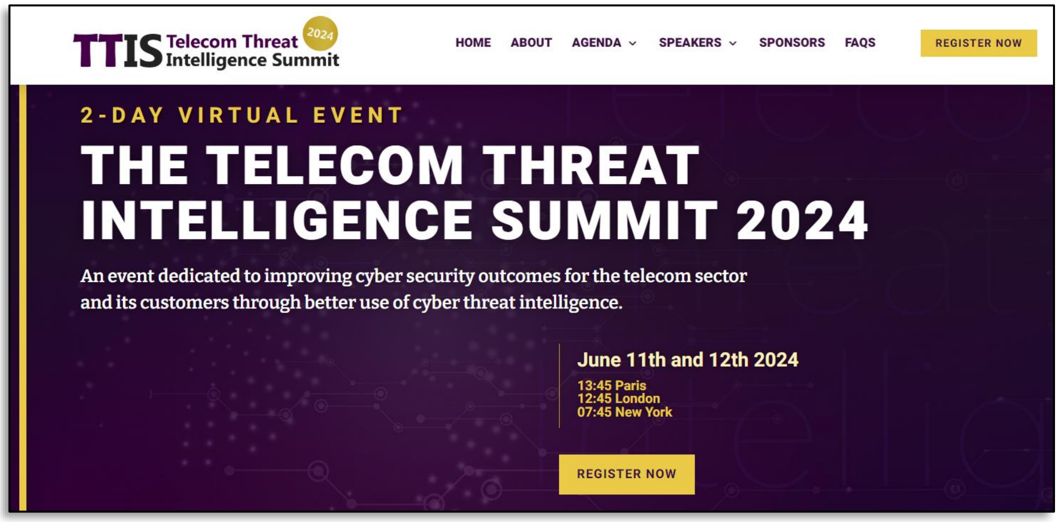
The still slow rollout of 5G SA has driven the big network security vendors to slow down investment in new 5G security solutions. The products and features they’ve already built in anticipation of rapid 5G SA momentum are there - still waiting for demand to pick up.

The MWC messaging of big NGFW vendors like Palo Alto Networks, Fortinet as well as Juniper focused much more on growing telco channels for sell-through business rather than revenue growth from selling into them directly. None of them appeared to have anything new to say to a mobile operator CTO or CISO. There were one or two exceptions, however. From very different portfolio starting points, Netscout and Enea came to MWC to expound on new 5G security solutions for providing better visibility and threat detection in 5G SA environments. On aggregate therefore - and excluding investment in 3GPP-specified network security requirements – it would appear that at this time new investment in 5G security for telco networks is flatlining at best.

Palo Alto Networks and CTOne focused on private 5G deployments

Palo Alto Networks and CTOne, a Trend Micro subsidiary, focused on private 5G networks more than on the telcos themselves. They both pushed solutions and partnerships for baking security into private 5G deployments from day one – and according to enterprise security operations requirements rather than bare minimum 3GPP security standards.

HardenStance's annual Telecom Threat Intelligence Summit


TTIS Telecom Threat Intelligence Summit 2024

2-DAY VIRTUAL EVENT

THE TELECOM THREAT INTELLIGENCE SUMMIT 2024

An event dedicated to improving cyber security outcomes for the telecom sector and its customers through better use of cyber threat intelligence.

June 11th and 12th 2024
13:45 Paris
12:45 London
07:45 New York

Register here for HardenStance's 2024 Telecom Threat Intelligence Summit

Allot is looking at potentially leveraging some of its in-house DPI technology for the SECaaS product line for the first time.

HardenStance MWC meeting reports with vendors

1. Allot

Meeting with Angel Fernandez, VP, Cybersecurity, Product Sales & Strategic Partnerships

Allot had a number of new things to share centring on Allot Network Secure, the company's Security as a Service (SECaaS) offering for telcos targeting SMBs/SMEs and consumers (or both).

- **A new network firewall feature**. At the end of last year, Allot deployed a new network firewall feature for Network Secure for a lead telco customer in North America. It's a simple network firewall proposition featuring basic things like port and IP blocking. It targets SMBs or SMEs that typically can't afford, or wouldn't know how to manage, a more advanced Next Gen Firewall from a specialist vendor.

  This feature is now GA, augmenting the value proposition for telco customers that are looking to target the highly underserved SMB/ SME market. Allot is also looking at potentially leveraging some of its in-house DPI technology for the SECaaS product line for the first time. The plan is to introduce it for things like content filtering by application or specific flows within an application.

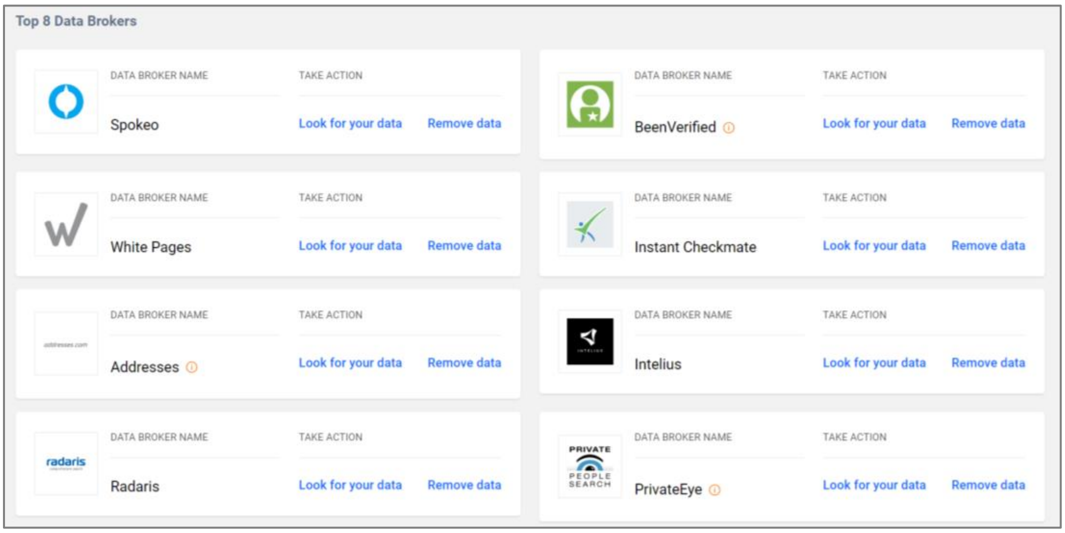
- **Adjustments for the introduction of new encryption algorithms.** A new release of Network Secure will include AI/ML for managing Encrypted Client Hello (ECH), the new standard that prevents networks from being able to see which websites its users are visiting. With metadata no longer in the clear (unencrypted), the Q2 release of Network Secure leverages AI/ML with what Allot will only call "other inputs" to ascertain whether the website the user is trying to access is malicious or not. Adjusting to ECH was the primary driver of investing in AI/ML but Allot is also leveraging that investment to enhance the security features of Network Secure – specifically new anomaly detection and DNS tunnelling protection features. Due to Google's early support of a pre-standard version of Kyber, one of NIST's four selected PQC algorithms, in Google Chrome, Allot is also working on having to adjust its software to accommodate the different packet flows that arise with Kyber.

2. Bitdefender

Meeting with Bruno Rodriguez, VP, Global Sales, Service Providers; Paul Palmer, VP, EMEA Sales.

As well as going direct and leveraging telcos and other partners as channels to market, Bitdefender also does good business selling its cybersecurity software to other leading technology vendors. Among the OEM customers it cites are Cisco (for Cisco Secure Endpoint and Cisco Umbrella), Microsoft and Facebook.

Digital Identity Protection from Bitdefender



Top 8 Data Brokers

DATA BROKER NAME	TAKE ACTION	
Spokeo	Look for your data	Remove data
BeenVerified ⓘ	Look for your data	Remove data
White Pages	Look for your data	Remove data
Instant Checkmate	Look for your data	Remove data
Addresses ⓘ	Look for your data	Remove data
Intelius	Look for your data	Remove data
Radaris	Look for your data	Remove data
PrivateEye ⓘ	Look for your data	Remove data

Source: Bitdefender

Bitdefender detects activity like a home camera participating in a botnet and generating internal or inside-out DDoS attack traffic.

The company has been working with telecom operators for the last five or six years and has evolved a consumer security portfolio for telcos to resell across the three main pillars that span that market space:

- **Endpoint security** –Bitdefender's core business. A differentiating feature that's offered is Bitdefender Digital Identity Protection. As shown in the graphic above, this does present a potentially compelling and straightforward way for a consumer to exercise their right to require that a data broker delete the data they have on them. By clicking on 'Remove', the data broker is legally obliged to delete your data and contact you to confirm that it has been done (though whether the data is immediately deleted in order to be legally compliant only to then be "reinstated" later may, in some cases, be another matter).
- **Home router security** – it has a partnership with Netgear that promotes the 'Netgear Armor Powered by Bitdefender' product line. As a commercial proof point, there are currently 2.3 million Bitdefender-enabled home routers in the field protecting 50 million connected devices with a large North American operator. One differentiator the company cites is a virtual patching system that blocks an exploit until a patch can be implemented. Another is botnet abuse detection whereby Bitdefender detects activity like a home camera participating in a botnet and generating internal or inside-out DDoS attack traffic that consumes bandwidth on the operator's network.
- **Network Security.** Bitdefender offers customers two types of DNS-based network security for consumers. It cites Windtre, an Italian service provider as a customer for its basic, non-disruptive, offer whereby Bitdefender just provides a threat intel feed into the service provider's DNS infrastructure. In addition, Bitdefender is also open to reselling specialist DNS-based network security vendors to telcos to augment its endpoint and home router security portfolio.

As did F-Secure, Bitdefender pointed to momentum behind 'prpl', the telco-backed opensource home router project which some leading telcos see as offering a path to revenue growth in home networking applications and services (including cybersecurity applications and services). Bitdefender relayed that there is a sizxable telco RFP upcoming for a Fixed Wireless Access (FWA) home router which specifies purpl as the mandatory OS.

3. CTOne

Meeting with Jack Hu, Product Marketing Manager and Steve Neville, Director of Strategic Growth, Trend Micro.

Established as a subsidiary of Trend Micro in January 2023, CTOne is offering two mobile network security solutions into the telecom sector.

- **A comprehensive security solution for private mobile networks.** Drawing on Trend Micro's portfolio and layering on additional mobile network domain security expertise, the solution offers both endpoint and network security for private mobile network deployments. A Java applet on the organization's SIM cards extracts, correlates and acts on endpoint data. Vulnerability exploitation, malicious content, and suspicious network behaviours are identified and blocked at the network level.
- **A POC for an ORAN security solution with Taiwanese and Japanese telcos** This combines CTOne's assets in mobile network security with the vulnerability discovery and disclosure heritage of Trend Micro. This is derived in large part from Trend's acquisition of Tipping Point in 2015. Tipping Point founded the popular Zero Day Initiative (ZDI), a community of thousands of researchers, in 2003.

  This solution consists of an agent based approach to monitoring traffic in the Central Unit (CU) and Distributed Unit (DU) elements of an ORAN deployment. As part of ongoing trials, CTOne says it has found vulnerabilities in the E2 interface between the RAN Intelligent Controller (RIC) and the CU and DU as well as in xApps and rApps. Consistent with its responsible disclosure policies, the company will shortly be sharing these vulnerabilities with relevant ecosystem players via the ZDI.

One of CTOne's solutions consists of an agent based approach to monitoring traffic in the CU and DU elements of an ORAN deployment.

4. DigiCert

Meeting with Avesta Hojjati, VP of Engineering

DigiCert is one of the world's leading providers of high-assurance TLS/SSL, PKI, IoT and signing solutions. One of the company's core mission's at MWC was to reinforce its credentials as an established player and partner as telcos prepare to undertake their migration to PQC cryptography. Its value proposition comprises three core pillars.

- **Standards.** The company has a deep understanding of the PQC algorithms themselves. It has worked closely with the NIST algorithm selection process and also has a rich pedigree of working with standards organizations like 3GPP on encryption and signing requirements for the telecom sector. DigiCert has deep understanding of how PQC cryptography differs from contemporary standards as well as how different NIST-selected algorithms compare to one another in terms of key sizes and how that impacts telecom networks.
- **Products.** DigiCert has a portfolio of crypto discovery and lifecycle management products. For discovery, the company can deploy its own product or integrate with existing discovery solutions. It leverages AI/ML as part of the process of determining which assets are most and least vulnerable to the quantum threat.

  DigiCert is a proven leader in automated lifecycle management and brings that portfolio to bear in the PQC era. The company points to how the cracking of the SIKE PQC algorithm demonstrates how important it is to be able to introduce and replace different algorithms in an organization's infrastructure with minimal disruption – a key component of crypto agility.

- **Advisory.** DigiCert's advisory service brings the human and organizational know-how to help leaders and their teams navigate the many internal challenges of creating and adhering to a quantum safe roadmap. It can help align people, processes and technology to de-risk that migration plan.

5. Enea

Meeting with Cathal Mc Daid, VP, Technology; Stephanie Huf, CMO; and Claire Murphy, Head of Campaigns.

There were three main take-aways from the meeting with Enea. The first two point to some interesting new directions for its mobile network security roadmap, coming up on the third anniversary of the company acquiring AdaptiveMobile Security.

- Neither Enea nor the former AdaptiveMobile Security are names you would normally associate with solutions for preventing voice fraud but that's changing. The rules engine of the company's signaling firewall platform is in the process of being refreshed to be able to block some fraudulent voice calls. This is the first step in a long term commitment to expanding Enea's footprint in voice fraud prevention. Enea doesn't see itself competing with existing voice fraud prevention solutions that use traditional rules engines. Rather it believes telcos are becoming more open than in the past to augmenting those with additional real time blocking capabilities.
- Work is ongoing with regard to combining some of Enea's IP heritage with the signaling firewall to build some kind of 'visibility and detection' overlay probe for hardening 5G networks against cyber attacks. The idea is for these probes to be deployed in either a subset of the most important 5G network functions or even all of them. The probe will upload request and response packets that could feed back either into Enea's signaling firewall or into some kind of SIEM-like function for threat detection and mitigation. Enea sees the potential here to better defend 5G networks, including against insider attacks. It sees this as also aligning well with telco customer demand for distributing threat detection away from big centralized firewalls at the edge of the core network. This is in the early developmental stage right now. Enea has discussed overlay probes within GSMA and is looking for partners to put the idea to work in a POC trial.
- The company reports seeing 98-99% accuracy in its new application of AI/ML to classifying most categories of A2P text messages. This is to better support variable and dynamic charging regimes. Nothing new as regards using AI/ML in security or fraud use cases, though.

Work at Enea is ongoing with regard to some kind of 'visibility and detection' overlay probe for hardening 5G networks against cyber attacks.

6. Ericsson

Meeting with Keijo Mononen, General Manager, Security Solutions

This year, Ericsson hosted four dedicated cybersecurity demos on its exhibition stand. These featured 5G security, cloud RAN security, cloud native security and Ericsson Security Manager (ESM), the company's security automation and orchestration platform.

In the run up to MWC, Ericsson released a new White Paper on "Zero Trust Architecture for Advancing Mobile Network Security Operations". Among other things, this provides Ericsson's guidance to mobile operators on how to implement zero trust access as described in the April 2023 Zero Trust Maturity Model (ZTMM) published by the U.S Cybersecurity and Infrastructure Security Agency (CISA).

Extensive discussion of post quantum cryptography in several other parts of the FIRA, prompted dialogue around what, if anything, Ericsson can offer telcos in this market space today. It turns out that while it's unlikely to be in any way fully competitive with specialist cryptographic management software platforms, Ericsson does position the Ericsson Security Manager (ESM) as capable of supporting cryptographic inventory for telcos. Among its crypto features, ESM can assure that the right encryption is being applied for each interface, whether it be an internal or external interface.

7. F-Secure

Meeting with Timo Laaksonen, President and CEO, F-Secure and TL Viswanathan, Chief Products Business Officer

F-Secure is the market leader in selling consumer security software to telecom operators, estimating its market share in endpoint security software sales to telcos at around 40%. The company has augmented its' heritage in endpoint security software by expanding into network security, with partners including Whalebone, and home router security with its own product. F-Secure is a leader in reconciling a consumers' need for strong security with ease of use and strong user engagement.

The company has already led the way in tailoring cybersecurity features that make themselves visible to users at specific moments of vulnerability. These include a bright green screen surround manifesting itself on their device whenever the user accesses a banking or on-line shopping app. In the evolution of its roadmap of "visible value" features, F-Secure will be enabling users to do things like intuitively tailor the feedback their security app gives them according to their own personal appetite for that kind of informaiton. This could include their own personal risk profile; how their risk profile compares with that of others; how it's changed; and how to further reduce risk.

F-Secure pointed to momentum behind 'prpl', the telco-backed opensource home router project which some telcos see as offering a path to revenue growth.

F-Secure presented a balanced view of how AI can augment consumer cybersecurity, with the aim of moving fast with adoption, but nevertheless being hypersenstive to the risk of breaking consumer trust. The company emphasizes that false positives must be avoided at all costs.

F-Secure says it has been using AI for some years. Its latest application of it is behind its 'Text Message Checker', a good use of an AI bot for detecting known anomalies amongst vast data sets. Text Message Checker allows Android and IoS users to verify suspicious text messages including iMessage, WhatsApp, Facebook Messenger, Telegam etc as well as SMS. As well as being bundled into F-Secure's portfolio it's also a free service available to anyone via the F-Secure website.

As did Bitdefender, F-Secure pointed to momentum behind 'prpl', the telco-backed opensource home router project which some telcos see as offering a path to revenue growth in home networking applications and services (including cybersecurity applications and services). The company believes the market would be better served by a consolidation of the three different projects – prpl, Reference Design Kit (RDK) and OpenWrt. There is nevertheless enthusiasm about prpl products now being in production deployment with the first commercial launches scheduled for later this year.

8. F5

Meeting with Raffaele D'Albenzio, SA-Sales; Philip Klatte, Sr. Product Manager; Marcus Sorour, Director Corp Comms EMEA

F5 served up three new CSP-related proof-points for its core strategy of securing applications anywhere – in hardware or software; in the cloud or on premises.

- **The availability of VELOS, F5's new 4u multi terrabit hardware platform, supporting throughput of up to 760 Gbit/s (L4 and L7).** A large North American telco is the lead customer for VELOS and has deployed it to secure the user plane at scale on the 4G GI LAN and the 5G N6 interface as they scale up to meet rapidly increasing bandwidth consumption, including with fixed wireless access services. Initially this lead customer is leveraging VELOS for firewalling but there are several other potential use cases, including in-line DDoS mitigation to defend the operator's network infrastructure.

- **Progress against the security roadmap for the Service Proxy for Kubernetes (SPK).** From its original conception, security has been a key driver of SPK, a cloud native application traffic management solution developed to compensate for some of the inherent incompatibilities between Kubernetes and telco operating requirements. SPK is designed to enable operators to extend Kubernetes using Custom Resource Definitions (CRDs) rather than break out of it in parts of their architecture as many telcos are still having to do. SPK enables this while providing the necessary features for doing it securely. Work on an enhanced 'Secure SPK' release has recently been completed – more to come soon.
- **A partnership with Ericsson, whereby F5 is now the preferred application security provider for the Ericsson Wallet Platform**. This currently supports over 400 million wallets across 24 countries, processing over 2.8 billion transactions worth more than USD 40 billion every month through open API-ecosystem and advanced financial service offerings. The collaboration was pitched as marking a significant shift in Ericsson's go-to-market strategy to extend its reach telcos to target banks, fintechs, and enterprises globally. It will enable customers to manage and secure the ever-increasing number of APIs they need to support for agility, speed and financial regulation in mobile financial services.

9. Fortinet

According to Fortinet, its digital wellness service for the home is delivering a positive return on investment for telco partners in less than 6 months.

Meeting with Ronen Shpirer, Director, 4G and 5G Solutions Marketing

Fortinet's top level strategy is focused on security operations, unified SASE and secure networking. In terms of solutions that are unique to the telco infrastructure, both current sales and further roadmap development are both being held back by still slowish rollout of 5G SA. Fortinet was nevertheless able to point to growing opportunities in compliance by way of helping telcos align with new cybersecurity regulations. In the UK, for example, Fortinet is working with one operator to design and enforce segmentation and isolation of network operations and maintenance domains.

A lot of Fortinet's talking points centred on partnering with telcos as channel partners, including in the Managed Security Services Provider (MSSP) space. The company seems to have emerged well from Telefonica Tech's recent consolidation of partners for its flexWAN portfolio, which saw some vendors shown the door. Telefonica Tech's flexWAN portfolio of converged security connectivity offers enterprise customers worldwide secure SDWAN, SASE, SD Branch and Zero Trust Network Access services.

Another example was a digital wellness service for the home, delivered in partnership with Fortinet's partner, NetHive, to a Tier 1 Italian operator. According to Fortinet, this is delivering a positive return on investment for telco partners in less than 6 months.

The main new feature highlighted in the portfolio was Fortinet Advisor, the company's GenAI assistant, which has recently been launched with its FortiSIEM and FortiSOAR products. This is enabling security operations centre operatives to investigate and remediate threats faster, albeit it's not especially focused on telecom operator use cases. Fortinet Advisor will be progressively rolled out across the company's portfolio throughout this year.

10. Hiya

Meeting with Patchen Noelke, VP, Marketing; Elise Harrington, Senior Communications Manager; and James Lau CTO

Spunt out in 2016 from White Pages, the U.S provider of online directory services, fraud screening and identity verification services, Hiya is a specialist in voice spam and fraud analytics. Hiya claims to reach 450 million subscribers world-wide through its telco customers and other telecom ecosystem partners as well as more than 400 enterprise customers. Carrier customers include a lot of big names in the U.S. The announcement of Virgin Media O2 as a customer just before MWC builds on contract to supply EE announced last year to take Hiya's reach in the UK to more than 64% of mobile users.

The company has integrations with the telephony application servers of Ericsson, Nokia, Titan.ium and Mavenir. It also has a world-wide partnership with Samsung's smartphone business. This powers 'Samsung Smart Call' spam and fraud protection features in 40 markets where Samsung's share of the smartphone market is typically somewhere in the 10-20% range.

Hiya's core analytics engine, the Hiya Voice Security Network, is AI-driven, enabling it to be continually learning every second. Network data is fed in and processed at the rate of more than 15,000 data points per second. Phone numbers are pseudonymized for privacy. The system boasts higher than four nines uptime and average latency of less than 20 milliseconds at the 95th percentile. Hiya also leverages its own honeypot to lure voices scammers and get ahead of what the next wave of scams might look like.

The company pitches Hiya Registration – which businesses can use to register bona fide numbers – as "the telecom industry's first and only global SaaS-based phone number registration product that is free and provides full self-service number management and transparency."

Hiya's core analytics engine, the Hiya Voice Security Network, is AI-driven, enabling it to be continually learning every second.

EE became a customer last year and as of MWC had deployed Hiya to protect around 1 million of its 17 million customers. EE should achieve full coverage to reach substantially all of its customers by around the middle of this year. Telenor is also a Hiya customer but leverages a different part of the portfolio, using its device SDK instead.

11. Juniper Networks

Meeting with Kedar Dhuru, Senior Director, Security Product Management and Shishir Singh, SVP and General Manager, Core Technologies.

In terms of its 'Connected Security' portfolio, Juniper's focus at MWC was on the new architecture of its new scale-out connected security architecture; new iterations of its virtual SRX firewalls; and a roadmap for deeper integration of cyber threat intelligence into telco operations.

- **The Connected Security Distributed Services Architecture**. By fully decoupling an SRX firewall's forwarding and security services layers and integrating it with the MX series router, the latter can now be used as an intelligent forwarding engine and load balancer for independent scaling flexibility without chassis limitations. Deployed with Juniper Security Director Cloud, the operational experience is designed to be as simple as managing one logical element, irrespective of how many additional firewall engines are added to the architecture, or their format factor.
- **Juniper SecIntel security intelligence detects and blocks command-and-control (C&C) traffic discovered by Juniper's Advanced Threat Prevention (ATP) solution at wire speed**. AI-Predictive threat prevention predicts and prevents known and zero-day malware on the wire by using AI on packet snippets and reduces false positives by filtering out non-threatening activities.
- **Four new iterations of the SRX firewall series**. These now feature wire-speed MACsec along with natively embedded TPM 2.0 chips. Cryptographically signed device IDs also allow security administrators and network operators to remotely verify the trust posture of devices.

In the quantum safety space, Juniper has completed integration of its vSRX virtual firewall with the new Symmetric Key Agreement Platform (SKA) from Arqit Quantum Inc. Arqit's development of the SKA has been driven by President Biden's White House National Security Memorandum #10 of May 2022. This mandates that U.S government agencies must adopt symmetric key protections for National Security Systems (NSS) to meet the challenge of quantum computing. Arqit has found a way of augmenting the symmetric key exchanges in the establishment of IPsec tunnels to make them more quantum resistant. The SKA is designed to be both complimentary to and compliant with IPsec, as well as compliant to National Security Memorandum #10. Juniper supports IPsec across its telecom operator product and services portfolio across fixed and mobile networks, including the MX router series as well as the SRX firewall

12. Mobileum

Meeting with Bernardo Lucas, Chief Marketing and Strategy Officer

Mobileum is seeing increased demand for SMS firewalls. This is driven, the company says, by a volte face on the part of some customers who were assuming during 2022 and 2023 that SMS firewalls were becoming irrelevant for the 5G era. Whereas grey routing has traditionally been a big driver for SMS firewalls, Mobileum reports protecting users against phishing and smishing as the bigger driver now.

Whereas grey routing has traditionally been a big driver for SMS firewalls, Mobileum reports protecting users against phishing and smishing as the bigger driver now.

A new URL scanner feature, announced in January, scores the reputation of URLs embedded in SMS messages in real time, allowing telco customers to deploy advanced filters to block malicious ones. Mobileum reported customers being increasingly motivated to invest in its portfolio arising from regulatory mandates now more than being focused on more monetization-driven use cases. Mobileum flagged the growing problem of fraudulent and unwanted voice calls at MWC in 2023 and pointed to it again this year and the market opportunity it's creating for its voice firewall solutions.

Mobileum also reported growth in its managed security business. This is not so much full scale managed services of the 24/7, 365 days a year, variety. Rather its higher demand for deployment and tuning and more frequent status reviews with customers. This reflects either more risk, complexity and regulatory exposure or deeper downsizing of telco operations teams diluting the quality and quantity of available in-house expertise to manage parts of the network security portfolio. In some cases it's both.

13. Napatech

Meeting with Charlie Ashton, Senior Director, Business Development

From a cybersecurity perspective, Napatech, a leading supplier of Network Interface Cards (NICs) or what it calls Smart Network Interface Cards (SmartNICs), highlighted its new Intel-based Infrastructure Processing Unit (IPU). Napatech announced this last year and has been shipping it since January.

One use case being advanced is offload of TLS, an encryption protocol for which there is a huge new requirement specified by 3GPP with 5G SA networks at scale. Rather than deploy TLS on a host server's CPU core, the new IPU gives telcos the opportunity to offload it while also maintaining full software compatibility at the application level.

14. Netnumber

Meeting with Steve Legge, CEO

The divesting of its network software business – Titan.ium Software, acquired by Lumine Group – a year ago could not have been better timed by Netnumber. The marked rise in some types of voice and messaging fraud over these same last 12 months – and the accompanying increase in engagement by regulators to intervene on customers' behalf – is providing a great opportunity for the company to sharpen its value proposition and meet growing demand for solutions to these problems.

Netnumber's unique global platform, hosted on AWS, delivers consolidated, real time, global intelligence software as a service on billions of phone numbers in countries throughout the world. As well as telecom operators, Netnumber counts Communications Platform as a Service (CPaaS) providers and large enterprises that buy messaging services in bulk amongst its customers.

Of the many types of fraud out there, there aren't many that Netnumber's real time data on things like phone number verification and reputation scores can't contribute to identifying, flagging and helping its customers block. Right now, the company is seeing interest in addressing a variety of different types of fraud. However, consistent with broader market trends, the company reports particular interest in helping customers combat Artificially Inflated Traffic (AIT); CLI spoofing and account takeover.

Independence from the business that is now Titanium Software is enabling Netnumber to more accurately tailor its' products to its customers and build the right value proposition and marketing message for them. In the case of many of its' telco customers, the prospective buyer of Netnumber services is a different individual and a different department to the buyer of network software products.

One example of how this refocusing of the portfolio is moving on is the positioning of NumeriCheck, a new service Netnumber launched last April. NumeriCheck allows phone numbers to be flagged as invalid when one or more checked indicators points to something suspicious. Netnumber sees customers using it for a number of use cases including user account verification, traffic routing and fraud prevention.

MobileStream and Arbor Sightline Mobile are targeting mobile network security operations and 5G network security operations in particular.

15. Netscout

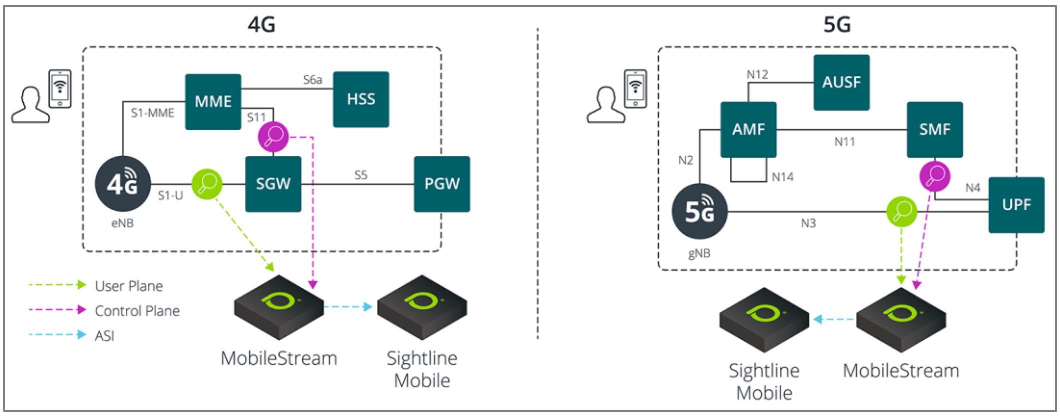
Meeting with Darren Anstee, CTO for Security

Having not exhibited last year, it was good to see Netscout back at MWC again this year. One of the drivers of that decision is bound to have been last May's launch of two new products – MobileStream and Arbor Sightline Mobile – targeting mobile network security operations and 5G network security operations in particular.

As shown in the diagram below, MobileStream extracts user and control plane telemetry to provide granular visibility from within the mobile core network. Arbor Sightline Mobile then correlates MobileStream data with things like subscriber and device identities to detect DDoS and other service-impacting traffic anomalies.

Greater visibility, threat detection and mitigation are certainly required as 5G SA scales up. The dynamism of a much more open cloud native network composed of microservices is an unforgiving environment for meeting stringent business service KPIs and SLAs, including in relation to network slices.

New Security Solutions for 4G and 5G Networks



Source: Netscout

That said, Netscout has also been pointing out for some time that 5G Fixed Wireless Access (FWA) exposes the mobile core – whether it's a 4G core or a 5G core – to the exact same risk of DDoS and other attacks from poorly secured IoT devices in the home that cable and other fixed line ISPs have been exposed to for years. Hence demand for the two products shouldn't be contingent just on 5G SA.

16. Nokia

Meeting with Manish Gulyani; VP and General Manager, Nokia Deepfield; James Watt, President of Optical Networks and Heidi Adams, Head of Global Marketing, IP/Optical; as well as booth tour of Cybersecurity Dome demo.

Nokia had two primary cybersecurity messages to convey at MWC this year. From its IP/Optical portfolio, the company promoted an adapted and layered approach to quantum-safe networks. This uses a physics-based cryptographic offer, enabling IP, MPLS, Ethernet and Optical connectivity. This solution leverages Pre-Shared Keys, symmetric out of band distribution, and AES cipher block encryption techniques to harden engineered connectivity against the quantum threat today.

To scale this solution, Nokia promotes its widely deployed, and NATO certified, 1830 SMS (Security Management Server) centralized key management platform. The solution works with Nokia's 1830 family of WDM optical line systems, as well as at L2, L2.5 and L3 with the Nokia 7750 Service Router portfolio.

Nokia has trained the OpenAI algorithms on telecom network topologies as well as threat intelligence and attack and defensive playbooks from multiple sources.

The company also announced the integration of a telco GenAI Assistant with the NetGuard Cybersecurity Dome. This is what Nokia calls its 'XDR' solution, running on 'Sentinel', Microsoft's Security Incident and Event Management (SIEM) platform. Cybersecurity Dome monitors and correlates telemetry from sources like logs from Kubernetes, 5G Network Functions and NetGuard EDR, to build telecom network threat signatures it can recognize and act upon to protect telco network infrastructure.

The GenAI Assistant integration also leverages Microsoft technology in the form of Microsoft Azure OpenAI Service which powers Microsoft Copilot, including Copilot for Security. Nokia went to great lengths to establish that the training data and use cases for Cybersecurity Dome are completely different to Copilot for Security. Nokia has trained the OpenAI algorithms on telecom network topologies spanning RAN, transport and core, as well as threat intelligence and attack and defensive playbooks from multiple sources. These include the MITRE ATT&CK framework and MITRE's 'FIve G Hierarchy of Threats' (FiGHT) framework which is focused on 5G threats.

The use cases for the new integration are centred on leveraging GenAI to sit above all that telco threat data and present analysts in a telco's Security Operations Centre (SOC) with ready access to relevant information throughout the lifecycle of an incident. So information is presented, including with accompanying Frequently Asked Questions (FAQ) options. This provides valuable context around things like the specific types of malware identified; variations against the norm of an individual user or device's behaviour; remediation options; and pre-population of incident reports and configuration of which individuals, departments and organizations such reports should be sent to.

Where use of classical or traditional AI in cybersecurity use cases aims at faster and more accurate detection of potential threats themselves, Nokia's application of GenAI enables SOC analysts to understand and process them faster through incident response. Each can make its own contribution to reducing a telco's Mean Time To Detection (MTTD) and Mean Time To Respond (MTTR) rates.

17. Palo Alto Networks

Meeting with Lenny Burakovsky, Vice President, Product Management

On the Wednesday before MWC, Palo Alto Networks' previously high flying share price plummeted by 28% on adverse market reaction to the company CEO's positioning of its 'platformization' strategy. This consists of encouraging and incentivizing customers to divert spending from individual best of breed products to Palo Alto Networks' ecosystem or platform of pre-integrated cyber security solutions.

It was hardly surprising then that, extreme stock market volatility notwithstanding, Palo Alto Networks' big announcement at MWC consisted of, that's right, 'platformization'. Together with Celona, Druid, Ataya, Netscout, Nvidia, and NTT Data from the world of 5G networks, performance assurance, cybersecurity, systems integration and AI, Palo Alto Networks and partners have assembled pre-integrated solutions to simplify private 5G deployments and embed enterprise grade security into their foundations.

In the broader world of enterprise security, platformization is controversial. There are modern day nuances, but the fundamentals of the debate are still single vendor versus managing multiple best of breed vendors. This debate is nowhere near as controversial in the world of private 5G because it's such a specialized, niche market. For organizations with limited in-house 5G or cybersecurity skillsets, a pre-integrated 5G ecosystem with in-built security is a no-brainer. Even among those with substantial cybersecurity resources, only a minority is going to prefer staffing up its own team, defining its own architecture, and procuring its own solutions for private 5G deployments. The initial lead markets for this are proving to be North America and Asia Pacific.

In the broader world of enterprise security, platformization is controversial. This debate is nowhere near as controversial in the world of private 5G because it's such a specialized, niche market.

Having done much of the heavy lifting to 'platformize' this approach, Palo Alto Networks is looking for like-minded partners, from its announced partners as well as further afield, to help standardize 5G enterprise security in relevant industry standards fora.

18. SandboxAQ

SandboxAQ is an enterprise SaaS company, which describes itself as providing solutions at the nexus of AI and quantum technology. The company's core team came out of Alphabet Inc. Its chairman is former Google CEO and Chair, Eric Schmidt. SandboxAQ's Security Suite is a cryptographic management software platform that provides a full range of services for achieving cryptographic agility. Central to its' value proposition is saving time through automated discovery and management of cryptographic assets as well as the remediation of flaws such as obsolete certificates. Across its portfolio, the company partners NVIDIA to simulate quantum mechanics using AI.

The company has already published customer case studies with Vodafone and Softbank. With Softbank, SandboxAQ has tested and compared the performance of contemporary elliptic curve-based encryption protocols against several pre-standard versions of the NIST PQC algorithms. To deliver Quantum Key Distribution (QKD) solutions, SandboxAQ is partnered with EvolutionQ. SandboxAQ promotes the company's BasejumpQDN, a software layer that manages and secures QKD delivery and optimizes QKD use for efficiency, what it calls 'adaptive network stability', and reduced latency.

19.Thales

Meeting with Manoj Bhati, Manager and Strategy, 5G Security and Julien Baudouin, Marketing Team Manager, Digital Identity and Security Business.

The recent acquisition of Imperva is only the latest in a series of moves that is consolidating Thales' position as one of Europe's largest cybersecurity companies (as well as its largest defence contractor). Through its world-leading SIM card business, extensive portfolio of encryption solutions, and dedicated 5G security portfolio, Thales is deeply embedded in the cyber security roadmaps of many of the world's leading telcos.

Thales is able to point to one of the strongest POC proof-points in partnering the telecom sector for quantum safety roadmaps. Last December, the company announced that South Korea's SK Telecom had successfully trialled Thales 5G PQC SIM cards in its 5G SA network. This used a pre-standard version of Kyber, one of NIST's first set of PQC algorithms. The partners made progress in understanding some of the implications and requirements on the handset side for managing a PQC algorithm's larger key sizes.

The OS upgradeability feature of the Thales 5G SIM has potential to make an important long term contribution to crypto agility. The company reckons 99% of an OS can be upgraded over the air. That includes any crypto algorithms, whether they be contemporary or future PQC algorithms.

The Hardware Subscriber Module (HSM) side of Thales, which counts big telecom names among its customers like Ericsson, is also doing early work on quantum safety. In early trials, Thales has been renewing RSA or other contemporary certificates with PQC certificates. The same types of trials with pre-standard versions of all four of the NIST algorithms are underway with the company's extensive portfolio of high speed encryption products for protecting data in motion.

Thales observes that the financial sector is currently leading with preparation for the post quantum era to protect against financially motivated cyber attacks. Telcos, which are more likely to be targeted by nation state cyber operations, are some way behind.

20. Titan.ium Platform

Meeting with Olivier de Rocquigny, SVP, Global Carrier Sales and Patrik Rokyta, CTO.

Titanium Platform was spun out from NetNumber and acquired by Lumine Group a year ago. The company defines its core focus as signaling, routing, subscriber data management, and security, allowing network operators to simplify and virtualize their core network functions and interoperate legacy and next-gen networks.

In early trials, Thales has been renewing RSA or other contemporary certificates with PQC certificates.

At last year's MWC, Titanium Platform and its competitors were touting their capabilities in the still very nascent market for 3GPP-specified Security Edge Protection Proxy (SEPP) products. With hardly any 5G SA deployed a year ago, it was a little like a lot of bald men fighting over a comb. There's been some progress in the last year, both in the 5G and SEPP market in general as well as in the customer references Titanium Platform can cite. Specifically, the company can point to a key lead customer in the form of Deutsche Telekom Global Carrier. Last November DT announced commercial deployments supporting its 5G SA roaming services worldwide, leveraging Titanium's SEPP.

In Europe the company finds itself in an unusual position in relation to its support of STIR/SHAKEN, the U.S-developed standard for combating phone number spoofing. Ofcom has recently rejected STIR/SHAKEN for use within the UK, which casts doubt as to how much further adoption will go globally. After all, if the invariably U.S-friendly Brits won't adopt a U.. standard like STIR/SHAKEN, who will? Believe it or not, the answer is the not-always-quite-so-U.S-friendly French. Yes, ARCEP, the French regulator, has mandated the deployment of STIR/SHAKEN for all national SIP traffic (representing the large majority of all calls) by all the country's telcos.

Titanium Platform is the supplier of STIR/SHAKEN solutions to SFR, France's second largest telecom operator. In January, SFR announced the standard was in live production deployment throughout its network, which implies that the same is either already true of other big French operators like Orange and Bouygues or it will be soon. Although the standard is live in the network now, SFR isn't actually using it to block messages yet.

This puts Titanium Platform in an unusual position. If much of the rest of the world follows France, the company is very well placed to grow business in this market space and succeed. If the rest of the world follows the UK, then the current competitive advantage it enjoys may not be worth quite so much.

21. VMware by Broadcom

Meeting with Sam Rastogi, Product Marketing Engineer (VMware by Broadcom) Manoj Sharma, Global Head, Security Strategy (Symantec)

With the company's recent acquisition by VMware having finally closed at the end of last year, VMware's big news at MWC was a new SASE product from which the VMware brand name itself has been withdrawn. The new product is the very carefully calibrated "New VeloCloud SASE, secured by Symantec". It's a welcome new lease of life for the generally well-liked VeloCloud brand and an extension of the VeloCloudSD-WAN and SASE roadmap. Importantly, though, the SASE security stack is now provided by Symantec, another Broadcom buy.

22. Whalebone

Meeting with Ondrej Hrabal, Product Marketing Manager

Whalebone is on a roll with a tremendous run of telco customer account wins in the second half of last year for its DNS-based network security solution. A string of wins with incumbent telcos in Central and Eastern Europe culminated with landing O2 Telefonica in Germany at the end of last year. Having scaled up to reach 80 people at the end of 2023 and annual revenues somewhere in the €5 - €10 million range, the plan is to grow to 150 people by the end of 2024.

Whatever the merits of its underlying technology, differentiated marketing is a very important part of Whalebone's ongoing success. Yes, that sounds a little 'cringey' as an analyst's account of meeting with the company's marketing guy. But give HardenStance a little credit. This conclusion is not driven by the marketing guy's own pitch. It's largely driven by having viewed and listened to the words of many of Whalebone's telco customer CMOs, CTOs and Product Managers who speak in large numbers of video interview testimonials on Whalebone's website.

Whatever the merits of its underlying technology, differentiated marketing is a very important part of Whalebone's ongoing success.

The marketing strategy is built on four very simple pillars:

1. Make expert hand-holding that leverages experience from other telco accounts persistently available to the telco customer. Most telcos have a limited awareness of what works well and what doesn't when it comes to creating successful multi-channel opt-in campaigns for a service like network security.
2. Work with the telco to ensure that that experience-informed marketing savvy makes its way from Whalebone all the way to the end consumer.
3. Persuade telco customers to go on the record and share their experience with Whalebone in video testimonials that are then posted on the company's website.
4. Make an ongoing investment in the website to communicate success to other telco account prospects. Compared with its competitors in the network security space, the Whalebone website is already a lot more compelling for a telco CMO or product manager looking for examples of a vendor's successes. Not satisfied with that, Whalebone will shortly be relaunching its website, promising even richer content.

It's possible that against one or two, or even several, threat detection or cost metrics, some of Whalebone's competitors may be able to boast equivalent or even superior technical performance. It may be possible but it's also not all that relevant. Whalebone is doing well in significant part due to marketing savvy. Unless its' competitors catch up in this key area, there's no reason why Whalebone's strong win rate should slow. ■

"MWC24: Taking Stock of Telco Security", Copyright: Patrick Donegan, HardenStance Ltd, 2024

More Information

- **Virtual Event**: Register for HardenStance's two-day "Telecom Threat Intelligence Summit 2024", taking place on June 11th and 12th 2024.
- **Briefing**: "A Quantum-Safe Roadmap for Telcos" (the quantum-safety section of this report reproduced as a dedicated report, March 2024)
- **Briefing**: "Telco Strategies for Consumer Security" (January 2024)
- **Blog**: After Kyivstar, Which Telco's Next? (January 2024)
- **White Paper**: "Telco Security Takeaways from the NIS2 Directive" (Nov 2023)

- **Report**: "Risk Management in the Telco Spotlight" (September 2023)
- **Briefing**: “Threat Intel in Telecoms (TTIS 2023)” (August 2023)
- **White Paper:** "Aligning Spectrum Policy with Cybersecurity Goals" (May 2023)
- **Briefing** "MWC23: Taking Stock of Telco Security" (March 2023)
- **Briefing**: "Intelligence-Driven DDoS Defence" (February 2023)
- **Briefing**: "Securing IP Services in Router Silicon" (March 2022)
- **GSMA event recording:** "Third Post Quantum Network Seminar" (MWC 2024)

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum. HardenStance is also a formally recognized Cyber Threat Alliance ‘Champion’. **www.hardenstance.com**.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): **Registration Link**.

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.