No.52
March 2022

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/SPONSORED

Securing IP Services in Router Silicon

Sponsored by Nokia

- Nokia has augmented its IP network security portfolio with the new FP5 processor.
- An enhanced DDoS protection capability and a new encryption solution provide telecom operators with new tools to secure IP services, reduce costs and grow revenues from within the router infrastructure.
- As with any differentiated capabilities, customers need educating on these new value propositions and how their organizations can adapt to exploit them.

The FP5 Enhances Nokia's IP Security Portfolio

Last September's launch of the FP5 network processor, supporting high-density 800GE and 1.6 Tbit/s clear channel routing interfaces, adds new capabilities to Nokia's IP network security portfolio for telecom operators. This is centered on the 7750 Service Router for core and edge networks.

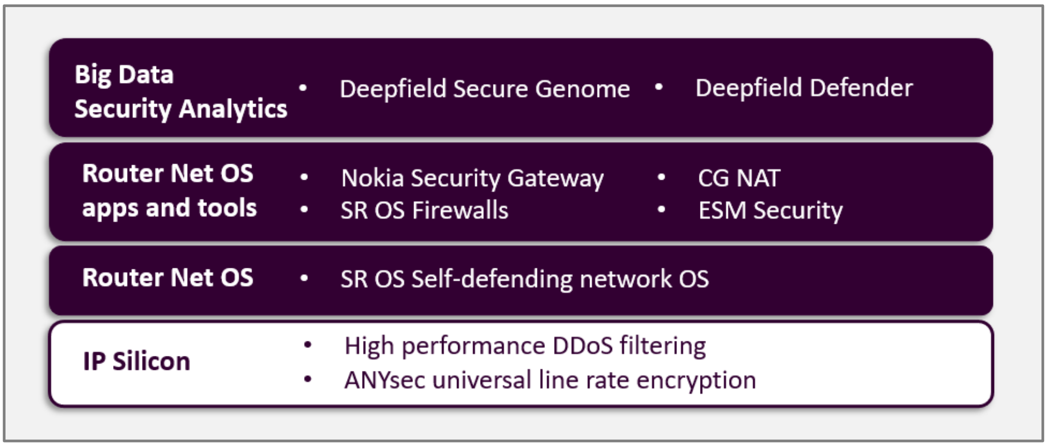
Last September's launch of the FP5 adds new capabilities to Nokia's IP network security portfolio.

From a network security perspective the new release enhances Nokia's DDoS protection solution with deeper packet inspection and better filtering capabilities. A new 'ANYSec' solution also enables operators to offer differentiated end-to-end encryption of IP transport services. The value proposition for telecom operators is three-fold:

- Reduce Total Cost of Ownership (TCO) by driving DDoS protection and encryption of IP transport services as well as core routing from the 7750 SR rather than from three separate platforms – with zero performance impact.
- Harden the operator's own security posture – and that of its customers – against growing business risk, including to critical infrastructure, from security threats.
- Augment revenues by growing revenues from premium network security services.

Nokia's full stack approach to IP network security is shown in **Figure 1**. This Briefing reviews Nokia's DDoS protection and encryption offer at the IP silicon layer.

Figure 1: Nokia's Multi-Layered, Embedded, Approach to IP Network Security



Big Data Security Analytics
- Deepfield Secure Genome
- Deepfield Defender

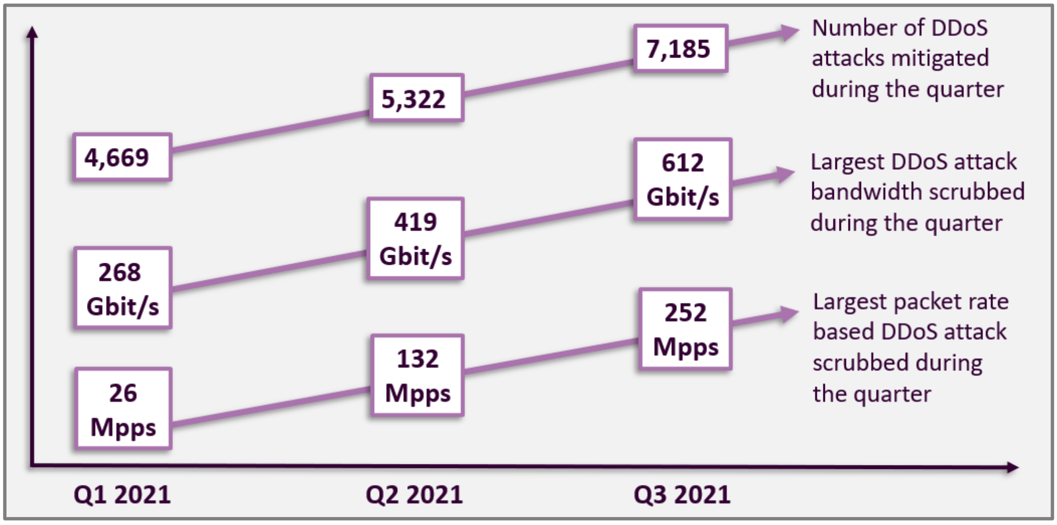
Router Net OS apps and tools
- Nokia Security Gateway
- SR OS Firewalls
- CG NAT
- ESM Security

Router Net OS
- SR OS Self-defending network OS

IP Silicon
- High performance DDoS filtering
- ANYsec universal line rate encryption

Source: HardenStance/Nokia

Figure 2: Highlights from Lumen's Quarterly DDoS Report Q1 – Q3 2021



Source: HardenStance/Lumen

Enhanced Filtering Against Growing DDoS Threats

DDoS threats continue to pose a major threat to the availability and performance of network infrastructure. In January 2022, Microsoft announced that it had fended off a 3.74 Tbit/s DDoS attack on an Azure customer in Asia in November 2021. This easily beat the previous record of three separate 2.4 Tbit/s attacks reported over the previous 18 months by Amazon, Google and Microsoft.

As shown in **Figure 2**, telecom operators like Lumen are reporting substantial quarter-on-quarter increases in key threat metrics like the number of attacks, largest attack bandwidth consumed, and size of packet rate they are seeing. In conjunction with a major spike in ransomware attacks, the last couple of years have also seen DDoS attacks used as part of double or triple extortion attacks where the threat of a DDoS attack or leaking encrypted data is used to intimidate victims into paying the ransom.

Routers tend to serve as the junior partner to the layer of solutions from specialist DDoS protection vendors.

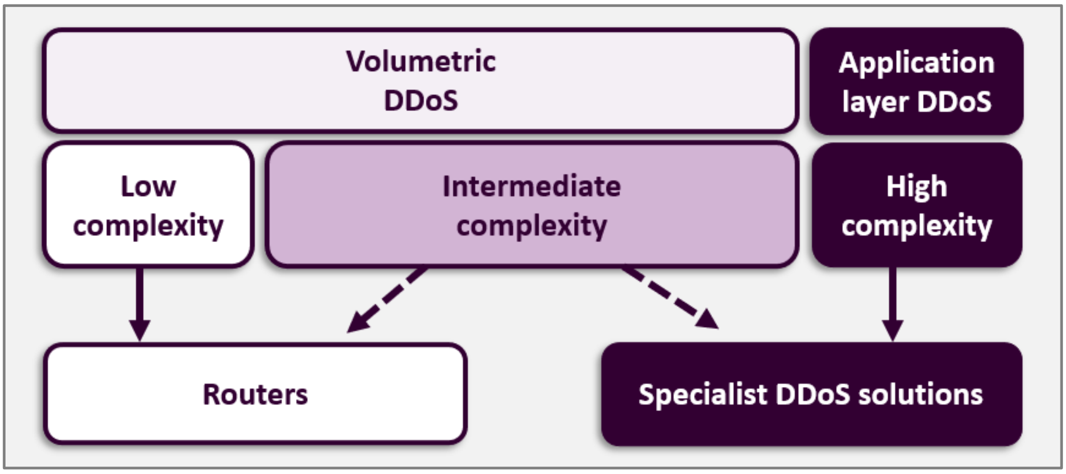
Routers Already Play a Significant Role in DDoS Protection

Core and edge routers already play an integral part in a layered approach to any telecom operator's DDoS protection strategy. The flow telemetry they generate is one of the most important feeds operators use to make detection decisions about whether a given packet is good or bad, and the best way in which bad packets should be dropped. Once detections are made, routers also feature in the mitigation phase by way of filters being generated on them to automatically drop unwanted traffic.

In terms of the proportion of DDoS attacks that they actively detect and mitigate in today's telecom networks, routers tend to serve as very much the junior partner to a layer of solutions from specialist DDoS protection vendors like NETSCOUT and Radware. This second layer comprises DDoS detection appliances deployed in the network together with access to DDoS mitigation or scrubbing centers that are either deployed in the network or consumed by the operator as a cloud service.

When dealing with the most complex attacks, nearly all of which are application layer attacks, leading DDoS specialists have clear advantages. These include how deep they can inspect packets as well as being able to view entire packet streams. Specialized DDoS solutions can also interpose themselves between entities, interrogate suspicious clients, and leverage responses to build richer context around traffic and reduce the risk of under or over-blocking. Being stateless, routers can't do this. Hence, they are less able than specialist DDoS solutions to defend against the most complex attacks. These typically compromise anywhere from 10-15% of total DDoS traffic.

Figure 3: The Contest for the Middle Ground in DDoS Protection



Source: HardenStance

At the other end of the scale – the simplest volumetric attacks – flow telemetry from routers is undoubtedly good enough for parsing DDoS traffic, reaching good decisions on which packets to drop, and then deploying filters on routers to mitigate these attacks.

It's the large swathe of DDoS attack traffic between those extremes – defined as representing 'Intermedia complexity' in **Figure 3** – that is more contentious. Telcos still tend to lean heavily on specialists' DDoS solutions rather than their routers for this traffic, which tends to mean paying these specialists to defend against a large majority of all DDoS attacks they see.

Telcos persist in leaning so heavily on specialist DDoS vendors for a number of reasons, some of which are cultural or organizational.

Telcos Pay a Heavy Price for Relying So Heavily on DDoS Specialists

Telcos currently pay a hefty price premium for this:

- A lot of investment in network bandwidth is needed to backhaul suspect traffic to and from scrubbing centres – and as shown those traffic volumes are still increasing.
- It nearly always costs more to execute any networking function from specialist products than from multi-purpose platforms and DDoS protection is no different.
- Moreover, for the scale that telecom operators need today, let alone what they'll need in future, the specialized DDoS protection market is still not very price competitive. For example, NETSCOUT is generally recognized as reaping high to very high margins for its line of Arbor DDoS solutions.

Telcos persist in leaning so heavily on specialist DDoS vendors for a number of reasons, some of which are cultural or organizational. There's the force of habit that comes from an established model of doing things (and long-established personal relationships). There are also issues of organizational immaturity and interdepartmental rivalries that get in the way of network and security operations teams cooperating with one another.

Network and security operations teams tend to point to the following technical limitations of routers for DDoS defence for all but the most straightforward attacks:

- Limitations in their packet inspection capability;
- Limitations in the number of filters they can support;
- Delays that can last minutes or tens of minutes in the speed with which filters can be deployed. When a business customer's online ordering, online payment system or remote access VPN concentrator are under attack, rapid mitigation is critical.
- Concern that configuring routers with DDoS protection filters risks exposing core routers to inadvertent misconfigurations.

New Opportunities Arising from Market Evolution and New Features

Most router vendors concentrate a lot of their effort on winning the large middle segment of DDoS protection business that currently goes to specialist DDoS vendors by partnering those same specialist vendors, a strategy that might be thought of as "if you can't beat them, join them."

Nokia is taking a different approach. By aligning the roadmaps of Deepfield Secure Genome and the FP5, Nokia wants to persuade telcos to drive a lot of that large middle segment of intermediate complexity DDoS traffic onto the 7750 SR. The company has some generic market trends in its favour as well as some new product features.

Here's what's happening in terms of market trends:

- The increasing volume of DDoS attack traffic is putting upward pressure on the total cost of DDoS protection at multi-terabyte and petabyte scale. Where DDoS mitigation services charge according to traffic volume, the potential cost savings of dealing with DDoS traffic in-line in the IP network can look increasingly attractive.
- Customer demand for lower latency – whether for video, gaming and VR/AR services or for 5G's Ultra Reliable Low Latency Communications (URLLC) – also favours in-line blocking decisions. As well as taking up a full slot, integrating a third-party DDoS protection blade in a router chassis adds latency. Even in an all-DDoS specialist solution, backhauling traffic back and forth to a scrubbing centre adds latency.

Nokia can now go deeper into a packet to view some of the DNS and other information needed to identify and stop more complex attacks.

Enhancements to Nokia's DDoS Protection Solution

With the new FP5 release, Nokia points to the following enhancements to its suite of DDoS protection capabilities. The new commitments it makes are as follows:

- It's not just '5 Tuple' packet classification across five different values of a TCP/IP connection that's supported now. Using the additional security context obtained from the cloud-based Deepfield Secure Genome, and Deepfield Defender's security analytics capability (**See Figure 1**), Nokia can now go deeper into a packet to view some of the DNS and other information needed to identify and stop more complex reflection and botnet-based attacks.
- As with previous generations of Nokia's FP silicon, filtering is done at wire speed independent of the number of filter rules applied.
- Filters can be deployed at scale in seconds or minutes rather than tens of minutes.
- As well as continuing to support filter configurations according to the industry norm of using BGP Flowspec, Nokia now supports it via NETCONF. Nokia advocates using NETCONF to isolate filter configurations from BGP as a way to reduce the risk of misconfigurations. Different customers are likely to take a variety of views regarding the comparative risk profiles of each option, based in part on their own organizational set-up. Ultimately, designing and adhering to robust and secure processes in day-to-day network and security operations is just as important in determining real world risk levels as the choice of filtering tool - if not more so.

Network Encryption Services for Data in Transit

The second new solution enabled by the FP5 is a differentiated encryption capability for IP transport services. Telecom operators themselves need a range of encryption options tailored to different use cases for locking down their infrastructure. From a customer perspective, encrypting application layer payloads with Transport Layer Security (TLS) is enough for most enterprises but many also need to supplement that with additional network layer security.

L1-L3 encryption options have different profiles. Optical encryption is great until you want to extend a service to places where you need to invest in dark fibre or someone else's L2 access service. Since it is implemented in silicon, L2 MACsec is great from a latency perspective. But having to manually configure the decryption and re-encryption at each router hop so that each packet can be inspected to see where it's going next is operationally complex. This also increases the risk of man-in-the-middle attacks.

IPsec does provide end-to-end encryption but instead of being embedded in silicon it typically requires dedicated hardware via a dedicated router blade or separate platform. The need for CPU intervention in IPsec drives latency measured in microseconds rather than nanoseconds with MACsec. Also, unlike MACsec, IPsec doesn't encrypt routing information.

Telecom operators have to match the best available network encryption options to their own requirements and those of their customers in an evolving market environment that can be characterized as follows:

ANYsec enables native L2, L2.5 and L3 encryption end to end, at line rate, across engineered networks based on IP, MPLS and segment routing.

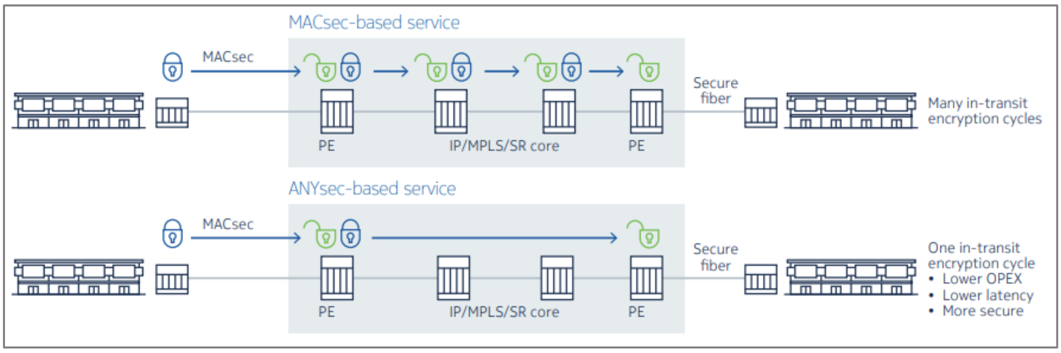
- **Data is much less static - more and more active - across increasing numbers of sites.** This is because cloud and enterprise customers are becoming distributed across more and more sites. Whether it arises from more employees working from home or accelerating investment in edge clouds, this proliferation of sites that sensitive data is entering and exiting from represents a growing threat surface for all stakeholders – enterprises, cloud providers and telcos.
- **As shown by recent high-profile incidents, critical industries like hospitals and energy providers are increasingly vulnerable to cyber-attacks**. In some cases, these are overtly or covertly supported by nation states seeking information superiority over adversaries. Just one example of the type of risk that data in transit faces without network encryption is Border Gateway Protocol (BGP) leaks or hijackings whereby Internet traffic is rerouted – either maliciously or due to benign error. In recent years there have been several high-profile incidents. In August 2019, European operators such as KPN, Swisscom, Numericable SFR and Bouyges Telecom were among victims that saw their traffic wrongly routed through China Telecom's network for anywhere from a few minutes to more than two hours.
- **Despite heightened risk, the imperative of further accelerating digital transformation isn't seriously questioned in business circles**. Indeed, via Ultra Reliable Low Latency Communications (URLLC) 5G is expressly designed to expose critical infrastructure to the full potential of hyper connectivity – hence also the full risk. If digital transformation is to scale safely at the pace that business leaders are demanding, cyber security across endpoints, networks and clouds must improve - on the part of those using the networks and those providing them.
- **Enterprise customers don't always have a good understanding of their optimal encryption requirements.** Customer understanding of the real-world cost and impact of different network encryption options – taking full account of all capex and opex costs as well as performance impacts – can be very poor. They should be open to persuasion on the best options for them from trusted partners.

ANYSec Extends MACsec to any L2.5 or L3 Networks

Embedded in the FP5 chip, Nokia's 'ANYsec' solution is based on MACsec encryption, leveraging both its WAN and LAN modes. It enables native L2, L2.5 and L3 encryption end to end, at line rate, across engineered networks based on IP, MPLS and segment routing from provider edge (PE) to PE.

The 'Any' in ANYSec refers to a telecom operator being able to encrypt any service (internal, wholesale or high-speed VPN) over any transport (IP, MPLS, Segment Routing or other) at any time (switching it on or off from within the network without needing a lot of advanced planning around where different devices need to be deployed).

Figure 4: ANYsec-based Secure High-Speed VPNs



Source: Nokia

To extend the encryption end to end across engineered L2.5 and L3 networks, ANYsec enables MPLS labels, segment routing labels and IP addresses to be inserted in the clear as well as Ethernet and VLAN tags. End-to-end encryption is maintained irrespective of what L2.5 or L3 mechanisms are used to engineer them - and irrespective of what networks, geographies and jurisdictions the flows transit through. Other routers at other hops in the path don't need any involvement in the encryption cycle. This removes the hop-by-hop complexity traditionally associated with using MACsec in the WAN environment and further reduces latency. It also allows ANYsec to work in a multi-vendor environment featuring other vendors' routers in addition to the Nokia 7705 SR.

ANYsec can also be embedded in very high capacity, low latency, VPNs for individual enterprise customers.

As ANYsec encryption is end to end, the data can't be exposed by a man-in-the-middle attack. To return to the BGP hijacking example, ANYsec can't protect the BGP hijacking itself – this is a function of the router's BGP capability. However, the end to end encryption does prevent the hijacker from being able to view or manipulate the hijacked network data.

Three Initial Use Cases for ANYsec

Nokia sees three main uses cases for ANYsec. The first is locking down the operator's own infrastructure to support its brand as a trusted provider. This same proposition can be extended to wholesale services for other carriers, assuring the wholesale customer that their flows will be encrypted end to end no matter where they go right at the point of hand off. ANYsec can also be embedded in very high capacity, low latency, VPNs for individual enterprise customers. One example is Data Centre Interconnect at 400 Gigabit/s spanning multiple clouds, where a customer wants to switch at a label level instead of using VLANs.

The Opportunity for Telecom Operators

The most compelling parts of Nokia's enhanced network security propositions delivered from the FP5 are the following:

- **Capex and Opex Savings**: No CTO can see an opportunity to deliver more services from their routing infrastructure instead of from dedicated platforms, without immediately thinking 'CAPEX and OPEX savings'. There are standalone cost savings to be realized with just the DDoS protection or just the ANYsec proposition – more so by leveraging both.
- **Zero Performance Impact**: This explicit commitment from Nokia is arresting. The company commits that you can run the 7750 SR's network security features as hot as you like, using every last one of the DDoS filters and encrypting every single flow with ANYsec, and there will be zero performance impact on the core routing functions.

- **Low latency**: To borrow from the system availability language of 'five nines', telecom operators are probably at something like three or four nines in terms of what they are able to deliver by way of end-to-end latency today. Getting to the fourth or fifth 'nine' as they are targeting now will be extremely challenging. When every millisecond counts, delivering network security services from router silicon at line rate can make a significant contribution to achieving stringent latency targets.
- **Incremental revenue growth**: There's an opportunity to charge a premium for both DDoS protection and encryption services as well as bake them into core services to benefit all customers. Where significant cost savings can be realized, pricing can potentially be reduced to serve segments of the business market for whom current pricing is too high.

The Challenges for Telecom Operators

Some of the challenges telecom operators face in considering how these network security service capabilities do or don't fit in their environment include the following:

Embedding security in routers doesn't just "simplify things". Nor does it make things "more complex"– it actually does some of both.

- **Hardware-driven services in an increasingly software-driven market**. The trajectory of telecom service evolution is predicated on reducing dependency on hardware and increasing dependency on cloud native software to improve operational agility. Many cloud providers, not to mention some cloud evangelists within telco organizations, can be expected to argue against leveraging core and edge routers for anything much besides routing. These arguments go along the lines that delivering network services from within telco router silicon runs counter to 'software-ization' or 'network cloudification'.

  Several points arise here. First, vertically integrated routers aren't going anywhere any time soon. While many of Nokia's Broadband Network Gateways (BNG) customers run the control plane as virtualized software on servers, they invariably prefer the power of the 7750 for the user plane. Second, the network security market is still heavily dependent on specialist hardware. There are certainly cloud-based elements to most DDoS protection solutions (the Deepfield analytics component of Nokia's runs in the cloud, for example) but they still tend to have substantial hardware-dependencies. Virtualization has to advance in lock step with considerations relating to cost, performance, latency and security.
- **Complexity and simplification at the platform and network level**. Business cases must be evaluated using appropriate and consistent assumptions. Embedding security in routers doesn't just "simplify things". Nor does it make things "more complex". It actually does some of both. At a network level, removing dedicated platforms clearly simplifies. This is where big cost savings can potentially be made. But at the product level of the 7750 SR and the personnel who operate it, converging security operations onto routing platforms does also add some amount of complexity and risk to operations compared with each party having their own dedicated platform. That risk has to be acknowledged and steps taken to mitigate it in order to get simplification and cost reduction at the network level.
- **Managing inter-departmental boundaries and rivalries**: As alluded to above, converging security services onto routers requires a security team to have controlled access to the router infrastructure. It also requires that both teams design and follow operational procedures that ensure neither overwrites nor otherwise interferes with the other's configurations. Errors here pose a significant risk to network or service performance and to security. There could potentially be a third team in the mix too - the telco's Managed Security Services Provider (MSSP) team.

  There are no major technology barriers to telcos doing this well, and many already do. But there are also examples of telcos where operational efficiencies and revenue opportunities are consistently overlooked because a lack of organizational maturity drives an uncollaborative culture between network and security operations. Extracting more security value from Nokia's IP portfolio is more a function of managing human behaviour and corporate culture than a function of technology.

Building a trusted brand: Whichever path they choose, telecom operators have to extend their efforts to build their brand as trusted providers as customers become increasingly dependent on their digital environment; as cyber threats to critical infrastructure increase; and as both customers and regulators demand more by way of the security of IP services. This is especially important at the level of premium services that telcos charge for. For example, in the case of premium DDoS protection services delivered from the network, customers will need to trust that reducing dependency on a dedicated appliance in the network to protect their business carries no new risk.

Many businesses also like the control that managing their own encryption keys via an on-premises appliance gives them. ANYsec requires trusting the telecom operator with the management of encryption keys within the operator's own network. The fact that 7750 routers are invariably deployed in large, trusted data centres is certainly a good starting point, but many customers will still have high expectations of understanding how the security of those keys is managed. As well as building a compelling proposition here, telecom operators need to invest in their brand as a trusted provider to communicate the value proposition. ■

More Information

- Nokia's IP Network Security Portfolio
- Nokia Deepfield Intelligence Report: The State of DDoS in 2021

About Nokia

At Nokia, we create technology that helps the world act together. As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs. Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

About HardenStance

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

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report. HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same. The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim arising in relation to the contents of this report.