White Paper

HardenStance

5G Security to Drive Enterprise Investment

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

May 2018

HardenStance

"Trusted Research, Analysis and Insight in IT & Telecom Security"

Executive Summary

- Enterprise Chief Security Officers (CSOs) will have a big say in 5G investment decisions. Unless security options are diverse, customizable, open and transparent, CSOs won't sign-off on new 5G use cases on the scale that telcos are hoping for.
- Key aspects of 5G security that enterprises will scrutinize include virtualization security, network slicing, edge use cases and endpoint security. Telcos and their 5G ecosystem partners have to get these right.
- Enterprise CSOs must engage in the 5G ecosystem to specify the security they want.
- The big cloud providers have strong relationships with enterprise accounts. Telcos should consider partnering them to deliver 5G security options to these customers.
- As 5G drives security that is increasingly dynamic and adaptive, many telcos will need security integration partners as well as multiple best of breed vendors.
- Strong baseline security in 5G will require highly efficient, scalable, infrastructure.

"Whereas 4G is largely independent of the cloud, the cloud-native 5G network will host enterprise applications and become meshed with the cloud."

New enterprise use-cases to grow telco revenues

The first 5G networks have been deployed at the Winter Olympics in Korea and the Commonwealth Games in Australia. U.S operators are vying for 5G leadership in ultra-fast mobile broadband services. AT&T wants 5G live in twelve cities by the end of 2018.

These largely consumer-driven use cases are giving the 5G ecosystem a critical kick-start. However, the greater opportunity lies in leveraging 5G's unique capabilities to drive incremental revenues from new vertical industry use cases. Key among the new capabilities that 5G will bring to enterprise use cases are a cloud-native architecture allowing dynamic distribution of network resources; differentiated radio resource options that are optimized for different applications; and the ability to create unique, logically private, networks for enterprises through network slicing.

Combined with analytics platforms that can be augmented by machine learning, 5G will transform the networking tools that are available to enterprises to optimize their operational efficiency and deliver new applications and services to their customers.

Spending on 5G use cases requires a CSO sign-off

Chief Security Officers (CSOs) – or their equivalents – have always had a role in specifying compliance and security requirements related to ICT purchasing. But there are three very good reasons to believe that their influence in designing and signing off on investment in new 5G use cases will be greater than anything we've seen before.

- **The status of CSOs in their companies is rising**. In its 2018 "Global State of Information Security" survey, PwC states that 40% of CSOs report to their CEO now while 27% report to the Board of Directors. That wasn't the case a few years ago.
- **5G creates new security risk.** Whereas 4G is largely independent of the cloud, the cloud-native 5G network will host enterprise applications and become meshed with the cloud. CSOs have to manage the new risks this introduces.
- **There is significant momentum behind a push-back against the 'animal spirits' that drove the IT revolution.** In the enterprise, DevSecOps with security baked in to development is the new DevOps. The new General Data Protection Regulation (GDPR) that gives users more control over their data imposes strict data protection regulations on any business that serves EU citizens. And following greater public scrutiny of its data sharing policies in March 2018, Facebook lost $100 billion in market cap and faced the backlash of the "Delete Facebook" movement.

Telcos that are counting on enterprise customers committing large investments in new 5G use cases need to understand the implications of this. They are expecting enterprise

CSOs to sign off on increasingly complex use cases when these CSOs will need to have even tighter security controls over their IT environment than ever before.

Telcos and other 5G ecosystem stakeholders will therefore have to accord a whole new level of priority to seeking out and listening to the security requirements of these enterprise CSOs - and then aligning with those requirements. Telcos that do that well will have a good chance of growing new 5G enterprise revenues. Those that don't won't.

Key trends in enterprise IT security

A 5G security portfolio to support new enterprise use cases needs to build on the current enterprise IT security landscape. Some key factors and trends are shown below:

- The threat posed to businesses by cyber-attacks and the requirements imposed on enterprises by regulators as regards data protection are both increasing markedly.
- As well as protecting their own assets, enterprises are increasingly having to extend their security policies to protect their customers on the network and in the cloud. Some think of themselves almost as security 'service providers' in their own right.

"One of the biggest challenges facing CSOs is to build a unified security architecture extending across all the enterprise's infrastructures."

- Virtualization is well established in the enterprise. Hence a growing number of enterprises are well versed in securing virtual machine and container environments.
- Organizations are evolving from hosting IT assets and security controls on-premises to hosting them in the cloud (often via a hybrid model that embraces both).
- The IT security environment isn't just multi-vendor in terms of hardware and software now. Enterprises are choosing multi-cloud – leveraging two or more public cloud providers to host different data, servers, security controls or other assets. They want to move workloads between clouds dynamically and securely - either for supplier diversity or because one provider is the best for a specific requirement. Some big firms even source from two Managed Security Service Providers (MSSPs).
- One of the biggest challenges facing CSOs is how to build a unified security architecture extending across all the enterprise's on-premise, public and private, cloud and multi-cloud, infrastructures rather than operating multiple security silos.
- As suppliers to enterprises, telcos are more regulated than cloud providers as regards privacy, uptime and incident reporting but this balance may be set to shift.

Business must be able to trust the 5G ecosystem

Businesses are certainly interested in 5G's potential. The automotive industry has distinguished itself as an early adopter. Leading automotive manufacturers are investing heavily in trials of 5G-enabled autonomous vehicles. The 5G Automotive Association (5GAA) is driving significant engagement including in 5G standardization. Most other industry verticals aren't as heavily engaged in 5G development yet but that will come.

For enterprise CSOs to support many new use cases, the 5G ecosystem won't just have to show a clear path to new revenues or new cost savings. The 5G ecosystem will also have to be trusted to protect the Confidentiality, Integrity and Availability (CIA) of enterprise data at rest, in use and in transit.

Enterprises can certainly count on industry standards bodies building the foundation of the traditional transport and network layer security for 5G, according to the same high standards of previous generations of mobile technology. Indeed, that work is already well underway. For example, 3GPP's SA3 Technical Specification group recently announced completion of TS 33.501 on "The Security Architecture and Procedures For 5G Systems."

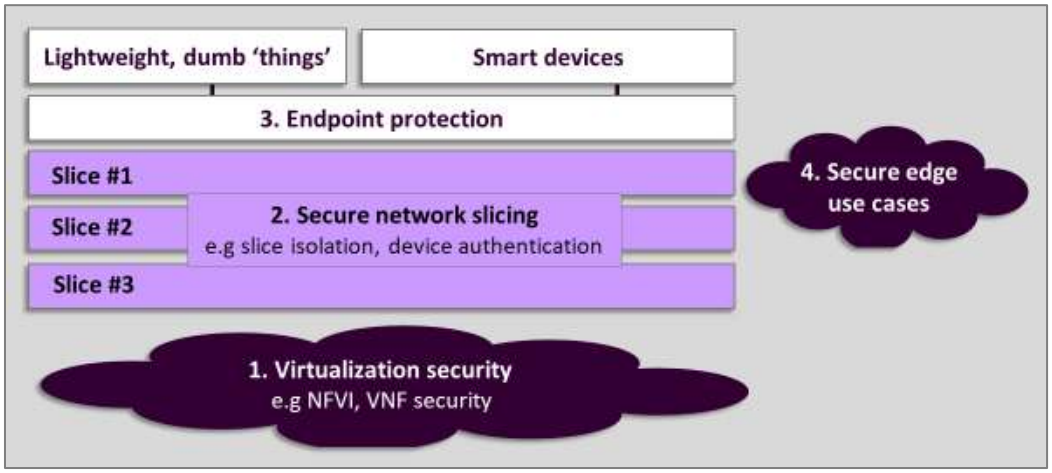
But enterprises will also expect to 'kick the tyres' of potential 5G use cases from a security standpoint. They will want to understand which 5G security standards have been implemented in the network (and perhaps how). CSOs will need to identify what

more is needed on top of the baseline 5G security to support those use cases that can serve their business. And they will need to figure out how their existing IT security architecture – and the existing commercial partnerships and SLAs that underpin that – can be mapped to support 5G-enabled use cases.

5G security challenges for enterprise use cases

This section addresses some key aspects of 5G security that enterprises will pay very close attention to when they evaluate the new use cases that are put to them. Specifically, it looks at some key security aspects of the cloud-native virtualized infrastructure; edge use cases; network slicing; and endpoint security.

Figure 1: Key 5G security issues for enterprise CSOs



Source: HardenStance

"To secure the telco's NFV environment, controls are needed to protect NFVI hosts from compromised VNFs."

Secure virtualization in a cloud-native environment

Most telco NFV deployments to date consist of VNFs statically deployed on Virtual Machines (VMs) running on standard servers in isolated, domain-specific, silos. It qualifies as NFV but it creates nothing like the opportunity – or risk – of exploding VNFs throughout a distributed network on shared hardware that cloud-native 5G creates. Given today's available technology, cloud native necessarily means containers, albeit there's the option to run containers in VMs as well as on bare metal.

To secure the telco's NFV environment, controls are needed to protect NFVI hosts from compromised VNFs; protect VNFs from compromised NFVI hosts; and isolate VNFs from interfering with one another and leaking data via cross-contamination of malware.

The evolution to cloud-native containers poses new security challenges, and this is one reason this transition is taking time among telcos. One security challenge is the rapid speed at which applications are developed and deployed in a container environment. This poses risks until the security model is locked down. Another is that most containers have a lifespan ranging from a few microseconds to no more than a few hours. This changes the security model in a number of ways, including from an Incident Response perspective. Part of the solution lies in migrating to DevSecOps.

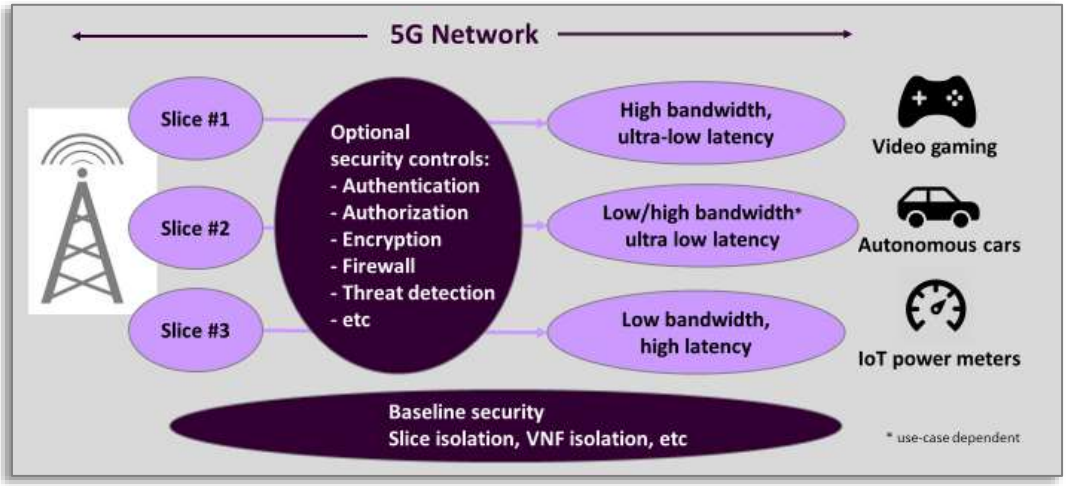
Security requirements for network slicing

The security aspects of network slicing are still at a formative stage. One of the two fundamental requirements is a variable menu of security features to allow stronger or weaker security to be served up to devices, depending on the application and the sensitivity of the data collected, analysed and stored within the slice. The second is a trusted 5G slicing environment that provides guarantees that telcos and enterprises cannot view one another's data from within a network slice.

This environment will initially evolve as a hybrid of standards-based and proprietary implementations before becoming more fully standardized over time. Companies that want to create new digital experiences for customers will want tighter control of the infrastructure that these applications run on, including the security features.

Enterprises won't just expect to be able to choose different types of slices and to customize them accordingly. They will also expect to be able to mix and match their slices from different slice providers – for example, those providing slices of raw capacity and specialized providers delivering slices that are customized for specific use cases.

Figure 2: Baseline security with enterprise options for network slicing



Source: HardenStance

"Protections for the management interface that enterprises use to manage their slices will also be needed."

Among key security features, enterprises will expect strict isolation between network slices across cloud, RAN and transport domains as well as strict isolation of each VNF within each slice. Protections for the management interface that enterprises use to manage their slices will also be needed. This is to prevent slices or individual functions or applications within slices being compromised or even deleted by unauthorized parties.

Depending on the application and the sensitivity of the data, enterprises will expect the ability to require that a given device must either authenticate separately onto each and every one of its slices or to require initial authentication onto a first slice followed just by authorization onto subsequent slices. Protections will also be needed against the particular vulnerability to DDoS attacks of slices that are configured for low capacity.

Security requirements for edge computing

Distributed computing at the edge – one of the key promises of the 5G network – throws up very different security issues. Many CSOs are only now starting to get used to a centralized cloud model in which visibility, control and auditability are enabled, tracked and presented differently than they were in the traditional on-premises security model.

CSOs are going to need clarity around how data is secured when the recently-centralized IT security model is flipped on its head so that network, storage and compute resources are distributed across large numbers of 5G sites. Among potential solutions are going to be the following:

- Some edge use cases require that a telco's VNFs shares the same hardware instance as the enterprise's own software instances, like analytics. Here software instances of telcos and enterprise customers need protection from one another, much as different telco VNFs need protecting from each other in the telco domain.
- Encryption key management to protect the confidentiality and integrity of enterprise applications will need to be approached differently at remote sites. Hardware Security Modules (HSMs) that provide a root of trust in the network can be expected

to have an expanded role in 5G but they are too costly to deploy at most edge sites. One option is so called Secure Enclave technology. These are hardware encrypted zones created at the chip level that give developers the means of leveraging the CPU to create isolated, trusted, memory regions. These non-addressable memory resources are isolated from the physical RAM and encrypted to protect sensitive data and code from unauthorized exposure.

The limited availability of compute resources at edge sites can make it challenging to prioritize security features over other capabilities. Security can also be an inhibitor rather than an enabler of the low latency that drives many 5G edge use cases.

In seeking to overcome some of these limitations, telcos may want to consider models in which they control the applications at the edge and provide API access to the policy that is enforced or the analytics that are generated. For example, it could prove more efficient for a telco to implement IP blacklisting for many enterprises than for each one to deploy it independently.

More needs to be done to integrate the security component into edge use cases effectively. Consideration will also need to be given to how existing cloud policy management capabilities can be extended to the edge.

"From the perspective of an enterprise, it's the confidentiality and integrity of data generated by their own 'things' that matters most."

Endpoint security for IoT 'things'

At the level of the broader 5G and ICT ecosystems, the growth of IoT represents a major threat to the "A" – Availability – out of the three key security pillars of Confidentiality, Integrity and Availability. The IoT-driven Mirai botnet that took down large parts of the Internet in October 2016 is only the harbinger of worse things to come.

But from the perspective of an enterprise, it's the confidentiality and integrity of data generated by their own 'things' deployed in the field that matters most. Among the capabilities enterprises will want to consider are basic white-listing principles that assume as a starting point that devices are blocked from accessing any application unless they are expressly permitted to. Network-based threat detection in IoT gateways will be important for lightweight IoT sensors whose own footprint is too tiny to support security controls. Identity management and end to end provisioning will also be key.

In an IoT market operating at what is expected to be very high scale, enterprises will also be interested in the re-attachment rates of 'things' immediately following a network outage. According some devices high prioritization in the reattachment process, or lower prioritization at lower cost, depending on the needs of the application, should be made easier by the capabilities of 5G.

Endpoint security for smart devices

A different end point security model will be required in the case of smart devices. Laptops, smartphones and tablets have become increasingly powerful over the course of the 4G investment cycle. Evolving into the 5G era, the variety of these smart devices will accelerate, including "devices" such as autonomous cars.

Whereas relatively dumb 'things' can be expected to rely heavily on storage and application logic stored in the cloud, many 5G use cases will require intelligent endpoints to store a lot more data, some of which may be highly sensitive. In some edge use cases, for example, limited available network resources, backhaul cost constraints or low latency requirements – or all three – will drive greater data storage and compute requirements onto these smart 5G endpoints.

As well as basic endpoint security like antivirus and encryption that runs on smart devices today, enterprises will want to consider capabilities like sandboxing and Data Loss Prevention (DLP) software on smart 5G devices. DLP software does real-time monitoring of data at rest, in use and in transit looking for – and blocking – unauthorized attempts at data exfiltration. Having traditionally been deployed in network

infrastructure and PCs, DLP has started making its way onto mobile devices in the last couple of years including as a feature integrated with popular enterprise Mobile Device Management (MDM) solutions. 5G looks set to accelerate momentum around this emerging product category that some are starting to label 'Mobile Threat Defence'.

5G security principles for winning enterprise trust

To bring about a thriving security ecosystem that enterprises will trust and invest in, HardenStance recommends that key stakeholders should drive the 5G security ecosystem according to the eight principles shown in **Figure 3.**

Figure 3: 5G security principles for winning enterprise trust

Source: HardenStance

"The telecom industry has done quite a bit of reaching out to enterprises, though perhaps not directly enough to the CSO community yet."

1. Enterprise-driven

The menu of 5G security options that is presented to enterprise customers has to be driven by the needs of those customers. The automotive industry is already engaging heavily with the telecom industry on 5G but most other enterprise verticals aren't. That has to change. The telecom industry has done quite a bit of reaching out to enterprises, though perhaps not directly enough to the CSO community yet. The CSO community needs to do more too. For example, professional CSO associations should be nominating representatives to contribute to security groups in telecom standards bodies.

2. Diverse & Customizable

Reflecting the variety of potential use cases, enterprises will expect to be able to choose from a diverse menu of flexible 5G security options that they can customize to their unique requirements. That will also require a variety of ways of consuming and paying for security functions, including billing models that reflect temporary bursts of demand.

3. Transparent

Network slicing will require a commitment to transparency on the part of telcos. To deliver new customer experiences, enterprises will expect tighter control of the network performance parameters within their slice(s) as well as security controls. They will expect real-time or near real-time visibility and reporting into what the slice provider is delivering from a performance and security perspective. They'll also want the ability to query log data.

While the telco has sole responsibility for isolation of VNFs at the infrastructure level, telcos and their enterprise customers will have to share responsibility as regards isolation of VNFs and the enterprise's applications within the slice. This will require both parties taking steps to establish a high level of trust.

Slice providers can choose to deny enterprises this kind of visibility and control if they want – so long as they're not then surprised when customer uptake fails to meet their

expectations. The right balance here clearly requires rigorous security controls on the slice provider's side to ensure that enterprises only get visibility into their own slices and no other network resources.

4. Automated & Orchestrated

"So-called 'zero-touch' automation isn't likely for some time yet in the case of threat mitigation."

Enabled by cloud-native virtualization, a high level of automation is key to enabling rapid instantiation of security services. As enabled by the features supported by some individual products in spaces like security monitoring, Intrusion Prevention Systems (IPS) and DDoS protection, aspects of security detection are already highly automated. It's in the area of automating aspects of protection that some telcos are still lagging. Specifically, there's a long way to go for some telcos in automating security patching of their entire estate of security instances across network domains.

So-called 'zero-touch' automation isn't likely for some time yet in the case of threat mitigation. The sophistication of some Advanced Persistent Threats (APT) will require detailed investigation by human security analysts – augmented by artificial intelligence – for the foreseeable future. A key goal of automating security is precisely to redeploy security analysts from mundane tasks to focus on threats that pose a higher risk.

5G security also needs to be highly orchestrated. That means automated, service-level, life-cycle management with service assurance as well as fulfilment of security functions end to end. This is an area where different ideas are still proliferating throughout the telecom sector. As well as being driven by dedicated orchestration platforms, automation is also being driven by some SDN controllers. There are also different ideas around whether stand-alone, dedicated security orchestrators are preferable to integrating security orchestration into the broader orchestration function. The means by which different orchestrators will talk to one another is also still to be defined. There's more work to be done on what is a core requirement for 5G security.

5. Easy to Use

It may sound obvious but it can't be repeated often enough: ease of use has to be front and centre in the design of any security product or service. If it isn't easy to use, many customers simply won't use it.

6. Shared

Cyber threats are such a serious threat to business and society now that threat intelligence needs to be shared much more widely. As an example, coinciding with the very start of the 5G era, Deutsche Telekom has extended its "Life is for sharing" marketing tag-line to "Security is for sharing".

Threat intelligence needs to be shared more widely between the internal and customer-facing security domains in the telco (yes, that can be done while remaining compliant with regulations and contractual commitments). More threat intelligence sharing is also needed between telcos. BT's deep sharing of threat intel with other UK ISPs is a good example and is backed by the UK's world-class National Cyber Security Centre (NCSC).

Sharing also needs to be done more broadly across countries and across industry verticals. The Cyber Threat Alliance, whose members include more than a dozen of the world's largest security vendors, is an excellent force for positive change in this area.

7. Open and Federated

The menu of enterprise security options for 5G has to map to the patchwork of different security functions that are woven in to the existing enterprise security environment. As characterized on page three, these comprise components from multiple partners including cloud providers, telcos and security vendors.

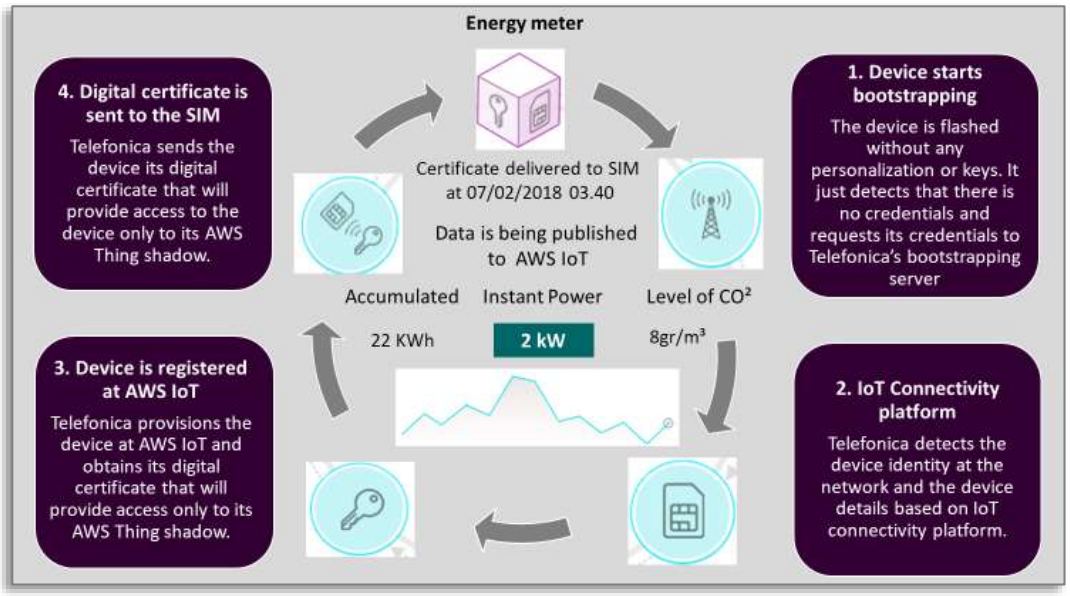
Telcos should consider partnering in 5G security services rather than trying to control everything themselves end to end. In particular, they should consider partnerships with

cloud providers that have strong relationships with enterprise accounts as well as substantial IoT security plays. Current enterprise security partnerships between telcos and cloud providers that have potential to evolve into 5G include the following:

- AT&T partners AWS in a number of areas including secure cloud connectivity, threat intelligence and application security for IoT.
- Deutsche Telekom's IT services business, T-Systems, is helping to build out Microsoft's first cloud data centres in Germany. As the "data trustee" for Microsoft Cloud services, T-Systems provides additional security controls for customer data that can only be accessed via T-Systems or direct from customers themselves.
- Telefonica showcased a partnership with AWS at Mobile World Congress earlier this year. As shown in **Figure 4,** via their Cloud Credentials Broker (CCB) trials the two companies are partnering around the provisioning of authentication credentials into SIMs in IoT use cases.

"AT&T partners AWS in a number of areas of enterprise security."

Figure 4: Telefonica and AWS are trialling a Cloud Credentials Broker (CCB)



Source: HardenStance/Telefonica

Provided they take an open approach, telcos are certainly in a good position to derive competitive advantage in the 5G security services space. The IT world has become more open in terms of the interoperability of different hardware and software components. But in the context of the big global cloud platforms, IT has simultaneously become more closed, proprietary and fragmented from an enterprise perspective.

The opportunity for telcos is to combine their strong heritage in security standardization at the transport and network layers, with momentum in software-driven standardization of SDN and NFV, to drive further standardization of the 5G security ecosystem. The goal should be to enable security components to inter-operate and federate with one another at a more granular level than they can today. CSOs the world over will support that.

8. Integrated

As described throughout this paper, the instantiation and management of security services will go from being largely static in 4G networks to being highly dynamic and adaptive in 5G. Achieving the highest level of performance, as well as the highest level of security efficacy, will require drawing on multiple best-of-breed security vendors.

At the same time, managing that step-change towards far greater dynamism in the security architecture and security operations will prove challenging for many telcos.

While opening their network to a greater variety of specialist security vendors, many telcos may also want to partner larger security integration partners for support in assuring end-to-end integration of their security services suite in this new environment.

Efficiency of the telco's security infrastructure

The foundational infrastructure that underpins a telecom operator's 5G security architecture needs to be able to support the principles listed above with unprecedented scalability and efficiency to drive cost out of the network.

This requirement will be driven by the unprecedented volumes of devices that are expected to attach to the 5G network and the unprecedented variety of services and security features that will be required to support them.

Supporting this while also enabling the operator to achieve its profitability targets will require extreme efficiency in the operator's utilization of hardware and software components throughout the virtualized 5G infrastructure ■

About the sponsors

The sponsors of this White Paper are F5 Networks, Gemalto and Symantec.

About F5 Networks

Service provider (SP) survival today hinges on the ability to optimize network operations, leverage every monetization opportunity, and ensure that network availability and data integrity are reliably sustained. Thriving into the future depends on them adopting strategies that support the coming zettabytes of 5G video traffic and innumerable IoT devices.

F5 solutions help service providers to establish a future-scaled network today by consolidating and simplifying infrastructure deployments, speeding the release of new services, and delivering comprehensive end-to-end security solutions. F5 brings its expertise to the SP world via best-in-class, scalable and secure application-delivery controller technology. Comprehensive capabilities offer service providers the stability needed to cost-effectively and securely scale infrastructure deployment, rapidly spin up new services, and adapt to changing traffic dynamics.

About Gemalto

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2017 annual revenues of €3 billion and customers in over 180 countries. We bring trust to an increasingly connected world. From secure software to biometrics and encryption, our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between.

Gemalto's solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things. Our 15,000 employees operate out of 114 offices, 40 personalization and data centers, and 35 research and software development centers located in 47 countries. For more information visit www.gemalto.com.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, allows organizations, governments, and people to secure their most important data wherever it lives. Enterprises across the world rely on Symantec for integrated cyber defense against sophisticated attacks across endpoints, infrastructure, and cloud.

More than 50 million people and families rely on Symantec's Norton and LifeLock Digital Safety platform to help protect their personal information, devices, home networks, and identities at home and across their devices.

Symantec mobile security solutions offer the most comprehensive, highly accurate and effective mobile threat defense, delivering superior depth of threat intelligence to predict and detect an extensive range of existing and unknown threats. Symantec's predictive technology uses a layered approach that leverages massive crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection

About HardenStance

HardenStance is a leading independent industry analyst firm delivering trusted research, analysis and insight in IT and telecom security. www.hardenstance.com