White Paper

HardenStance

A Service-Based Security Posture for 5G

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

NETSCOUT

February 2022

Executive Summary

- Competition from big 5G vendors and hyper-scalers – as well as regulator-imposed cyber security mandates for critical infrastructure – will drive mobile operator sales and operations teams to innovate faster in 5G business services than they expect.
- As well as providing rich monetisation features, 5G SA is an unforgiving environment for meeting stringent business service KPIs and SLAs. A service-based security posture provides the framework for fulfilling 5G's promise while also mitigating risk.
- As the voice of enterprise CISOs becomes more prominent in 5G use cases, competition will drive demand for enterprise visibility into 5G networks and services. Failure to meet this requirement risks being a 'show-stopper' for many customers.

'It's 5G Competition, Jim, But Not as We Know It'

The variety of models for delivering 5G business services is depicted in **Figure 1.** At the launch of the first 4G networks back in 2009, none among AWS, Google and Azure nor Ericsson, Nokia and Huawei featured in the competitive landscape. Back then, a telco's primary competition came from other telcos. Things are very different this time. When AWS CEO, Adam Selipsky, told 'AWS re:Invent' at the end of 2021 that his company will offer its own private 5G network solutions, he boasted that "it's shockingly easy" to set up and operate. His company's commitment is just one example.

So far, the big winners in private 5G are system vendors Ericsson, Nokia and Huawei.

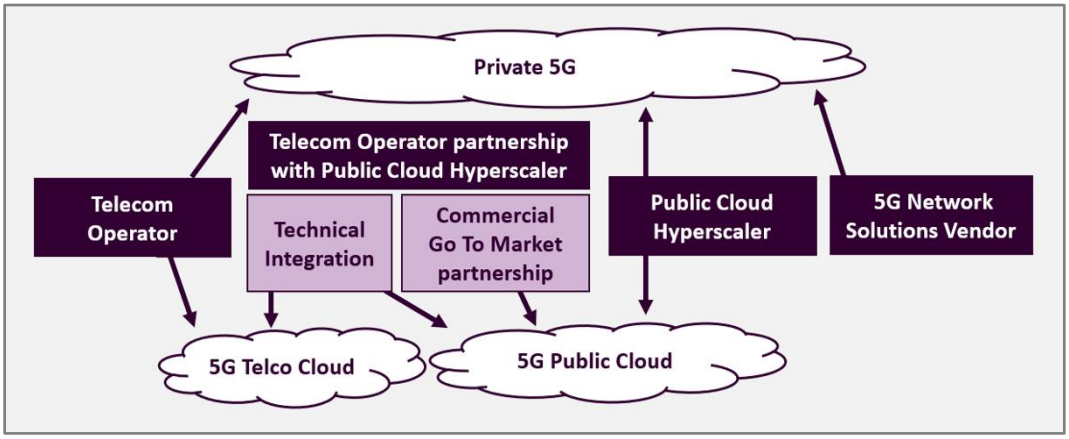
So far, the big winners when it comes to building and operating private 5G networks – where companies buy their own 5G spectrum and typically outsource the building and operating of the 5G network - are systems vendors Ericsson, Nokia and Huawei. Telecom analyst firm, Analysys Mason, states in a November 2021 research note that "operators are prime contractors in less than a third of private network contracts worldwide. This figure is even lower in the U.S. where operators are the primary contractors on fewer than 10% of private networks."

Google, AWS and Microsoft are all Targeting the 5G Business Market

As well as AWS, all the other big public cloud providers are also committing to 5G business services. That includes Google, Microsoft (which acquired 5G core software providers, Affirmed Networks and Metaswitch) and Oracle which has a long pedigree in telecom networks as well as a competitive public cloud offer.

Most Private 5G is 5G Non-Standalone (NSA), with a 5G RAN interworking with a 4G core. Beyond this initial phase, the far larger opportunity is enabled by the functionality offered by Standalone (SA) 5G Core (5GC) networks. These will only start rolling out at scale during 2022. This is where Communications Service Providers (CSPs) can enter the market in advanced 5G business services, leveraging their scale and reach.

Figure 1: The Competitive Landscape in 5G Business Services



Source: HardenStance

In this market, CSPs won't just encounter other CSPs building out their own 5G networks. They will also encounter competitor CSPs deploying 5G Network Functions (NFs) in public clouds or even aligning with public cloud providers in joint go-to-market partnerships.

Operators that excel in delivering mMTC and URLLC will have a chance of achieving revenue growth through 5G. Generally speaking, those that don't won't.

This White Paper describes the opportunity in 5G business services and the supporting need for stringent Key Performance Indicators (KPIs) across the network, and diverse Service Level Agreements (SLAs) for different customers around performance and security. It looks at just how unforgiving a real-world, software-driven, 5G SA environment will be for day-to-day network operations charged with fulfilling the promise of 5G services. It looks at the knock-on effect of these challenges on enterprise sales teams charged with selling 5G business services. And it describes a service-based security posture for continuous risk management to drive efficient 5G operations and accelerate adoption of 5G business services.

3GPP Tools for Delivering 5G Business Services

As detailed in the dedicated section at the bottom of this page, the 5G standards support three primary types of use case. eMBB, mMTC and URLLC. The latter two are the potential game-changers with 5G. Operators that excel in delivering these services will have a chance of achieving revenue growth through 5G. Generally speaking, those that don't won't. These use cases are built off the 3GPP-defined Service-Based Architecture (SBA), the telecom industry's own adaptation of the IT industry's software programmable Service Oriented Architecture (SOA). The SBA enables the spinning up of network slices that can be used to deliver disparate customer and services requirements, using separate control and user plane 5GC Network Functions (NFs).

The Three Primary Use Cases of 5G as Specified in 3GPP Standards

3GPP's specifications enable CSPs to roll out and support three primary use cases for 5G:

1 **Enhanced Mobile Broadband (eMBB)**. This is already in widespread use throughout the world with 5G NSA networks, including for Fixed Wireless Access (FWA).

The other two are optimized for machine-centric, IoT use cases in the 5G SA network. They differentiate the 5G service suite from anything that mobile networks have been capable of previously. These are:

2 **Massive Machine Type Communications (mMTC).** This allows billions of simple, low-power, devices to be supported efficiently. These tolerate high latency and typically transmit low data volumes at irregular intervals.

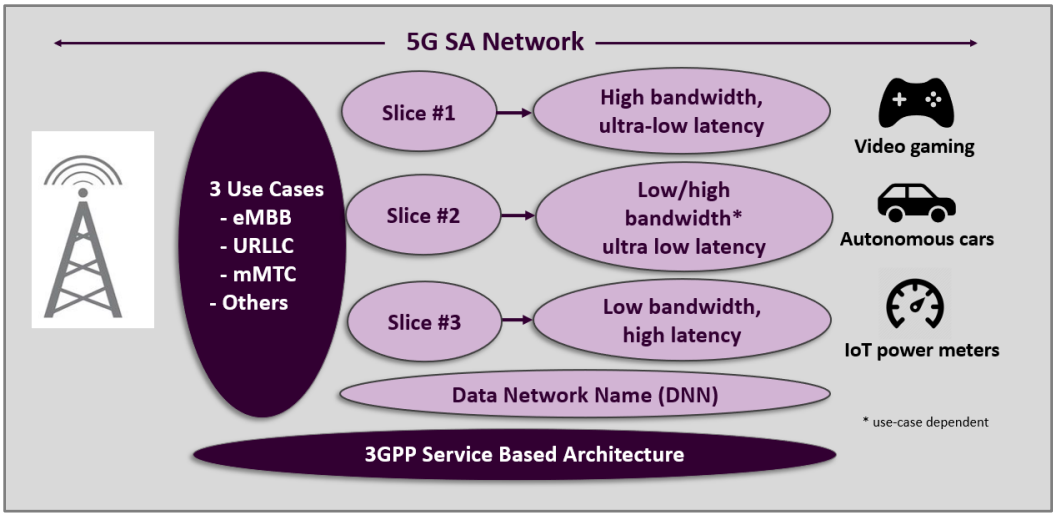
3 **Ultra-Reliable Low Latency Communications (URLLC).** This caters for the opposite requirement - sub 5 millisecond latency, ultra-reliable connectivity for smart machines, robots and vehicles that are typically business critical and can require high data volumes.

Network Slicing for eMBB, mTTC and URLLC Use Cases

The latter two machine-centric use cases can be delivered either via a private 5G network or via 5G network slicing. This allows 5G NFs to run multiple logical networks on a shared physical infrastructure. Each logical network is configured to achieve customised performance parameters as an enabler of different URLLC and mMTC use cases. Network slicing for shared (multi-tenant) and private (single tenant) use cases is key to generating incremental revenue from 5G. But whilst the architectural specifications are provided by 3GPP, how slicing is operationalized is down to individual operators.

As 5GC deployments will only start scaling up worldwide from 2022, network slicing is in its infancy. Most trials and proofs of concept currently involve FWA and some Mobile Virtual Network Operator (MVNO) use cases. With maturity, many more use cases are possible, including URLLC and mMTC.

Figure 2: Network Slicing and DNN Use Case Examples



Source: HardenStance

As discussed on page 3, and shown in **Figure 2**, 5G SA has numerous features that enable business services. Among them, Data Network Names (DNN) and network slicing are key. DNN will be very familiar to operators and enterprise customers alike as it is the 5G equivalent of an Access Point Name (APN) in 4G. By contrast, network slicing represents a marked departure in mobile network capabilities, allowing the creation of multiple, separate, logical networks.

Recent months have seen governments stepping up their commitment to protecting critical infrastructure with unprecedented, concerted action to arrest ransomware gang leaders.

Government Requirements for Critical Industries

Whether they like it or not, providers of 5G business services have to plan for defending their services and customers against hostile adversaries in the cyber realm. That might be an unconventional consideration to put forward in a telecom sector White Paper but 5G SA business services are being launched in an era of unprecedented cyber risk.

The main issue is that a lot of organizations that mobile operator enterprise sales teams are targeting for mMTC and URLLC are precisely ones that have been subjected to high profile cyber attacks of late. Some from among a long list of examples of recent attacks on critical infrastructure are a significant intrusion into a public water treatment plant (City of Oldsmar, Florida, USA) and ransomware attacks on health services (e.g HSE, Ireland) and energy companies (e.g Colonial Pipeline, United States).

It has taken too long for leading governments to start responding forcefully but it's finally happening now. They recognise that it's not just privacy and livelihoods at risk when critical infrastructure is hit by cyber attacks – it's also public health and human lives. And it's not just criminal gangs making money or scoring political points that are carrying out these attacks - it's also nation state cyber adversaries seeking information superiority to manipulate critical infrastructure and subvert national security.

Recent months have seen governments stepping up their commitment to protecting critical infrastructure with unprecedented, concerted action to arrest ransomware gang leaders and criminalise activities and transactions that enable them. Leading governments are also driving individual industry regulators (for water, energy, transport etc), to mandate additional, service-specific security requirements to protect new IT infrastructure projects in their particular sector – including mMTC and URLLC use cases.

A 5G services landscape in which government is getting increasingly involved in ramping up cyber security requirements – on some of their largest customers and on themselves – is perhaps not one that mobile operators would have chosen. However, this is the unavoidable reality. Rather than be passive recipients of new security mandates mobile operators need to get ahead of the curve, do the work, and be able to shape them.

The Unforgiving Side of a 5G SA Environment

Within the telecom sector there is certainly a recognition of the opportunity that 5G SA presents but there's also apprehension around the risk (though more of the former tends to make it into the public domain). A lot of this caution comes from operations teams being concerned about the new challenges that the 5G SA environment will present for operations across the 5G network as a whole, regarding performance, availability and integrity, as well as for fulfilling requirements for specific business services.

Caution When it Comes to Network Slicing

While slicing is an enabler of new use cases, there is quite a lot of caution. For example, operations teams are cautious about the number of slices they will be able or willing to support; how dynamically they will be able or willing to configure them; what SLAs they are comfortable letting sales teams sign up to; what visibility and control they can have into the 5G network to help them meet internal KPIs and customer SLAs; and what control and visibility into their network resources and services they're comfortable sharing with enterprise customers.

Within a lot of mobile operators there is certainly a recognition of the opportunity that 5G SA presents but there's also apprehension around the risk.

At least five factors are driving this caution. These are:

- General fear of change, rooted in part in their status as regulated, licensed entities.
- Operational challenges arising from lack of experience with network slicing and gaps in network slicing standards.
- Underestimating the potential of hyper-scalers to aggressively 'push the envelope' to lead in 5G business services – if not as a partner, then as a competitor.
- Insufficient understanding of the problem – or of potential fixes – relating to how unforgiving the 5G SA environment will be and the risk this poses to achieving target KPIs and business service SLAs at scale.
- Lack of familiarity with the security-related requirements of enterprise customers and what these imply for operational requirements and SLAs.

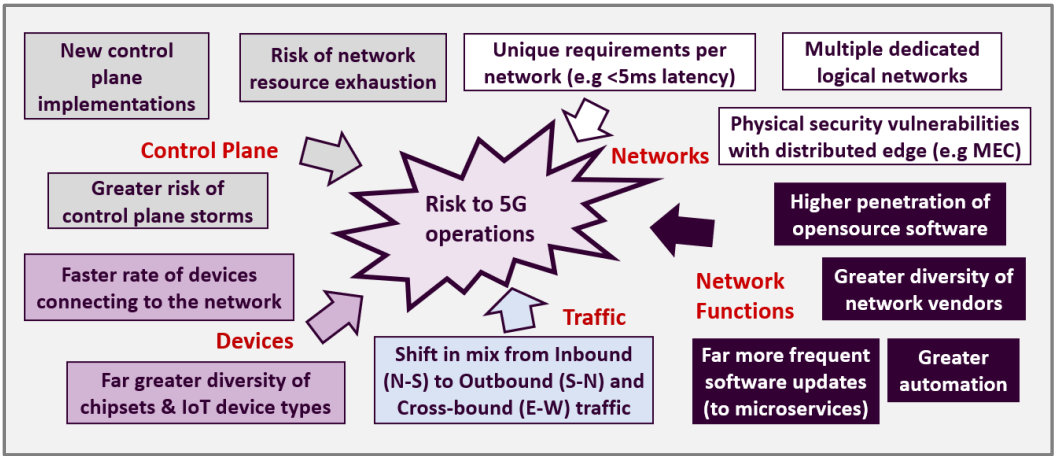
The remainder of this paper addresses the last two of these five factors and provides guidance on navigating a way through them to accelerate 5G SA service readiness. This begins with understanding that driving the right actions requires persistent, detailed, engagement with internal stakeholders, customers, regulators and partners. This is needed to understand the risks, scope requirements, and ensure investment in the right solutions. A high level communications strategy that proclaims how seriously the operator takes security is only the barest minimum of table stakes.

With New Opportunity Comes New Risk

"In most cases, strengths and weaknesses are two sides of the same coin. A strength in one situation is a weakness in another. It's a very subtle thing to talk about strengths and weaknesses because almost always they're the same thing."

This quote, attributed to Steve Jobs, is about human personalities. However it is oddly applicable to 5G operations. It's precisely the open and distributed architecture, the software-programmability, automation and simultaneous support of multiple logical networks supporting different performance parameters, that makes 3GPP's toolkit of 5G SA service enablers so compelling. But those same characteristics also introduce a lot of risks, some of which will be new – or at least different – to mobile network operations teams. Key examples of the unforgiving side of the 5G SA environment and the risk this poses to operations are summarised in **Figure 3** as well as discussed on the next page.

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



Source: HardenStance

New Risk in Integrating, Deploying and Managing Network Functions

- **Frequent updates change the nature of risk with telecom software deployment.** The SBA introduces the potential for a Continuous Integration and Continuous Delivery (CI/CD) pipeline whereby Containerised Network Functions (CNFs) are updated on the fly much more frequently than in a legacy deployment. In a one-for-one comparison, an automated approach to updating a tiny piece of software can certainly be expected to have a faster, better, more predictable impact on network performance than a long-winded, manual deployment of a monolithic release. But among tens or hundreds of thousands of updates, there's a clear risk that a subset will introduce or escalate errors that negatively affect performance – cumulatively or in their own right. Errors in automation present a risk of isolated misconfigurations or threats being propagated throughout the network. Network topologies themselves are also much more flexible, contributing to new risk as well as new opportunity.

The prospects of an operator supporting several millions or tens of millions of mMTC 'things' in a 5G network is daunting.

- **Greater vendor diversity creates more risk of security incidents and greater risk of integration and inter-operability problems in pre and post-production**. For simplicity, most operators will launch initial 5G SA deployments with very few vendors, many with a single vendor. Over time, however, they will move to a multi-vendor environment. The design of the SBA explicitly allows for this in the 5G core. In the MEC layer, operators will need to select and integrate a MEC platform provider and separate MEC application developers and partners. OpenRAN also drives greater diversity of vendor hardware and software components in those parts of the network where operators deploy it.
- **Use of open source software is increasing – and with it the requirement to proactively manage open source security risk**. Whether it's integrated and used directly by a CSP itself or by a vendor integrated into their own releases, open source software has been consistently growing its share of telecom software deployed in CSP networks. This carries risks that have to be managed and monitored.

New Risks from New End-Points and Services

- **Greater Diversity of Devices and Chipsets:** Analyst firm Transforma Insights is forecasting that the installed base of cellular IoT connections worldwide will increase from 1.37 billion in 2021 to 5 billion in 2030. It estimates that 2.71 billion of the 2030 number will be mMTC. For many mobile operators, the prospects of supporting several millions or tens of millions of mMTC 'things' in a 5G network is daunting. The diversity of chipsets underpinning these deployments will expand, as will the number of applications they run. All of this triggers diversity of behaviours,

increased risk that vulnerable devices will be connected to the network, and the potential for network and service availability, performance and integrity to be impacted.

- **Greater Risk from Control Plane Anomalies**: Poor implementations of control plane protocols, especially in IoT 'things', is just one of the factors that increase the risk to the availability or performance of unique 5G services posed by control plane storms and other resource consuming behaviours, whether malicious or not. One common example is the risk of devices attempting and reattempting to do the same thing over and over again, despite having already succeeded. It's not new but with greater volume and variety of devices, the risk increases. Synchronicity is another factor, whereby big spikes in control traffic can arise from the same network or application resources being accessed simultaneously or within a very short timeframe. And, of course, there's the ever-present and growing threat from malicious actors. There's nothing new about this, either, but the greater volume and variety of connections and services within the 5G environment increases the risk.
- **Greater Risk from User Plane Botnets and DDoS:** As with the control plane, user plane anomalies can be triggered both maliciously and due to poor implementation. The poorly secured consumer and SOHO infrastructure that drives the threats plaguing today's fixed broadband services pose a threat to 5G SA services too. In particular, in conjunction with 5G's much higher data rates, these threats will present themselves to Fixed Wireless Access (FWA) and WiFi replacement use cases.

Poor implementations of the signaling stack in IoT 'things' is just one of the factors that increases the risk posed by control plane storms.

- **IoT Service Integrity and Determinism:** There are other risks in play too. For example, in the case of small, battery-powered 'things', a cellular-connected business case is calculated based on a device being online for a given amount of time per day, week, month or year. If it exceeds that threshold, it risks dropping out of service weeks, months or even years before it's due to and triggering an SLA penalty clause. The communications within many IoT services can be expected to be deterministic – for example, in terms of the applications accessed and data transferred. Supervising devices that may be involved in mission or safety critical services will be an essential capability needed by mobile operators to build both trust and adoption of these services.
- **Multiple Services and Slices with Differing Needs:** Dating back more than ten years to the launch of iPhone and Android devices on 4G, mobile operators have been accustomed to supporting an abundance of different applications. Mobile operators have become adept at enabling what is now called "the app economy". What they're not at all used to, however, is running multiple services with differing SLAs – covering performance, availability and security – for multiple business customers across the same or multiple network slices.

In the face of all the benign and malign factors cited above conspiring to disrupt or degrade any one device, application, network or service, mobile operators have to somehow ensure that every 5G device, application, network or service should behave or perform exactly as expected. As set out below, a service-based security posture is a critical enabler of that goal.

A New Layer of Service-Based Security

3GPP provides a necessary but insufficient foundation for a service-based 5G security posture. The devices, data and applications that use a 5G service are protected by 3GPP authentication and encryption features. As with previous generations of mobile technology, these ensure only authorised parties can access and deploy devices and that traffic can't be intercepted other than for law enforcement.

Core features of 4G operational network security, like perimeter firewalls at roaming interfaces and offload points to block bad inbound traffic, are still needed. On their own, though, these are not enough to protect against the new and continuous risks to security inside 5G SA networks from locally connected devices. 5G operators should therefore look to an additional layer of service-based security as shown in **Figure 4**. This extends the capabilities of traditional service assurance to capture the control and user-plane traffic flows traversing a multi-vendor 5G SA environment to enable pervasive, focused visibility into services, as well as proactive and reactive security monitoring. It should include real-time visualization of benign and malicious threats to the performance of unique networks and services, as well as to the network as a whole. And it should provide security operations with tools for responding both proactively and reactively to risks that may impact the network and the services it delivers.

One way to think about service-based security is in terms of three distinct layers – the infrastructure layer, control plane and user plane:

One way to think about Service-Based Security is in terms of three distinct layers – the infrastructure layer, control plane and user plane.

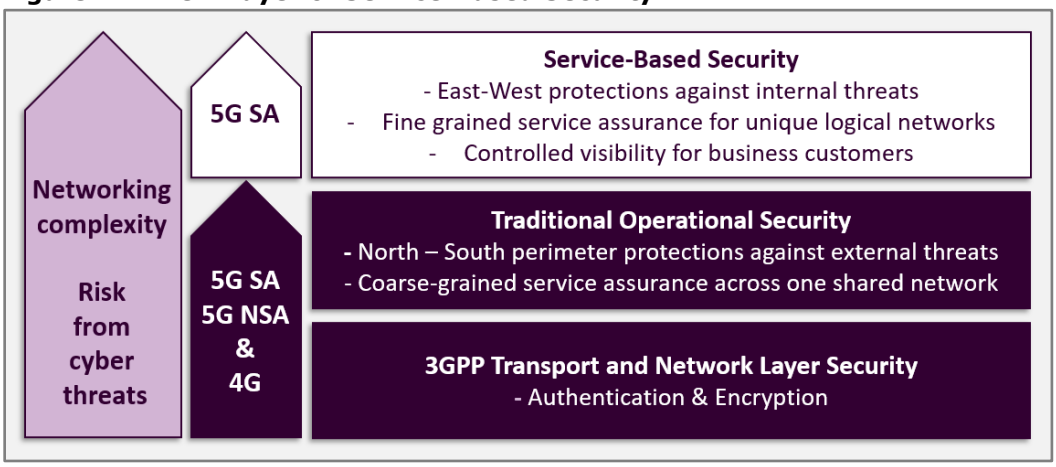
Infrastructure Monitoring Across the Multivendor Environment

Infrastructure monitoring allows security operations to monitor communications between network infrastructure, management platforms and other elements so that any unusual activity, such as use of low security ciphers, can be quickly identified. Examples include what protocols are being used; what new ports are being opened; what devices are attaching to the network; what new communications are taking place; and changes in traffic levels and characteristics. In short, given the more open nature of the 5G SA network, security operations require a comprehensive model of communications so that any potential configuration error or malicious activity can be quickly identified and stopped before there is any impact to service integrity or data confidentiality.

Control Plane Monitoring

Security operations needs to be able to monitor the 5G control plane to ensure everything is behaving as it should – at the device, application, network and service levels. Control and user plane functions are separated so they can scale independently, and network slicing allows unique control plane instances to be dedicated to specific services where needed. However, in most cases multiple services can be expected to

Figure 4: A New Layer of Service-Based Security



Source: HardenStance

share control plane instances, and underneath it all there is a common, finite pool of hardware resources. Any impact to control plane performance and availability, such as from control plane storms, could have a significant impact to one or more services. This is nothing new, but the combined effect of new devices implementing new services and new control plane implementations substantially increases the level of risk.

The control plane must be monitored for large-scale events, such as storms, as well as more subtle changes around unusual error messages and the like. These may indicate underlying interoperability or resource exhaustion issues – whether they are malicious or not. At the level of a given type of customer 'IoT' device type, in use with a specific critical service, the security team also needs to understand both baseline behaviours and typical outliers as well as be able to monitor whether either or both are changing to ensure service integrity and SLA compliance.

The control plane must be monitored for large scale events, such as storms, as well as more subtle changes around unusual error messages and the like.

User Plane Monitoring

Given the increased throughput available, promise of low latency, and larger number of connected devices, user plane monitoring needs to take on a different character for 5G SA. For consumer broadband services, the DDoS and Botnet issues that have plagued wireline networks will become a much bigger problem and will need to be managed to protect and assure both network infrastructure, service availability and performance.

More focused monitoring will be needed for business services. User plane traffic transmitted by IoT 'things' tends to be highly deterministic. They tend to talk to a finite number of other network elements, using a finite number of protocols, usually at predictable, well-defined, intervals. Any deviation from the norm could represent an early indication of malfunction or compromise. Being able to proactively detect user plane abnormalities in these services, when they first appear, is critical to de-risking these services and fulfilling SLAs.

Integration, Integration, Integration

Every mobile operator has well established configuration, reporting, ticket management and policy tools for monitoring and detection. New security capabilities will need to integrate with these. Mobile operators are used to using firewalls to block traffic and policy controls to manage user devices that exceed the quota – these mechanisms will be extended to protect 5G SA networks and services.

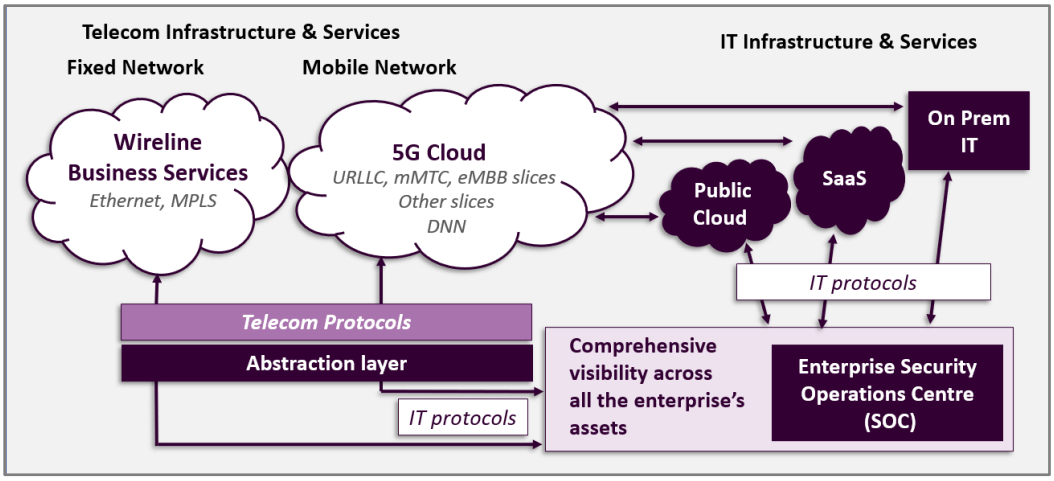
Using fine-grained security analytics to drive the blocking, re-direction and rate-limiting capabilities within the mobile network by inter-working with 5G's Policy Control Function (PCF), the equivalent of the Policy and Charing Rules Function (PCRF) in 4G, will be key.

Enterprise Customers Will Expect Visibility Too

The case for service-based security in 5G SA should resonate very well with any mobile operator's security operations team. But an enterprise customer's own security team will also expect service-based security for visibility into their organization's use of the 5G cloud. In some cases they will also need that visibility to carry out supply chain security audits of their 5G cloud provider.

This is easy enough with a private 5G network – you own the network, you're the exclusive user of it, so you get whatever visibility into it you want. It's more complex in the case of 5G services delivered by a mobile operator or other service provider. Even though the resources of different business customers can be logically segmented, they're delivered from the same physical network. Even if it doesn't own the actual 5G network, the enterprise still owns the 5G end points and applications. That user organization is accountable for its own security posture.

Figure 5: Enterprise Customers Expect Visibility Into Their 5G Cloud



Source: HardenStance

Enterprise Chief Information Security Officers (CISOs) should be in the vanguard of an organization's business case discussions with 5G providers. The CISO team requires security visibility into the 5G cloud on a par with the visibility it gets into compute and storage resources in the public cloud.

For a lot of enterprise CISOs this will be non-negotiable. Being offered a 'black box' 5G network service will likely be a deal-breaker. There will be requirements for telemetry feeds from the 5G network to be fed directly into the enterprise Security Operations Centre (SOC). CISO teams will want to converge those feeds with their public cloud and on-premises security feeds for a comprehensive view of the organization's cyber security posture across all its assets.

Mobile operator enterprise account teams have little insight into customer demand for visibility into the mobile network.

Customer Need Presents Opportunity and Risk

As well as many years experience giving enterprise customers visibility into the status of their compute and storage assets, public cloud providers are experienced in delivering overlay cyber security capabilities that help address enterprise requirements. Culturally they tend to be well disposed to want to innovate around these types of capability.

Today's telecom world is different. Some – but by no means all – CSPs have Managed Security Service Provider (MSSP) businesses affiliated to their wireline business. These businesses are well versed in understanding, scoping, creating and delivering security services – including SOC visibility - across fixed network services and fixed IT assets.

By contrast, mobile operator organizations have hardly any comparable experience because 4G doesn't support the kind of customization of network resources that 5G does. Mobile operator enterprise account teams therefore have little experience with customer demand for visibility and security into mobile services. With limited insight from sales, mobile network engineering and operations teams also have a limited view of how to meet emerging business customer requirements – let alone in a way that takes no additional risk with the operator's own security posture. If CSPs are to avoid being out-innovated by more agile competitors in 5G business services, this has to change.

Mobile Operators Must First Protect Their Own Network

Over the course of thirty years and three different generations of digital mobile technology, the first requirement of mobile network security has consistently been to protect the mobile network itself. In that respect, at least, 5G SA is no different.

No mobile operator can risk giving a business customer unhindered visibility into its own network operations. Allowing customers to see configuration data relating to the paths and relationships between the operator's assets and paths out onto the Internet is a

potential national security risk, let alone a commercial risk for a telco. Furthermore, in a multi-service context, whether using slicing or not, a mobile operator can't allow one customer to see another customer's assets or traffic telemetry. The risk is especially high in the case of a public network slice which is configured for one industrial sector's needs and then shared by a number of competitors in that same sector.

It's nevertheless worth bearing in mind that there are illegitimate as well as legitimate barriers to sharing relevant network information with customers. For example, how many wireline customers are being billed a hefty premium today for a "dedicated" service that – if they were able to see under the hood – they would see is actually being shared by other customers?

Where 5G SA represents a departure from all previous mobile generations is that, as well as protecting the mobile network itself, it is equally important to deliver the security needed by different services and the customers who buy them. This will require a layer of abstraction. Currently, very few enterprise CISOs have much idea about the types of 5G network telemetry and security event data that are likely to be relevant to their goals. However, this will evolve. Operators and enterprise customers will need on-boarding agreements relating to services that define SLAs, shared telemetry and events.

Very few enterprise CISOs have much idea about the types of 5G network telemetry and security event data that are likely to be relevant to their goals.

At this stage of the 5G market's development, an operator's wireline MSSP business shouldn't be expected to help much with this aspect – they're not generally familiar with mobile networks. But their experience in capturing the security requirements of enterprise CISO teams, developing them into commercial propositions, and then deploying and billing for them across the telco organization is still a valuable resource for mobile operator affiliates to draw on.

Businesses Will Pay for Visibility

Visibility and security within 5G business services can clearly qualify as value-added capabilities, rather than something that's baked in. Business customers will need varying levels of both service and security assurance dependent on their use case, and the SLAs required. Business services with no security requirements will be few and far between. Mobile operators therefore need to create a portfolio of generally available, revenue generating, 5G security services rather than custom propositions to be negotiated with a handful of big customers.

User plane data will be relatively straightforward to expose. Even in the case of public network slices shared by more than one customer, the building blocks for meeting customer requirements are straight forward enough. An operator knows which endpoints should be accessing a given service. Detected threats for that service can be parsed out, and only the relevant records sent to each business customer – much as MSSPs already do today with wireline security services.

Exposing Control Plane Messages is More Challenging

Exposing 5G control plane information is more challenging. A public slice's control plane could be shared by several customers. Hence the misbehaviour of one customer's assets can potentially disrupt another customer's service. The 5G operator is responsible for assuring the availability, performance and integrity of the control plane for all customers, but each customer must also be accountable. Exposing control plane events and threats can certainly help enterprise security teams understand what is going on, but it must be done with appropriate controls. Part of that means ensuring that the huge volume and variety of control plane messages is abstracted and presented in such a way that the enterprise SOC can extract only those relevant messages that present as high fidelity alerts relative to the customer's own security posture.

A flexible visibility platform offering both session and KPI data, across multi-vendor 5G networks and services, driving performance, availability and security analytics is key. This platform must provide enough abstraction to prevent 'over-sharing' on the part of

the network operator, whilst also ensuring that shared data can be used by enterprise customers to meet their risk management needs. Without these capabilities operators will find their ability to meet service requirements limited, reducing their ability to drive growth from new 5G business services. ■

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against security, availability, and performance disruptions. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Omnis® Cyber Intelligence delivers the fastest and most scalable network security solution available on the market. NETSCOUT nGenius® service assurance solutions provide real-time, contextual analysis of service, network, and application performance. And Arbor® Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets.

To learn more about improving service, network, and application performance in physical or virtual data centers or in the cloud, and how NETSCOUT's security and performance solutions can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The Cyber Threat Alliance, The GSMA and ETSI. To learn more visit www.hardenstance.com