Welcome

Welcome to our second annual customer conference! This year's event is branded NEXUS to represent the many interconnected bonds between our technologies, industry direction and you as members of our NetNumber family. As we collectively embark on the journey towards 5G, microservices, and modernization of "old to new", our goal is to provide an oasis – NEXUS19 – within this intersection for dialogue, reflection and information sharing.

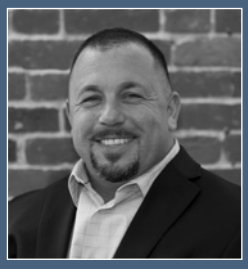
Our industry is in an unprecedented state of transformation, driven by user demands, technology innovations and new business opportunities. In the days and pages which follow, we'll help you prepare for the next phase of your transformation.

On stage you'll hear the challenges customers like you are facing, and how they are addressing those challenges with NetNumber solutions. Industry leaders will share insights into industry trends such as agile and DevOps methodologies, leading the next generation workforce, and security issues threatening your network today and in the future.

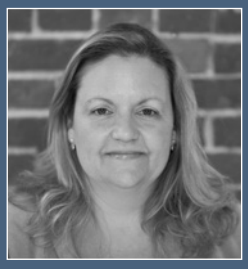
In the pages of this magazine you'll find content to share with your colleagues back in the office to help educate them about how to ease the transition from today's 2G-3G-4G networks to 5G by deploying the NetNumber TITAN All-G Platform, and the growing importance of data and analytics in securing networks.

We are proud to have selected Warsaw as the location for this year's event. It is a city with deep historic traditions as well as a city of transformation. And this is the heartbeat of our TITAN Platform, which has been deployed your networks.

We are thrilled you are a member of the NetNumber family, and we are proud to be a partner on your journey!



Matt Rosenberg
Chief Revenue Officer



Kim Gibbons
Chief Marketing Officer

Maintaining momentum amid endless network evolution

Ensuring legacy networks go the distance

How does a communications service provider (CSP) balance the need to migrate customers to the latest generation services, while transforming networks to be future-ready – and modernize legacy systems that will continue to play an important role for many years to come?

Stranded, high and dry, marooned

CSPs around the world are under pressure as they continue to evolve and modernize their networks – from circuit switched to VoIP and IMS, and from GSM and CDMA to LTE and EPC Diameter-based networks – at the same time as preparing for 5G. They must continue to support a large base of 2G, 3G and PSTN-based customers who will, for beyond the foreseeable future, put large demand on the legacy Signaling System 7 (SS7) infrastructure.

SS7 networks were first deployed more than 30 years ago. The maturity of the technology has led to an erosion of investment in the Signaling Transfer Point (STP) market around the globe, which in turn has highlighted the crucial need to maintain the integrity of the SS7 network. The situation is a cause of major concern to service providers.

Analyst firm Exact Ventures estimate that at the end of 2018 there were 284 million Message Signal Units (MSU) worldwide. They are gradually being retired, as traffic shifts to 4G voice (and eventually 5G) and links are consolidated, but the base will decline slowly.

Regardless, the STP plays a critical role in the SS7 system, routing and relaying signaling messages between endpoints and other transfer-points. With so many of these endpoints in service, it's important to maintain the sustainability of the current SS7 signaling infrastructure during evolution and transformation.

Multiple incumbent vendors have decided to divest themselves of and move away from end-of-life assets such as STP. They have chosen to retire legacy and proprietary equipment although it is still instrumental in generating important revenue streams for CSPs and vital to the continued running of their networks and services.

The situation puts CSPs in a predicament. They face the challenge of putting customer services at risk and increased costs, and negotiating out-of-warranty support contracts, or choosing to consolidate and modernize by moving to a platform with a future-proof architecture and operational environment.

A major question on the lips of CSPs worldwide is, "What do I do with my SS7 Signaling Transfer Points?".

Evolution and transformation

As CSPs look to refresh their SS7 networks, they need STPs that can de-risk their business, and help protect current revenue streams and transition them to a new software environment based on NFV.

When making transformation investment choices, CSPs want a software option for new core network technology. Many have realized that continually adding 'service silos' only creates continued signaling chaos and doesn't achieve the efficiency they need to propel them into a sustainable future. Therefore, new solutions that foster agility, better time to market, simpler vendor management, and lower operating costs will win mindshare – as the cost of poorly performing or failed signaling is too much to risk.

A platform for the future

From frequent discussions with CSPs around the world, NetNumber identified the following as key requirements for these transformation and modernisation projects:

- New deployment practice and architecture akin to NFV, cloud-native, mesh networks, containers and microservices at the edge.
- Powerful security solutions that protect the previously unprotected signaling core, and offer fraud management, prevent caller line identification (CLI) spoofing and secure authentication.
- Significant reduction of legacy internal signaling inefficiencies.
- Products that cultivate faster time-to-market configurations and options.
- Bundled solutions that marry 2G, 3G and 4G plus future generation services and applications.
- Access and use of real-time data and analytics across the software-based, virtualized, multi-device environment.

The NetNumber TITAN platform is engineered for CSPs looking for a software future. As part of an SS7 signaling transformation solution, it offers a replacement STP compatible with other applications in networks while being capable of supporting today's revenues.

In addition to STP, TITAN handles Signaling Firewall and Diameter Signaling Control (DSC) on the same platform, ensuring security is taken into account throughout network evolution.

The platform has a flexible service layer, allowing it to handle diverse customer-specific use-cases, in addition to bringing forward legacy services onto a new architecture and is engineered to be 5G-ready.

The dark skies of security concerns are forming over 5G

Network transformation and modernization is revealing a proliferation of concerns regarding security, fraud and privacy, which if left unchecked will lead to significant problems, and legal and financial penalties, for progressive communication service providers (CSPs).

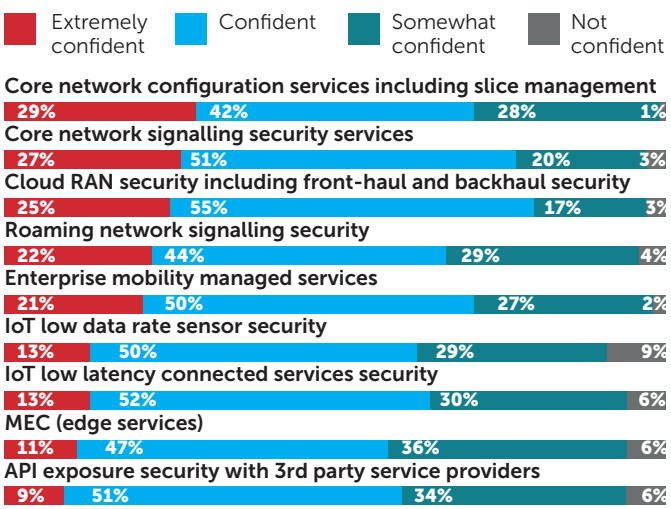
To counter this, the industry is turning to network vendors, and regulatory and standardization bodies to come together and collaborate to keep our communications, data and privacy secure. Independently these interested parties, along with CSPs, have their own contextual concerns and challenges.

In a recent webinar hosted by Light Reading, NetNumber's Senior Manager for Product Development (Security and Routing), Pieter Veenstra and Jim Hodges from Heavy Reading discussed some essential research and a report on *Securing 5G Networks*. This article adds depth, insight and conclusions to that survey's responses and findings.

In 2016 Pieter started his editorship in the GSMA Fraud and Security Group (FASG) for the definition of Signaling Firewall requirements for SS7 and Diameter, to enhance the protection of international roaming traffic between mobile networks worldwide. Due to his extensive background at Dutch operator KPN, Pieter is involved in new use case definitions and core network simplification programs with customers. He is also responsible for establishing new partnerships based on the NetNumber TITAN Centralized Signaling, Routing and Control (CSRC) paradigm.

Confidence in securing 5G's control plane

The first discussion point from the report concerned control plane considerations. There were open questions about the ability and relative confidence levels associated the range of standard 5G security use cases used in the study.



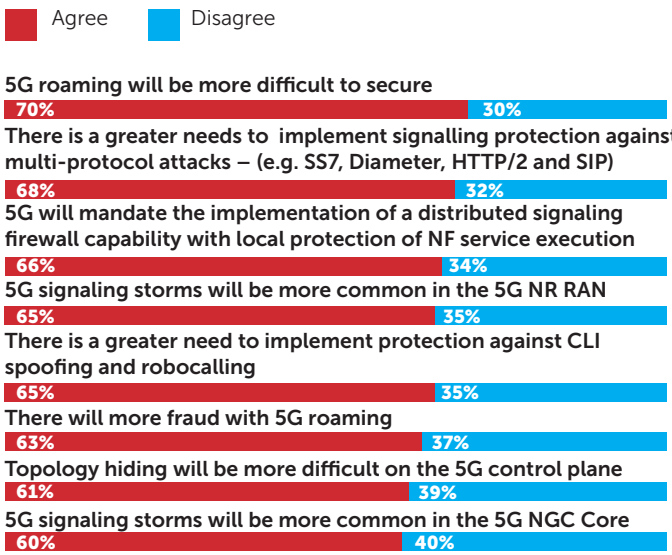
While about half were 'confident', breaking down the numbers further, they translate into about 40% being either only 'somewhat confident" or 'not confident', which is not a strong endorsement.

The increasing complexity of 5G's control plane concerns operators regarding the impending paradigm shift and evolving trust model, with multiple actors, network slicing, distributed service execution and the use of internet protocols, etc. In conversations with our customers, NetNumber hear similar concerns, which come with different challenges. For example:

- The potential for attacks such as signaling storms, malware etc. on the expected billions of IoT devices and sensors.
- The multiplication of computer power that Mobile Edge Computing (MEC) brings, also introduces security risks when malware infiltrates with direct access to core elements.
- Security challenges due to API exposure, with a new trust model around distributed control over network resources.

Reasons for low confidence

If we look deeper into why there are low relatively levels of confidence in security, based on the level of 'agree' responses, it's clear that a majority of respondents expect more fraud, more signaling storms in the core and radio access network (RAN), multi-protocol attacks and even greater threats of Caller Line ID (CLI) spoofing and robocalling.

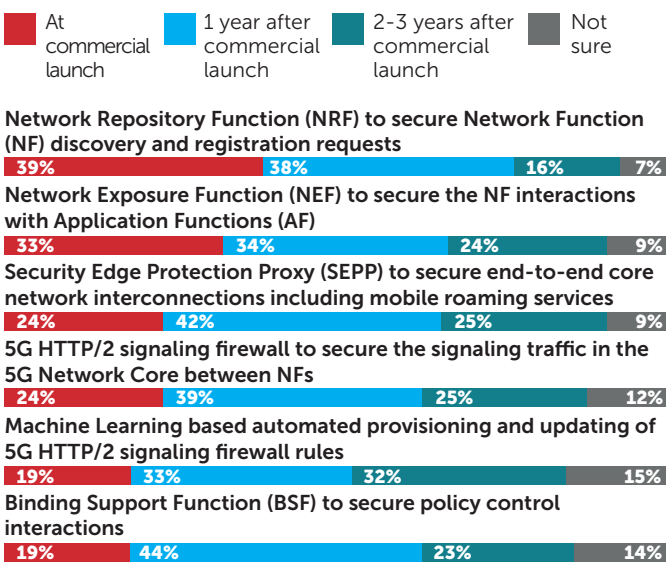


The expectation is that the security of mobile roaming in a pure 5G ecosystem will be solved by the 'security by design' Security Edge Protection Proxy (SEPP) and signaling encryption over the N32 interface. However, fundamental issues arise when 5G has to co-exist with the SS7 and Diameter world which is inherently less secure. The main risk is introduced when access to the IPX signaling network is via SS7 or Diameter but the receiving mobile network operator assumes the same trust as if the traffic were secured via SEPPs and N32 methods.

Today operators are faced with a steep increase in fraud cases. 5G brings elementary enhancements in native 5G core networks with concealed (encrypted) identity, such as international mobile subscriber identity-catcher (IMSI) over the radio access network, and the two-way verification of roaming network identity. But to begin with, there will be no native 5G core, so as the magnitude of devices connected to the network increases, so does the potential impact of security breaches.

Implementing 5G security

To address control plane security challenges, service providers are starting with the basics. This translates into supporting the Network Repository Function (NRF) to secure network discovery and Network Exposure Function (NEF) to secure applications at commercial launch. However, it's notable that even here Machine Learning and automation had relatively high commercial scores. While the SEPP scored third place in the survey, it drove considerable discussion at the GSMA MWC 2019, suggesting it will be deployed not long after commercial launch, even before 5G roaming traffic starts to ramp up.



The SEPP will undoubtedly bring many security improvements for mobile roaming compared to the existing practices with SS7 and Diameter. However, there are still many issues not covered in 3GPP Release 15 that are fundamental to running an operational service like load distribution, error handling or failover mechanism, etc. These functions will first be available with 3GPP Release 16.

Consequently, our expectation is that 3GPP Release 15 is ready for deployment in operators' core environment, but as 'islands' of 5G. We need to wait for 3GPP Release 16 before 3GPP core networks will be interconnected and 5G roaming traffic starts to increase. We saw a similar situation with IMS.

In parallel, a secured version of Diameter for mobile roaming is close to finalization in the GSMA DESS group, which may bridge the time until 3GPP Release 16 implementations are ready to be deployed between operator networks. This may take some time because the 3GPP standardization groups are still preoccupied with the completion and error patching of the 3GPP Release 15 standards for 5G phase 1.

Existing firewall support for 5G

One other important topic the survey addressed was how does the complexity around security in the 5G control plane impact the evolution path of existing 3G and 4G control plane signaling firewalls? Based on 'extremely important' response levels, HTTP/2 interworking with protocols such as Diameter is critical, while interworking with SIP and even SS7 is still very important.

Fraud via SIP is beginning to concern operators majorly in 3G and 4G, with vulnerability to CLI spoofing, robocalling and other forms of nuisance calls. Also, we see operators starting to ask for protection for the combination of SIP with mobile roaming services via SS7 and Diameter.

When 5G interconnection begins to roll-out, the 30-year old SS7 network will still be there – even bigger and carrying more roaming traffic than today. The steep uptake of mobile roaming will likely be due to developments such as the EU's 'roam like at home' and roaming support for M2M and IoT services. This will include static devices because many operators deploy M2M services with roaming arrangements in overseas networks.

The other issue is how interworking between HTTP/2 and SS7 will be implemented. There is a certain preference to interwork SS7 via Diameter to HTTP/2 and in reverse; but this is a 'poor man's solution', as it may only partially cover the SS7 attack interface. It could provide attackers with an entry point to the HTTP/2 core networks via imperfections of the two-stage interworking from SS7 via Diameter to HTTP/2.

Protecting CSPs' security armour

The prime concerns of CSPs right now must be security and data protection. Although 5G is designed and implemented with security and data protection in mind, CSPs cannot rest on their laurels because hacking is now so prevalent and insidious that it has become an outlaw industry in its own right. It is the dedicated enemy of network operators and telcos everywhere, using the same tools as they do, including AI, computing power and the Internet, to attack and defraud them.

Given the critical role of 5G in digital transformation and the more stringent legislation for data protection with, for example, the EU's General Data Protection Regulation, security in 5G is an absolute critical success factor for this new technology. However, the Light Reading report on Securing 5G Networks shows low confidence levels among respondents that will likely evolve as operators gain experience with the implementation of 5G core networks. 5G security will improve significantly, but the interworking with legacy networks will ask for special attention.

CSPs need comprehensive security, privacy and fraud-prevention strategies in place to cover the entire network infrastructure, not just 5G. Certainly 5G is being designed from the ground up with security at the forefront, but the complexity of networks continues to increase and hackers will sneak in through any chink in CSPs' armour and wreak expensive havoc. It's much better to prevent an attack than to clear up

5G market opportunities: Getting an edge on 5G and beyond

When it comes to communications service providers' (CSPs') business opportunities for 5G services, analysts' revenue estimates are all over the map. As a technology that carries so much promise across so many markets, 5G's success depends heavily on the combined influences of consumers, industrial demand, and the successful convergence of wireless and business IP networks.

Business computing & services growth

Network consolidation through 5G and IP convergence will bring a sea-change to business computing. Therefore, most analysts and CSPs agree that enterprise 5G solutions, devices and services will make up a large percentage of long-term growth and revenue opportunities – if properly productized and deployed. Top areas for these next-generation products include IoT, corporate cloud solutions and high-bandwidth telecom services such as HD business video, voice, security and technical support using augmented reality (AR).

Gartner analysts project that up to 90 percent of 5G IoT service revenue will come from enterprise businesses. Meanwhile, partner supply chains and high-speed global connectivity services will benefit from converged 5G network solutions, in many cases eventually supplanting current landline WAN connectivity over fiber and cable.

Tip of the 5G spear: Consumer services

While 5G enables the development of many new digital services, operators must first ramp up their deployments and transition current customers – mostly consumers and business customers – to the new world of 5G. With the lower cost of 5G bit rates for data as a potential enticement (depending on operators' monetization models), they can move many customers onto the new network.

It's no surprise then that according to an April 2019 survey of CSPs, 96 percent will focus their 5G support in 2019-2020 on supporting existing data services. This gives early adopters and migrating customers a step up in performance (through LTE uplink) and helps finance continued 5G investment. Most advanced 5G features and services cannot become widely available until substantial network density is reached. They include other consumer-driven services such as ultra-wideband wireless and mmWave deployment, which some carriers have rolled out in a very limited way in urban areas.

MEC and the cloud

Of course, it's the density that counts, so MEC is gaining traction. As mmWave and network slicing directly benefit from MEC, especially in reducing latency and expanding cloud computing access, the push is on for higher density operations, which includes proliferation of network-edge clouds. CSPs can, however, hedge their bets somewhat as existing LTE networks can leverage edge technology.

And just as the networks (IP and wireless) are merging, so is the competition, especially in MEC and edge virtualized environments. Traditional telecom carriers potentially are head-to-head with traditional IP network and cloud vendors. Even if RAN takes the lead on MEC for edge networks, the convergence, competition, and unseen risks of the merged networks will cause unpredictable market disruptions.

Further converged network challenges include:

- Programmable core operations for delivering Network-as-a-Service, allowing operators to customize slices for corporate customers and specific industrial applications.
- Overhaul of operators' business operation and support systems (B/OSS) with intelligent network functionality and automation for real-time pricing.
- Seamless security, performance and reliability across 3G and 4G and 5G networks, especially as 5G network density increases.

Overcoming 5G adoption challenges

While the path to full 5G capabilities is clear enough, how individual CSPs (and their customers) arrive is not fully mapped out. CSPs must decide the best course for their businesses and simultaneously evolve their systems to accommodate the new realties in a post-5G landscape.

Here are three main challenges we see for operators in the near and long term:

- Security is always a concern, and security in a 5G environment is even broader and far more complex than previous generations as IP and 5G converge.
- Performance is not just a matter of bits-per-second or latency, although those are service priorities, especially when service level agreements can make or break customers' revenue. Performance in a dense 5G network also includes responsiveness, real-time network management and reliability over many nodes.
- Adaptability is key, given the complexity of the 5G 'journey', systems must be in place that can easily and cost effectively adapt to changes in technology – without costly or complex

changes. Similarly, CSPs should be able to make changes to their business model and introduce innovative services and customizations that could drive substantial revenue.

Security through obscurity

Eighty-three percent of operators surveyed in recent Heavy Reading research agree that 5G security has been debated for years. The previous article (see page 4) discusses the industry's confidence in and the implementation expectations of 5G security against existing firewall capabilities.

Performance

The 1 millisecond performance requirement for full 5G support could delay full adoption and advanced applications. However, according the IHS Markit's 2019 Operator Survey, 37 percent indicated they are already deploying MEC infrastructure ahead of 5G deployments; an additional 47 percent intend to deploy MEC. Even with MEC, systems will require a far higher density of radio access antennas, improved operation support systems and, consequently, all new (or upgraded) data center infrastructure management systems (DCIMs) for remote management.

The 'last mile, or even last few feet – is not the bottleneck; the entire infrastructure and its management must be responsive and reliable. Hence, CSPs should look for innovative DCIM and MEC solutions that can easily integrate into their existing or planned systems.

Adaptability

The telecom market will become the most fluid in its history throughout and beyond 5G introduction and maturity. As mentioned, forces within and outside the telecom space are vying for market share, service revenue, and new ways in which to leverage the converged networks. With SDN and NFV, changes can occur over night with software-only modifications. Meanwhile, 5G standards (and programable core), security, and management will also be largely software-driven and subject to modifications and enhancements at any time.

These are all positive developments – if systems are in place to leverage them. The ease of introducing new services, the ability to add enhancements to existing systems (including LTE Advanced) and maintaining reliability and security at the highest levels are all hallmarks of an adaptable, business-forward strategy that should serve operators throughout the 5G journey and beyond.

NetNumber and the 5G Edge

Choice and flexibility in deployment

NetNumber's multi-protocol, multi-function All-G TITAN servers can be placed wherever and whenever needed – as central location hubs or as edge-based solutions supporting MEC. These edge servers can carry their own customizations if necessary, and NetNumber software connects them to one synchronized and seamlessly managed multi-protocol environment.

It's possible to deploy 2G, 3G, LTE or 5G in any combination on any TITAN edge with SS7, Diameter, and HTTP/2 interconnections.

> **"The fate of 5G hinges on how well – including how securely – the opportunities of the more open, distributed, 5G architecture can be captured**
>
> **Patrick Donegan,**
> **Founder and Principal Analyst at research firm HardenStance**

All-G TITAN currently supports NSA-NR, SA-NR and mmWave as well as Private LTE and IoT/M2M.

The unique, distributed architecture of TITAN makes it possible to address regional, local and private networks individually, yet retain central control, management and security. And as technology continues to evolve, or as service models change to address new opportunities and markets, TITAN adapts easily to fit future needs.

Edge-based performance, data center reliability

As an end edge-enabled device, TITAN reduces latency and management bottlenecks. The platform delivers centralized provisioning and management, combined with a powerful, distributed execution architecture that enables all service processing at the optimal location in an operator's network. As a software platform, new DCIMs and B/OSS are applications that can be added, changed, upgraded, and customized wherever needed.

TITAN's built-in geolocation replication adds a customizable layer of backup and failover, delivering the type of redundancy and fault-tolerance found in the largest enterprise data centers. Best practice high availability and data recovery processes ensure that traffic, data, and customer data are all protected.

Security

NetNumber has been instrumental in delivering the best security for next-generation systems – while maintaining support and innovations for legacy technology. Our award-winning, next-generation security solutions and firewall provide comprehensive multi-G security and fraud protection with real-time threat detection. NetNumber delivers inter-networking encryption from end-to-end, eliminating attack vectors within the network, while its signaling firewall protects against malicious attacks on inbound traffic and data.

Summing up

5G unifies and blends traditional communications networks with the global IP world. With all the promise it has for unrivalled innovation, new products and services, and potential revenue, its success depends on security, performance and flexibility. Due to the interdependence of multi-generation protocols for a smooth 5G transition, and the ongoing value of 3G and LTE, only a software-based solution can provide a true price-performance advantage. Hardware-based solutions are too costly and complex to adapt to changing conditions.

NetNumber is a leader in multi-protocol software development, research, integration and security with 20 years of expertise in delivering high-performance, high-volume solutions to network operators around the world.

Visit us at www.netnumber.com