CSPs face steep increases in security and fraud incidents. The acceleration in volume and increased impact are caused by factors such as:

- **Attack Surface Expansion**: simplified access to the core signaling networks facilitated with the widespread use of IP and internet with their inherent security vulnerabilities.
- **Hacking Industrialization**: sophisticated attack scenarios developed and executed by global criminal organizations enabled with computing and proliferation of knowledge.
- **Solution Fragmentation**: increased complexity of networks and service platforms complicated with the coexistence of consecutive technology solutions in parallel stovepipes.

To protect against such risks, NetNumber offers an extensive set of Security and Fraud Mitigation solutions as applications on the widely-deployed TITAN platform in the networks of TIER1 operators for mission-critical routing services:

1. Effort is limited by adding one or more of Security and Fraud Mitigation applications to an existing TITAN platform.
2. All applications benefit from the carrier-grade capabilities of the TITAN platform, like redundancy and NFV-readiness.

In addition, the NetNumber Signaling Firewall application can be complemented with NetNumber Global Data Services (GDS). This industry’s unique combination both fine tunes the firewall-filtering capabilities and greatly simplifies its daily operations with automated and accurate data feeds.

**Advantages of the TITAN Architecture**

The NetNumber TITAN Solutions Suite consists of six modules under the same TITAN architecture that address the signaling, routing, security, and control requirements of CSPs today.

With the Security and Fraud Mitigation applications on TITAN, these components are configured and orchestrated with a common management GUI and provisioned via standard APIs.

On TITAN, the Security and Fraud Mitigation applications can be combined easily with other applications to protect against multi-technology and multi-protocol types of threat vectors.

The distributed execution architecture with federated data in local TITAN Edges is a seamless fit with the distributed security paradigm required for NFV and Cloud deployments.

The TITAN architecture provides network-wide benefits to all modules in the NetNumber TITAN Solutions Suite as follows.
**NetNumber Security**

**Multi-Protocol Signaling Firewall**

Signaling security is a critical concern for operators today. The threats have become more complex, and facilitate manipulations of SS7 and Diameter networks for banking fraud, authentication theft, location tracking, eavesdropping, and denial of service attacks, among others.

As SS7 and, in future, Diameter play a mission-critical role in international roaming, operators are becoming proactive in protecting their signaling networks and their subscribers from such attacks, particularly with the growing dependence on mobile services and the rise of the Internet of Things (IoT).

NetNumber offers operators unprecedented protection with the industry’s most comprehensive multi-protocol signaling firewall application on its carrier-grade TITAN platform.

The NetNumber Signaling Firewall protects against all threats in GSMA’s FS.11 (SS7) and FS.19 (Diameter). It also offers a fully configurable environment to address further signaling vulnerabilities, ensuring that operators will be able to deal swiftly with new future attack vectors.

Furthermore, the flexibility of this configurable environment makes the NetNumber Signaling Firewall the right tool to protect interconnections with MVNOs and other MNOs, especially against the effects of uncontrollable IoT behavior with aggressive malware exploits.

NetNumber is honored its multi-protocol signaling firewall application has been recognized by the industry with both the “Most Robust IMS Security Solution” award at IMS World Forum 2017 and the “Best New Security Solution” award at SDN NFV World Congress 2017.

These awards validate NetNumber’s unique approach to solving one of the most pervasive issues facing operators anywhere in the world, and validates NetNumber’s leading efforts in the GSMA Fraud and Security Group (FASG) as the primary author and editor of key SS7 and Diameter Firewall security documents.

**USE CASE: Outbound Roamers Protected against Manipulated Location Updates**

When mobile users are traveling, the Home Public Mobile Network (HPMN) will constantly receive location updates that are processed in the Home Subscriber Server (HSS) to update the user profile.

These user profiles are a popular target for hackers, who get control over the user settings as enabler for eavesdropping on calls and SMS for attacks like banking fraud.

The NetNumber Signaling Firewall supports sophisticated plausibility checking capabilities that monitor the status of outbound roamers and thoroughly verify the incoming location updates messages in SS7 and Diameter against criteria like time-location before forwarding it to the HSS.

![Diagram showing the NetNumber Signaling Firewall protecting against Manipulated Location Updates](image)
NetNumber Security Suite – Inspection, Reporting, and Auto-Provisioning

The NetNumber Security Suite consists of the Signaling Firewall in TITAN surrounded by a family of additional applications and services. The NetNumber Security Suite provides comprehensive traffic inspection and reporting capabilities, as well as versatile auto-provisioning means using high quality data feeds from the NetNumber Global Data Services. The NetNumber Security Suite is evolving continuously to enhance its protection capabilities with additional data sources and to automate further its filtering and reporting functions.

Real-Time Inspection

In previous years, CSPs were somewhat reluctant to position SS7 firewalls in-line (i.e., as a front-end to Signaling Transfer Points [STPs] and Home Location Registers [HLRs]) due to concerns about performance and availability. However, these concerns do not apply to the NetNumber Signaling Firewall: this solution is built as an application on the carrier-grade TITAN platform, which is deployed in large core networks of TIER1 operators for time-critical, high-volume signaling, routing and database control services.

Consequently, TITAN is the ideal foundation for the NetNumber Signaling Firewall to be used in-line in both SS7 and Diameter networks. This ‘built-by-design’ criterion is of growing importance, considering the security demand for encryption of all signaling traffic by which existing monitoring systems become less useful. In addition, capacity of SS7 STPs is becoming scarce because of the unforeseen continued growth of SS7 roaming traffic and the extended lifespan of this 30-year-old technology.

In light of these developments, NetNumber has complemented its Signaling Firewall with an IPFIX-based real-time data streaming capability that offers an offload of all relevant signaling data contents for post-processing services like reporting and analytics.

Comprehensive Reporting

Information clustering, filtering, scoring, and graphical representation are key attributes for ease of use, given the rapid increase of security incidents and the complexity of today’s attack vectors.

NetNumber provides comprehensive and fully-integrated reporting facilities via a complementary and dedicated Business Intelligence and Analytics (BIA) system. The dedicated solution comes with pre-defined statistics and graphics, and can be extended easily with customized graphics and reports either via NetNumber Professional Services or by the customer.

Auto-Provisioning

The protective effectiveness of a firewall depends highly on both the accuracy and completeness of the data used by the filtering logic. If the data is inaccurate or incomplete, the firewall will be bypassed by potentially risky traffic and will erroneously block wanted traffic. This will result in many false/positives, customer complaints, and unnecessarily high workload for operational staff.

The problem also applies to mobile roaming traffic, with more than 1000 mobile operators exchanging SS7 and Diameter signaling messages end-to-end worldwide.

As part of NetNumber Global Data Services, a simple provisioning alternative is provided for the GSMA Cat.2 filtering rule for inbound roamers. This filtering rule requires an accurate provisioning of the MCC+MNC ranges of all 1000 mobile roaming partners worldwide.

CSPs report great difficulty in collecting and updating the MCC+MNC ranges because not all MNOs are accurately registered or update their details in the GSMA RAEX IR.21 database. Hackers are aware of these limitations and have succeeded in bypassing signaling firewalls.

NetNumber can help with an automated data feed to the Signaling Firewall as part of our Global Data Services. This automated process is not new to NetNumber customers, as automated data feeds are common practice for the routing services with NetNumber GDS.

Auto-Provisioning of GSMA SS7 Cat.2 data by the NetNumber Global Data Services
**NetNumber Fraud Mitigation**

CSPs face a steep increase in fraud incidents resulting in decreasing revenues and rising costs, undermining profit margins. Over time, the fraudsters have computerised their operations and need less time to create more damage. By using techniques such as fast-changing numbers, the fraudsters have learned to defeat traditional fraud mitigation solutions.

The NetNumber Centralized Routing Engine (CRE) application provides support for a wide variety of Fraud Mitigation Control solutions that help CSPs protect their business against the newest generation of fraud practices:

1. NetNumber CRE acts during call set-up whereby fraudulent or unwanted calls can be rejected or redirected in real-time. The advanced CRE routing policies allow for the protection against complex attack vectors, and the calls are mitigated in a graceful manner to ensure that the attacks do not result in further stress on the network.

2. For CSPs that have the NetNumber CRE deployed for their routing policies, the same TITAN infrastructure can act as the probe network if the fraud mitigation solution is either being implemented as part of NetNumber CRE logic or integrated with the fraud mitigation solution of a specialized vendor.

3. NetNumber CRE can be combined with other NetNumber applications on TITAN, or federated with external resources like a database. This allows for fraud mitigation solutions when combined with the NetNumber Signaling Firewall or double-checking data in an external BSS database.

The following are descriptions of sample use cases protected with the NetNumber Fraud Mitigation Control solutions.

**Toll Fraud**

Toll fraud is a growing global cybercrime that targets fixed-line and mobile voice services, yearly stealing billions of dollars of global communications revenue. This includes the well-known Wangire fraud involving many short-duration calls, mainly to mobile devices, leaving a missed call number that is either premium rate or contains advertising messages, in the hope the victim will call back. Toll fraud afflicts every level of the communications market, from global carriers to household consumers.

NetNumber offers a solution on top of the TITAN platform to detect new toll fraud cases in real-time. This is superior to existing solutions whereby the attack discovery is based on information retrieved from post-call information in Call Detail Records (CDRs) as the call blocking by the NetNumber Centralized Routing Engine (CRE) acts on the SIP and/or ISUP signaling during call setup.

**Robocalling**

In the United States alone, over 200 million unwanted phone calls are made each day. Consumers are urging carriers to protect them from these malicious calls. Comprehensive solutions capable of addressing a variety of network protocols are needed.

NetNumber’s Robocalling Services help users and networks detect and further enable users to control automated, prerecorded telephone calls. The NetNumber CRE application on TITAN provides operators with a single point of provisioning for routing policy updates that are applied in real-time across the network. Robocalling Services encompass a range of white-, black- and grey-list customer-defined services that sit at the heart of the network to determine how to manage, filter, and prevent robocalls.

**Spoofing**

More and more users receive calls and SMS with manipulated numbers or names in the Calling Line Identification (CLI) or Calling Name Delivery (CNAM) services. This is very annoying for users, and undermines the trust of their CSP services.

As part of NetNumber CRE anti-spoofing routing, control logic can enable CSPs to protect their subscribers against spoofed calls and SMS messages. The CRE application may be used in combination with the NetNumber Signaling Firewall to support plausibility checking of the location of mobile users to detect and block in real-time falsified incoming calls and SMS messages.

**Equipment Identity Register (EIR)**

Given the sensitive nature and increasing incidents of security threats globally, as well as their business impact, it is becoming more critical for CSPs to know if the devices connecting to their networks are authorized or have been reported as lost or stolen.

The NetNumber EIR application is designed for operational efficiency, high performance, and scalability. The application supports all three registries known as white, black and grey lists to make a distinction between all number series permitted, barred, and tracked, respectively. On request, advanced policies can be added to protect against more comprehensive criminal acts.
The Future of Signaling Security and Fraud Mitigation: Automation

According to principle security analyst Patrick Donegan, all security solutions lead to automation because of scarcity of human resources (growth of security incidents and limited security professionals) and ‘time to detection’. Today, time to detection is also essential for fraud mitigation since cyber criminals have learned how to bypass systems acting on post-call information.

NetNumber is investing in automation of its products and services. The TITAN platform includes sophisticated real-time data sharing routines between Masters and Edges and in between Edges essential for a distributed working platform. Scoring techniques are practiced daily for data aggregation and consolidation within NetNumber Global Data Services.

Additionally, NetNumber partners with vendors focused on pattern recognition and machine learning techniques.

NetNumber Security and Fraud Mitigation Features

**Signaling Firewall Features**
- SS7 message inspection on MTP, SCCP, TCAP, MAP, CAP, and INAP
- Diameter message inspection on Command Code layer and AVP layer
- Fully compliant with the guidelines in GSMA FS.11 (for SS7) and FS.19 (for Diameter)
- Versatile logging and reporting
- Fully geo-redundant deployment with identically configured sites
- High-Availability, All-Active solution with two or more Edges per site
- Centralized provisioning of data for rules like white, grey and black lists
- Replication of stateful signaling data to all other Firewall Edges
- Deployment options in existing networks, in NFV, or in the Cloud, or in some combination of these

**Anti-Robocalling Features**
- From simple black-listing solution to sophisticated pattern solutions
- Real-time call and message blocking and redirection capabilities with ENUM, SIP, Diameter, and SS7 (MAP and ISUP)
- Simple add-on to an existing TITAN CRE

**Anti-Spoofing Features**
- Advanced incoming trunk and source verifications in real-time at call setup and SMS message delivery
- Can be combined with the NetNumber Signaling Firewall and federated with databases for comprehensive checks

**Equipment Identity Register Features**
- IMEI check via MAP F/G
- IMEI check via Diameter S13
- Diameter-to-MAP interworking according to 3GPP TS 29.305
- Local services
- Black list, white list, and grey list
- Up to 2Bn entries
- Legacy EIR support via MAP
- EIR Query Emulation
- IMSI/IMEI pairing check capability to defend against cloning practices

**Toll Fraud Mitigation Features**
- Real-time rejection of fraudulent calls during call establishment
- Automated learning of fraud patterns with immediate protection effect
- Simple add-on to existing TITAN CRE implementations
- No need for a separate probe network

**NetNumber Recognized for “Best New Security Solution”**

**NETWORK TRANSFORMATION AWARDS 2017**

11 October 2017

THE WINNERS!

Layer123

About NetNumber

NetNumber, Inc. brings 17 years of experience delivering innovative signaling control solutions that enable carriers to accelerate implementation of new services across multiple generations of networks, while dramatically simplifying the core network and reducing operating costs. Today, we are the leading provider of Centralized Signaling and Routing Control (CSRC) solutions to the global communications industry. Please visit www.netnumber.com or contact your local account representative via sales@netnumber.com