MAVENIR™
Trust the Future

CallShield:
Voice Fraud, Voice Spam, and CLI Spoofing Protection

SOLUTION BRIEF

GROWING VOICE FRAUD LANDSCAPE

Mobile voice quality has significantly improved due to the natural evolution of mobile voice services and network architectures towards SIP/IP based interconnects and VoLTE/IMS, however this evolution has simultaneously introduced new opportunities for fraudsters.

Beyond traditional types of voice fraud, such as Revenue Share Fraud (IRSF) and Wangiri (missed call) fraud, fraudsters have begun to leverage SIP architectures for fake call centers and robocalls which has led to damage for mobile subscribers. This activity has caused a dramatic drop of legal enterprise voice traffic in the United States, leading to multiple regulator initiatives on preventing Caller ID spoofing and robocalling. This problem however is not limited to any geography, and is slowly spreading across Europe, Asia and the Middle East, as regulators prepare to step in and force Communications Service Providers (CSPs) to take action.

INTRODUCING MAVENIR’S CALLSHIELD

Mavenir has introduced the Mavenir CallShield solution to address growing challenges with Mobile Voice Communication Services. Mavenir’s CallShield leverages the Mavenir SpamShield framework as well as the recent developments in Real-Time Machine Learning (ML) to identify malicious call attempts and provide CSPs with controls to minimize voice fraud damage, protect subscribers, and revenue.

KEY BENEFITS

- Real-time fraud detection and blocking
- Identify fraud in seconds, rather than hours/days
- Automatically identify known and unknown fraud, without the need for new rules.

Europe Tier 1 Nuisance Call Case Study:

- 200 fraud numbers manually confirmed, 2,000 detected by ML models, identifying 100’s of thousands of nuisance calls detected per day

Europe Tier 1 Revenue Share Case Study:

- Comparison with side by side fraud system
- Detected 100% of known Wangiri
- Detected Wangiri missed by existing system

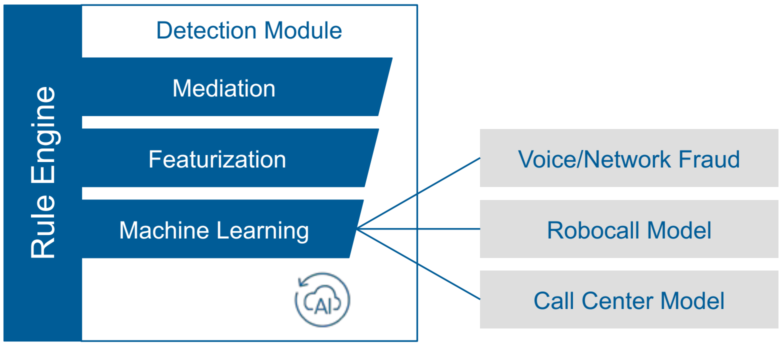
CALLSHIELD USE CASES: ROBOCALL / NUISANCE CALL DETECTION, FRAUDULENT CALL CENTER DETECTION, IRSF, WANGIRI FRAUD

CSPs can no longer rely on using only rules and thresholds for detection, as fraudsters themselves are using state of the art technology to avoid detection such as artificial intelligence to change behavior in real-time and CLI Spoofing for more successful Robocall attacks.

By using Mavenir's native ML algorithms to identify fraud and other anomalous network behaviour, reliance on rules can be avoided, providing higher accuracy, lower false positives, and the knowledge that known, future and unknown types of fraud will always be quickly identified. CallShield's framework allows flexible control of all processing and decision stages via rules leveraging both ML and Rule-Engine technologies.

CallShield is delivered with three ML models to automatically detect and classify behavioral anomalies across the following use cases:

- Voice Fraud Model (IRSF, Wangiri)
- Robocall Model
- Call Center Model



MACHINE LEARNING (ML)

Not all anomalous activity on an A CSPs network is fraudulent, but all fraud is anomalous. By using ML CallShield identifies anomalies without the need for new rules.

Dedicated ML algorithms are available to provide built-in focus on known fraud types such as: Robocalling, Nuisance Calling and Fraudulent Call Centers. Traditional fraud types are also supported, including IRSF, Wangiri Fraud / Missed Call Back Fraud, as well as providing methods to identify new forms of unknown and future fraud that don't exist today.

Unique real-time data featurization ensures a targeted ML approaches, with constantly improving detection precision to enable dedicated detection across the following use cases:

Robocall / Nuisance Call Detection:

Features used by ML include classifying abnormal traffic peaks, regular interval ranges, anomalous behavior classification, answer rates, voicemail redirect rates, typical duration patterns, social graph analysis, and other unknown anomalies.

Dedicated detection of neighbor spoofing, mirror spoofing and enterprise spoofing techniques are also supported. ML identifies this traffic for detailed monitoring, and analyzes all calls the caller-id initiates to callee's sharing the same range. Deep LSTM and CNN networks review entire neighborhoods holistically to identify Robocall / Nuisance Calls, and quickly identify clusters of suspect calls with near perfect accuracy, even if caller-ids are spoofed. This is completed through a combination of behavioral analysis and feature categorization, such as: counts of distinct qualifying B-numbers, targeted sequential B ranges, average and spread of ring and talk durations, standard deviation of pause time between calls, categorizing rates of unanswered calls, etc. Detection is independent of crowd sourced reports/ OEM solutions, but can leverage both as input.

CLI Spoofing

Protection against CLI Spoofing is also supported by offering prebuilt spoofing detection techniques. CLIs are examined to identify inaccuracies that may indicate spoofing, such as CLI lengths that are too long or too short, or even of an incorrect format or from an unallocated number range or fixed area code. CLI origination can also be examined to determine the validity of local CLI's originating from an offnet interconnect by performing on-net presence checks.

Fraudulent Call Center Model

ML supports dedicated features for fraudulent call centers, operating from dedicated bases and generating mass nuisance calls to subscribers. These call centers are often focused on specific frauds or scams. ML features support dedicated detection of these call centers in operation, including outbound call rate, declining call rate, voicemail durations, call origin (for example, non-geographic numbers).

Wangri,Voice Fraud (IRSF) Model

Features used by ML includes identifying sudden increases in traffic generating to a typically uncommon destination, time of calls, history of communication from the number, durations, time between calls, connection length, roaming status, IMEI change, average call duration.

MONETIZATION OPTIONS

When a telecommunications subscriber experiences large amounts of incoming spam calls, enterprises who need to reach their consumers struggle to gain consumer trust. To regain consumer trust and recoup the termination feeds for incoming calls, CallShield gives CSPs the opportunity to introduce additional identification services for trusted enterprise caller IDs, while also limiting the source originators for them. Trusted caller IDs can be added during call setup into the respective SIP headers. Additionally, these can be exposed through the REST API for OEM Apps, leveraging Caller Directory and other native OEM APIs for integration.

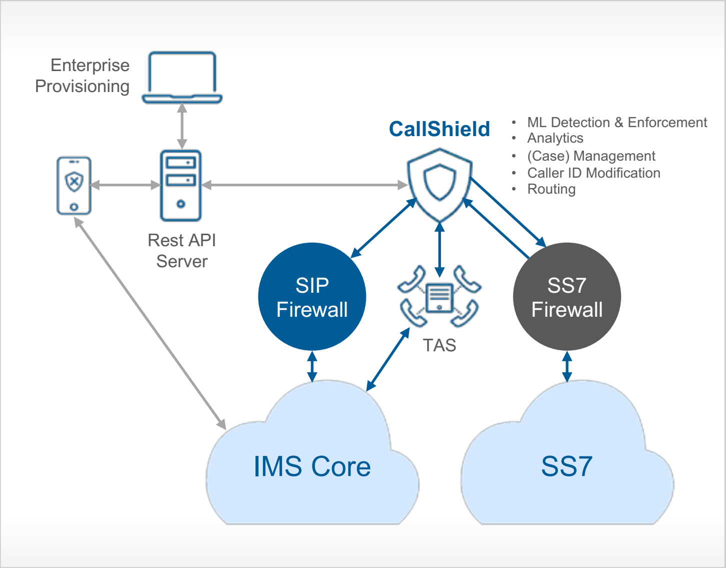
As some governments make the move to clamping down with hefty fines on illegitimate call centers, scam call originators and callers that do not respect do-no-call lists, CSPs are also seeing paths to a more reactive response to incoming Robocalls / Nuisance Calls. CSPs who leverage CallShield for detection and blocking can also utilize functionality to divert suspect calls to private and potentially chargeable voice mail systems that subscribers may choose to check if they wish.

When CSPs use CallShield, it helps them increases brand recognition and in the successful deployment of enterprise voice campaigns, it also ensures for protection of these Caller IDs from unauthorized use from unexpected sources.

INTEGRATION INTERFACES

Mavenir's Call Shield is part of Mavenir's Fraud and Security Suite that, which among other capabilities includes a set of network facing elements (Policy Enforcement Points) normally deployed as a firewall on a specific signalling or data stream. Mavenir's SIP Firewall is a default PEP, however we can support ISUP via SS7 Firewall.

In case of VoLTE networks direct integration with TAS or I-SBC is possible as well, assuming these elements support real-time Call Triggering interface to an external system. Using this interface CallShield can obtain required Voice Call Data as well as block or redirect the call (these capabilities are available on Mavenir TAS and I-SBC). REST API Server enables external CallShield integrations with providing APIs for OEM Caller Applications as well as for Enterprise Portals for provisioning.



ADVANTAGES OF MAVENIR'S CALL SHIELD

Mavenir has brought the latest in detection together from 10+ years of proprietary Machine Learning technology, enhanced with a fully scalable and highly adaptable solution suitable for CSPs, MNOs, MVNOs and wholesalers alike. The advantages of the Mavenir CallShield solution include:

- Real time detection, analysis, blocking, and subscriber warning
- Continuous real-time learning with a dynamic Machine Learning model
- Modular design utilizing a big data backend
- Enterprise support with Caller ID enrichment and management, with optional monetization
- Pre-integrated with Mavenir traffic-based solutions
- Various deployment options based on unique needs, including SaaS through Mavenir SMART Services

MAVENIR™

Trust the Future

About Mavenir

Mavenir is leveraging our DNA as a pioneer in advanced technology to focus on the vision of a single, software-based mobile network that can run on any cloud. We are reshaping the industry with our multi-generational, cloud-native, end-to-end software that is reducing complexity, de-risking digital transformation and rapidly modernizing networks. We are the trusted partner to customers around the globe, who are transforming the way the world connects — realizing the amazing new services and the promise of 5G and beyond.

For more on Mavenir solutions please visit our website at www.mavenir.com