MAVENIR
Trust the Future

Mavenir SpamShield Solution

Protect Application 2 Person(A2P) Revenue

SOLUTION BRIEF

WITH ADVANCED MONITORING, ANALYTICS, AND MACHINE LEARNING TOOLS FROM MAVENIR'S SPAMSHIELD, CSP'S CAN BLOCK MILLIONS OF FRAUDULENT MESSAGES FROM REACHING CUSTOMERS AND PROTECT REVENUES.

THE BUSINESS CASE – FRAUD AND SPAM IMPACTS TO REVENUE

Messaging is an important source of revenue for Communications Service Providers (CSPs). The number of smartphones accessing carrier networks across the globe is increasing every year. The numbers are staggering. Of the 7.10 billion mobile phones across the globe, 6.37 billion are smartphones, which means 80.6 % of the world population has a smart phone[1].

With the rise in smartphones, various notification capabilities were introduced, however SMS messaging is the most relevant channel. In addition to person-to-person messaging, banks, airlines and on-line services are constantly using Application to Person (A2P) to send notices, confirmations and authentication messages.

A2P text messages are another form of revenue for the CSPs, and selling value added services. While the revenue aspect of A2P is a boon for CSPs, it is estimated that between 5% -20% of all SMS messages are spam or fraud related[2]. Subscribers exposed to fraudulent traffic have a poor end-user experience, causing significant revenue loss with missed opportunities and compromising the channel for selling (A2P) value-added services.

CSPs are facing an increasing, ever-changing flow of spam and fraud traffic that is difficult to detect and control. By improving the effectiveness and timeliness of threat detection and responses with Mavenir's ML-based SpamShield, CSPs can strengthen their security posture against potential of harmful security events and keep revenue streams flowing.

REVENUE PROTECTION SCENARIOS

The growth of the A2P market and with millions of IoT and 5G connected "things" coming online

CSP's depend on the network more than ever.

The global A2P messaging market is anticipated to grow

at 6.7% CAGR through 2024, increasing the global revenues to over $21B[3].

As the industry continues to grow, so does the proliferation of spam and phishing attacks.

CSPs are facing losses in revenue from this area which are directly related to fraudsters.

1. Radicati Group 2021
2. Mavenir and GSMA

A2P Grey Route

Enterprises and aggregators trying to minimize their messaging termination fees may attempt to load balance message deliveries between the official A2P connections and other channels. In extreme cases, SIM boxes, Application farms or SS7 by-pass methods could also be used to terminate official A2P campaigns resulting in total revenue loss of these messages to the CSP. Usage of Application farms is becoming more widely spread fraudster technique which not only leads to the increased complexity of grey route blocking but also exposes Mobile users to the exploits and malware usually embedded into the respective campaigning applications.

A2P revenue by-pass

Some businesses have been identified as not legalizing their messaging termination business at all, and instead utilizing sophisticated SIM boxes, Application farms and leased global titles enabling sophisticated by-pass scenarios. This scenario has been recently exposed in the industry as Home-Routing by-pass, conducted using sophisticated SS7 operation encoding which allows direct message delivery to a mobile subscriber outside of the standard message delivery call-flow or any kind of centralized messaging infrastructure.

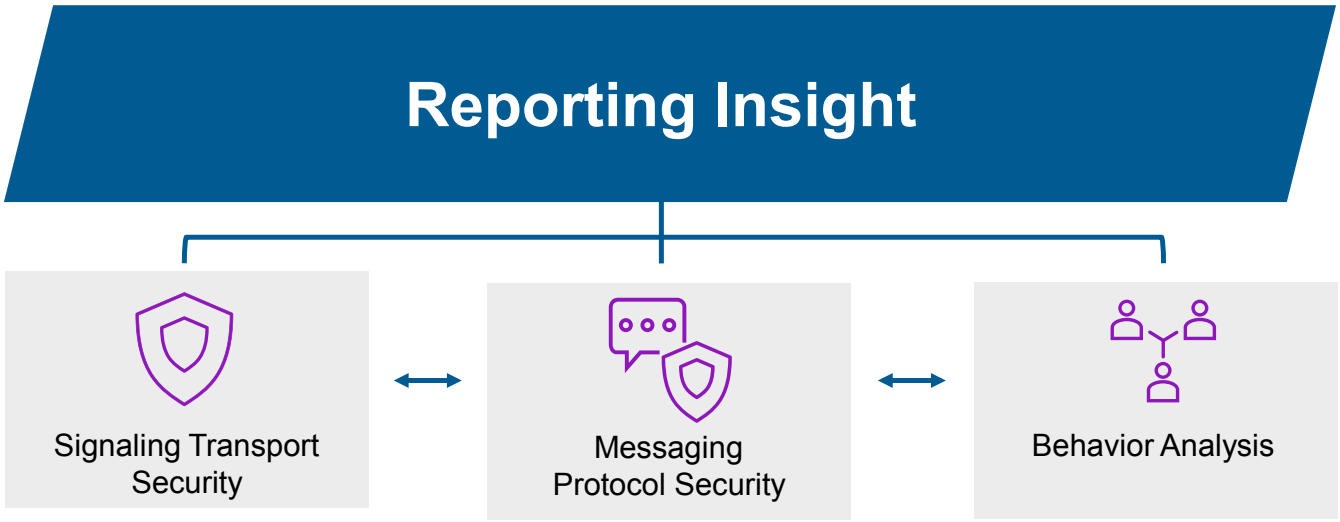
CSP's need to have a solution that offers:

- 360-degree view of the threat landscape
- Real-time detection and blocking of fraudulent traffic
- Sophisticated AI/ML algorithms with automatic detection and response
- Highly qualified fraud analysts and data scientists

MAVENIR'S SPAMSHIELD SOLUTION

Mavenir's SpamShield technology and machine learning can be deployed to carry out automated security analysis and defense. The SpamShield solution provides CSP's with 360-degree control to effectively address specific situations within their networks with speed and flexibility unrivaled by other market solutions.

Starting from detection of signaling vulnerabilities exploits in the core network using Mavenir's Signaling Firewall; SMS protocol level filtering and patented grey-route prevention on the Message Controller and a real-time Machine Learning based detection module that fingerprints the entire network's messaging traffic and engages proprietary ML technology to immediately identify A2P traffic patterns in the form of campaigns. Machine Learning algorithms perform A2P detection without the need to maintain complicated filtering and detection rules, ensuring any fraudster attempting to by-pass detection would be prevented using these ML fraud prediction techniques. Proprietary and specially tuned Machine Learning models also ensure quick adaptation to each mobile network's specific behavioral patterns and become efficient within a very short training period. The latest version of Machine Learning algorithms includes prediction capabilities to qualify detected fraud types which enables even more efficient monetization use cases. Mavenir provides the Security Management and Response Team (SMART) ensure proper daily operation of the platform enabling subscriber protection and revenue assurance in an OPEX efficient way.



ADDRESSING REVENUE PROTECTION

Mavenir's SpamShield solution has a modular structure and delivers each component to target a specific problem and match the CSP existing architecture.

A2P Revenue Bypass and Grey Route Blocking:

Costs: Cost bypass is where the CSP is not getting paid for part or all of what is due. Use of the SIM boxes to bypass international tariffs, and also used to send spam and nuisance texts.

Solution: Mavenir's SpamShield detects new campaigns that originate through SIM boxes, application farms as well as other bypass scenarios and blocks campaigns that fail to switch to official A2P channels.

ADDRESSING REVENUE PROTECTION SCENARIOS

The unique and innovative SpamShield solution uses real-time AI/machine learning technology with unique message fingerprinting algorithms that enable automatic detection of messaging fraud scenarios and even sophisticated by-pass methods used by the grey aggregators and fraudsters. While other vendor solutions must define rules and policies to perform detection and must know the attack vector, SpamShield will detect an attack vector automatically using finely tuned algorithms that adapt to the current network conditions and subscriber behavior to stop spammers and fraudsters in real-time. This technology has proven its efficiency in multiple head-to-head comparisons with other vendor solutions demonstrating much vastly improved precision.

Spam detection technology used by Mavenir is based on Artificial Intelligence (AI) principles and Machine Learning (ML) developed with a detailed understanding of the subject area, specially tuned for real-time detection. Traditional detection and prevention techniques are based on deterministic rules that are easily detected and bypassed by spammers and fraudsters. SpamShield AI/ML detection algorithms adapt to current network conditions and subscriber behavior to continually detect spammer and fraudster attempts.

SpamShield's advanced correlation techniques with external learning feeds include a spam reporting service, centralized spam database, hyperlink reputation statistics and call-back number reputation, all of which enable real-time prevention of malicious campaigns. AI/ML techniques implemented in SpamShield address traditional text-based messaging and multimedia content used in Rich Communications Services (RCS).

The solution addresses all major security use-cases for messaging channel control for SMS, MMS and RCS messaging protocols and provides CSPs with 360-degree control to effectively address harmful events within their networks.

The Value of SpamShield

SpamShield, Mavenir's world-leading messaging fraud control solution employs advanced machine learning techniques to rapidly identify and automatically control fraudulent traffic. CSPs can maximize additional A2P revenues and protect their customers with the latest in fraud technology.

3. Global A2P Messaging Market Report 2021: Analysis and Forecast 2020-2026 - ResearchAndMarkets.com|Business Wire
4. Research and Markets Report 2021

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