Built from a unique platform with AI/machine learning & big data analytics providing real-time network protection and fraud prevention

Network Security and Fraud Management Suite

Where security is compromised, fraud is inevitable. Traditional systems can no longer keep pace with the volume and velocity of criminal activity. Many existing systems can't uncover new fraud types; they overwhelm the user with false positives or use dated rules that only uncover fraud long after it has taken place. Furthermore, the most impacting types and methods of fraud are related to subscription fraud, PBX hacking, international revenue share fraud, interconnect bypass, premium rate service.

Mavenir's Network Security and Fraud Management Suite protects the network in real-time, and with predictive analytics and machine learning, the network is protected even as new vulnerabilities arise. Mavenir distinguishes between three main verticals within the fraud and security domain:

Messaging Revenue Assurance:

Protects the CSPs' revenue leakage based on innovative bypass techniques for A2P traffic. It offers efficient real-time detection of SPAM campaigns acknowledged by CSPs around the globe (SpamShield).

Network Signaling Security:

Provides Signaling Firewalling solutions that implement the GSMA mitigation recommendations (FS.11 and FS.19) to detect and prevent the signaling-based attacks from happening (Signaling Security)

Fraud Management:

A modern data approach to fight fraud in real time, based on a Big Data approach suited to manage the volume, velocity, and variety of structured and unstructured data over wireless networks. It relies on a unique, real-time fraud analytics platform, tailored for CSPs' most pressing needs (Equipment Identity Registry, Fraud and Data Analytics).

The key features include:

1. Easy-to-use / intuitive management interface for minimal response times to act on any unforeseen ongoing suspicious activity detected through sophisticated mitigation algorithms.
2. Powerful correlation engine offers detection of anomalous traffic patterns through efficient traffic profiling capabilities. The machine learning mechanisms behind the correlation engine create challenging obstacles for fraudulent activities to pass through unnoticed.
3. Supporting Analytics component enables CSPs to create interactive dashboards based on any required key performance indicators. The generated reports offer insights on the signaling traffic beyond security context helping the operators reveal any possible network optimizations or revise their interworking agreements.

Mavenir's cloud-native Network Security and Fraud Management Suite includes Messaging (SMS, MMS, and RCS) Spam and Fraud control, Equipment Identity Register (EIR), Signaling Firewall (Diameter, SIP, SS7 and GTP), Session Border Controller (vSBC) and Mobile Edge Gateway (including ePDG, SeGW, and HeNB-GW) enabling operators to understand, monitor, enforce and maintain network security. The security suite fully covers protection of the core mobile network including the messaging revenue of modern CSPs.