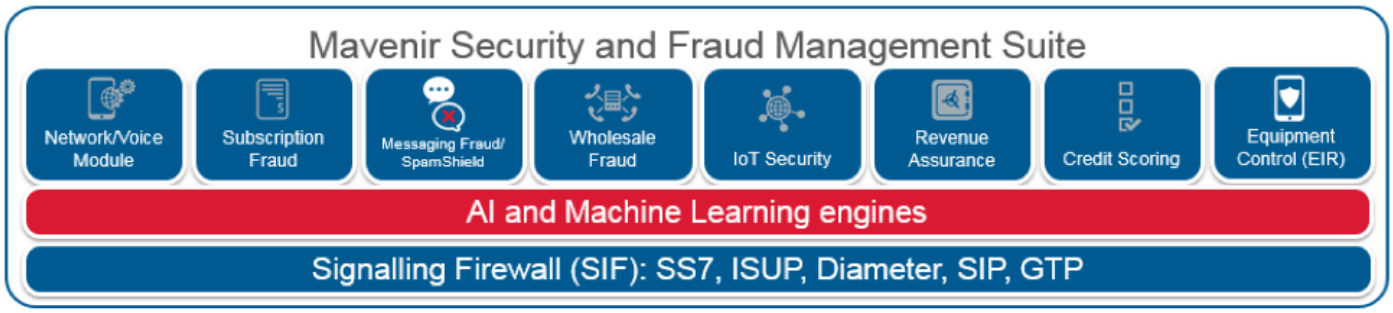
AI / Machine Learning Engines



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 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. It is the nature of Fraud that it never stops, it only changes as methods get more sophisticated.

Protecting networks from fraud can no longer rely on using rules/thresholds when fraudsters are using AI to commit fraud and change their behavior in real-time.

Machine learning identifies 'anomalous' behavior on a network (not all anomalous traffic is fraud, but all fraud is anomalous). The advantages of Machine Learning:

- Detects previously unknown fraud
- Analyzes hundreds of categorical and continuous features
- Delivers actionable insights in real-time
- Makes no assumptions about probability distributions
- Categorical and continuous feature integration
- Provides feature importance with alerts
- Unconstrained feature complexity
- Adversarial machine learning
- Unique models created for individual Operators, and applicable across MNO's, MVNO's and Wholesalers alike
- Proven at world largest carriers