# SIP Security



## OVERVIEW

The global VoIP market is growing significantly with the increasing penetration of VoLTE networks, the surge in VoIP traffic, etc. This has led to Session Initiation Protocol (SIP) becoming a de-facto protocol for voice-over IP (VoIP) communication. SIP is an application layer protocol for creating and terminating sessions with one or more participants.

As SIP-enabled services and devices continue to become more widely used, there is an increasing need to prioritize safeguarding the assets against undesirable exploitations and attacks. Due to its open architecture, SIP-enabled services are vulnerable to various types of threats and attacks. The need of the hour is to have a more dynamic fraud detecting and preventing mechanism that goes beyond the SBCs and firewalls.

Subex's SIP Security solution protects the network from outside attacks and abuse before they cause any damage to the network or your subscribers with our multi-layered security mechanism, which comprises signatures, heuristics, and machine learning techniques to prevent such attacks. Some of the main fraud and security attacks addressed by our solution*:

| | | | |
|---|---|---|---|
| **01** CLI Spoofing | **03** PBX/IP PBX Hacking | **05** Wangiri Fraud | **07** A-number Refiling |
| **02** Early detection of IRSF | **04** SIP Register Flood Attack | **06** Malicious User Agent Attacks | |

For more information write to info@subex.com

Regional offices:  Dubai    |   Ipswich

*indicative list

# FEATURES

**01** **Multi-Tier Detection:**
Our solution combines a 3-tier strategy - Signatures, Heuristics, and Machine Learning to detect vulnerabilities.

**02** **Proactive & Self-learning Capability:**
Our solution's Machine-Learning and automated attack surface identification is a perfect solution designed to secure the network from new and unidentified potential risks and zero days.

**03** **Stateful System:**
Being stateful in nature, our solution has the capability to tear down the call in a particular state of the call.

**04** **Agentless and Non-Intrusive:**
Our solution does not require agents to be deployed at endpoints. The solution is non-intrusive, requiring no updates to the existing ecosystem.

**05** **Intelligent Anomaly Detection:**
Our solution's anomaly detection algorithms enable the early detection of unknown patterns, avoid false positives, and improve the accuracy of alarms.

**06** **Active Threat Intelligence:**
Our solution provides threat intel sourced from Subex's global honeypot network with over 400 different architectures and 4000+ devices in over 66 different locations worldwide.

# BUSINESS BENEFITS

**Minimal Fraud Run-time:**
Detects any form of threat in the signaling setup and tears down such attempts before the transaction is set up, thus reducing fraud run-time drastically.

**Positive Brand Image:**
Safeguards customers from attacks, reduces customer churn, improves customer experience, thus helps build a positive brand image.

**Comprehensive Threat Coverage:**
Increases threat coverage across various services and network layers with active threat intelligence and focused threat libraries.

**Increased Accuracy:**
Decreases false positives significantly with AI/ML models, thus increasing accuracy.

**Quick ROI:**
Ensures quick returns for your investments with rapid deployment and swift commencement.

**Future-Proof Network Against Next-Gen Frauds:**
Our solution is equipped with an anomaly engine capable of identifying unknown unknowns, making it future-ready.