

TECHNOLOGY OVERVIEW

Fraud & Security

Cellusys Security enables mobile operators to detect, prevent and control signalling and messaging security risks in real time across SS7, Diameter, SIP, GTP, HTTP/2 and SMS environments.

Operators face

- Cross-protocol attack scenarios spanning SS7, Diameter, SIP, GTP and SMS
- CLI spoofing, IRSF, Wangiri, flash call abuse and SIM box bypass
- Subscriber data exposure through signalling exploitation
- Revenue leakage from grey routes and interconnect abuse
- Regulatory and GSMA compliance pressure
- Limited visibility across legacy and next-generation signalling layers

Typical use cases

- Detection and blocking of CLI spoofing and voice-related revenue abuse
- Correlation of signalling anomalies across SS7, Diameter, GTP and SIP
- Protection against SMS spam, smishing and grey route manipulation
- Identification of unauthorised signalling queries and subscriber data exposure
- Monitoring and reporting of GSMA violations (FS.11, FS.19, FS.20)
- AI-assisted and intelligence-driven rule updates to address emerging threat patterns
- Pre-launch vulnerability assessment of exposed signalling interfaces

Solution Portfolio

Product	Description
Signalling Firewall	Multi-protocol signalling protection across SS7, Diameter, GTP, SIP and HTTP/2
Voice Firewall	Detection and prevention of voice fraud including CLI spoofing and IRSF
SMS Firewall	Filtering and control of SMS fraud, spam and grey route traffic
Penetration Testing	Proactive testing of signalling interfaces to identify exploitable weaknesses
TCG	Voice traffic control and governance mechanisms for secure interconnect management
Managed Security Services	Ongoing monitoring, optimisation and operational management of deployed security solutions

Architecture & operation

- Deployed inline or in monitoring mode at signalling and messaging interconnect boundaries
- Inspects SS7, Diameter, GTP, SIP, HTTP/2 and SMS traffic
- Applies configurable, protocol-aware rules aligned with GSMA recommendations and operator policies
- Correlates signalling events and traffic behaviour to identify coordinated threat patterns
- Enhances detection accuracy through risk scoring and intelligence updates
- Executes configurable actions including blocking, modification, rate limiting or alerting
- Supports flexible inbound and outbound API integration for external system connectivity
- Designed with redundancy to support resilient network deployments
- Provides detailed logging, reporting and compliance visibility

Deployment & integration

- In-line and loopback configuration options
- Deployment across SS7, Diameter, SIP and HTTP/2 environments
- GTP transparent or routed implementation
- Integration with STP, DRA, SBC and core signalling elements
- REST API integration for external systems
- Data export and SIEM integration
- Redundancy support at hardware, deployment and logical level

How we work

Typical project duration

30–60 days, depending on deployment scope and environment readiness.

Implementation phases

Deployment, configuration, testing and operational handover.

Proof of Concept option

Testing and evaluation can be performed prior to full deployment.

Level of configuration/customisation

Configurable security rules aligned with GSMA guidelines and operator requirements.

Operator involvement required

Coordination with network, security and fraud teams during deployment and optimisation.

Managed service or support model

Support options include 24x7x365 for live systems or business-hours support for lab environments, with optional Professional or Managed Services available as required.