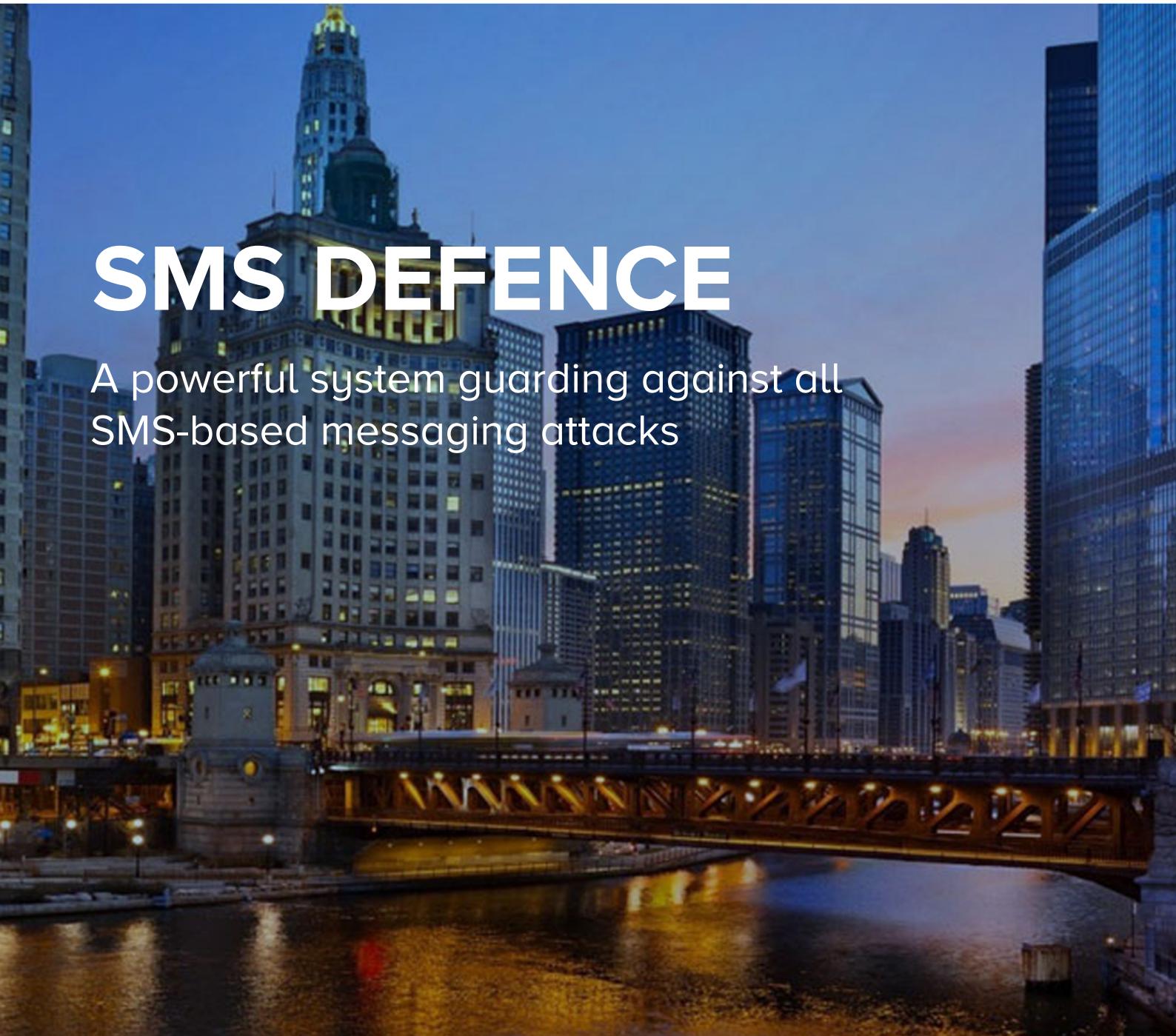


Cellusys®

SMS DEFENCE

A powerful system guarding against all
SMS-based messaging attacks



In 2015, SMS is now a digital lifeline for social, personal, business, and financial communications – and subscribers expect and demand a faultless service. But with more than 6 billion users globally, SMS is a magnet for spammers and fraudsters.

The GSM Association has determined that the following threats are most prevalent:

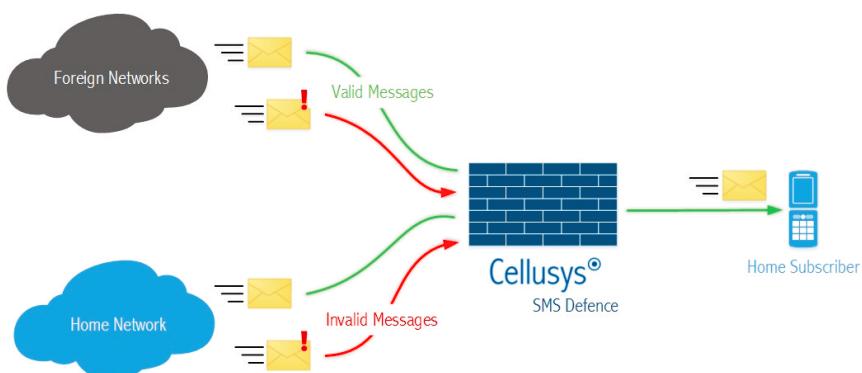
| Type | What Happens | Risk to the Operator |
|-----------------|---|---|
| Spamming | Unwanted messages are delivered to subscribers. | Irritated subscribers, degraded performance, blamed for relay. |
| Flooding | Remote system sends massive numbers of messages targeting subscribers and nodes | Overload in the signaling network, home operator incurs relay operator costs |
| Faking | Foreign system illegally uses identity of SMSC | Home operator cannot collect termination fees |
| Spoofing | Messages sent illegally by simulating subscribers in a roaming situation | Subscribers wrongfully billed for unsent messages and perhaps unwanted content |
| Viruses | Hacker engine launches messages luring subscribers to a download site with viruses | Compromised handsets cause customer service problems and may send unwanted messages |
| Smishing | Messages that appear to be from a valid company attempt to acquire subscriber information | Subscriber annoyance, billing issues, potential to spread viruses and then more spam. |

With SMS spam and fraud on the rise, the potential financial damage for subscribers and operators, is ever more substantial.

- Unauthorized entities such as bulk SMS providers are sending SMS via networks without the operator realising a termination fee
- Reduced rate of adoption of revenue-producing services, as spam destroys trust in an operator, leading subscribers to opt out of emerging mobile advertising and m-commerce opportunities
- Subscribers are switching to more reliable networks (subscriber churn)
- Increased SMSC licensing costs due to increased volume of fraudulent messages
- Failure to attract new subscribers to the network, with negative public opinion of the quality of service
- Fraudsters are using the identities of other subscribers – billing cannot be completed
- Call centre costs are high, with calls from disgruntled customers (DDOS and licensing costs)

Cellusys SMS Defence

Cellusys SMS Defence is the most stable and powerful defence against all SMS-based messaging attacks. The system is easy to use. It enables networks to give their subscribers the most secure and safe SMS service.



How does Cellusys SMS Defence combat SMS misuse?

Detailed/Comprehensive Reporting

An Operator needs first to be aware of the problems that are occurring on the network. Cellusys SMS Defence gives the network operator detailed trend analysis and real-time reports of SMS activity. The system generates call detail records, graphs, and spreadsheet reports; and it highlights problem areas that need to be addressed.

Real Time Alerting

This comprehensive notification system alerts the relevant team. SNMP traps, SMS, and emails can be sent to the NOC team when threats and notable events occur that may require action.

Cellusys Differentiators

AVG Integration

Cellusys has partnered and integrated with AVG, a world leader in anti-virus and threat detection. The Cellusys Global Threat Network is regularly updated with new threat definitions from AVG, which SMS Defence uses in scanning SMS content. With AVG you will get the most up to date counter measures against Smishing attacks.

Powerful Rules Engine

Operators can define any message policy they wish to apply to SMS passing through the network. The system provides a multitude of matching criteria, to enable the implementation of broad policies or attain fine-grained control. SMS Defence can block messages, return error messages, and even inform the message sender that the SMS has been delivered when in fact it has been removed from the network.

Complete Protection

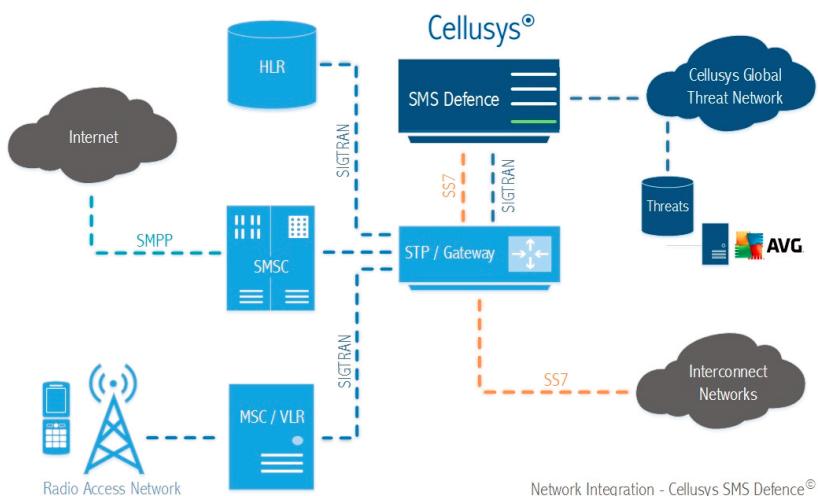
Advanced SMS Firewall algorithms even protect your subscribers when they are roaming in another country. Message flows are manipulated to re-route SMS through SMS Defence for screening, before being delivered to roamer.

Multiple Network Support

If a Mobile Operator has MVNOs, acts as an International SMS Gateway, or is an SMS Hubber, then SMS Defence is needed for each network. Cellusys SMS Defence can be configured with multiple virtual instances; each instance can be used by an individual network with its own message policies. One physical installation with multiple interfaces means that effectively, each network has its own SMS Defence system.

Network Integration

SMS Defence is engineered to integrate with any network's STPs (Signalling Transfer Points) or Signalling Gateways. The system supports both traditional TDM links and SIGTRAN M2PA or M3UA links. It tailors to the technical capabilities of your network elements.



All Cellusys technology is architected to be highly scalable. If there is a need to upgrade the system to handle a higher volume of traffic, this can be done easily, simply by adding additional Message Processor machines. These machines will integrate with only minor configuration changes. Large increases in load can be handled with negligible upgrade costs and minimal effort.

Cellusys SMS Defence Value Proposition

① Realise Revenue for all terminating SMS

Identify and block SMS from senders who do not pay a termination fee. A2P messaging, bulk SMS providers, and corporate SMS (Banking, OTP, etc.) can be blocked until commercial agreements are put in place.

② Renegotiate Roaming Contracts

With Cellusys SMS Defence, you can block SMS from foreign operators until a more favourable roaming contract is negotiated.

③ Sub-contract to MVNOs

If you have MVNOs, you can sell this SMS Defence service on to them – as the system is able to split traffic for multiple networks.

④ Centralised CDRs

CDRs are created for every message processed, and they are stored centrally. So you can access CDRs easily to analyse, verify billing, etc.

⑤ Reduce licensing costs of SMSCs

As you block fraudulent SMS, there will be a reduction in messaging volume on the core of the network where you pay for bandwidth.

⑥ Reduce costs of customer care.

Reduce subscriber churn

Less spam means more satisfied customers, which means lower costs at your call centres. And it means fewer people leaving your network.

⑦ Unlimited Message Licensing

With your Cellusys SMS Defence license, you can process an unlimited number of messages. Expand your system when you need to, and you won't incur any additional software licensing fees.