adaptivemobile™
trusted network protection

AdaptiveMobile Messaging Security

Protecting the Borderless Network

Product Overview

Mobile operators across the globe are facing intense competition as their messaging services mature and new entrants in their markets emerge. To protect their revenues and margins they need continual protection against the latest messaging security threats, across SMS, Email, MMS or RCS / SIP (IP Messaging).

Whether from regulatory pressure, subscriber complaints over spam, or new over-the-top messaging apps – every operator today is struggling to maintain the profitability of their SMS. Yet it still remains the most widely used and commercially successful messaging service.

AdaptiveMobile Messaging Security can help operators take the right steps to tackle a broad range of challenges to their messaging services. Using in-network controls, subscriber reputation and advanced threat detection algorithms, the Messaging Security platform can identify and block spammers, service gateways and app broadcasts – protecting an operator's current and future messaging businesses.

Benefits

Scalable system wide approach

- System wide visibility of traffic, source and state
- Centralised control and management
- Shared configurations across all data centres
- Virtualisation support for faster deployment, upgrade and expansion

Comprehensive reporting

- Built-in Big-Data approach
- Drill-down threat details
- Actionable insights

Customer care / operational monitoring

- Customer care tools to respond to queries, retrieve subscriber history /filtering decisions and update customer reputation and policy
- System wide monitoring and network integration

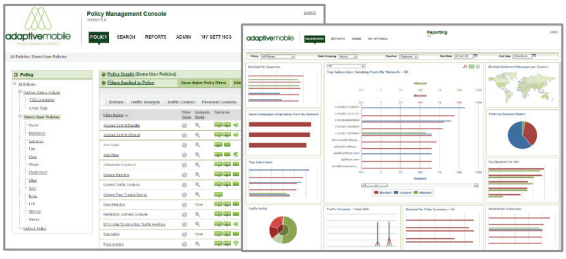

Figure 1 – AdaptiveMobile Messaging Security Policy Management and Reporting

Typical Applications

AdaptiveMobile Messaging Security can be used for the following purposes to ensure operators can:

Close Commercial Loopholes

- Identify Service Gateways and block Grey Routes – to prevent an operator's network being the network of choice for grey-market organisations
- Improve revenue generation from legitimate brands and service activation messages

Block Security Threats

- Meet regulatory guidelines and prevent regulatory involvement
- Maintain the value of wholesale services
- Block spam and unsolicited messaging from MO sources
- Control app hacking and virtual operator use of their network
- Block competitive operator messages
- Retain existing subscribers and roaming revenue

Secure New Services

- Ensure new services such as RCS are secure from technical and commercial loopholes

Functional Components

Security Engine

- Operates passively or actively within the network
  Sigtran / SMPP / SIP / MMS integration
- Detect known spam campaigns in real-time using proprietary, constantly-updated Fingerprints
- Evaluates all other traffic with a proprietary Spam Analysis Engine to detect “suspicious” traffic that may be new campaigns
- Application of additional operator-specific policies to traffic.
- Application of subscriber-specific policies to traffic
- Near-zero false positives
- Near-zero latency for legitimate users

Security Centre

- The AdaptiveMobile Security Practice evaluates and confirms new threats detected across our global network
- Detection and reputation stats are fed back from all deployments
- Anonymised “cluster definitions” are fed back from the Analytics platform
- Cartridge updates with fingerprints for new threats
- Algorithm updates for Fingerprint Engine and Spam Analysis Engine
- Ongoing mobile malware and threat research

Security Reporting

- Collates and processes suspect traffic to identify new messaging threats; and to determine the reputation of devices connecting to your network
- Suspicious traffic is “clustered” until there is evidence of a new distinct threat or campaign
- Behaviour patterns of senders of known threats and campaigns are used to build a reputational profile of the device
- Correlations between threat and targets to identify associated SIM cards
- Analysis of trending call to actions to identify potential frauds
- Reputation-based controls
- Spam gang correlation

Security Policy

- Can operate in a fully automated “Black-box” mode, without the need for operator administration
- Provides the flexibility for operators to respond to local requirements such as:
- Category-based selection of fingerprints
- Override individual campaigns
- Override / reset / whitelist of individual source reputation
- Rich policy hierarchy and filter set

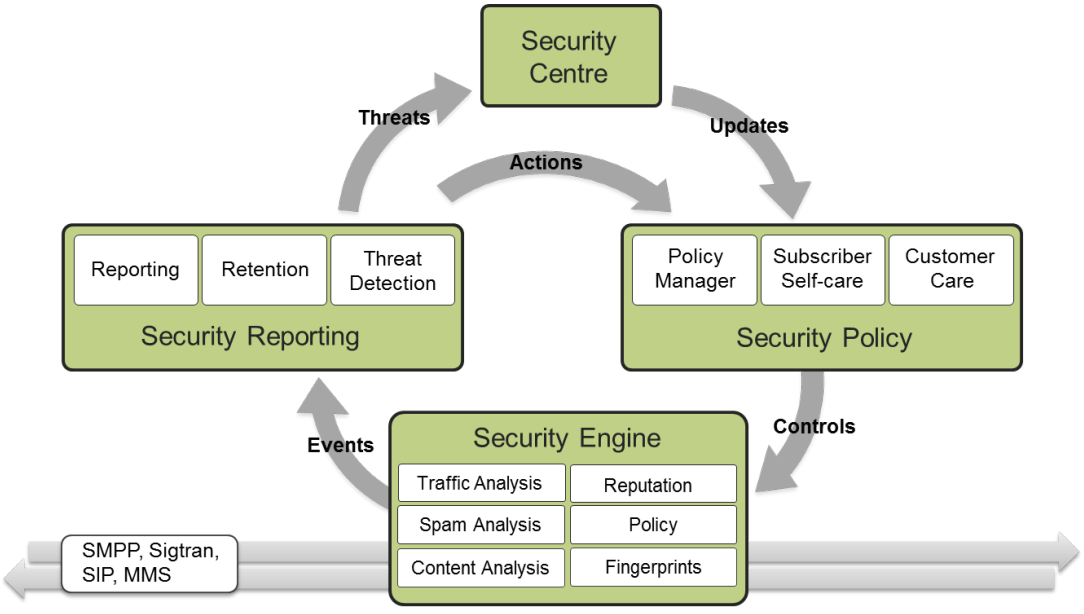

Figure 2 – AdaptiveMobile Network Protection Platform

Key Features

Tamper-resistant Fingerprints

- Fingerprinting algorithms proven to consistently defeat continual threat metamorphosis

Sophisticated New Threat Discovery

- In-network proprietary algorithms to constantly hunt for and identify suspicious new threat types, delivering up to zero-minute protection

Real-time Reputation & Traffic Analysis

- System-wide behaviour and content-based reputation of all sources driving policy decisions

Sophisticated Security Policy Structure

- Comprehensive and flexible policy capabilities to respond to new requirements without service deterioration

Global Security Analytics

- Global security team with "Big-Security" threat analytics platform to support in-network threat detection and remediation

Advantages of AdaptiveMobile Messaging Security

- **The market leading platform for mobile operators around the world**
- **Proven through deployment in over 40 networks including some of the largest messaging environments**
- **Proven reduction in messaging abuse and subscriber complaints as validated through the GSMA's own Spam Reporting Service**
- **The most comprehensive messaging security platform for mobile operators**
  - Sophisticated policy structure
  - Real-time system-wide reputation and traffic analysis engines
  - Industry-leading spam fingerprint and discovery algorithms
  - Backed up with the only global security research practice dedicated to mobile messaging threats

Head Office
Ferry House, 48-52 Lower Mount Street, Dublin 2.
Contact: sales@adaptivemobile.com

Regional Sales Contact Numbers:
US, Canada, Latin America Sales: +1 972 377 0014
UK Sales: +44 808 120 7638
Middle East Sales: +97144 33 75 83
Africa Sales: +27 83 7044111
Asia Sales: +66 89 87 42 32
European Sales: +353 (1) 524 9000

Regional Operational Support Contact Numbers:
UK: +44 208 114 9589
Ireland: +353 1 514 3945
France: +33 975 180 171
India: 000-800-100-7129
US, Canada, Latin America: +1 877 267 0444

For discussion of typical use cases, overview of AdaptiveMobile's existing deployments or a full walkthrough of service provider experience, contact your local office:
www.adaptivemobile.com/contact-us

About AdaptiveMobile
AdaptiveMobile is the world leader in mobile security protecting over one billion subscribers worldwide and the only mobile security company offering products designed to protect all services on both fixed and mobile networks through in-network and cloud solutions. With deep expertise and a unique focus on network-to-handset security, AdaptiveMobile's award winning security solutions provide its customers with advanced threat detection and actionable intelligence, combined with the most comprehensive mobile security products available on the market today. AdaptiveMobile's sophisticated, revenue-generating security-as-a-service portfolio empowers consumers and enterprises alike to take greater control of their own security. AdaptiveMobile was founded in 2003 and boasts some of the world's largest mobile operators as customers and the leading security and telecom equipment vendors as partners. The company is headquartered in Dublin with offices in the North America, Europe, South Africa, Middle East and Asia Pacific.

www.adaptivemobile.com

MAAWG MESSAGING ANTI-ABUSE WORKING GROUP · GSMA GSM World · oma Open Mobile Alliance · IWF Member DO the right thing