adaptivemobile™
trusted network protection

AdaptiveMobile Security Practice

Overview & Case Study

AdaptiveMobile's Security Practice provide a suite of managed security services – undertaking analysis of potential threats in networks and delivering customized configurations and security cartridges containing profiles of active & potential attacks.

These services are provided using AdaptiveMobile's network-centric security software platform NPP, which gives operators the ability to identify threats from compromised devices connecting to their network, the ability to surgically control application traffic flows for selected devices in real time and to interact with subscribers to resolve the threat.

Advanced Threat Detection

Detecting new advanced mobile treats and exploits

Dark Data Forsensics

Global security network leveraging our unique insight from 30 billion dark data events and one billion mobile subscribers a day

Actionable Intelligence

Continual Signature updates to our platforms across the globe and delivery of enhanced security offerings to operators

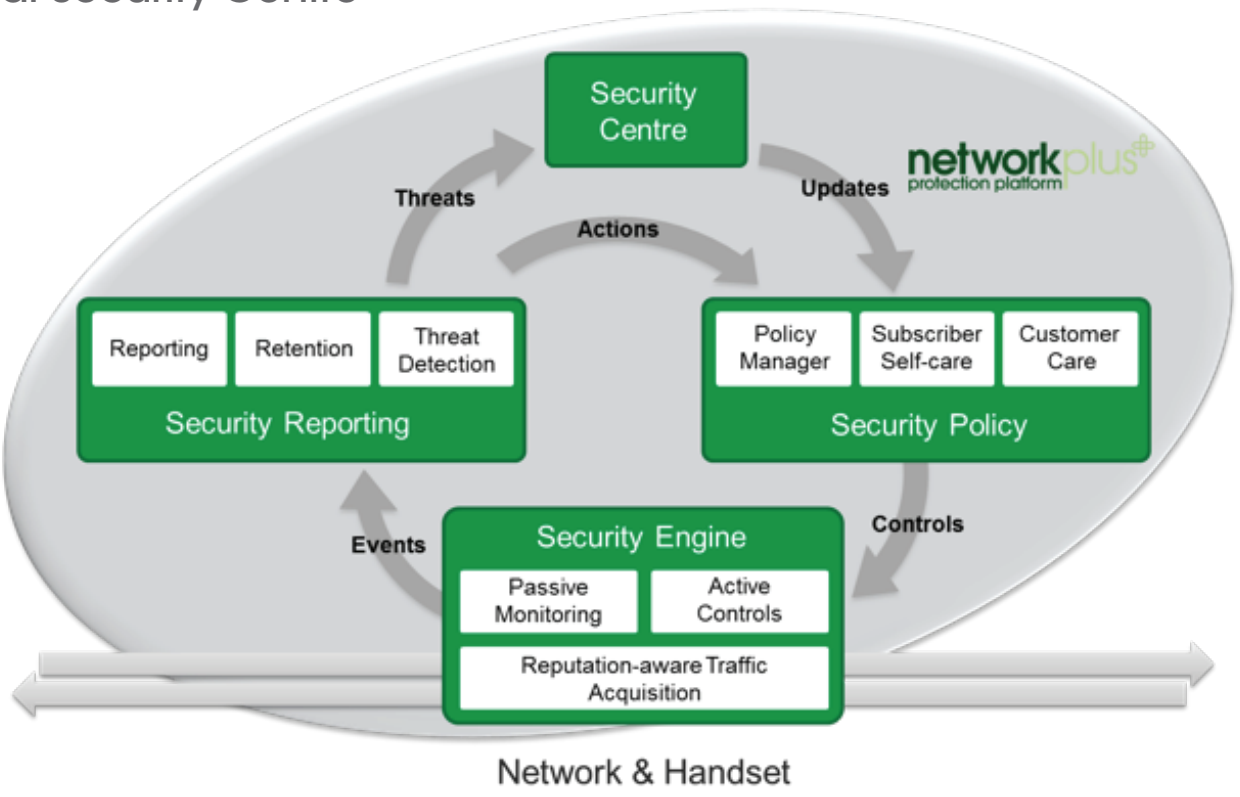
Our unique approach to security within networks – whether mobile, Wi-Fi, DSL or cable – is built upon four core principles:

- **Security Analytics:** the continual correlation of events across different application services in order to detect new threats and compromised devices.
- **Behavioral Reputation:** building and maintaining a set of reputation attributes for each device connecting to the network, influencing how traffic will be manipulated, and the subscriber experience.
- **Surgical Control:** the ability to dynamically select traffic from specific devices or for specific services for active real-time filtering while allowing traffic from uncompromised users to flow without additional latency.
- **Individual Granularity:** being able to scale to deliver individual level granular controls for hundreds of millions of subscribers, allowing for parental and corporate self-care within the network.

The Global Security Practice collates statistics, suspect traffic profiles, and subscriber reports; and generates new threat signatures and threat analysis engines that are automatically updated within each network deployment.

The Security Practice has a unique real-time insight in to Global Mobile Threats with unparalleled sources of data to identify and analyse, to deliver protection and provide informed statements on emerging trends in attacks, phishing and spam. In addition to delivering appropriate security databases and configurations for threat response, the Security Practice, using the Global Security Centre product, also provides intelligence on sources of attacks and the cross border exploitation of service boundaries (Multiple bearers, OTT services and inter-provider).

Global Security Centre



Service Offerings

AdaptiveMobile Security Practice provides three service packages, aimed at meeting the specific needs of various operators requirements.

Bronze Service

A service for operators who want to address known Spam in their network.
Note this is only applicable to those operators who have an established customer feedback system in place for spam as service configuration is driven primarily by received customer complaint feedback.

Service suits typically inbound off-net (MT) traffic deployments.

Functional Components	Includes	Requirements upon Operator	Delivery
Global Fingerprints	Known call to actions (blacklists, numbers) and fingerprints	None	Automated Cartridge feed from existing Security Centre. Typically 1 update per month.
Subscriber Submitted Fingerprints	Collection of operator's subscriber spam reports (e.g. SRS, 1909 etc.) data and delivery as a fingerprint feed	Operator to provide regular feed of data, either via flat file, via AdaptiveMobile specified SMPP interface into AdaptiveMobile Security Centre, or direct from MO traffic routing to Shortcode.	Automated Cartridge feed from existing Security Centre. Frequency determined by submission profile
Active National Spam Fingerprints	Known high impact spam campaigns with triggered activity in network	System integration to AdaptiveMobile Security Centre	Automated Cartridge feed
Quarterly Security Reviews	Review calls of overall trends and spam activity.	Mutually available schedule	For initial period calls once per week for the first 6 weeks. Then every 2 weeks until end of first quarter After first quarter, call once every 3 months

Silver Service

For those operators who need to address both Spam and Unsolicited Commercial Communication

Service configuration is based upon specific suspicious traffic measured within the network, so the operator can be sure that the profile of spam seen specifically within their network is addressed.

Service suits both on-net (MO) and off-net inbound (MT) protection.

Suitable also for markets where no subscriber spam complaint mechanism exists.

Service includes all Bronze capabilities plus:

Functional Components	Includes	Requirements upon Operator	Delivery
Active Defence	Active monitoring of traffic to find current campaigns active & active spammers both on-net and inbound.	None Security Practice recommend filter configurations, and analyse resultant triggered traffic	Cartridge feed of Fingerprints Cartridge feed of Blacklist URL's Configuration of PMC filters
Operator Specific (Active Discovery) Fingerprints	Identification of new spam attacks and creation of new fingerprint sets that applies to that specific operators network.	None Active monitoring of suspicious traffic, Fingerprints delivered as spam discovered & validated	Cartridge feed
Fortnightly Security Review	Routine detailed review with Operator covering: - spam campaigns active - spammers of interest - new & emerging security threats - recommendations on system configuration evolution	Mutually available schedule	For initial period calls once per week for the first 3 months. Then every 2 weeks.
Additional System Tuning	Delivery of additional filters, policies and filter configuration refinements to address changes in spammer behaviour analysed	Review of results and endorsement of changes	Ongoing PMC access Cartridge feed of appropriate components
Abusive Spammer Detection	Determination of spammers who have exceeded agreed thresholds or specific service usage profiles. Utilising analysis of traffic, subscriber activity and reputation, specific subscribers can be identified that are sending spam volumes in excess of an agreed threshold.	Requires systems and data access to PMC, TSM / Analytics (Quarantine) & Reporting	Supply of subscriber details or automatic configuration of system Blacklist

Gold Service

Designed for those Operators who are seeking to fully address all forms of SMS abuse in their network including Spam & Unsolicited Commercial Communication.

Commonly taken by Tier-1 operators & those in specific regulatory environments.

Service includes all Silver capabilities plus:

Functional Components	Includes	Requirements upon Operator	Delivery
Active Defence	Active monitoring of traffic to find current campaigns active & active spammers both on-net and inbound.	None Security Practice recommend filter configurations, and analyse resultant triggered traffic	Cartridge feed of Fingerprints Cartridge feed of Blacklist URL's Configuration of PMC filters
Operator Specific (Active Discovery) Fingerprints	Identification of new spam attacks and creation of new fingerprint sets that applies to that specific operators network.	None Active monitoring of suspicious traffic, Fingerprints delivered as spam discovered & validated	Cartridge feed
Weekly Security Review	Routine detailed review with operator covering: - spam campaigns active - spammers of interest - new & emerging security threats - recommendations on system configuration evolution	Mutually available schedule	Fortnightly calls with operator
Security Analyst prime	Analysis of reasonable volume of operator queries on spam and abusive subscriber activity. Ongoing consultation on system tuning and network profile.	Prime point of contact for specific spam related queries	Nominated prime point of contact for email queries
Abusive Spammer Detection	Determination of spammers who have exceeded agreed thresholds or specific service usage profiles. Utilising analysis of traffic, subscriber activity and reputation, specific subscribers can be identified.	Requires systems and data access to PMC, TSM / Analytics (Quarantine) & ERM	Supply of subscriber details or automatic configuration of system Blacklist
Spammer Detection Analytics Algorithms	Application of off-line analytics that can determine additional spammer behaviours through post processing of traffic data.	Connectivity / Processing capacity on server	Algorithms provided by AdaptiveMobile Security Practice

Case Study

Delivering Measurable market value

Addressing SMS Abuse: Tier one mobile operator, USA

The low SMS tariffs in the USA created from fierce competition between mobile operators has resulted in North America being the major source of SMS abuse globally[1]. Threat volumes have been such that operators have periodically blacklisted US carriers, which has resulted in customer care complaints for this operator. The operator has taken the Gold package of AdaptiveMobile's Security Practice, which in conjunction with Adaptive Mobile NPP, gives them filtering of SMS traffic to remove spam and frauds before it is delivered to their subscribers or to other operators.

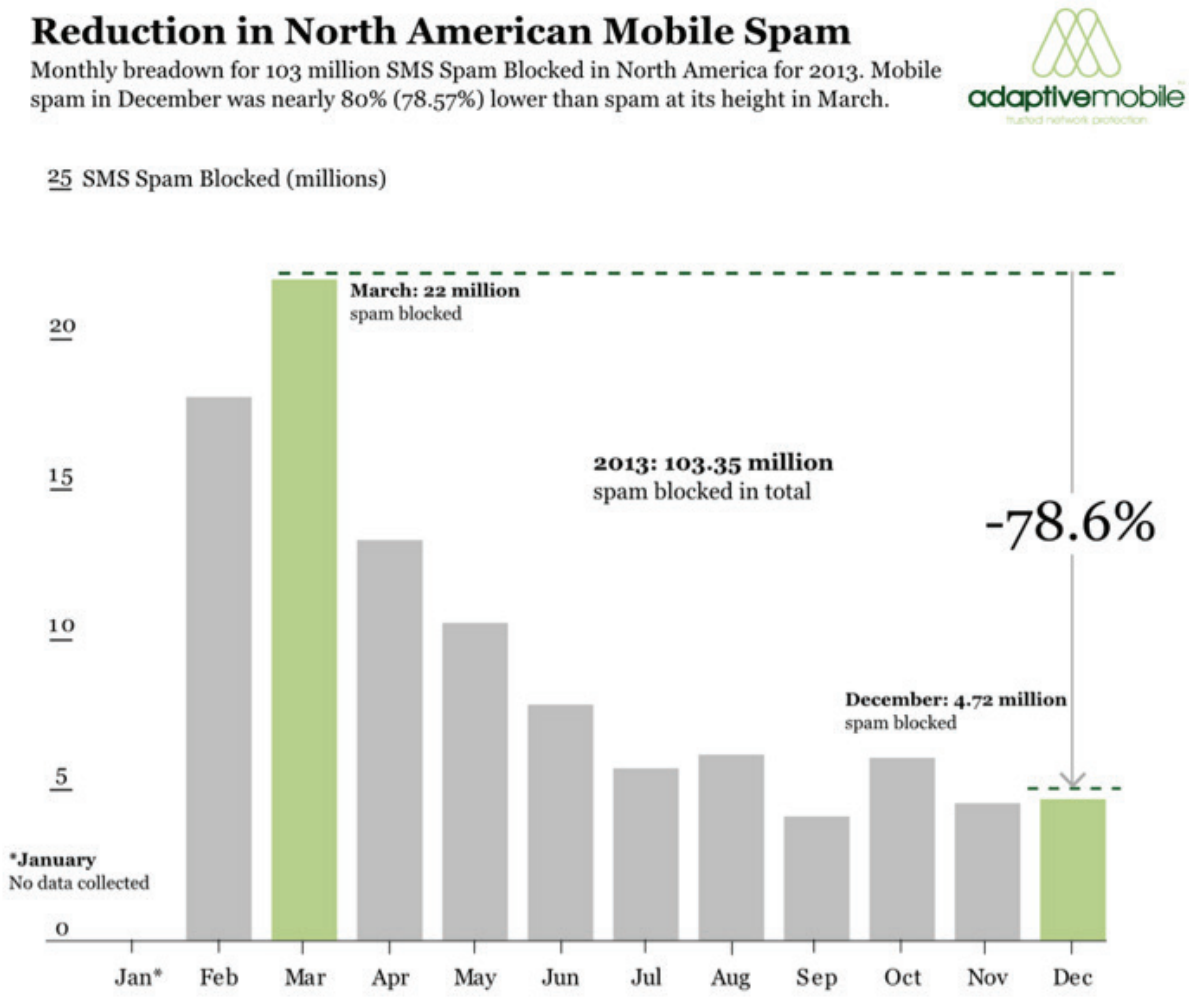
The results include:

- Reduction of 99.9% in on-network generated abuse & spam

- 78% reduction overall in inbound spam to the network

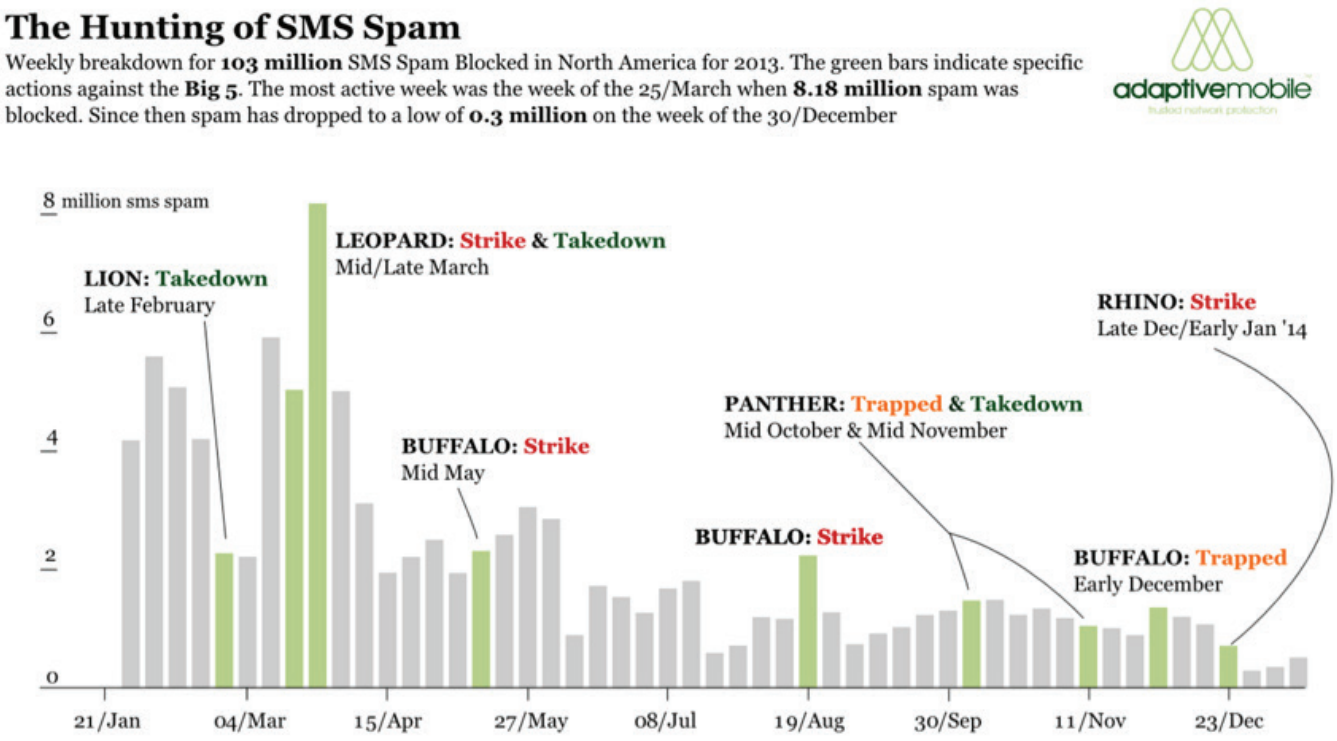
- 98% reduction in customer complaints

This has also achieved significant improvement in the customer experience both in reducing unwanted messaging with consequential revenue and subscriber credit loss and addressing network cell congestion due to heavy spammers. Costs associated with these impacts are known to exceed a million dollars a month.



[1] *Adaptive Mobile, US SMS Spam Ecosystem, December 2012*

The diagram below illustrates the nature of spammers, the activities undertaken by AdaptiveMobile Security Practice to counter their activities, and the successes achieved. The results of these activities can be seen in the following section.



AdaptiveMobile's Security Practice, in conjunction with NPP is the most effective platform globally for addressing mobile messaging spam because:

- The results are the blocking of messages known to be spam/fraud, preventing false positives which would result in lost revenue and customer complaints
- We identify new suspicious SMS patterns, including identifying SIM banks and spammers that are operating campaigns across multiple devices
- We identify persistent spammers and dynamically respond, blocking or quarantining messages; throttling or restricting service for the device
- We provide a global review mechanism that correlates information on suspect new threats from this operator with those from other operators, to produce and disseminate new fingerprints
- Operators retain the ability for local control to decide which variants of spam should be blocked for all users; and to offer individual users the ability to set their own policies for greater protection.

The results above are representative of the effect that AdaptiveMobile's Security Practice services achieve in networks worldwide.

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

www.adaptivemobile.com

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.

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