



AdaptiveMobile Threat Intelligence Service

Overview

AdaptiveMobile's Threat Intelligence Service provide a suite of mobile 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 Forensics

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

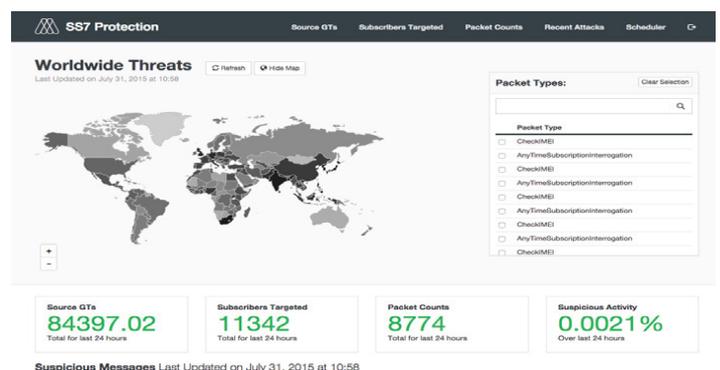
Our unique approach to security within networks – whether mobile, Wi-Fi, DSL or cable – is built upon four core principles:

- **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.

Threat Intelligence Services

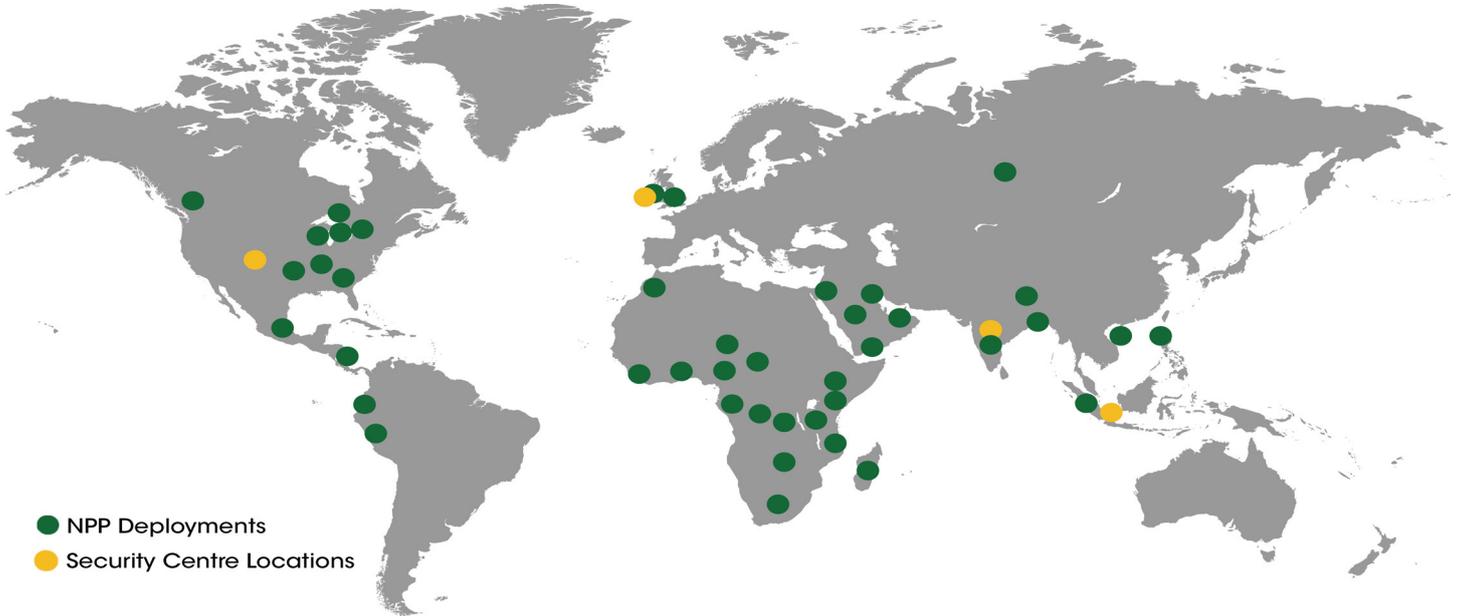
AdaptiveMobile Threat Intelligence Unit provides services for Messaging Security, Messaging Revenue Assurance and Signalling Protection. These consist of three Messaging Abuse Prevention service packages, a SIM Bank Detection service package, a Grey Route Controls service package, and two Signalling Protection service packages, all aimed at meeting the specific requirements of various operators.

All services are provided using AdaptiveMobile's network-centric security software platform NPP



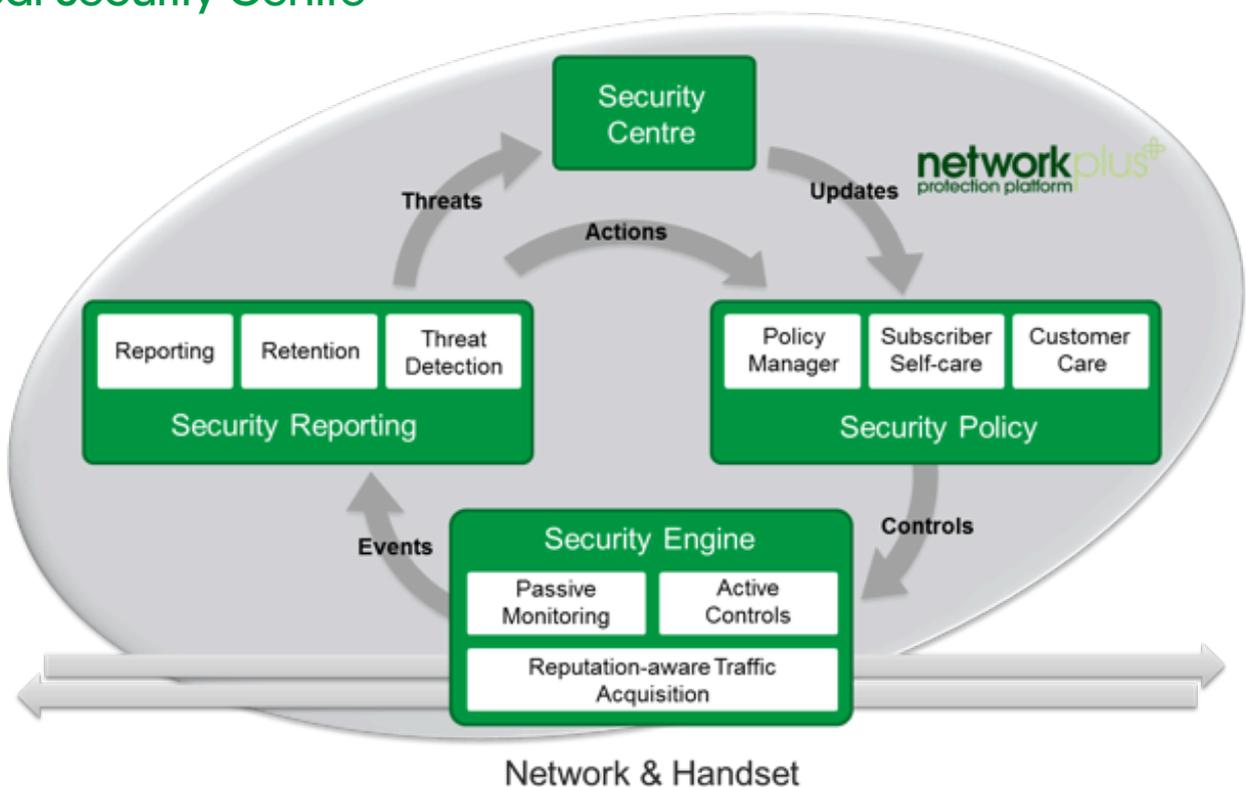


The Threat Intelligence Service collates statistics, suspect traffic profiles, and subscriber reports from around the world and generates new threat signatures that are automatically updated within each network deployment.



The Threat Intelligence Service 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 Threat Intelligence Service, using the Global Security Centre, 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





Messaging Security Services

Messaging Abuse Prevention - 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 or where there is an existing Silver Service customer in the country who is feeding the Security Centre.

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

Messaging Abuse Prevention - Silver Service

A 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. Service includes all Bronze capabilities

Messaging Abuse Prevention - Gold Service

A 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 and Bronze capabilities:

Messaging Revenue Assurance Services

SIM Bank Detection Service

A service for operators who want to address SIM Banks that are present in their network.

SIM Banks are groups of numbers that send service or marketing content to large amounts of recipients. The recipients may typically be subscribers, such as App users receiving authentication codes via SMS. The SIM Bank traffic may go both nationally and internationally, however, it does not use the appropriate business solution set up by operators. This causes extra and unnecessary termination fees for the originating operator, especially for international traffic.

The content of SIM Bank traffic may consist of marketing and service messages. However, as the people who operate the SIM Bank are only providing the delivery service, there may be messaging abuse traffic included.

The AdaptiveMobile SIM Bank Detection service focuses on detecting and blocking international SIM Bank traffic, forcing traffic onto legitimate routes that can then be properly controlled and charged for by the operator.

Grey Route Controls Service

A service for operators who want to control grey routes in their network.

Grey Route traffic occurs where commercial messages are carried over connections where the receiving operator is not getting paid appropriately.

Incoming grey route traffic from other operators is typically service or marketing content that has been initially sent via least cost SMS aggregator channels, much of which bypasses the operator's normal business charging processes. By controlling the incoming flow of this grey route traffic the operator can identify missed revenue, as well as build closer account relationships with the brands who initially send these messages and require their SMS services.

The AdaptiveMobile Grey Route Controls Service focuses on detecting and blocking international grey route traffic. AdaptiveMobile's Threat Intelligence Service using the Network Protection Platform can identify and control grey route traffic: using in-network controls, subscriber reputation and advanced discovery and detection algorithms, forcing traffic onto legitimate inbound routes that can then be properly controlled and charged for by the operator

Please refer to the Grey Route Controls Service Overview document for more detail on this service.



Signalling Protection Services

A service for operators who want to protect their subscribers and networks from a growing range of new threats now made possible via easier access to the signalling network. The AdaptiveMobile Threat Intelligence Unit complements the deployment of Signalling Protection to offer a set of services that meets operators needs to tailor to best understand defence and react to suspicious signalling activity using extensive expertise in signalling and mobile security.

The Signalling Security Analysis & Tuning Service Package is designed specifically to support security and fraud departments by allowing them to use the experience of the AdaptiveMobile TIU to commission an initial in-depth analysis of the current signalling network and any particular threats that their network may be experiencing, in order to identify and implement custom rules and procedures to address those threats, as well as other activity for the operator to monitor.

The Signalling Security Investigation and Diagnosis Managed Service Package is designed for operators to get the unique experience and expertise of the AdaptiveMobile TIU to help assist in the follow-up investigation of suspect or confirmed attacks over the signalling network, and to help plan countermeasures and changes to the rulesets as appropriate to respond to new scenarios. For the Managed service, operator staff can log incidents for review via a shared incident tracking system.

Signalling Security Analysis & Tuning Service Package

- Analyse current signalling traffic for a client network, both inbound and outbound to determine current characteristics & threats to address by the Signalling Protection Solution
- Present detected suspect and abnormal signalling activity to Mobile Operator to review and discuss
- Advise and recommend Signalling Protection rules and strategy to implement - based on the operators' network, current traffic and accepted risk profile

3 Hours of Signalling Security Investigation and Diagnosis Managed Service are included to address incidents raised

Signalling Security Investigation and Diagnosis Managed Service Package (80 Hours)

- Analyse the Security Alerts raised by customer, to identify potential incidents. .
- Investigate internally or in conjunction with the operator, to determine whether observed activity is expected or potentially suspicious, depending on the operators' own network setup
- Update Signalling Protection rules to mitigate future Incidents, where agreed.

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: +44 207 049 0421
Middle East Sales: +97144 33 75 83
Africa Sales: +27 87 5502315
Asia Sales: +65 31 58 12 83
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: +1 877 267 0444
Latin America: +52 5584211344

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

