ENEA
AdaptiveMobile Security

SERVICE OVERVIEW

# AdaptiveMobile Threat Intelligence Unit

## AdaptiveMobile Security's Threat Intelligence Unit (TIU) provides a suite of mobile security services, undertaking analysis of potential threats in networks and delivering customized configurations and security cartridges containing profiles of active and potential attacks.

These services are provided using AdaptiveMobile's Industry-leading Network Protection Platform (NPP), which gives operators the ability to identify threats on 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

**Uncovering new and emerging advanced mobile threats and exploits to messaging and signalling traffic**

### Dark Data Forsensics

**Global security network leveraging our unique insight from 10's of billions data events and over 2 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 operators' networks is built upon four core principles:

### Security Analytics

The continual correlation of events across different application services and protocols in order to detect new complex messaging and signalling threats seen across the globe.

### 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.

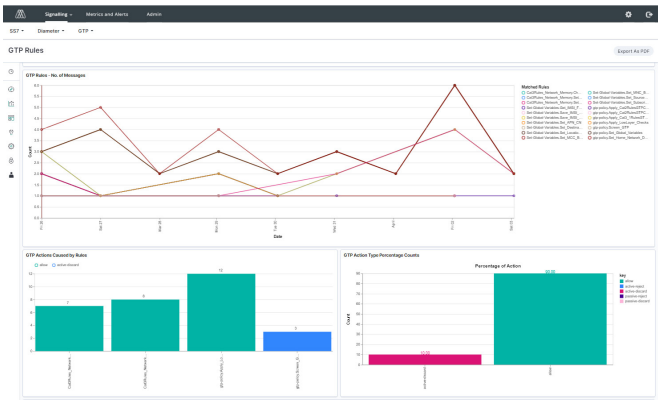
### Behavioral Reputation

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.

### Advanced Intelligence

The development of best-in-class, industry-leading, proprietary algorithms to discover the latest threats and enable faster identification and prevention of new attacks.

# Threat Intelligence Services




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

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

The Threat Intelligence Unit 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 Unit 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 Unit, 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

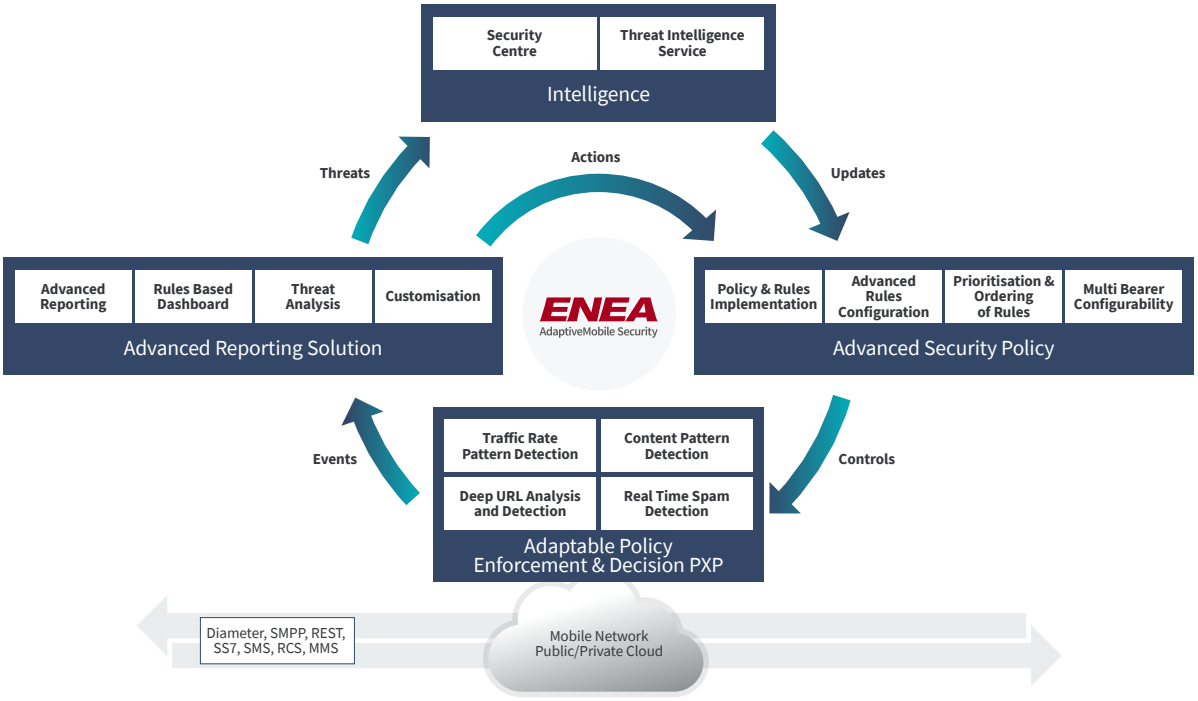



Figure 1 – AdaptiveMobile Network Protection Platform

## Messaging Security Services

### Messaging Abuse Prevention Service

Mobile messaging abuse (often called Spam) is messaging sent over mobile channels that is classified as messaging that is Bulk and Unsolicited, from the perspective of the recipient. As well as being personally harmful and dangerous to the recipient, this type of messaging normally constitutes a violation of the sending or receiving networks Terms & Conditions regarding the use of the mobile device, as well as local statues and laws.

Messaging Abuse or Spam, are messages that are sent by various groups, ranging from and including:

- simple over-aggressive marketing companies whose recipients have not signed up,
- payday loan merchants trying to push aggressive loan products,
- phishers who are trying to phish login details for websites,
- bank account attackers, trying to fool user into ringing up automated helplines in order to gain access to their accounts.

There can be many various forms of spam in between as well. Others types of messaging abuse can include mobile handset infected with mobile malware, sending out spam on behalf of a worm, to ‘attack’ messages being sent from one device to another, in the hope of disabling it.

The TIU Messaging Abuse Prevention Service is designed to allow a customer to deal with 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.

Please refer to the Messaging Abuse Prevention Service Description documents for more detail on this service.

# 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 and SIM Bank Service Description documents for more detail on these services.

# 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 SS7, Diameter and GTP-C networks.

The AdaptiveMobile Threat Intelligence Unit's services complement the deployment of the AdaptiveMobile Signalling Protection product. The TIU offers a set of services that meets operators' needs to best understand, defend and react to suspicious SS7, Diameter and GTP-C activity using AdaptiveMobile's extensive expertise in signalling and mobile security.

## Signalling Security Analysis & Tuning Service

The Signalling Security Analysis & Tuning Service Package is designed specifically to support security and fraud departments in their initial deployment of the signalling firewall. It allows them to use the experience of the AdaptiveMobile TIU to commission an initial in-depth analysis of the current SS7/Diameter/GTP-C network and any particular threats that their network may be experiencing, following deployment of SS7/ Diameter/GTP protection. This will enable them to identify and implement custom rules and procedures to address those threats.

## Signalling Protection Baseline Service Package

The Signalling Protection Baseline Service Package provides operators with a quarterly review of the signalling firewall performance by AdaptiveMobile's TIU, on top of the standard platform support, to help plan countermeasures and changes to the rulesets as appropriate to respond to new scenarios. A quarterly report is issued to the operator recommending configuration changes on the existing platform as well as details of new scenarios which should be addressed. Configuration changes are applied on request by AdaptiveMobile Technical Support as part of the standard support contract.

## Signalling Protection Subscription Service Package

The TIU Signalling Protection Subscription Service Package is designed for operators to get the unique experience and expertise of the AdaptiveMobile TIU to assist in the follow-up investigation of suspect or confirmed attacks over the SS7, Diameter and GTP-C networks, and to help plan countermeasures and changes to the rulesets as appropriate to respond to new scenarios. For the service, operator staff can log incidents for review via a shared incident tracking system

Please refer to the Signalling Protection Service Description document for more detail on these services.

## About Enea AdaptiveMobile Security

Enea AdaptiveMobile Security is a world leader in mobile network security, everyday protecting over 80 Mobile Operators and billions of mobile subscribers and devices globally from fraudsters, criminals and nation states. We have the strongest 5G core network security team, who are designing, planning and building the very best in 5G core network security solutions focussing on threat-intelligence, security heritage and protocol correlation.

Enea AdaptiveMobile Security brings a unique security perspective on real-time mobile network traffic. The global insight provided by our 5G, Signalling and Messaging thought leaders, security specialist teams and Threat Intelligence Unit, combined with our signalling and network protection software that sits at the heart of the network, ensures Enea AdaptiveMobile Security remains at the forefront of the latest advancements in mobile networks and their security, and continues to be the trusted partner of many of the world's largest Mobile Operators.

For more information on how Enea AdaptiveMobile Security can help you protect your communications infrastructure, subscribers and revenues, please contact **sales@adaptivemobile.com**.

### Legal Notices



**HEAD OFFICE**

Ferry House, 48-52 Lower Mount St, Dublin 2.

Contact: sales@adaptivemobile.com

**www.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: +44 208 584 0041

Ireland: +353 1 514 3945

India: 000-800-100-7129

US, Canada: +1 877 267 0444

LATAM: +525584211344