CLOUDMARK®

Mobile Messaging Threats and Requirements for Security Solutions

CLOUDMARK®

CONTENTS

MOBILE MESSAGING SECURITY LANDSCAPE

Mobile messaging generated 130 billion USD in worldwide revenues in 2008 and this figure continues to grow rapidly. As subscribers increasingly rely on their mobile phones for everyday communications, mobile applications and financial transactions, they become an attractive and lucrative target for attackers.

Mobile messaging threats affect the entire mobile ecosystem, causing significant costs and headaches to both operators and subscribers. Abusive traffic is costly for operators, wasting valuable network resources, increasing customer support costs, and threatening subscriber adoption of future mobile services. Subscribers are directly impacted by receipt of malicious messages and expect their operators to provide a secure mobile experience. As mobile operators develop value added services to enhance their revenue stream, they must preserve and foster a trusted user experience for their subscribers through effective messaging security solutions.

CLOUDMARK MOBILE PLATFORM

Cloudmark Mobile Platform is a high-performance, carrier-grade messaging security solution that provides real time threat intelligence from global sources and offers content and subscriber level policy controls to effectively combat messaging threats. It enables operators to combat ever-growing mobile messaging and security threats as they occur without any service interruption or manual operator involvement.

Backed by a unique and powerful combination of Advanced Message Fingerprinting and real-time feedback from the Cloudmark Global Threat Network, Cloudmark Mobile Platform is able to rapidly detect all categories of mobile messaging security threats before they reach the subscriber.

Cloudmark Mobile Platform solution provides operators with the technology, tools, and expertise to protect subscribers from sophisticated messaging attacks and threats.

Benefits

Broad Protection from all Forms of Mobile Threats

Cloudmark Mobile Platform offers protection against all categories of mobile messaging threats from the Internet as well as SMS message spam from internal or external mobile networks. Since Cloudmark's core fingerprinting technology is format and content agnostic, it is capable of detecting spam, fraud, phishing and virus attacks that arrive in any format, such as email, SMS messages, MMS messages or binary attachment. It can also detect messaging threats and fraud in any language, including those using double-byte characters.

Enables Customizable Subscriber Experience

Cloudmark Mobile Platform supplies operators with the foundation to offer new value-added security services based on subscriber controls, such as advanced parental controls for child protection.

Protects the Operator Network and Provides Operational Efficiency

Cloudmark Mobile Platform reduces abusive traffic and maintains stability. Operational resources are freed up from addressing fire-drills and customer complaints related to messaging attacks.

Provides Network Control and Visibility

Cloudmark Mobile Platform provides operators with broad visibility into their network so that effective policies to mitigate messaging attacks and threats can be created.

KEY FEATURES

Carrier-class Performance and Scalability

Cloudmark Mobile Platform is architected to provide the high scalability and efficiency that operators require. The lightweight nature of Cloudmark's Advanced Message Fingerprinting technology enables extremely high message throughput enabling more efficient utilization of operator infrastructure together with lower operational expenses.

Automatic Threat Intelligence Updates

Cloudmark Mobile Platform offers the industry's most effective messaging security protection, stopping new threat outbreaks in real time without requiring any operator intervention.

Cloudmark Mobile Platform automatically receives threat intelligence updates every 15 seconds from the Cloudmark Global Threat Network – providing the latest threat updates for the:

- **Content filtering service (Cloudmark Authority®)**
- **Sender intelligence service (Cloudmark Sender Intelligence)**

With Cloudmark Mobile Platform, operators can identify malicious senders and content before attackers can impact the network or subscribers.

Intelligence-based Routing Decision

Cloudmark Mobile Platform handles inspection of all message attributes and content. Operators can specify one of several routing actions to take on messages that match a policy including Block, Allow and other routing actions.

Policy Definition and Enforcement

Cloudmark Mobile Platform offers various policy-based traffic control and monitoring, enabling operators with multiple ways to control and monitor traffic and mitigate the risk of threats. This includes, Protocol Control Policy, Content Control Policy and Subscriber Control Policies.

High Accuracy in Detecting SMS Spam

Traditional heuristics and rules-based solutions look for recurring patterns within a message and other trends. With a maximum limit of 160 characters, an SMS message doesn't provide much data to analyze for these types of solutions. In addition, competing solutions look for high volume outbreaks but overlook targeted attacks.

Cloudmark Mobile Platform employs a combination of Advanced Message Finger-printing algorithms, honeypots and corroborated user feedback to provide the most accurate coverage for SMS attacks. Compared to solutions that apply static rules or message volume thresholds to identify threats, Cloudmark Mobile Platform enables much higher accuracy in detecting the spam.

Text Agnostic

Cloudmark's unique text-agnostic threat analysis enables Cloudmark to stop spam in all languages (including those using double-byte characters such as Chinese, Japanese and Cyrillic) and formats, including image, SMS and MMS spam.

Advanced On-Net/Off-Net Threat Detection

Cloudmark Mobile Platform complements existing anti-spoofing, flooding and faking solutions that may be deployed in an operator environment and goes beyond protocol level controls that counteract signaling fraud between mobile networks to also catch mobile attacks that have already entered in the networks.

Centrally-Managed Policy Control

Cloudmark Mobile Platform provides centrally managed, single-point management for policy definition, analytics, reporting and configuration.

Traffic Analysis

With Cloudmark Mobile Platform, operators can select to log a copy of the entire message for later review. The logging functionality includes several configuration options to limit how many copies of a message are kept and to automatically age out messages after certain duration.

Seamless Integration

Cloudmark Mobile Platform seamlessly integrates into the mobile network without risk of service disruption. It integrates with the operator's operations and business support systems incorporating subscriber policy settings and other information into message handling policies.
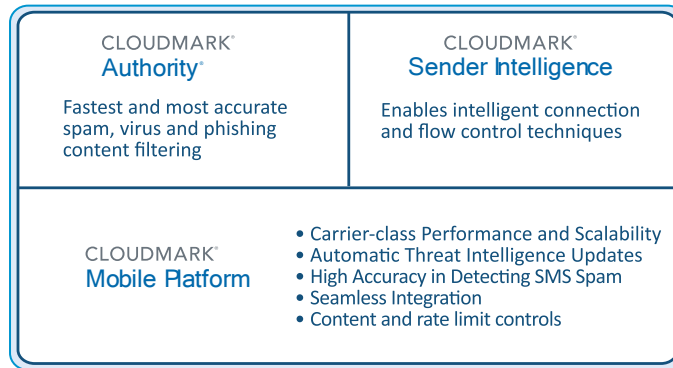
Detailed Reporting for Mobile Operators

Cloudmark Mobile Platform Management Console includes detailed reports on traffic across all nodes in the cluster.

In addition, the Cloudmark Network Feedback System provides mobile service providers with visibility into filtering performance, as well as insight into customer feedback with detailed daily, weekly and monthly statistical reporting. This system provides operations and management with a clear picture of subscriber issues, threat trends and the overall effectiveness of the Cloudmark solution.

SYSTEMS OVERVIEW

Cloudmark Mobile Platform is a high-performance carrier-grade messaging security solution that combines global threat detection with local policy control capabilities. Cloudmark Mobile Platform is comprised of the following major components, detailed descriptions of each are provided after the figure.

- **Protocol Control Policies**
  Protocol policies enable operators to set controls based on attributes of the message outside of the content or based on volume patterns over time, such as rate limiting, throttling or controlling the delivery of certain types of messages.

- **Content Control Policies**
  Content policies allow operators to control how messages are delivered based on the contents of the message including keyword filtering and other content analysis.

- **Security Services**
  Cloudmark Mobile Platform Security Services include a suite of threat intelligence services that provide real time updates from the latest information about threats occurring globally. These services provide the industry's most effective messaging security intelligence, stopping new threat outbreaks in real time without requiring any operator intervention.

  - **Cloudmark Authority®,** an automated content filtering service is essential to automatically detect and block evolving mobile messaging attacks that elude basic filters, policies and manual response. Cloudmark Authority delivers automatic protection and real time updates to mobile operators.

  - **Cloudmark Sender Intelligence** provides operators with valuable data and visibility into mobile sender reputation within and outside of their network. This comprehensive sender reputation service allows operators to proactively prevent attacks and fraud from known malicious senders.

- **Operator Data Access**
  The operator data access component of Cloudmark Mobile Platform provides a central point of access to an operator's subscriber data such as user preferences and business logic to be leveraged as part of Cloudmark Mobile Platform policies.

CLOUDMARK® **Authority®** Fastest and most accurate spam, virus and phishing content filtering	CLOUDMARK® **Sender Intelligence** Enables intelligent connection and flow control techniques
CLOUDMARK® **Mobile Platform**	• Carrier-class Performance and Scalability • Automatic Threat Intelligence Updates • High Accuracy in Detecting SMS Spam • Seamless Integration • Content and rate limit controls

- **Network Integration**
  Cloudmark Mobile Platform seamlessly integrates into the mobile network without risk of service disruption. It is designed for high availability and to scale horizontally. It can integrate as a call-out function with the existing SMSC, SMS Router, STP or Signaling Gateway.

  Cloudmark Mobile Platform integrates with the operator's operations and business support systems incorporating subscriber policy settings and other information into message handling policies.

  With Cloudmark Authority automated content filtering service and the Cloudmark Sender Intelligence service, Cloudmark Mobile Platform also receives automated updates every 15 seconds —providing the latest threat updates for content filtering and blocking of malicious spam sources.

- **Cloudmark Mobile Platform Management Console**
  Cloudmark Mobile Platform Management Console is a web-based management console that offers a single, central management point to control the configuration and policies on all nodes/servers. It enables customer administrative, operations and abuse teams to monitor threat trends and implement new messaging rules and offers a view into the system's configuration, with all the underlying logic for various services via operator configured workflow elements.

  Cloudmark Mobile Platform Management Console provides operators with a management dashboard including several automated reporting tools for a view into the amount of threats that are on the network at any given time and with the data necessary to investigate any threat outbreaks.
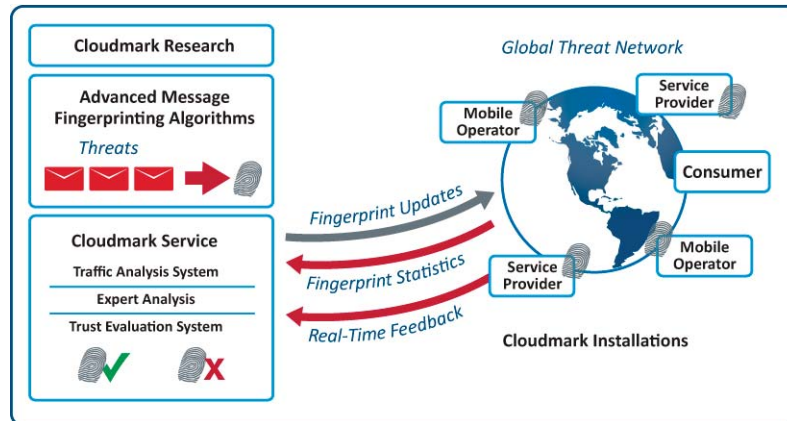
Figure 2: Cloudmark Global Threat Network System

TECHNOLOGY OVERVIEW

The technology components and automated processes underpinning Cloudmark Mobile Platform drive the system's high accuracy and efficiency. Cloudmark leverages a combination of sophisticated message fingerprinting algorithms, the world's largest threat detection network (the Cloudmark Global Threat Network), traffic pattern analysis and a trust evaluation system that analyzes and corroborates all feedback unlike any other in the industry. This enables Cloudmark to stop all forms of messaging threats with the industry's highest level of accuracy while minimizing infrastructure and operational costs.

Cloudmark Advanced Message Fingerprinting Algorithms

Over the years, Cloudmark has developed a set of intelligent fingerprinting algorithms to identify and track spam, phishing, fraud, virus and other malicious attacks throughout the network. Cloudmark's fingerprinting algorithms (now in their sixth generation), work in tandem to target different threat attributes embedded in a message and have the ability to identify all mutations in a given attack, such as changes in content, image, sender, URL, or other attributes, so that threat variants are stopped in zero time – before they are transmitted to mobile subscribers.

Cloudmark Global Threat Network

The Cloudmark Global Threat Network, consisting of over one billion reporters in 190 countries, is based on the premise of networked collective intelligence. Members of the Global Threat Network span mobile operator abuse teams, systems administrators, automated spam traps and end users. The millions of Global Threat Network reporters who provide real time feedback help enable Cloudmark to block the latest threats typically within minutes of attack origination. This approach contributes to faster detection of threats and more accurate classification of messages.

6

Trust Evaluation System

All feedback sent to the Cloudmark Global Threat Network is corroborated and analyzed in real time by the Trust Evaluation System. The Trust Evaluation System tracks the reputation of each reporter and determines a known threat message based on the several attributes surrounding the reporter and a fully automated data analysis process that is also designed to correct any inaccuracies based on continuous message corroboration.

For more information
visit us at www.cloudmark.com

Americas Headquarters	**Asia Pacific Headquarters**	**Europe Headquarters**
Cloudmark, Inc.	Cloudmark, Inc.	Cloudmark Europe Ltd.
San Francisco, USA	Singapore	London, UK