Cloudmark Platform For Mobile

Understanding Cloudmark's Carrier-Grade SMS Security Capabilities

Tolly Report #221135
Commissioned by
Cloudmark, a Proofpoint company

November 2021

Executive Summary

For decades, email users have had to contend with junk mail as well as dangerous messages showing up in the inbox. The deluge of nuisance and malevolent messages that have targeted email users also now target SMS users: spam, malware, phishing, and social engineering. According to a study by Tessian Ltd, the increase in work-from-anywhere has triggered an increase in security attacks[1].

The problems are manifold for both the mobile network operator (MNO) and the user. Studies have shown that users are more likely to read and interact with SMS messages than they are with email. A compilation of industry statistics by VoiceSage noted that 82% of people said that they open every text compared to 20% of their emails[2]. The same sources noted that 19% of SMS links are clicked compared to a mere 2% of email links. Thus, the exposure to harm is higher at the user level with SMS. For an MNO, delivering spam and abuse negatively impacts customer satisfaction and revenue potential. Effective SMS[3] security translates not only to safety for your users but provides a positive impact on your bottom line.

Legitimate traffic can present challenges as well. Application-to-Person (A2P) SMS traffic continues to grow. Unfortunately, some users attempt to bypass higher A2P message charges by sending this traffic on Person-to-Person (P2P) communications routes. This practice, known as using "grey routes," deprives the MNO of legitimate revenue.

Since its founding nearly two decades ago, Cloudmark's core focus has been messaging security. Over that time Cloudmark has built a security solution that leverages both artificial intelligence (AI) and machine learning (ML) to enhance and automate message security. Cloudmark supports various mobile messaging standards including SMS, MMS, and Rich Communications Services (RCS) messaging.

Cloudmark solutions are highly flexible, enabling quickly deployable integrations that utilize a combination of technologies to detect a variety of traffic attributes such as the ones found in nefarious and complex smishing[4] attacks. Cloudmark leverages functionalities including machine learning and predictive artificial intelligence, along with novel algorithms and technology for message and content fingerprinting, call-to-action/URL analysis, and threat data from the Cloudmark Global Threat Network.

Additionally, Cloudmark's Spam Reporting Service (SRS) ensures that Cloudmark solutions incorporate direct user feedback to assure accuracy in the detection of spam, fraud and smishing. Altogether, this means the Cloudmark Platform for Mobile provides

[1] https://www.tessian.com/research/the-future-of-hybrid-working/

[2] https://www.voicesage.com/blog/sms-compared-to-email-infograph/

[3] For simplicity, this paper will refer to the various message types as SMS. Most discussion also includes MMS and RCS message types.

[4] A term coined to represent "phishing" attacks carried out via SMS.

MNOs with the tools they need to guarantee that only messages that consumers expect, want, and need to receive, are successfully delivered.

Threat Protection & Control

Global Threat Network

The best way to stop a threat is to be aware of the threat. With a global customer base, Cloudmark scans over 15 billion mobile (SMS, MMS, RCS) and email messages daily. Cloudmark's interconnected systems form the basis for the Cloudmark Global Threat Network. Threats detected at one point on the globe are immediately recognized by Cloudmark systems around the world.

Proofpoint's vast network of operators, subscribers, network probes, and registration databases allows Cloudmark to proactively discover and track the reputation of new URLs, domains, and URL shorteners, often before a single message is sent.

Sophisticated Fingerprinting

Just as fingerprints are unique to individuals, Cloudmark builds digital fingerprints to identify threats uniquely and rapidly. Cloudmark can "see through" many spammer obfuscation techniques via fingerprinting. This digital ID is built using both message content and message metadata that includes sender and other message origination data.

Smishing Protection via AI/ML

Many smishing attacks have features in common. These include a "call to action" that would typically include a telephone number or URL. Cloudmark's AI/ML can help determine whether messages with these characteristics are legitimate or fraudulent by evaluating the URL landing page in real time and checking to see if the URL is newly registered - an indicator of smishing.

Similarly, Cloudmark's AI/ML uses knowledge of the message sender's origin and related metadata and tag information to help determine dynamically whether a message is benign or malevolent.

Platform Flexibility & Automation

Ultimately, deciding whether to block or forward a message largely depends upon company policy. That is why Cloudmark provides for users to build their own rules to define those policies for their system. If desired, MNOs even have the ability to set policies to put the Cloudmark Platform for Mobile in a default "distrust" mode[5].

Once in place, the system is automated and responds dynamically to incoming messages and handles each according to the policies in place.

[5] Implementing zero trust (distrust mode) can create extremely high false positives and the blocking many messages that consumers expect, want, and often, need to receive.

Spam Reporting Service - Feedback

In those instances where a spam message is forwarded in error rather than blocked, Cloudmark provides a simple mechanism for the user to report a message as spam/smishing. This information is fed back into the analysis platform.

Policy Compliance & Monetization

Compliance and monetization hinge on acceptable use policies for both content and message routing.

Acceptable Use - Message Content

Some message content is acceptable in certain contexts. Cloudmark analytics provides a window into the messaging traffic that helps companies build policies to match their acceptable use policies.

Acceptable Use - Message Routing - Grey Routes

With message traffic itself, the route it travels might violate your company's acceptable use policy. There are times when bulk messages, which should traverse A2P routes, are intentionally or inadvertently sent over P2P routes that should be used only by low volume individual-to-individual messages. Use of these "grey routes" could both violate your company's acceptable use policy and cost your company money. Bulk message routes typically cost more than individual's P2P SMS service which is most often included with mobile service at no additional charge.

Deployment & Operations

Cloudmark's heritage is in carrier-grade messaging. Thus, it is no surprise that Cloudmark provides carrier-grade availability.

Cloudmark Platform for Mobile can be deployed any way that best suits your needs: cloud, on-premises, hybrid, or managed cloud/multi-tenant.

The solution supports common communications protocols and protects all relevant message types. The solution integrates directly with reporting systems such as Splunk while also supporting open standards such as REST API and SNMP.

Cloudmark can deploy scanning services for customers very quickly. Once deployed, system tuning and configuration will be baselined and updates to meet customers' needs can be done on a daily or weekly basis.

Threat Protection & Control

Knowledge is power when it comes to providing security. The more data points and information a security solution has access to, the more secure it can make the environment. Cloudmark Platform for Mobile leverages many and varied information sources to protect SMS, MMS, and RCS users from junk (spam) and malevolent messages (phishing/smishing, malware, ransomware).

Global Threat Network

Over the course of more than two decades, Cloudmark has built up a global customer base of nearly 30 mobile operators, including many of the largest, tier-1 mobile operators; 100+ Internet Service Providers (ISPs); and 20+ hosting providers; and also receives data from 50,000 connected enterprise networks. That base is leveraged for the benefit of all its customers. Every Cloudmark system is connected to the Global Threat Network. Each system benefits from the threats reported by other systems around the world. Once validated by Cloudmark, emerging threat information can be distributed as a real-time update to other systems, thus improving effectiveness.

For example, a threat emerging in the United Kingdom can be detected, identified, and blocked for a United States-based Cloudmark customer before the business day even begins in the US. And vice versa!

At the core of Cloudmark's protection is support for protecting users from spam, smishing, abuse and fraudulent messages sent by "bad actors" and criminals. Cloudmark can also protect users from Acceptable Use Policy (AUP) violations such as "SHAFT[6]" content.

Mobile network operators and service providers that implement feedback are at a distinct advantage as their end-users are better protected than MNOs which "fly blind" on traffic in their network.

Cloudmark notes that its Global Threat Network is sourced with data from scanning tens of billions of messages based on reputation and content filtering of over four billion messages each day. Threat updates constantly refresh providing near-instantaneous blocking of new attacks. In addition to sourcing from other Cloudmark deployments, the Global Threat Network is supplied feedback from a worldwide customer base using multiple data feeds including the Cloudmark Spam Reporting Service.

Sophisticated Fingerprinting

To stop a threat or intercept spam you must first identify it. You know that, I know that and the senders of SMS spam[7] know that. Cloudmark recognizes that a message is

[6] This acronym stands for sex, hate, alcohol, firearms, & tobacco.

[7] Again, for simplicity "spam" will be used generically to represent both unwanted and malevolent SMS messages. Malevolent messages could represent abusive content, SHAFT violations, smishing and other potentially fraudulent and criminal messages.

suspicious by the content of the message itself or by other underlying characteristics. These characteristics include information related to the sender, message origination, content that the message links to, or other metadata.

Often the first order of business for spam senders is obfuscation - trying to hide the fact that their message is spam.

This can be done in many ways. 10,000 identical messages could be a good indicator of spam, so often the spammer will make minor changes to each message. Similarly, a single number sending the identical message to 10,000 recipients could be a good indicator of spam, so often spammer will use a pool of sending numbers to try to hide what they are doing. Spammers might change the letter "o" to a zero to avoid a dictionary match with common spam terms. The list goes on and on - and expands over time.

To counter both known and future obfuscation techniques, Cloudmark uses a technique it calls fingerprinting in conjunction with its proprietary hashing algorithms. In brief, fingerprinting breaks up the message into different components and uses those components to build out a "hash" value that identifies the message. According to Cloudmark, this approach defeats spammers who try to make minor changes to messages to avoid raising flags.

Importantly, Cloudmark's fingerprinting approach is language- and character set-agnostic and defeats common spamming obfuscation techniques, including using letters from different languages, to try to circumvent detection.

Cloudmark can identify a cluster of messages that, while not identical, are likely part of the same spam campaign. This provides both for better reporting on message activity and enables better enforcement. This improved reporting is valuable to mobile network operators as it provides deep insight into traffic and messages within their network.

Smishing Protection via AI/ML

Messages frequently require deeper inspection to determine whether they may be a threat and should be blocked. Smishing attacks typically contain Calls-to-Action (CTA), these could include URLs, telephone numbers, email addresses, etc. Cloudmark's AI and ML use this CTA data to help determine whether a message is suspect.

If necessary, Cloudmark analyzes the target landing-pages in real-time. Cloudmark determines the likelihood that a domain is fraudulent via the registrar/TLD reputation or age - likely a sign of scam or malevolent messages.

As a smishing attack is frequently more than just a one-off spam message, Cloudmark applies multiple detection strategies to each message interaction. For example, analysis is conducted to determine if the sending pattern of messages is suspicious, even when absent of CTA's, and whether there are suspect leading phrases being used in the text.

Cloudmark also utilizes details of the message sender and the path it travels, in order to ensure that legitimate messages are identified and not blocked (False-Positives).

Increasingly, smishing attacks use human soft/social skills to entrap the victims. Cloudmark tracks Sender/Recipient behavior and linguistic triggers, in order to identify, alert and block this abuse vector, even without CTA included in the message.

Cloudmark has patented, innovative advanced anti-smishing techniques, in order to reduce the footprint of this threat-space, and ensure that end-customers and financial institutions are protected by this MNO service.

Message Sender Route & Tag Information

Identifying a spam message on its own just by viewing it without context can be a challenge. Really, context is everything. By knowing that 10,000 similar, but slightly different messages just went out, from 10,000 different numbers, we now have a good reason to believe that it could be spam. Knowing that the message originates from a trusted sender could mean that the same message is part of a legitimate campaign. Thus, it is important for an SMS security system to track and analyze various pieces of meta-information and "tags" related to a message.

Expanding upon previous remarks, key elements of message information tracked by Cloudmark include message originator, inter-carrier information, sender-type, country, brand, campaign, etc.

If a message arrived via an untrusted sender and has other markings of spam, the AI/ML mechanism can use these factors to determine whether a message is blocked, throttled, or delivered.

Platform Flexibility

As will be discussed in detail in the next section, not all decisions to block or forward a message are immediately straightforward. There are some messages that might appear to be spam but, based on particulars of the sender or recipient, might not be spam. Thus, it is important to be able to integrate a company's own acceptable use policy into the security platform.

Cloudmark provides tools for users to build custom rule sets that "fine tune" what triggers per-operator spam and abuse policies. These policies can be linked to particular users and/or message routes to provide a highly customizable message processing environment.

The platform set-up can be easily configured both during deployment or once in production, in order to address all messaging use-cases; as they are defined, to address existing desired configuration and also to respond to new use-cases or platform requirements. This ensures that the platform can evolve and provides the power to react to new threats or newly invented functionality, for long-term success.

Platform Automation

The platform effectively "runs itself." It reacts automatically to incoming threats, both known and new, to dynamically respond and either block or alert (or log). Allow/Deny policy decisions don't have to be made slowly and manually, the platform simply needs

to be set with the rules chosen by the customer. Messaging traffic is analyzed on-the-fly to filter unwanted traffic automatically.

Custom Operator-Specific Policy is simple to implement, either by utilizing the Fraud-Management GUI to adjust thresholds/actions or via simple cloud-based API control.

Cloudmark abuse and legitimate traffic data-feeds ensure that the platform is always prepared for new messaging threats and bulk traffic, to ensure optimal control and protection.

Multiple clustering techniques group messages, so that the MNO can develop an overall understanding of message campaigns, rather than being unaware of the messaging actors leveraging their own infrastructure.

This ensures that MNO can focus principally on strategic messaging policies, and platform-wide messaging visibility - rather than being forced to constantly manage every unknown campaign messaging spike. This leads inevitably to the ability to maximize platform monetization and reduce exploitation by poor quality messaging partners.

Spam Reporting Service - Feedback

There are times, of course, when a spam message reaches a user before it has been identified and blocked. Cloudmark provides a simple way to provide feedback into the Cloudmark system to notify the system about the missed spam. Originally working with the GSM Association (GSMA), Cloudmark invented and deployed for MNOs the global standard Spam Reporting Service. This service allows users worldwide to report spam and abuse. On select smart-phone devices, users can simply identify spam messages by pushing the spam "button" (1-step reporting). Other multi-step reporting options are also fully supported, enabling all end-users to report spam via forwarding to short code. In the US and UK this short code is 7726 ("spam" on the phone's keypad). That information is then provided to the MNO, fed to the Cloudmark Global Threat Network, and integrated into the spam analysis process.

Policy Compliance & Monetization

When it comes to threat protection, immediate action is required to keep the threat at bay. With compliance some flexibility is in order. That is, take the time to be able to evaluate whether a message violates acceptable use policy. Cloudmark reports, the mobile network operator decides. For legitimate bulk traffic, Cloudmark by default reports transgressions and irregularities relative to agreed policies but doesn't block the message. For person-to-person (P2P) acceptable user policy violations, the message is blocked. Cloudmark allows clients to customize their own approach to violations.

There are several facets to "acceptable use" and they include message content and message routing. Cloudmark provides reporting and analytics to delve into both areas.

Acceptable Use - Message Content

Should messages offering cannabis related products be blocked as spam? The answer is usually, "it depends." In some geographies, cannabis related products might be illegal based on local regulations. In such cases, it would be appropriate to block the messages.

These product messages might be emanating from a known, legitimate source of such products and presented in a manner that complies with applicable laws and operator policies. In this case, the MNO may choose to deliver the messages to their customers. Cloudmark analytics provide the insights that help make these decisions. And, as noted in the prior section, Cloudmark provides the mechanism to enforce policies once they are put in place.

Acceptable Use - Message Routing - Grey Routes

Message traffic is either person-to-person (P2P) or, if the message is part of a campaign, generated by an automated system, or other commercial messaging, it would be classified as application-to-person (A2P) traffic. Because of the volume of messages, A2P traffic is generally governed by specific bulk messaging contracts.

Cloudmark message analytics provide insights into traffic patterns and can identify situations where A2P traffic is inappropriately flowing across P2P routes. Such instances are known as "grey routes." Here too, immediate blocking may not be the desired outcome. Rather, knowledge of this traffic, including information such as volume, rate, and the type of messaging, can be used to contact campaign vendors to rectify the routes being used. In some cases, the grey routes might be from a third-party source with the brand owners unaware of the possible contract compliance issues. Compliance issues could include rate or frequency of transmission, message delivery fees, priority information, or other specific information.

Deployment & Operations

Cloudmark Platform for Mobile can be deployed in your data center, in the cloud or in hybrid approach that includes elements of both. Cloudmark's long history enables it to deliver a solution that provides flexibility to fit the needs of the particular message types, interfaces, and other relevant operator and enterprise requirements including meeting the stringent availability and reliability requirements of tier-1 mobile network operators. Cloudmark Security Operations Center provides 24x7x365 "follow the sun" support. Key deployment and operations elements are summarized in Table 2.

Deployment & Operations Summary

Cloudmark Platform for Mobile

Category	Feature
Proofpoint Operational Excellence	Carrier-grade availability, 24x7x365 follow-the sun support, Cloudmark Security Operations Center
Deployment Options	Cloud, On-premises, Hybrid, Managed Cloud/Multi-Tenant
Communications Protocols Supported	SMS (SMPP, REST, Diameter), MMS (MM1, MM3, MM4, and MM7), RCS, Email to SMS, SMTP
Message Types Protected	MO, MT, A2P, P2P, M2M, 10DLC, Short Code, Email
Out-of-the-box Reporting Integrations	Splunk, ELK, REST API, SNMP

Category	Feature
Platform Requirements	Physical or virtual server environment running RHEL or CentOS
Performance Characteristics	Industry-leading TPS throughput with full-filtering, and sub-5ms average verdicts
Data Feeds	STOP-codes, SRS
Malware Feeds	Cloudmark Authority, Canary, Proofpoint honeypots
Deployment Duration	Full: under six months
	New policy: under four weeks
	Configuration change: under two days

Source: Cloudmark November 2021

Table 2

About Tolly...

The Tolly Group companies have been delivering world-class IT services for over 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

221135-qs1-wt-2021-11-21-VerL