AN INTERVIEW WITH CLOUDMARK, A PROOFPOINT COMPANY

Leading Vendor in Juniper Research's SMS Firewall Providers Positioning Index

JUNIPER RESEARCH

1.1 Introduction to Grey Route Prevention & SMS Firewalls

Juniper Research anticipates that the most significant near-term opportunity for network operators remains with international and domestic A2P (Application-to-Person) services. Historically, mobile messaging protection has been highly focused on safeguarding subscribers, however, increasing new threats also require augmented protection and filtering to protect enterprise brands and operator revenue. To do this, operators must implement SMS filtering solutions; enabling the effective identification of grey and black route SMS traffic. Without this ability, operators miss out on monetisation opportunities for A2P messaging. Next-generation firewalls will enable operators to gain increased insights on both A2P and P2P (Person-to-Person) messaging traffic.

By using grey routes to masquerade A2P SMS messages as P2P, fraudsters can directly impact operator revenue. As it is the operators' responsibility to correctly distinguish A2P from P2P traffic, many network operators are implementing traffic control measures, such as firewalls, to identify potentially fraudulent activity and prevent revenue leakage.

Juniper Research forecasts that the proportion of A2P SMS traffic delivered via grey routes will decrease from 20.2% in 2020 to 4.2% in 2025; driven by increased investment in firewalls and other security-oriented technology. As a result, operator revenue lost through grey routes will also decrease; plummeting from $5.8 billion in 2020 to $1.2 billion in 2025. Revenue loss as a result of grey routes decreases due to insertion of SMS Firewalls, and this represents a monetization opportunity for network operators to increase revenue while also increasing end-user satisfaction and trust.

1.2 Vendor Assessment

Due to the ongoing importance of grey route prevention, Juniper Research has deemed it necessary to provide an analysis of leading SMS Firewall Providers. Juniper Research assessed 20 vendors in terms of their security offerings and their position in the market. To qualify for the Leaderboard, companies must be involved in the direct provision of SMS firewalls or grey route provision.

The companies included here have developed specific expertise in SMS filtering solutions, although some embarked on the route earlier than others and, therefore, have wider customer bases or geographical reach. It includes established specialists through to companies where SMS firewalls are part of a vendor's wider product offerings.

This research covers a significant number of vendors; however, we cannot guarantee that all players in the market are included. Our approach is to use a standard template to summarize the capability of players offering SMS firewall solutions. This template concludes with our view of the key strengths and strategic development opportunities for each vendor.

We also provide our view of vendor positioning using our Juniper Research Positioning Index technique. This technique, which applies quantitative scoring to qualitative information, enables us to assess each player's capability and capacity, as well as its product and position in the

broader market for SMS firewall services. The resulting Positioning Index exhibits our view of relative vendor positioning.

We have assessed each vendor's capabilities against the following criteria:

Table 1.1: SMS Firewall Providers – Juniper Research Vendor Positioning Scoring Criteria

Category	Factor	Description
Agility (y-axis score)	Financial Strength	This is a measure of a company's revenue relating to messaging security offerings, including SMS firewalls. In the case of large, multinational companies, Juniper Research sought out information about divisional revenue. When this information was not available, assumptions were made based on the percentage of total revenue attributable to the relevant division.
	Customer Presence & Branding Strength	This factor reflects the strength of a vendor's brand and marketing capability.
	Experience in the Sector	This measure reflects the total experience of each vendor offering an SMS firewall solution. It takes into consideration the amount of time spent in the wider messaging market and its progress since doing so.
Innovation (x-axis score)	Innovative Features	This factor is an analysis of each vendor's offerings, in terms of features that Juniper Research considers to be innovative. Features that stand out from the competition are considered here, as well as those that are likely to appeal to potential customers.
	Digital Investment	This measure represents each company's activity in acquisitions. The higher the number of acquisitions, a greater level of investment in digital advances is assumed.
	Future Business Prospects	This factor reflects Juniper Research's view on an enterprise's future in the messaging security market.
Presence (indicated as bubble size)	Corporate Size	This measure is based on the size of each vendor; taking into consideration its operations and number of employees.

Source: Juniper Research

1.3 Limitations & Interpretations

Our assessment is based on a combination of quantitative measures, where they are available (such as revenue and number of employees) that indicate relative strength, and also of qualitative judgement, based on available market and vendor information as published. In addition, we have added our in-house knowledge from meetings and interviews with a range of industry players. We have also used publicly available information to arrive at a broad, indicative positioning of vendors in this market, on a 'best efforts' basis.

However, we would also caution that our analysis is almost by nature based on incomplete information and therefore with some elements of this analysis we have had to be more judgemental than others. For example, with some vendors, less detailed financial information is typically available if they are not publicly listed companies. This is particularly the case when assessing early-stage companies, where a degree of secrecy may be advantageous to avoid other companies replicating elements of the business model or strategy.

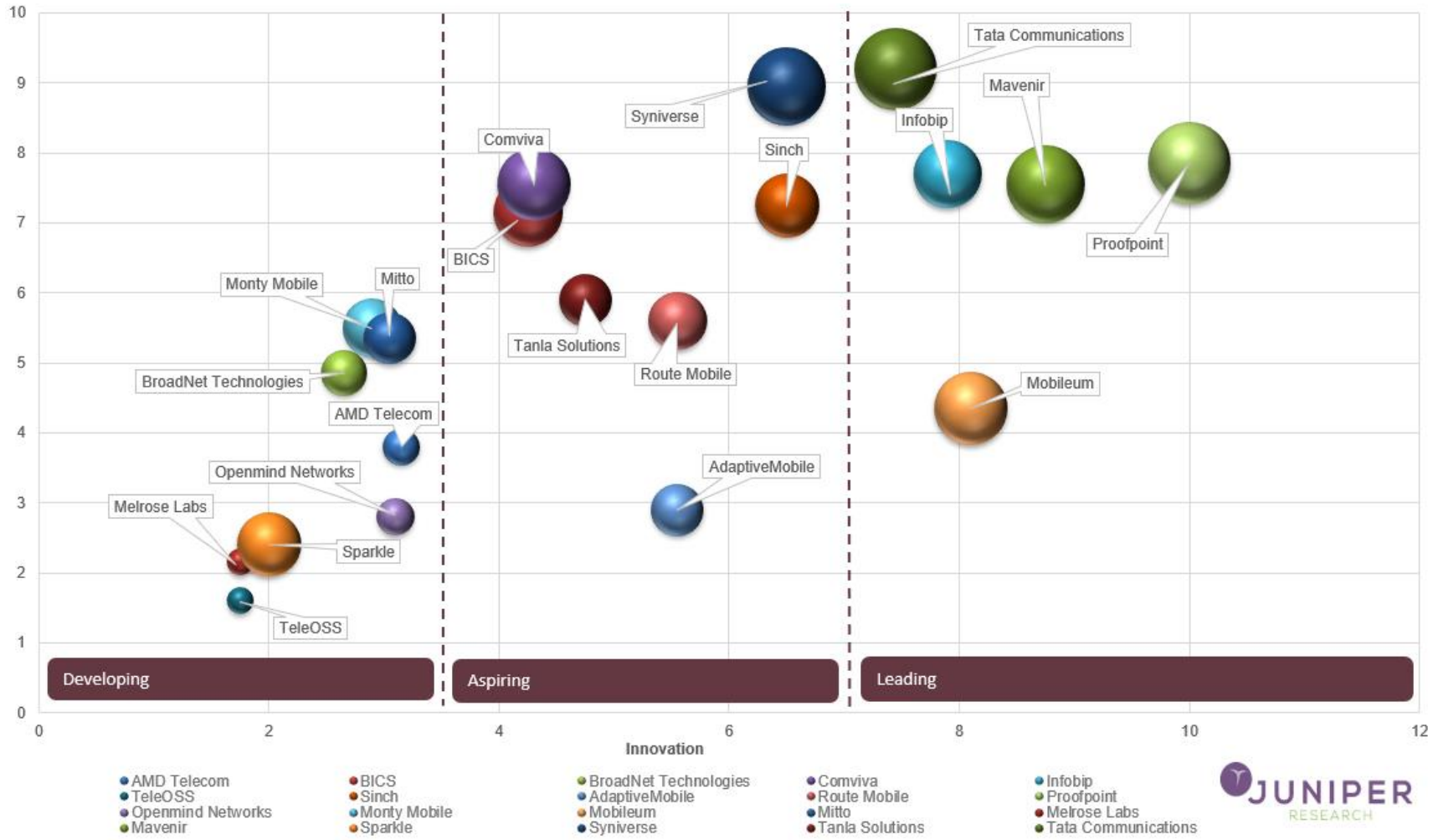
We also remind readers that the list of vendors considered is not exhaustive across the entire market but rather selective. Juniper Research endeavours to provide accurate information. While every information or comment is believed to be correct at the time of publication, Juniper Research cannot accept any responsibility for its completeness or accuracy, and the analysis is presented on a 'best efforts' basis.

The Positioning Index compares the positioning of platform providers based on Juniper Research's scoring of each company against the above criteria that Juniper Research has defined. The Positioning Index is designed to compare how the vendors position themselves in the market based on these criteria; relative placement in one particular unit of the Positioning Index does not imply that any one vendor is necessarily better placed than others. For example, one vendor's objectives will be different from the next and the vendor may be very successfully fulfilling them without being placed in the top right box of the Positioning Index, which is the traditional location for the leading players.

Therefore, for avoidance of doubt in interpreting the Positioning Index, we are not suggesting that any single area in the Positioning Index implies in any way that a group of vendors is more advantageously positioned than another group, just differently positioned.

The Positioning Index is also valid at a specific point in time, August 2020. It does not indicate how we expect this positioning to change in future, or indeed in which direction we believe that the vendors are moving. We caution against companies taking any decisions based on this analysis; it is merely intended as an analytical summary by Juniper Research as an independent third party.

Figure 1.2: Juniper Research SMS Firewall Providers Positioning Index



Source: Juniper Research

1.4 Proofpoint Overview

proofpoint®

Incorporated in July 2003, Proofpoint is a provider of omnichannel cybersecurity and compliance solutions. Proofpoint's Cloudmark SMS firewall protects SMS, MMS, and RCS and is pre-integrated with leading SMSC (Short Message Service Centre) and MMSC (Multi-media Messaging Service Centre) vendors.

The SMS firewall solution offered by Proofpoint uses machine-learning technology to identify patterns in traffic and adjust accordingly.

Proofpoint has also made significant digital investment; acquiring eight companies since March 2015.

In particular, Proofpoint's acquisition of Cloudmark aligns with the company's dedication and focus on cybersecurity and cyber threats. Proofpoint has provided the Cloudmark Division with a higher level of R&D funding and extended the reach of the global threat data, as well as the resource and experience of the SOC (Security Operations Centre), given the breadth of cybersecurity products in the combined Proofpoint portfolio.

The extension of both the SOC and Cloudmark Global Threat Network increased the accuracy and response time of threat detections provided by Proofpoint and Cloudmark solutions.

Figure 1.3: Proofpoint Acquisitions: March 2015 – Present

Company	Specialism	Date	Cost ($m)
The Defence Works	Digital Security	May-2020	Undisclosed
ObserveIT	Digital Security	Nov-2019	$225.0
Meta Networks	WAN (Wide-Access Networks)	May-2019	$120.0
Wombat Security Technologies	Digital Security	Feb-2018	$225.0
Cloudmark	Digital Security	Nov-2017	$110.0
FireLayers	Cloud Security	Oct-2016	$55.0
Socialware	Software & Services	Nov-2015	$9.0
Emerging Threats	Cybersecurity Research	March-2015	$40.0

Source: Juniper Research

1.5 Cloudmark Profile

i. Corporate

Founded in 2001, Cloudmark was acquired by Proofpoint in November 2017. Cloudmark is focused on messaging security; offering solutions for mobile messaging (SMS, MMS, RCS) and email.

Key executives at Cloudmark include Jacinta Tobin (Vice President – Global Sales and Operations, Cloudmark Division); Michael Laudon (Vice President and General Manager – Engineering and Product Management, Cloudmark Division); Angela Knox (Vice President of Engineering, Cloudmark Division); Mike Reading (Senior Director of Professional Services, Cloudmark Division).

ii. Geographical Spread

With headquarters in San Francisco, US, Cloudmark also has offices in France, Japan, and the UK.

iii. Key Clients & Strategic Partnerships

Cloudmark's solutions are the most widely integrated platform in carriers' messaging infrastructures today. Cloudmark's solutions process tens of billions of messages with reputation filtering and content filter over 4 billion messages per day. They are used by over 150 of the world's leading service providers. The company has a near 100% success rate in winning trials against competitors; consistently unseating incumbent vendors such as Adaptive Mobile, RealNetworks, Symantec/Broadcom, and Cisco. Cloudmark's solutions leverage accuracy, scalability, and comprehensiveness, which, together with automated self-learning policies and speed of stopping all new types of attacks, have benefited service providers around the world over the last decade.

iv. High-level View of Offerings

Proofpoint's Cloudmark division offers the industry's fastest and most accurate anti-spam, anti-phishing, anti-smishing, and anti-virus messaging security solutions for Mobile Network Operators, messaging providers such as CPaaS (Communications Platform as a Service), MaaP (Messaging as a Platform) providers, and Internet Service Providers. Cloudmark's products and solutions are proven to have a major impact on service provider infrastructure cost reduction; driving increased ARPU (Average Revenue Per User); improving end-customer satisfaction, and reducing end-customer churn related to phishing and spam. The Cloudmark deployment methodology leverages an optimized combination of proprietary algorithms, automation, carrier-grade design, security expertise, and the world's largest Global Threat Intelligence Network powered by over 450 million spam, phishing, and malware reporters worldwide.

The Cloudmark division of Proofpoint is geared exclusively to serve the messaging security needs of large-scale CSPs (Communications Service Providers) and has a proven track record in deploying and supporting messaging security solutions at the largest mobile, fixed-line operators, and message service providers in the world. Cloudmark dedicates most of its research and development investments to solving carrier-specific messaging security and operational issues.

The success of the Cloudmark's solution stems from its industry-leading anti-spam, anti-phishing, and anti-virus accuracy, while also delivering the highest processing efficiency. Cloudmark's sophisticated technology protects against advanced forms of spam, smishing, phishing, malware, and blended threats. Designed from the start to serve the needs of the most demanding service provider environments, Cloudmark's products and solutions deliver carrier-grade performance, scalability, and availability.

Cloudmark offers a variety of products and solutions providing messaging security for evolving threats. These products and solutions can be grouped into three categories: 1) products for mobile operators and mobile messaging providers, 2) products for Internet service, hosting companies, and email providers, and 3) managed security services providing threat insight and intelligence.

1.6 Juniper Research Q&A: Jacinta Tobin

Juniper Research interviewed Jacinta Tobin, Vice President of Global Sales and Operations for Cloudmark, a Proofpoint Company in November 2020.

Ms. Tobin is responsible for Global Sales, Business Development and Marketing for Cloudmark, a Proofpoint company. Tobin is an industry leader and contributor to the Cybercrime Support Network. She is also a founding board member of the M3AAWG (Messaging, Malware, Mobile, Anti-Abuse Working Group), an association focused on combating botnets, malware, spam, viruses, DoS (Denial of Service) attacks and other online exploitations. She has been recognized as one of the Top 50 Most Influential Women in Technology and one of Silicon Valley's Top Irish Technology Executives. Ms. Tobin holds a Bachelor of Business Administration in International Business from University of Cologne, and a Bachelor's degree in International Marketing and Languages from the University of Dublin.

1.6.1 How can Cloudmark's Firewall Solutions Mitigate the Threats Present in the Messaging Market Today?

The Cloudmark Platform for Mobile is the product identified in Juniper Research's report as an SMS firewall, and is a market leader in protecting and mitigating against mobile messaging threats today and protecting subscribers, enterprise brands, and preserving network operator revenue streams. Collectively, Cloudmark's products and solutions for mobile messaging protection are based on leading technology, data, and expertise. The technology leverages proprietary algorithms that utilize predictive machine learning and artificial intelligence to uniquely categorise, cluster and fingerprint messages, content, and patterns which are then used to identify and track global threats.

Additionally, Cloudmark offers its SRS (Spam Reporting Service) which is the world's largest mobile threat collection system, enabling simple collection and summarized reporting on spam, smishing, and voice spam. Data ingested by the SRS system is used to generate automated near real-time threat updates that are pushed out to Cloudmark's customer environments around the world multiple times per minute. Mobile network operators can leverage the trend data generated by SRS to make informed policy and technology decisions; ensuring their security investments are directed in the most impactful manner.

These tools and techniques enable Cloudmark's solutions to stop bad actors and also pass this information via the Cloudmark Global Threat Network to sites globally; enabling learning and more rapid response to related or similar threats in these other regions. Expert analysts and threat investigators interact with the Cloudmark Global Threat Network to increase both accuracy and identification of changing or evolving threats, since bad actors often make modifications in an attempt to 'game' the detection systems. The Cloudmark multi-layered approach of advanced algorithms, rich data, and expert intervention provides exceedingly high accuracy of detecting threats in a nimble and responsive manner. These techniques are often successful against competitive solutions that utilize limited, static techniques that are difficult revise and enhance.

1.6.2 How Does Cloudmark See Market Threats Evolving in the Future and How is Cloudmark Preparing for These Future Threats?

The mobile communications landscape is evolving to include more MMS and RCS message growth, in addition to traditional SMS messaging. The variety of messaging platforms and increasing traffic from CPaaS and MaaP solutions changes the landscape, creates new attack surfaces, and makes issues like Grey Traffic or Grey Routes more prevalent; causing operators to be increasingly concerned about revenue leakage and loss.

In addition, B2C (Business to Consumer) marketing messaging is expected to grow at a CAGR (Compound Annual Growth Rate) of 7.2% over the next seven years. All this makes the mobile channel ripe for fraud and identity theft both now and in the future through this expansion. As mobile devices continue to advance, more and more of this commercial traffic will be sent via MMS and RCS mechanisms so that businesses can take advantage of a better, richer user experience. Cloudmark is ready and prepared to protect operators, consumers, and brands across SMS, MMS, RCS, and OTT channels such as CPaaS and MaaP.

Operators can rest assured that the Cloudmark technology is designed to support this evolution and the associated threats, as providing this protection is not new to Cloudmark. With a history of over 20 years of processing both text messages and multimedia messages, originating with the need to detect email spam, Cloudmark is prepared to protect subscribers, brands, and operators across the evolving messaging platforms. Cloudmark's proprietary algorithms have been designed to be agnostic to the messaging platforms: email, SMS, MMS, RCS, others. This combined with the other techniques and technologies of statistical linguistical categorization, clustering, and finger printing; predictive machine learning and artificial intelligence; automation; threat data from the world's largest Global Threat Intelligence Network; and expert human intervention, provides the most comprehensive technology platform for products and solutions to respond, expand, and grow with these evolving threats.

1.6.3 What are the Key Hurdles that Stakeholders Face in the Market, and How do Your Solutions Enable Them to Overcome These?

Threats both in mobile and email continue to evolve and expand. Cloudmark's products and solutions are comprehensive and prepared for the evolving threat landscape. Mobile and email messaging is increasing globally, and the amount of mobile messaging traffic is growing at a very rapid pace. Mobile messaging is a highly trusted communication channel

and users are much more apt to read and access links/URLs contained in mobile messages than those in email. This level of trust combined with the reach of mobile devices makes mobile messaging a very attractive platform for commercial and marketing activity and increases the need to secure and preserve operator revenue streams based on mobile marketing.

Increased commercial and marketing mobile messaging is primarily due to A2P messaging, and another hurdle that mobile operators face is from lost revenue due to so called Grey Routes. High accuracy, rapid identification and classification of messages is a key attribute of the Cloudmark Platform and a requirement for operators to properly monetize all of the A2P traffic. The Cloudmark Platform enables operators to rapidly identify A2P traffic and ensure it is properly rated, and utilizes the proper operator-interconnect mechanisms. Advanced, detailed, and evidential analysis and reporting available from the Cloudmark Platform provide operators with the collateral necessary to enforce billing agreements and therefore monetize this traffic.

Cloudmark's foundational technology, data and expertise allows Cloudmark's products and solutions to respond to changing and moving threats and bad actors, positions the products to be outstanding solutions for the changing and expanding mobile landscape. The multi-layered approach leverages a variety of techniques to produce the best and highest accuracy of detection in the industry. This positions Cloudmark exceedingly well for the changing market.

Cloudmark's products and solutions for mobile messaging protection are based on leading technology, data, and expertise. As mentioned previously, the technology leverages proprietary, patented algorithms that utilize predictive machine learning and artificial intelligence to uniquely categorize, cluster, and fingerprint messages, content, and patterns which are then used identify and track global threats. These techniques enable Cloudmark's solutions to stop bad actors and also pass this information via the Cloudmark Global Threat Network to sites globally; enabling learning and more rapid response to related or similar threats in these other regions. Expert analysts and threat investigators interact with the Cloudmark Global Threat Network to increase both accuracy and identification of changing or evolving threats since threats are often modified in an attempt to circumvent detection.

The Cloudmark's multi-layered approach of advanced algorithms, rich data, and expert intervention provides exceedingly high accuracy of detecting threats in an exceedingly nimble and responsive manner.