Cloudmark Security Platform for Email

Solution Guide

November 2014
Cloudmark Security Platform for Email

Introduction
Email has been a favored mechanism for exchanging information for decades. The ability to quickly send and receive messages universally between disparate messaging environments is core to both professional productivity and personal activities. Securing this means of communication is instrumental to ensuring email’s continued usefulness.

Email as Mechanism for Malicious Actors
Due to its success, malicious actors have spent a great deal of time and effort to subvert email to their desired usage. From excessive numbers of unwanted messages on one side to messages containing dangerous content on the other, new email threats constantly arise.

Key Threats
Numerous issues arise when a malicious actor’s messages are permitted to propagate across the network. Resources are wasted, computer security is compromised and users’ personal and financial information can be stolen. It is important to recognize that all risks posed by different malicious message types are not equal.

Spam and other forms of unwanted messaging represent over 90% of email traffic. At the very least, messaging platforms must maintain enough extra capacity in order to accommodate the additional traffic load. If end users were forced to review all incoming messages, they would soon be overwhelmed and potentially become disenchanted with an email provider.

Malware and other forms of maliciously created software that infect a vulnerable system present a new set of concerns. They may compromise the security of the system or a user’s personal information may be stolen directly. The resources of an infected system may be coopted as part of a larger network of infected systems to launch additional attacks or send out massive quantities of malicious messages.

Phishing and spear phishing campaigns threaten to entice user to divulge personal information. Such messages appear as if they originated from a trusted source, often a person or organization with whom the user has a relationship. When they fall victim to phishing schemes, business, personal and financial information can be inadvertently divulged, leading to significant financial losses or identity theft.
Introduction to Cloudmark Security Platform for Email

Cloudmark Security Platform for Email is a software solution that provides comprehensive protection of messaging infrastructure and messaging traffic. With the Cloudmark solution, service providers can protect their systems and users, while gaining a deep insight into how messaging in their platform is used and misused.

Unlike other solutions, Cloudmark Security Platform provides comprehensive protection against a wide variety of message-borne threats. It is a continually evolving platform based on a unique, adaptable workflow engine that automatically protects your network against not only today's threats, but also against threats of the future.

The heart of the solution is Cloudmark's message inspection engine combined with data from Cloudmark's Global Threat Network, consisting of sender reputation and message threat data updated in real-time. Each arriving message is analyzed for sender information and message content. Malicious connections are blocked and unwanted messages are surgically removed from the message stream. Cloudmark Security Platform provides full visibility into detected threats, as well as monitoring and reporting metrics on the performance of the messaging infrastructure. Cluster-aware reporting is provided as part of the solution, and it can also be easily integrated with a multitude of third-party reporting solutions for even more detailed forensic analysis of traffic and threats.
The pure software nature of the solution enables complete flexibility. It may be deployed on Commercial Off The Shelf (COTS) hardware, supporting both bare-metal and virtualized deployment models, with full horizontal scalability as traffic requirements increase.

Centralized configuration management is provided to facilitate the distribution and updating of policy across an entire cluster. An HTTP REST interface is provided for external management of underlying platform functions. Full SNMP query capability is also supported for external statistics gathering and system monitoring.

In a clustered environment, Cloudmark Security Platform offers distributed data sharing across all participating nodes, allowing the entire cluster to act in concert rather than as individual nodes. Consequently, the cluster will converge on an attack much more rapidly than any individual node ever could.

**Detection and Prevention of Threats with Cloudmark Security Platform**

With messaging infrastructure increasingly under attack, as a target for abuse, or as the vector for malicious activities, protecting your messaging environment from these threats is vitally important.

Unlike rigidly designed appliances that provide one-size-fits-all policy functionality, or more simplistic software solutions, Cloudmark Security Platform for Email provides threat countermeasures that can detect and block threats automatically, while adapting to unique threats specific to your environment.

Numerous parameters of each connection and message arriving over the connection are analyzed in a layered approach. The platform will evaluate the sender's IP address, domain information, past behavior, volumetric analysis, authentication meta data (provided by SPF, DKIM, and DMARC), and information from content filters such as Cloudmark Authority to determine the nature of all messaging traffic.

These sources of information will be combined by the policy engine along with real-time updates from other cluster members, maximizing the detection of spam and other forms of malicious messaging, while reducing the potential for false positives. Competing solutions naively use a subset of available data points leading to inadequate spam detection, or unacceptably high false positive levels.
Multi-Layer Defensive Architecture

Numerous layers operate in concert within Cloudmark Security Platform for Email to provide the industry's best protection against spam and malware. Each layer provides additional capabilities to reinforce the defensive capabilities of the previous layer.

Key Technologies in Cloudmark Security Platform for Email

This document has described numerous solutions delivered to Cloudmark's customers. In this section, we provide a brief description of these technologies.

Cloudmark Security Platform for Email

- High-performance MTA, typically enabling 500%-1000% greater throughput than competing solutions or legacy open source deployments
- Software solution compatible with bare-metal and virtual deployments
- Visually scripted policy engine
- Centralized management of policy and configuration
- HTTP REST interface for controlling underlying platform operations and gathering of operational statistics
- SNMP interface for gathering live system statistics
- Uses unique engine for writing automated message handling policy, but leaving room for infinitely customizable intervention in the form of whitelists, blacklists, and configuration thresholds
- Integrates with many provisioning systems, databases, and other pre-existing data sources
(LDAP, MySQL, CSV, CDB, HTTP, RADIUS, etc.)

- Provides distributed data sharing between nodes for a single-view of traffic across entire cluster
- Integrates with many provisioning databases (LDAP, MySQL, CSV, CDB, HTTP, etc.)
- Provides message authentication capabilities (SPF, DKIM, DMARC)
- Supports both IPv4 and IPv6 messaging traffic
- Supports standard and store-and-forward MTA and proxy modes

**Cloudmark Authority Anti-Spam, Anti-Phishing, and Anti-Virus Filter**

- Fastest content filtering engine available
- Provides superior accuracy with low false positive rates
- Filters a variety of message types including both spam and malware
- Real-time data from the Cloudmark Global Threat Network to maintain up to the minute accuracy

**Cloudmark Authority Active Filter**

- Complementary technology to Cloudmark Authority
- Provides mail store cleanup actions when a message’s verdict is later corrected after messages have been filtered and delivered
- It becomes possible to act on, and remove, messages that were initially considered legitimate, but subsequently understood to be spam
- Works in concert with the Cloudmark Mailstore Integration Server to physically remove messages from Zimbra and Openwave message stores

**Cloudmark Sender Intelligence (CSI)**

"Cloudmark Sender Intelligence" represents a family of data feeds generated from Cloudmark’s Global Threat network to further enhance accuracy and performance of the Cloudmark Security Platform.
Cloudmark CSI Global

- Leverages the Global Threat Network to provide a comprehensive feed of IP-based sender reputation
- Allows direct action to be taken when senders attempt to the Cloudmark Security Platform for Email

Cloudmark CSI Local

- Per-provider feed containing sending limit recommendations on a per-IP basis
- Prevents unknown or sending IP addresses with low legitimate-to-spam sending ratios from sending excessive numbers of messages
- Used in concert with strict rate limits for previously unknown actors

Deployment Solutions

Network Border Protection of Existing Infrastructure

Protect current infrastructure, including MTAs and message stores from excessive malicious message volumes. In many deployments, the Cloudmark Security Platform can reduce incoming message volumes by more than 90%, taking the strain off of overloaded internal systems. Cloudmark Security Platform is truly horizontally scalable. As the number of subscribers grows, the platform’s flexible deployment capabilities allow for additional nodes to be deployed with minimal effort on bare-metal or within virtualized environments.

MTA Infrastructure Consolidation

Consolidate multi-level, disparate anti-abuse and MTA delivery infrastructure with Cloudmark Security Platform. The high performance platform is fully capable of delivering messages to a message store of choice using SMTP, LMTP, or HTTP protocols, streamlining complex existing infrastructure significantly. The platform provides integration ability to many provisioning systems and databases. Data derived from these systems can be utilized directly within the policy engine for the purposes of message routing, per-domain or per-user policy application, or any other message handling or modification actions.

Many customers have found the Cloudmark Security Platform to be 500%-1000% more efficient than their existing solution, leading to significant reduction in hardware, power, and operational requirements.
SMTP Proxy for Outbound Messaging

Many hosting and mobile providers experience problems with outbound spam emanating from systems not under their direct control. Shared IP address ranges, associated with large-scale NAT and shared hosting systems, are blocked by downstream providers. The Cloudmark Security Platform may be configured in SMTP proxy mode and deployed within the customer’s network to intercept outbound spam messages. Such filtering will occur seamlessly with no changes required to the existing mail handling infrastructure.

Threat Solutions

Preventing Spam Attacks Initiated from Large Network Ranges

Providers often find that entire remote IP subnets are being used for mounting spam campaigns. Cloudmark Security Platform provides straightforward capability for aggregating IP ranges to a specified CIDR and applying rate limits and volumetric controls to address attacks from rented or hijacked network ranges.

Additionally, the Cloudmark Security Platform provides a robust mechanism for maintaining and evolving counters and reputation measures for a variety of data points. In particular, the platform will build up a reputation measure for each sending CIDR, enabling proactive policy actions to be taken at the CIDR block level.

The Cloudmark Security Platform can also integrate the Cloudmark Sender Intelligence (CSI) Local feed. This feed is tailored on a per-provider basis to contain recommended sending limits for both IP addresses as well as CIDR aggregations, along with strict recommendations on sending limits for as yet unknown addresses. As senders exhibit continued clean sending practices, their corresponding rate limits will be raised.

Preventing “Hailstorm” Attacks

Spammers have found numerous ways of priming a targeted platform in preparation for a large spam run. In such cases, spammers simultaneously send large numbers of malicious messages before the receiving system gains enough precision to recognize that an attack is in progress. However, by the time the system gains the necessary precision, the malicious messages have already been delivered.
Cloudmark Security Platform provides numerous volumetric controls tuned on a per-IP and per-CIDR basis in order to reduce such damage by more than 99%. The platform provides the following functionality in overlapping layers: connection limits, volumetric controls over several time windows, TCP-level throttling and tar-pitting of messages in order to waste resources on the part of the spammer. The Cloudmark CSI Local feed, described in the previous section, provides an additional layer of protection for such attacks.

**Preventing “Snowshoe” Spam**

Spam is delivered from a broad number of IP addresses in very low numbers per source IP. Such attacks are often initiated from a network of systems participating in a botnet.

Cloudmark Security Platform correlates numerous IP addresses sending similar messages in order to stop the distributed attack. Cloudmark Security Platform is uniquely capable of sharing reputation data between nodes in a clustered environment, affording a single view of in-progress attacks and allowing all nodes to react simultaneously.

**Preventing Attacks from Known Bad Actors**

Often, malicious email is sent from IP addresses known to be bad actors. Numerous services endeavor to compile IP reputation for such senders into feeds.

Cloudmark Security Platform supports both IP reputation services and domain reputation services. In addition to third party services, Cloudmark offers the Cloudmark Sender Intelligence (CSI) Global feed, providing one of the most comprehensive and up to date listings of sending IP reputation data available.

**Message Content Scanning**

In some cases, malicious messages will evade all other defensive layers designed to analyze behavior and sender reputation in order to block such messages. At this point, accurate content filtering is the last line of defense and becomes critically important.

Cloudmark Security Platform integrates with numerous spam filtering technologies for content analysis and filtering, providing a final line of defense. Cloudmark Authority is the best spam filter currently available. It provides the most efficient and accurate spam and virus content filtering available. Cloudmark Authority leverages the data in the Global Threat Network to provide zero hour protection against malicious messages.
Remediating Malicious Messages After Delivery

Often, malicious messages will evade countermeasures for some period of time while the overall system learns what constitutes bad traffic. At a later time, these messages will be known to be spam, but that is too late for the messages that have been delivered to recipients’ mailboxes. Cloudmark Security Platform integrates with the Cloudmark Active Filter technology to generate notifications indicating both the recipient and the message identifier of each malicious message that should be removed from the message store. An additional component, Cloudmark Mailstore Integration, has been integrated with Zimbra and Openwave message stores to automatically remove the malicious messages identified by such notifications.

Platform Management Solutions

In order to be of the greatest value, a platform must be easy to configure, deploy and manage. Cloudmark Security Platform for Email has been carefully designed with each of these requirements in mind.

Virtualization

Many providers wish to deploy message-handling software on virtual servers. Reasons for virtualization may include: desire to maximize usage of hardware capacity, flexibility to dynamically bring online additional instances as traffic load increases.

Software Deployment

The Cloudmark Security Platform for Email is deployed using the native package manager supplied on Red Hat and Ubuntu OS distributions. While not explicitly supported, every effort has been made to ensure deployment on closely related Linux distributions.

Policy Tuning and Versioning

In response to ongoing attacks or changes in spammer tactics, policy and configuration may need to be tuned for greater effectiveness.

Cloudmark Security Platform for Email provides a visually scripted policy interface allowing the administrator full reign to modify existing policy to easily create or adjust the defensive capabilities of the platform.
An important feature of the platform provides the ability to version a configuration state of an instance. This is very useful for both rollback and distribution of policy to other instances within a cluster of nodes. At all times, the administrator can verify the currently installed policy version on cooperating nodes.

**Seamless Distribution of Policy and Configuration**

Once software is deployed, all relevant configuration and policy needs to be distributed. In some cases, a modification to policy may be necessary while the platform is taking traffic. In other words, it is necessary to update policy without shutting down message-handling nodes.

Cloudmark Security Platform for Email provides a centralized mechanism for both the updating and subsequent distribution of updates to policy and general system configuration to each participating instance. In the vast majority of cases, such a configuration push does not require a system restart; each node continues to handle traffic with no service interruption.

**Class of Service Policy**

In order to provide users with customized options, a platform must be supportive of mechanisms that permit per-user actions to be taken.

Cloudmark Security Platform for Email provides numerous mechanisms for providing per-user or Class of Service behaviors within the platform. The most important are the platform's Data Source Query Modules. These modules permit the policy engine to query external provisioning and policy data, including MySQL, LDAP, CSV, CDB, RADIUS and HTTP-enabled web services. The results of such queries are combined within policy in order to provide a customized per-user or Class of Service experience for each subscriber.
Visibility into Cloudmark Security Platform for Email

Managers of messaging systems demand visibility into the nature and volumes of traffic passing through systems under their control. Cloudmark Security Platform offers a rich set of charts and dashboards for visualizing both traffic type and traffic volume passing through the platform. Some examples are presented in the following sections.

Understanding the Composition of Messages in the Network

Cloudmark Security Platform for Email provides an interface to visualize messaging rates within the platform. This information makes it easy to compare the relative rates of malicious messages vs. overall traffic throughput.

Message Throughput

Cloudmark Security Platform for Email permits the administrator to visualize both incoming as well as outgoing traffic levels.

Message Verdicts

It is equally simple to see the message verdicts that have been scanned by a content filter.
Identifying Top Bad Actors in the Network

The Cloudmark Security Platform displays top malicious actors within a provider's environment. Numerous charts are available for displaying who is sending the greatest numbers of spam, virus, or suspect messages categorized by sending IP address or sending domain.

**Top Spammers by IP**
Quickly see the IP addresses responsible for the majority of spam.

**Top Spammers by Domain**
Quickly see the sending domains responsible for the majority of spam.
Conclusion

The Cloudmark Security Platform for Email provides a full messaging security solution. Its superior accuracy, threat-fighting capabilities and performance massively reduce the amount of unwanted and malicious traffic within a provider’s messaging infrastructure. Each solution presented within this document increases each customer’s satisfaction while reducing the demands placed upon a provider’s network.

The platform provides automatic, but flexible, policy that integrates intelligence from the Cloudmark Global Threat Network, reputation data, authentication mechanisms, external sender reputation feeds, and Cloudmark Authority content filtering. By comprehensively incorporating all sources of information, the platform provides broad visibility into the latest messaging threats, trends and traffic patterns, enabling rapid creation and deployment of effective security policies. Even rapidly morphing phishing attacks and zero-day malware outbreaks are quickly identified and stopped. With threats and spam under control, service providers can increase revenue and profits by offering new value-added security services to subscribers.

About Cloudmark

Cloudmark is the most trusted leader in security, protecting traffic, data and infrastructure for service providers, enterprises and consumers worldwide. Cloudmark’s patented solutions deliver immediate, adaptive and predictive protection from ever-evolving network threats with proven, carrier-grade scalability and operability, assuring business continuity while lowering infrastructure costs. Cloudmark leverages big data analytics from locally collected data and from our Global Threat Network—the world’s most comprehensive repository of global threat intelligence. Cloudmark protects more than 120 tier-one customers, including AT&T, Verizon, Swisscom, Comcast, Cox and NTT and more than 1 billion subscribers worldwide. For more info visit us at www.cloudmark.com.