

BENEFITS

Global Identification of Spam Sources

Cloudmark customers provide valuable statistics on received messages, including the message volume from each IP address and its categorization of spam or legitimate. This data originates from more than 100 ISPs and 35,000 enterprises globally, providing Cloudmark Sender Intelligence with a comprehensive data set for analysis.

Complete Coverage of Attacks and Threats

Cloudmark utilizes its Global Threat Network to track sender behavior and adjust reputation scores accordingly. The Global Threat Network supplies Cloudmark Sender Intelligence with the necessary information to track both high and low volume attacks and aggregated attacks from multiple senders.

Customized Analysis

Cloudmark's security operations task force team provides human analysis of customer specific traffic, complimenting its automated analysis to ensure that operators get the ultimate protection against future attacks.

Real Time Analysis

Feedback from Cloudmark's Global Threat Network enables Cloudmark Sender Intelligence to analyze traffic pattern, feedback, and fingerprint correlation statistics to establish and adjust sender reputation scores in near real time.

Dynamically Updated Protection

Cloudmark Sender Intelligence updates its data in real time allowing customers to download updates within minutes. Traditional technologies require 30 minutes or more to download updates and many will also involve an Internet query for each message, resulting in dangerous latency.

CLOUDMARK SENDER INTELLIGENCE: INTELLIGENCE AT THE EDGE

Operators rely on protocol level filtering as the first level of defense against spam attacks. As spam, phishing and virus attacks continue to evolve in complexity, service providers of all sizes are seeking more granular and automated ways of filtering their message traffic. While traditional DNSBLs provide a basic level of insight for these policies, operators continue to search for a more comprehensive form of reputation data to exert greater control over their protocol filtering management. Cloudmark Sender Intelligence provides an additive layer of security to traditional sender reputation services. It provides you with a comprehensive sender reputation service that enables operators to prevent spam, phishing, and malware attacks. Our service combines a global data set with specific feedback from your customers. The automated analysis is complemented by expert human analysis to ensure that your infrastructure is protected against current and future attacks. Data from Cloudmark Sender Intelligence SI can be integrated into network perimeter devices, such as edge mail transfer agents (MTAs) to protect messaging infrastructure.

Cloudmark Sender Intelligence analyzes multiple data sources to construct sender profiles which result in a more accurate characterization of senders. Cloudmark leverages statistics from its vast Global Threat Network, which includes over 1.6 billion mailboxes and millions of honeypot sources, to classify and analyze sender characteristics. In addition to its network, Cloudmark employs a variety of proprietary sender identification systems and third-party data to provide additional classifications of senders beyond reputation. Examples of Cloudmark's sender identification systems include Newsletter Sender Logic, which identifies newsletter senders, Mail Forwarders Identification, which identifies public mail forwarders, and Dynamic Space Analysis, which verifies that an IP is contained within a service provider's dynamic IP address range. Cloudmark's sophisticated analysis delivers a more detailed and accurate profile of sender reputation, volume, and classification which enables more granular policies and improved accuracy. The depth and breadth of Cloudmark's network and security experts allow Cloudmark Sender Intelligence to identify additional senders undetected by other reputations services, typically yielding an additional 50 percent filter rate for missed messages by traditional services.

THE CLOUDMARK ADVANTAGE

• Faster and more accurate sender categorization

Most sender reputation services rely solely on traffic pattern statistics. While this can be an effective approach for establishing reputation, it is a reactive approach that introduces latency during which environments are vulnerable to new spam sources. As attackers grow their botnets and use dynamic IPs to generate spam, traffic pattern analysis alone is no longer sufficient.

Cloudmark closes this vulnerability gap by combining fingerprint correlation statistics, a data source unique to Cloudmark, along with feedback statistics from users and honeypots to quickly identify spamming senders as well as good senders. By analyzing the correlation of multiple fingerprints in different messages, both spam and legitimate, Cloudmark Sender Intelligence proactively and reliably detects suspicious activity during the zero-hour attack phase, often before any relevant traffic pattern statistics emerge.

- **Unique protection for targeted attacks**

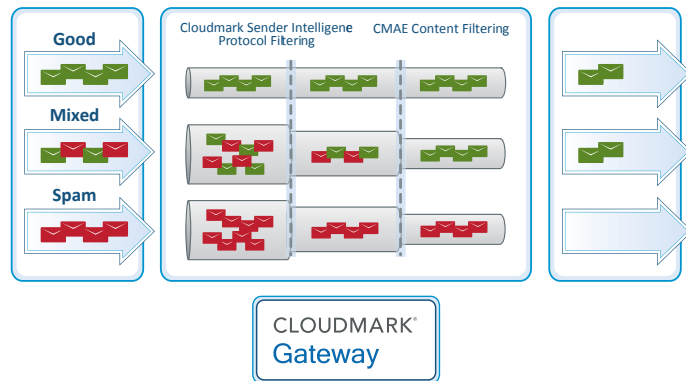
The Cloudmark Security Operations Center is comprised of e-mail security experts that focus their attention on operator data to uniquely stop targeted attacks. The team employs proactive actions to prevent future attacks on operator specific environments. These measures go beyond analyzing a base level of IP reputation data. CSI is the only reputation service that is able to stop targeted attacks.

CLOUDMARK SENDER INTELLIGENCE WITH CLOUDMARK GATEWAY

Cloudmark Sender Intelligence data enables Cloudmark Gateway to automatically apply policy to senders based on their reputation. As the connection request is received by Gateway, it will query the local copy of Cloudmark Sender Intelligence and receive the reputation of the sender along with any other data returned by it. Gateway will then determine the appropriate policy for the sender and take the pre-configured action, usually maximizing the bandwidth for senders with high reputation while constricting bandwidth for senders with a low reputation.

Complete connection management based on sender reputation provides a more granular method of limiting potentially malicious content from entering the network. With Cloudmark Sender Intelligence, Cloudmark Gateway can provide throttling based on groups of IP addresses that share a common reputation score or reputation characteristic in addition to just on a per IP address basis.

Cloudmark Sender Intelligence on Cloudmark Gateway



Cloudmark Gateway leverages Cloudmark Sender Intelligence data to handle traffic based on the reputation of senders. Cloudmark Sender Intelligence enables intelligent connection and flow control techniques, such as dropping connections from malicious senders, throttling connections from suspicious senders, and allowing good senders through without delay.

INDUSTRY AFFILIATIONS

For more information
visit us at www.cloudmark.com

