### Key Features

**Differential Rate Limiting Based on Historical Sending Patterns**
Cloudmark Sender Intelligence Local tracks sending patterns of legitimate senders over time on a per-customer basis and publishes suggested message acceptance limits per 5 minute, 60 minute, and 24 hour window.

**Automatic Protection Against Snowshoe Spam Attacks**
Cloudmark Sender Intelligence Local makes long-term IP reputation information available to operators through a personalized data feed. This allows operators to fine-tune dynamic rate-limits for known IP addresses, and to set aggressive default rate limits for IP addresses with no history. Ideal for blocking snowshoe spam attacks and botnet controlled sending IP addresses.

**Complete Coverage of Attacks and Threats**
The Cloudmark Global Threat Network tracks sender behavior, adjusts reputation scores accordingly, and supplies Cloudmark Sender Intelligence with the information necessary to track both high and low volume attacks as well as aggregated attacks from multiple senders.

**Customized Analysis**
The Cloudmark 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 Threat Analysis**
Feedback from the Cloudmark Global Threat Network enables Cloudmark Sender Intelligence to analyze traffic patterns, feedback, and fingerprint correlation statistics to establish and adjust sender reputation scores in near real time.

### Precision Rate Limiting Using Sender-Specific Reputation Data

Cloudmark research shows that on average, the vast majority of an ISP’s legitimate inbound email traffic originates from a relatively small set of connecting IP addresses:

- 90% of legitimate traffic originates from 5% of the connecting IP addresses
- 75% of legitimate traffic originates from only 1% of connecting IP addresses

Most ISPs have tools and procedures in place to recognize and accommodate the 1% of sending IP addresses that consistently deliver good traffic. The challenge is how to efficiently design and enforce policy for the other 99% of IP addresses.

In order to accomplish this task, ISPs have long desired differential rate limits based on historical sending patterns. Implementation, however, has been complicated by two challenges; 1) how to maintain a historical view on a per-IP basis, and 2) how to enforce differential rate limits based on this history. Cloudmark Sender Intelligence Local solves these problems by tracking legitimate long term reputation on a per-sending IP basis, allowing operators to confidently assign 5 minute, 60 minute, and 24 hour rate limits for individual IP addresses that have a history of sending legitimate traffic.
Highly Effective Defense Against Snowshoe Attacks

Snowshoe attacks are high volume spam campaigns that have been purposely designed to evade traditional network protections such as blacklisting services, volumetric analysis and arbitrary rate limits. Attackers typically spread large sending volumes over broad swaths of IP address space, ensuring they stay well below detection thresholds by sending low rates of traffic from each individual IP address.

Because the IP addresses that snowshoe attackers utilize often don’t have historical sending patterns established within an ISPs messaging platform, applying a customer-specific data feed to show historical sending patterns can help to quickly identify these new, malicious senders. Cloudmark Sender Intelligence Local is designed specifically to block these, and similar types of attacks as those coming from botnets, that attempt to circumvent blacklisting defenses by using snowshoe tactics. By establishing customer-specific historical sending patterns for each sender, operators are able to apply and enforce more dynamic throttling policies against senders with no historical sending behavior record.

Operator-Specific IP Reputation Feed Published by Cloudmark

Cloudmark collects detailed IP statistical data from every operator in our network. This data is collected every 60 seconds, maintained operator-by-operator, and forms a unique, operator-specific history of the sending patterns of IP addresses that have connected to each individual platform over time. As a result, this data is an authoritative resource for identification of IP addresses with little or no related sending history.

Cloudmark Sender Intelligence Local makes this historical IP reputation available to operators through a personalized data feed. The feed contains information about sending IP addresses for individual operators, based on a rolling historical window. Recommended rate limits, also based on the historical data, are included with the feed. Rate limits for IP addresses will be adjusted over time based on changes in legitimate traffic volumes. This allows operators to fine-tune dynamic rate-limits for known IP addresses, and to set aggressive default rate limits for IP addresses with no history.

The Cloudmark Advantage: Real-Time Global Threat Information

Designed to work in concert with Cloudmark Sender Intelligence Global and Cloudmark Authority, Cloudmark Sender Intelligence Local provides a customer-specific historical IP reputation feed to further reduce traffic from abusive mail sources towards service provider messaging platforms. These layered defenses offer the best messaging anti-abuse protection currently available:

- Cloudmark Sender Intelligence Global is used to blacklist known-bad and heavily throttle suspected spam senders based on observed sending behavior
- Cloudmark Sender Intelligence Local is used to set safe throttling limits for known good senders based on long term observed legitimate sending behavior
- Cloudmark Authority is used to scan received message content and acts as a barometer for the legitimacy of sending IP addresses

In short, Cloudmark Sender Intelligence Global is leveraged to block known-bad content and Cloudmark Sender Intelligence Local is used to identify good senders. Any IP addresses not matching either reputation list are classified as “unknown” and are allowed very limited sending rates to block any spamming attempts from new IP address ranges.

Sophisticated analysis delivers a more detailed and accurate profile of sender reputation, volume and classification, which enables more granular policies and improves accuracy. The depth and breadth of the Cloudmark Global Threat Network and knowledgable security experts enable Cloudmark Sender Intelligence to identify additional rogue senders that may go undetected by other reputation services.

Cloudmark Industry Affiliations:

More Information:
www.cloudmark.com