

BENEFITS

Industry-Leading Accuracy

Cloudmark ActiveFilter extends the industry-leading accuracy of Cloudmark Authority® by enabling detection of spam messages that have been delivered in the previous seconds or minutes.

No Rescanning

Cloudmark ActiveFilter acts upon specific messages within the mail store that have changed classification and doesn't require rescanning of all previously delivered messages.

Negligible Performance Impact

Similar to the solution itself, ActiveFilter creates a negligible impact on system resources because it searches only for message ID's of spam messages. There's no rescanning of terabytes or petabytes of email.

Minimized Storage Requirements

Most carriers find that their online storage requirements decrease by as much as 20 percent through the use of Cloudmark ActiveFilter.

Carrier-Grade Scalability

ActiveFilter is designed to support even the largest carrier implementations due to its resource efficiency.

Favorable User Experience

With Cloudmark ActiveFilter, users are exposed to fewer spam and phishing attacks, leading to greater user satisfaction and lower subscriber churn.

GREATER ACCURACY THROUGH EFFICIENT MAIL STORE CLEANUP

The messaging security landscape has long resembled an arms race between attackers and messaging security providers. To penetrate perimeter defenses and successfully deliver spam to user inboxes, spammers are constantly altering their message contents in an effort to get their messages delivered before anti-spam defenses start to detect and block them. This practice has increased in the total volume of spam sent, which now constitutes more than 95 percent of all email traffic.

Today, spammers employ extremely sophisticated techniques, including leveraging the size and power of botnets, to ensure their messages get delivered. Botnet-infected computers now compromise 15% of the world's computers and are responsible for sending more than 90% of all spam. Spammers use botnets to send out millions of rapidly changing messages in less than a minute from service provider networks. These attacks are difficult to detect and evade volume based spam filters since only a small number of messages need to be sent from each computer in a one million bot strong botnet to amount to a very large spam attack. Bots are intelligently implemented and have the ability to tell if individual bots are blacklisted, shifting the spam sending to hosts that are known to still be able to deliver to specific service provider networks.

These types of attacks represent a significant challenge to service providers. Even with the most effective filtering and anti-spam policies in place, a small amount of spam can get through to the mail store, clogging up the mail store with spam. Cloudmark ActiveFilter is able to delete spam that has slipped past existing defenses before users have logged in and checked their mail, increasing accuracy to well over 99%.

THE CLOUDMARK ADVANTAGE

The small percentage of spam messages missed initially are typically identified by Cloudmark within seconds after delivery. Cloudmark ActiveFilter for Mail Stores increases overall spam capture rates and accuracy by continuously reviewing newly-available fingerprints to see if messages already delivered to the mail store, but not reviewed by users, were actually spam. This reduces the impact of high-speed attacks that attempt to capitalize on any degree of latency in spam filter updates by providing the ability to retroactively act upon spam messages that were able to evade the gauntlet of IP reputation, throttling, and content filtering functions at the network edge.

It is generally accepted that re-scanning the entire mail store for missed spam messages is not feasible for a typical carrier due to the high resource demand required to reprocess terabytes or petabytes of data in the mail store. Cloudmark ActiveFilter is designed so that it is unnecessary to rescan every message in the mail store. Instead, it uses a "push" paradigm that moves or deletes only specific stored messages that have been identified as spam after initial delivery, but prior to users checking their inbox, causing minimal CPU impact.

FAST AND EFFICIENT

Cloudmark uses a unique combination of Advanced Message Fingerprinting and real-time threat reporting from the Cloudmark Global Threat Network, consisting of over 1.6 billion trusted users in 190 countries, ensuring fast and efficient response times. Cloudmark's Advanced Message Fingerprinting technology reduces a spam message to a lightweight set

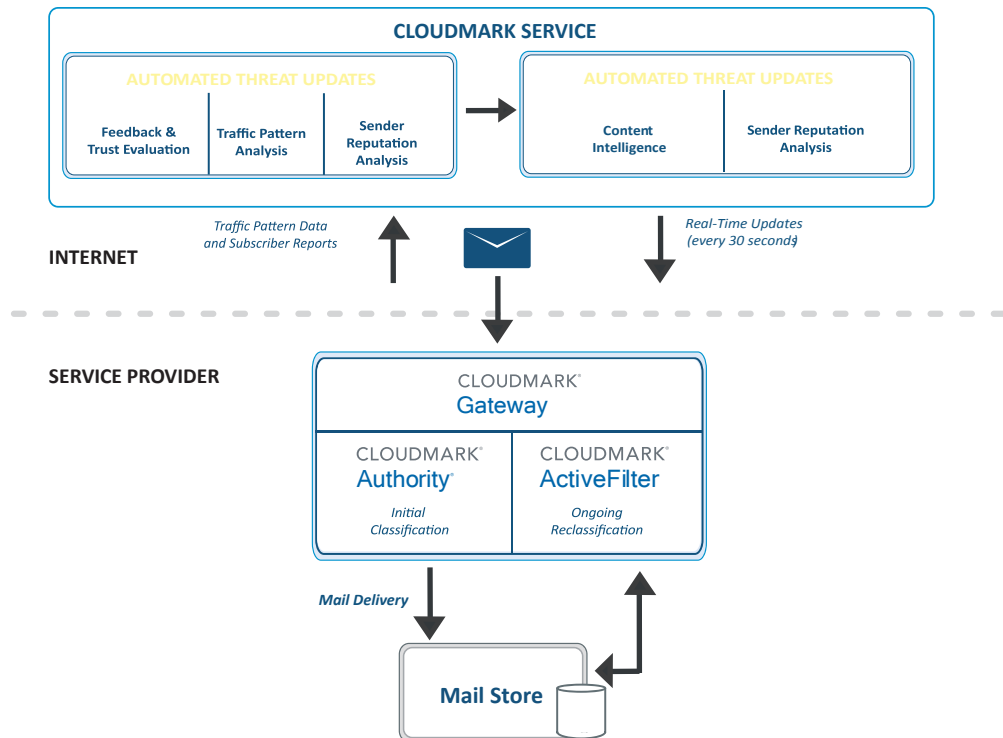
of fingerprints. Cloudmark ActiveFilter then caches the fingerprints that have been scanned and delivered to the mail store while also continually monitoring for new fingerprint updates from Cloudmark's Global Threat Network. If there is a match between a newly-identified spam fingerprint and a message in the mail store, Cloudmark ActiveFilter interacts the mail store to take action on just that specific message.

Cloudmark ActiveFilter virtually neutralizes any advantages of advanced spam distribution techniques designed to evade traditional content filters. The result is dramatically lower levels of spam being stored in the mail store and minimal impact to CPU and disk resources.

CLoudMARK ACTIVEFILTER PROCESS FLOW

As messages are scanned by the gateway MTA, Cloudmark ActiveFilter keeps track of fingerprints for messages deemed to be legitimate at initial reception time. As new spammy fingerprints are discovered and are downloaded by Cloudmark Authority®, the new spam fingerprints are compared against ActiveFilter's cache of legitimate messages to check if any of the initially legitimate messages were actually missed spam. Messages are only scanned a single time, as they're arriving at the edge MTA.

If a missed spam message is found, ActiveFilter is able to undertake the prescribed action within the user's policy to remediate the missed spam message on the backend mail store host, deleting the message or moving it to the user's junk folder before the user has checked their inbox.



INDUSTRY AFFILIATIONS