



# CLOUDMARK AUTHORITY<sup>®</sup> for SpamAssassin<sup>™</sup>

## FEATURES / BENEFITS

### Anti-spam, Anti-virus, and Anti-phishing

Cloudmark Authority offers comprehensive protection against inbound and outbound spam, phishing, and virus attacks. Cloudmark's industry-leading accuracy and real-time response drive higher customer satisfaction and lower support costs. By also blocking outbound abuse, service providers are able to maximize bandwidth, ensure high performance and keep their mail servers from being "blacklisted" by other networks.

### Content Categorization

This feature categorizes messaging abuse by type, allowing service providers to apply specific policies for category – e.g., block phishing, quarantine viruses, hold newsletters and folder spam. Individual handling of messages increases subscriber satisfaction and lowers infrastructure costs.

### Cloudmark Network Feedback System<sup>™</sup> (CNFS)

CNFS empowers service providers and subscribers to provide feedback and automatically address misclassifications, such as false positives and false negatives. Feedback from administrators, abuse desks and subscribers is immediately analyzed by the Cloudmark Trust Evaluation System leading to improved filtering on Cloudmark Authority in near real time.

### Real-time and Historical Reporting

Cloudmark offers daily, weekly and monthly statistical reporting that gives systems administrators and management unprecedented insight into filtering performance, subscriber-level feedback and messaging abuse volumes coming into their systems. This information can be used by the service provider for better resource planning, policy decision-making and customer support initiatives.

## Carrier-Grade Messaging Security for the Apache SpamAssassin Platform

Cloudmark Authority, a carrier-grade software plug-in for SpamAssassin<sup>™</sup>, delivers the industry's fastest and most accurate spam, phishing and virus protection. Designed to integrate seamlessly into virtually any SpamAssassin implementation, Cloudmark Authority offers service providers significant improvements in both filtering accuracy and performance.

Messaging abuse has grown considerably and now constitutes up to 95% of all email traffic overwhelming traditional spam filters and impacting customer satisfaction. Cloudmark utilizes a unique combination of Advanced Message Fingerprinting<sup>™</sup> and corroborated reporting from the Global Threat Network, the industry's most sophisticated threat detection system, to rapidly detect messaging abuse with over 98% accuracy and near zero false positives. Even with this high level of speed and accuracy, Cloudmark Authority requires only a fraction of the processing power of alternative solutions. Cloudmark Authority frees service provider resources, lowers storage requirements and delivers an outstanding user experience.

### REAL-TIME THREAT RESPONSE

Cloudmark is able to detect emerging threats faster than any other solution. Real-time feedback from the Cloudmark Global Threat Network is analyzed, corroborated and automatically distributed to Cloudmark Authority via micro-updates every 30-60 seconds. In addition, Advanced Message Fingerprinting enables immediate detection of mutated threats or techniques associated with known spam, phishing or virus threats.

### UNMATCHED ACCURACY

Cloudmark has a 100% win rate against competitive solutions in service provider accuracy trials. Cloudmark Authority filters abusive emails with greater than 98% accuracy and near zero false positives. Continual report corroboration and system self-correction ensure high accuracy now and in the future. Due to content and language-agnostic analysis, Cloudmark is able to stop spam in any form, format or language including image spam, phishing URLs and foreign language spam using double-byte characters like Chinese, Japanese and Cyrillic.

### INFRASTRUCTURE AND OPERATIONAL SAVINGS

Built for carrier environments, Cloudmark Authority delivers 10 times faster message throughput than competitive solutions. Scanning is performed as a lookup against a local cache of the latest threat fingerprints rather than intensive rules-based processing. This superior performance translates to higher infrastructure efficiency and significantly reduced systems total cost of ownership (TCO).

### EASY TO INSTALL AND ADMINISTER

With years of experience supporting SpamAssassin, Cloudmark has engineered Cloudmark Authority for out-of-the-box integration with virtually any SpamAssassin implementation. Cloudmark Authority is able to fully leverage existing policies, rules, lists, database, and processes. In addition, Cloudmark automatically publishes the latest threat data every 30-60 seconds so there's no need for manual updates. Cloudmark Authority significantly reduces administrative time while delivering the highest level of protection against new threat outbreaks.

## OPERATING SYSTEM REQUIREMENTS

### Linux (32 bit and x86-64)

Note: Cloudmark supports any Linux distribution with the required libraries installed.

### Solaris 10 (SPARC and x86-64)

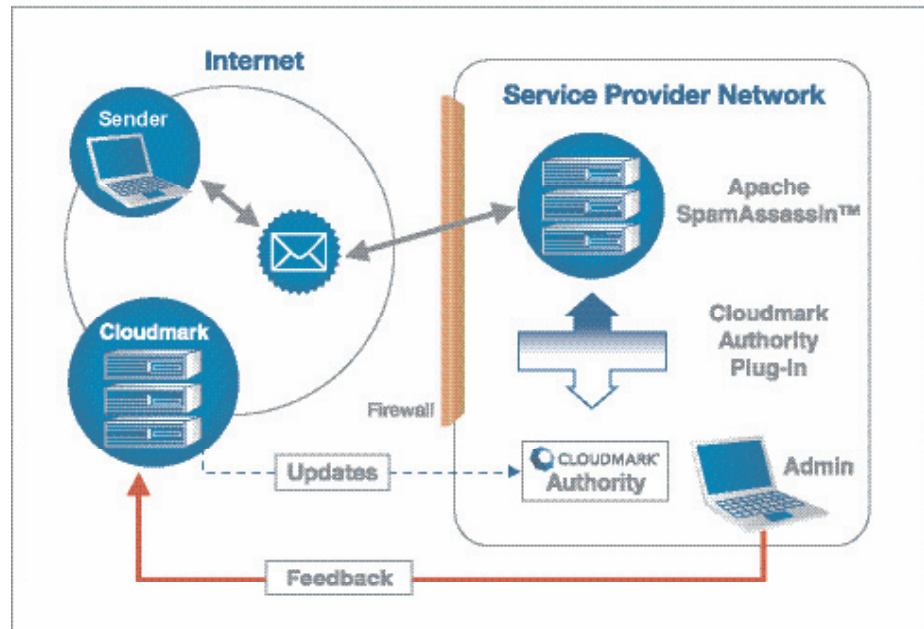
### FreeBSD 5, FreeBSD 6 (32 bit)

Apache SpamAssassin 3.0 or greater (installed and running)

## PERL REQUIREMENTS

Perl 5.8

## CLOUDMARK AUTHORITY PLUG-IN IN THE SERVICE PROVIDER NETWORK



For more information visit us at [www.cloudmark.com](http://www.cloudmark.com)

Headquarters  
128 King Street, 2nd Floor  
San Francisco, CA 94107 USA  
Ph: +1 415 543 1220  
Fax: +1 415 543 1233

Cloudmark Europe, Ltd.  
Garrick House, 26-27  
Southampton Street  
London, WC2E 7RS  
Ph: + 44 (0) 207 717 8410  
Fax :+ 44 (0) 207 717 8401

Asia Pacific Office  
45/F The Lee Gardens  
33 Hysan Avenue  
Causeway Bay  
Hong Kong  
Ph: +852 3180 7768