



CLOUDMARK AUTHORITY® for Service Providers

FEATURES / BENEFITS

Anti-spam, Anti-virus and Anti-phishing Protection

Cloudmark Authority is a comprehensive solution that protects email users from both inbound and outbound spam, phishing and virus attacks. Cloudmark's industry-leading accuracy and zero hour response means a clean inbox for your subscribers and fewer support issues.

Content Categorization

This feature categorizes messaging abuse, allowing service providers to apply specific policies for each category – e.g., block phishing, quarantine viruses and hold newsletters. Individualized handling of messages increases subscriber satisfaction and reduces infrastructure costs.

Cloudmark Network Feedback System™

The Cloudmark Network Feedback System (CNFS) empowers service providers to address misclassifications automatically without relying on vendor research or requiring manual intervention. Feedback from administrators, abuse desks and subscribers is immediately and automatically analyzed by the Cloudmark Trust Evaluation System leading to improved filtering on Cloudmark Authority in near real time.

Secure Copy of Latest Threat Data

Cloudmark Authority maintains a secure local cache of the latest threat fingerprints on each server, which is updated every 30 to 60 seconds (depending on your requirements). This provides full system redundancy and enables filtering to continue even if the network connection to the Cloudmark backend service is temporarily interrupted.

Real-Time and Historical Reporting

Cloudmark also provides real-time and historical security intelligence at the system level down to the subscriber level. Service providers have full visibility into how well Cloudmark Authority is protecting their network, as well as insight into subscriber feedback for better policy decision-making and infrastructure planning.

Carrier-Grade Protection against Spam, Phishing and Viruses

Cloudmark Authority, a carrier-grade software solution, delivers the industry's fastest and most accurate spam, phishing and virus protection. Cloudmark uses a unique combination of Advanced Message Fingerprinting™ and real-time threat reporting from the Cloudmark Global Threat Network, consisting of trusted users in 190 countries around the globe. Cloudmark Authority blocks abusive messages with greater than 98% accuracy and near zero false positives. In addition to this high level of accuracy, Cloudmark Authority requires significantly less processing power than competitive solutions, lowering CPU requirements by up to 90%.

Cloudmark Authority frees network resources, lowers storage requirements and delivers an immediate improvement in the email user experience. As a result, Cloudmark Authority is the fastest growing anti-abuse solution on carrier MTAs in the world.

CARRIER-GRADE SCALABILITY AND RELIABILITY

Designed for large-scale carrier deployments, Cloudmark Authority delivers up to 20 times faster messaging throughput than competitive solutions while utilizing up to 90% less CPU. This superior performance translates to higher infrastructure efficiency and significantly reduced systems total cost of ownership (TCO). Cloudmark Authority's distributed architecture together with a full local cache of the latest threat data stored at each installation enable the highest level of filtering reliability.

REAL-TIME THREAT RESPONSE

Cloudmark Authority is able to detect new threats faster than any other solution. Real-time feedback from the Cloudmark Global Threat Network is analyzed, corroborated and automatically distributed to Cloudmark Authority installations every 30-60 seconds via micro-updates. In addition, Advanced Message Fingerprinting technology uses innovative algorithms to track and identify mutated attacks and those using known spamming techniques.

UNMATCHED ACCURACY

Cloudmark has a 100% win rate against competitive solutions in service provider accuracy trials. Cloudmark Authority filters email threats 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 threat analysis, Cloudmark is able to stop spam in all formats and languages including those using double-byte characters like Chinese, Japanese and Cyrillic.

BROAD THREAT PROTECTION

Cloudmark Authority offers complete inbound and outbound protection against all forms of messaging abuse – spam, viruses and phishing – on fixed and mobile networks. There is no need to purchase, integrate or manage separate solutions for different types of threats.

OPERATING SYSTEM REQUIREMENTS

Solaris

Solaris 8, 9, 10

FreeBSD

FreeBSD 5, 6

Windows

Windows Server 2000
Windows Server 2003

Linux

Cloudmark supports any Linux distribution with the required libraries installed, and certified RedHat Enterprise Linux ES 2.1 or higher or RedHat 8 or higher

COMPATIBILITY

Solaris

- 32 bit (SPARC platform)
- 64 bit (SPARC platform)
- X86_64 bit (Intel platform)

FreeBSD

- 32 bit x86
- 64 bit x86

Windows

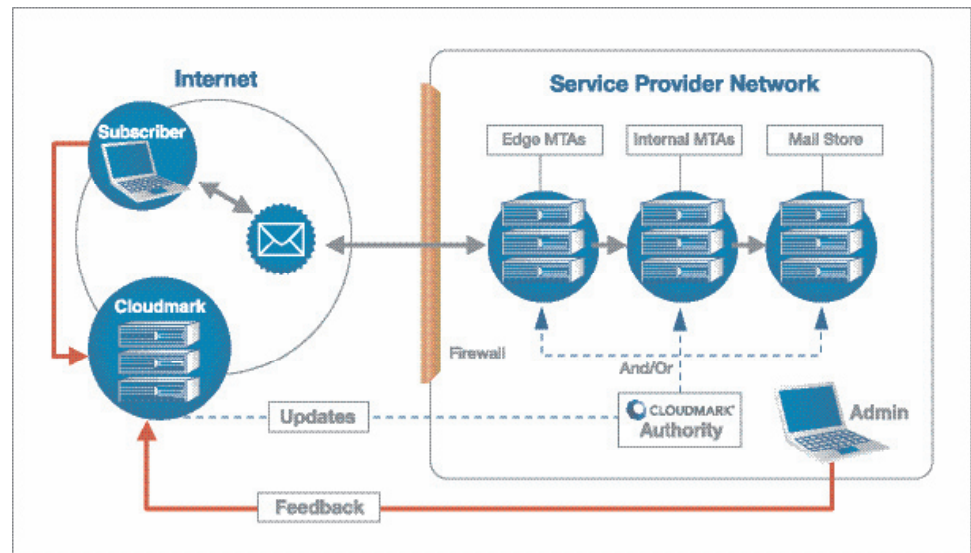
- 32 bit x86
- 64 bit x86

Linux

- 32 bit x86
- 64 bit x86

CLOUDMARK AUTHORITY IN THE SERVICE PROVIDER NETWORK

Cloudmark Authority is a fully automated system designed to block spam, phishing, viruses and other forms of messaging abuse. It can be integrated at any point along the message delivery path.



For more information visit us at 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