

## CLoudmark IMMUNITY

Real-time, automated and best-of-breed gateway anti-spam and anti-phishing protection for today's enterprises

### KEY BENEFITS

#### UNPARALLELED ACCURACY RIGHT OUT OF THE BOX

Blocks over 98% of spam and phishing attacks with near-zero false positives, enabling employees to focus on the emails they need.

#### UNIQUELY BLOCKS PHISHING ATTACKS

Real-time reputation data derived from trusted feedback forms a highly effective defense against short-lived phishing attacks.

#### AUTOMATED PROTECTION

Highly sophisticated fingerprint algorithms uniquely identify email. No IT administrator intervention is required, which frees up valuable time and IT resources.

#### ANTI-SPAM AND ANTI-PHISHING PROTECTION WHICH IMPROVES FURTHER OVER TIME

Cloudmark Immunity's unique feedback system improves accuracy in real time.

#### NO ONGOING MANAGEMENT

Cloudmark Immunity's closed-loop feedback system provides a simple way for users to report feedback and automatically uses it to improve accuracy—all without administrator or vendor intervention.

#### FLEXIBLE CONFIGURATION, SETUP AND DEPLOYMENT

Cloudmark Immunity plugs into existing infrastructures, and provides highly flexible user configuration, message handling and deployment options.

### ZERO-HOUR ANTI-SPAM AND ANTI-PHISHING RESPONSE

**THE NETWORK CLASSIFIER:** Cloudmark harnesses the power of the world's largest email threat network, consisting of millions of users in over 160 countries to process over half a billion messages a day. Real-time human feedback submitted into the Cloudmark Collaborative Network is automatically analyzed to block attacks within 20 seconds to 3 minutes of origin. This feedback is communicated to the gateway via automated micro updates.

A Trust Evaluation System is used to track the reputation of each member of the network, so that new threats are stopped immediately without the need for manual feedback review by the software vendor or operations centers.

#### ADD POWERFUL FINGERPRINT ALGORITHMS TO THE MIX

Cloudmark Immunity employs five fingerprinting algorithms—the same five fingerprinting algorithms used in all of Cloudmark's solutions. Immunity maintains an in-memory list of all known bad fingerprints, updating its list every minute with the latest data from the Cloudmark Collaborative Network. As each message comes in, Immunity generates the list of fingerprints for the message and checks each against its cache of known bad fingerprints; if there is a match then the message is marked as spam.

#### ANTI-SPAM AND ANTI-PHISHING PROTECTION WHICH IMPROVES FURTHER OVER TIME

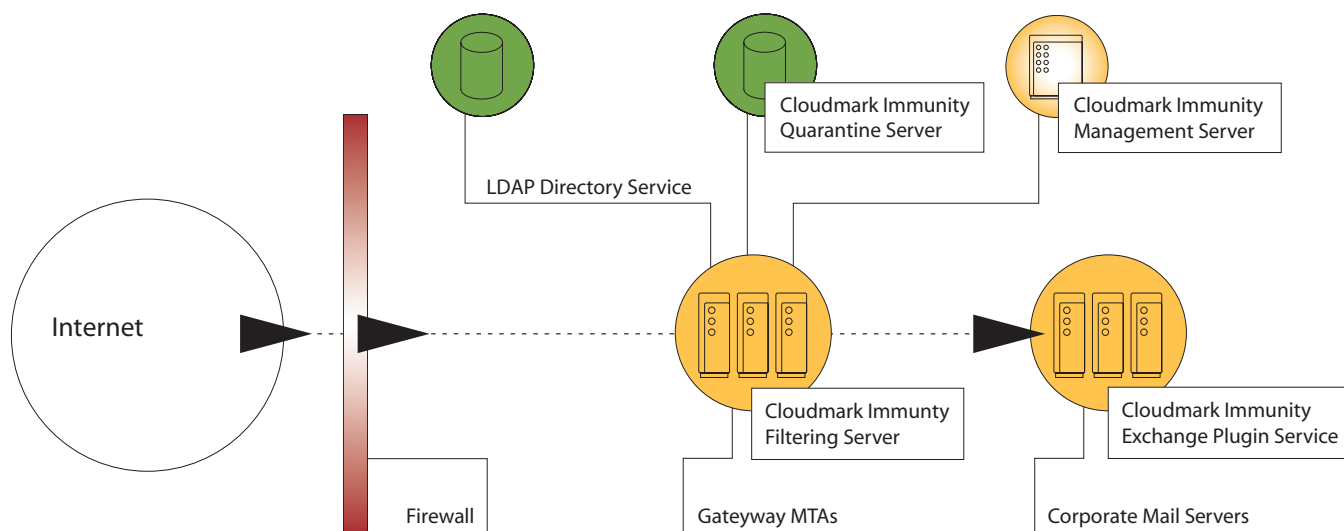
**THE FEEDBACK CLASSIFIER:** At the heart of Immunity is its Feedback Classifier, which enables end-users to report feedback. Organizations are able to achieve the highest accuracy rates and zero false positives through adaptive learning of what users consider legitimate or email abuse.

#### NO ONGOING MANAGEMENT

The Cloudmark Feedback Classifier improves filtering automatically, which frees administrators and users from the time-consuming, error-prone management of lists and rules. Although automatic, administrators retain overall control of how feedback is incorporated and by whom, and can override the classification and/or scope of feedback, if necessary.

Immunity's drag-and-drop feedback reporting enables users to indicate which messages they consider abuse or legitimate by simply dragging them into or out of their Spam Folder, without the need for any client-side software. Users do not need to infer information about the sender or domain as with whitelists and blacklists.

## CLOUDMARK IMMUNITY ENTERPRISE TOPOLOGY



Cloudmark Immunity deploys easily on existing infrastructure and runs on popular Linux, Solaris and Windows platforms.

### FLEXIBLE CONFIGURATION, SETUP AND DEPLOYMENT

Cloudmark Immunity is easy to deploy in nearly any environment. It runs on multiple platforms—Linux, Solaris or Windows—and supports both enterprise-class databases for the gateway quarantine and Microsoft Exchange for the mail server quarantine. Immunity's functional components can be split among separate servers and managed by a single management console. Immunity is designed for low impact on system resources and carrier-class scalability, allowing the filtering software to be installed on an existing Mail Transfer Agent (MTA) without the need for additional hardware.

### IMPROVED GROUP MANAGEMENT

Cloudmark Immunity provides flexible options for user management, feedback incorporation and message handling. User settings can be configured on a per-user, per-group or organization-wide basis using LDAP Directory Services. These settings determine which users are permitted to report feedback, the way they report it and whether it applies only to them or the entire organization. Phishing messages can be modified, deleted or stored in either a gateway quarantine or mail server quarantine (Spam Folder).

### BASIC SYSTEM REQUIREMENTS - WINDOWS AND LINUX

**OS** : Windows 2000/2003 Server  
: RedHat 8, Redhat ES 2.1, or higher  
**CPU** : 500Mhz x686 architecture  
**MEMORY** : 1GB RAM  
**STORAGE** : 300MB disk space

### BASIC SYSTEM REQUIREMENTS - SOLARIS

**OS** : Solaris 8 or 9  
**CPU** : SPARC or UltraSPARC server  
**MEMORY** : 1GB RAM  
**STORAGE** : 300MB disk space

**NOTE:** Storage requirements for quarantine depend on organization size and message retention policies.



### CLOUDMARK, INC.

128 King Street, 2nd Floor  
San Francisco, California 94107  
phone: 415.543.1220  
fax: 415.543.1233  
[www.cloudmark.com](http://www.cloudmark.com)  
[sales@cloudmark.com](mailto:sales@cloudmark.com)

© 2005 Cloudmark, Inc. All rights reserved. Cloudmark, the Cloudmark logo, Cloudmark Immunity, and Trust Evaluation System are trademarks or registered trademarks of Cloudmark Inc., for use in the United States and other countries. All other product or service names may be trademarks, registered trademarks, or service marks of their respective owners.