



# Cloudmark Server Edition

## BENEFITS

### Unparalleled Accuracy

Cloudmark blocks over 99% of spam, phishing, and virus attacks with near-zero false positives within moments of the launch of an attack.

### Ease of Administration

Functionality frees valuable administrative time and support resources. Without lists or rules to maintain, IT administrator intervention is not required.

### Installs in Minutes

Microsoft Exchange reboot or client-side software is not required.

### Efficient and Safe Mobile Messaging

Cloudmark Server Edition blocks spam and phishing attacks from reaching mobile devices, including Blackberry, Goodlink, and Palm devices via Blackberry Servers and Microsoft ActiveSync.

### Public Folder Support

Cloudmark Server Edition scans and protects public folders. Messaging abuse can be moved to a public folder, creating a centralized, administrator-controlled quarantine area.

## THE SIMPLEST, MOST EFFECTIVE ANTI-SPAM SOLUTION FOR MICROSOFT EXCHANGE ENVIRONMENTS

Cloudmark Server Edition delivers the industry's most effective and highest-performing anti-spam, anti-phishing, and zero-hour anti-virus protection available today.

Cloudmark Server Edition frees support resources, relieves system strain, and delivers an immediate improvement in filtering performance. This allows for fewer help desk calls, decreased administrative management, and reduced storage costs. As a result, it achieves the industry's lowest total cost of ownership.

### AUTOMATIC FEEDBACK

End users can contribute directly to the Cloudmark Global Threat Network with simple drag-and-drop functionality that automatically reports corrections to the Cloudmark network.

### ZERO-HOUR VIRUS FILTERING

Cloudmark solutions provide the first line of defense against email-borne viruses. New virus threats are typically identified and filtered within a minute of first appearing in the Cloudmark Global Threat Network. The entire network is immediately protected, and threats are blocked before they can create damage and disruption. Now, emails that carry potential viruses are moved to a safe location for centralized, administrator-controlled quarantine.

### REPORTING

System administrators can view per-user statistics, including number of messages scanned, number of messages classified as spam, and number of messages blocked and unblocked by the end user.

### THE CLOUDMARK GLOBAL THREAT NETWORK

The Cloudmark Global Threat Network provides real-time feedback on spam, phishing, virus and other evolving threats. Combined with Cloudmark's distinctive, fully automated message analysis and classification process, it blocks the latest threats within moments of attack origin. The Global Threat Network processes billions of messages every day from over 1.6 billion mailboxes in 190 countries, including those managed by some of the largest wireline, wireless, and cable service providers in the world.

## FREE 15-DAY NO RISK TRIAL

Download now for instant protection.  
[www.cloudmark.com/server/download](http://www.cloudmark.com/server/download)

## SYSTEM REQUIREMENTS

### Cloudmark Server Processor

Intel Pentium or compatible 733-megahertz (Mhz) or higher processor

### Memory

256 megabytes (MB) of RAM, 512 MB recommended

### Operating System

Microsoft Windows 2000 Server/  
Microsoft Windows Server 2003/  
Microsoft Windows Small Business Server 2000 or 2003

### Mail Server

Microsoft Exchange 2000 Server/  
Microsoft Exchange Server 2003

### Hard Disk

20 MB of free disk space on the hard disk where you install CSE  
200 MB of free disk space on the system drive

### CSE Administrator Console Processor

Intel Pentium or compatible 733-megahertz (Mhz) or higher processor

### Memory

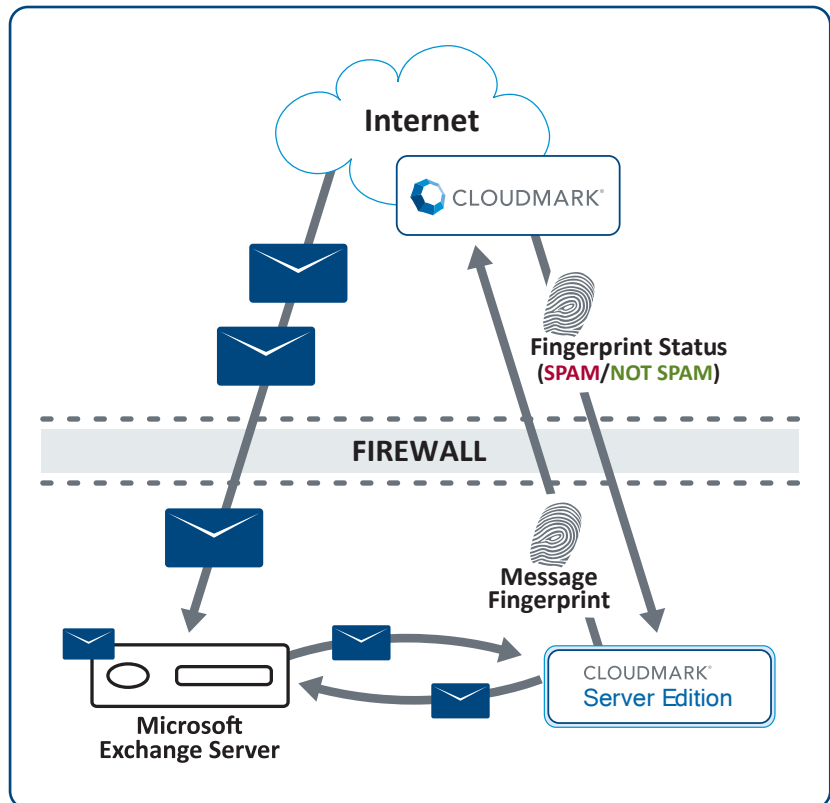
128 megabytes (MB) of RAM

### Operating System

Microsoft Windows 2000 Server/  
Microsoft Windows XP Professional/  
Microsoft Windows Server 2003/  
Microsoft Windows Small Business Server 2000 or 2003

### Hard Disk

5 MB of free disk space on the hard disk where you install CSE Administration Console



1. Email arrives at the Microsoft Exchange Server.
2. Cloudmark Server Edition uses fingerprinting algorithms to generate fingerprints for each message received that are then communicated to the Cloudmark Service.
3. Cloudmark service reports back on the status of messages (spam or legitimate).
4. If the message is spam, Cloudmark Server Edition instructs the Microsoft Exchange Server to move it to the spam folder.

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