

## KEY FEATURES AND BENEFITS

### Unmatched Intelligence

Only Cloudmark utilizes data on phishing and malware attacks from real users in addition to an extensive network of honeypots. Cloudmark is able to quickly detect low volume malicious attacks due to corroborated feedback from the Cloudmark Global Threat Network system and third party data partners.

### Industry Highest Accuracy

Cloudmark ensures the highest levels of accuracy through system-wide checks and balances. The Trust Evaluation System™ assigns a trust rating to each reporting source to ensure only reliable data is considered. Feedbacks are also corroborated before the data can be used. Continuously updated feedback immediately rectifies any malware false positives.

### Real-Time Protection

Since new phishing and malware attacks can be detected within minutes of its launch, Cloudmark often begins to block these attacks while they are still in progress, unlike other vendors employing static systems that are ineffective against fast-moving, transient attacks.

### ABOUT CLOUDMARK

Cloudmark, Inc. is a global leader in carrier-grade messaging security, delivering the most accurate, high-performance and comprehensive real-time spam, virus and phishing protection for fixed, mobile and social networks. Cloudmark patented solutions combine Advanced Message Fingerprinting technology based on innovative, highly efficient algorithms and a Global Threat Network consisting of trusted reporters in every country across the globe to provide security intelligence and filtering at all points of the messaging infrastructure. Cloudmark solutions protect more than 850 million mailboxes for the world's largest service provider networks, including over 75 percent of major ISPs in the United States and Japan.

## Complete, real-time protection against phishing and malware.

As Internet usage continues to grow, malicious attacks have evolved in sophistication, leaving users more susceptible to unsolicited attacks. Industry reports illustrate that there are more malicious code and unwanted programs released in 2008 than legitimate software applications. Within the first half of 2008 alone, there were 50,000 phishing attacks on over 25,000 unique domains. Today, there are many different types of threats that users may face, these include:

- Phishing websites disguised as legitimate institutions that steal confidential information
- Applications that are deployed undetected, resulting in unauthorized remote access

When user systems are infested with a Trojan and used as part of a botnet attack, those system resources are compromised; this abuse also impacts the service provider's own resources, consuming bandwidth and increasing resources needed to address the attack. Combined, these attacks negatively impact the service provider's reputation, often causing customer churn. In order to effectively combat and prevent these malicious attacks, service providers seek a solution that can detect malicious URLs quickly and accurately. Cloudmark provides the industry's most comprehensive, real-time phishing and malware protection to fight against these attacks and protect the service provider and the end user. Cloudmark utilizes real-time reporting from its Global Threat Network™ system along with fully automated data collection, analysis and update cycles to deliver the fastest response time to operators.

### Cloudmark Phishing and Malware URL Feed

The Cloudmark Phishing Malware URL Feed is an automated service that uses URL data collected by the Cloudmark Global Threat Network system. Cloudmark gathers live reports from its user base of over 850 million subscribers around the world to provide the latest information about new attacks. Once a URL has been confirmed to be malicious by Cloudmark, it is immediately added to the real-time data feed that service providers can retrieve. Cloudmark removes sites from the data feed once they no longer exist or are not seen by the Cloudmark Global Threat Network thereby ensuring our database remains continually accurate. Operators may leverage the data feed to develop better policies for network or web/browser level filtering.

### Cloudmark Authority Anti-Phishing and Anti-Malware Engines

The Cloudmark Authority Anti-Phishing and Anti-Malware engines scan inbound and outbound messages for malicious URLs at a rate 10 to 15 times faster than competitive solutions. Once a message containing a malicious URL is detected by the Cloudmark Global Threat Network system, it creates a new fingerprint. This fingerprint identifies and blocks the particular attack as well as future mutations. The set of known phishing and malware fingerprints is updated every 45 seconds, and new fingerprints are available within moments of a new attack being identified. At the time of detection, the malicious URLs are also added to the URL data feed every few minutes allowing customers to download and keep their systems updated.

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: +1.415.946-3800  
Fax: +1.415.946-3871

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