



ANTI-PHISHING SOLUTIONS

KEY FEATURES AND BENEFITS

Unmatched phishing intelligence

Only Cloudmark utilizes data on phishing attacks from real users instead of just “dumb” honeypots. Cloudmark is able to quickly detect low volume phishing attacks due to corroborated feedback from the Cloudmark Global Threat Network and the Trust Evaluation System

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 and corroborates all feedback. Continuously updated feedback immediately rectifies any phishing false positives. As a result, Cloudmark delivers more than 98% accuracy in filtering spam, viruses and phishing attacks with near-zero false positives.

Real-Time phishing protection

Within moments of the launch of a new phishing attack, Cloudmark begins blocking. Cloudmark stops attacks while they are still in progress, unlike other vendors employing static systems that are ineffective against fast-moving, transient attacks.

Carrier-Grade Performance and Scalability

Designed for large-scale carrier deployments, Cloudmark Authority with Anti-Phishing processes messages at near wire-speed throughput – 10 to 15 times faster than the nearest competitor while lowering CPU requirements by 90%. This capability minimizes infrastructure requirements and significantly lowers operational and hardware costs.

Cloudmark Phishing URL Feed and Cloudmark Anti-Phishing Engine

Phishing email attacks are a serious and rapidly growing problem for service providers, enterprises and consumers. Phishing differs from spam since it is generated by criminals intent on stealing personal data for financial gain. Phishers send emails and pose as legitimate institutions requesting sensitive information from email recipients. Phishing erodes consumer confidence in conducting business over the Internet and damages both institution and service provider brands.

Since phishing attacks are highly targeted and transient, they are difficult to stop. Traditional methods of capturing spam, which require seeing a sufficient volume of abuse before taking action, or solutions that rely on honeypots or probes for data collection do not work effectively against phishing threats.

Cloudmark Anti-Phishing™ utilizes real-time reporting from the Cloudmark Global Threat Network™ with fully automated data collection, analysis and update cycles to deliver the fastest response time to phishing attacks.

Cloudmark provides the industry’s most comprehensive, real-time phishing protection.

CLOUDMARK PHISHING URL FEED

The Cloudmark Phishing URL Feed is an automated service that uses phishing URL data collected by the Cloudmark Global Threat Network. Cloudmark gathers live reports from millions of reporters around the world to provide the latest information about new phishing attacks.

Once a URL has been confirmed as a true phishing site by the Cloudmark Trust Evaluation System (TES), the URL is immediately added to the real-time phishing feed that the service provider can retrieve over HTTP. Because phishing attacks are often short-lived, these feeds include only “live” URLs. URLs not seen by the Cloudmark Global Threat Network for more than five days are automatically removed. This Cloudmark service can be integrated into the service provider’s filtering policies for an additional layer of protection – without the need to replace the existing spam filtration system. This Cloudmark service can also be integrated into web-based filters such as browser plug-ins or Web proxy filters.

CLOUDMARK AUTHORITY ANTI-PHISHING ENGINE

The Cloudmark Authority Anti-Phishing engine is a module in the Cloudmark Authority messaging anti-abuse solution. This high-performance engine scans inbound and outbound messages for phishing at a rate 10 to 15 times faster than competitive solutions. Once a phishing message is found by the Cloudmark Global Threat Network and is validated by TES, the unique fingerprint for the message is automatically added to Cloudmark Authority’s cache. This fingerprint identifies and blocks the particular phishing attack as well as future mutations. The set of known phishing fingerprints is updated every 45 seconds, and new fingerprints are available within moments of a new attack being identified.

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.

Carmelite, 50 Victoria Embankment
Blackfriars, London EC4Y 0DX UK
Ph: +44 (0)207 100 5224
Fax: +44 (0)207 100 5224

Cloudmark Japan

Kato Building 6F
2-11-3 Iwamoto-cho
Chiyoda-ku
Tokyo 101-0032 Japan
Tel: +81 (3)5532 7636
Fax: +81 (3)5532 7373