

KEY BENEFITS

Automated rapid response to new outbreaks

Stop viruses in minutes, rather than hours or days, by avoiding the latency created by the manual collection, analysis, signature creation, QA and dissemination of new definitions of traditional anti-virus solutions.

Prevent proliferation without shutting down IP ranges or carrier services

Immediate identification and blocking of virus threats means your messaging services continue running and your customers' mail gets through without being blocked by other carriers, and vice versa.

Improved customer relations

Cloudmark protection affords users greater satisfaction, as mail does not have to be slowed for intensive scrutiny and processing.

Resistance to mutation

Without human intervention, Cloudmark automatically reverse-engineers the elements of the virus that are most likely to identify just that worm and its prospective variations.

Ease of use

No AV team intervention is necessary for protection against viruses, preventing delays in responsiveness.

Future proof

The AV fingerprinting algorithm is designed to identify viruses even in their mutated form.

Supported in existing Cloudmark solutions

The virus fingerprinting algorithm is incorporated in all of Cloudmark's solutions, from desktop to server to gateway, to provide broad protection.

AV Fingerprinting Algorithm

Cloudmark's new anti-virus fingerprinting algorithm rapidly detects and blocks email-borne viruses.

The threat and severity of viruses and worms is on the rise, making it perhaps one of the most dangerous issues a service provider must deal with in today's messaging environment. The risks are high, and the coping mechanisms required by carriers are extremely expensive. The burgeoning address books of a communications-intensive populace promote rapid, global proliferation of these treacherous threats. The ability to rapidly detect and block viruses to provide a first line of defense can save a service provider time, dollars and reputation.

Already known worldwide for industry-leading accuracy and efficiency, Cloudmark enhances its ability to rapidly detect and block all messaging threats with a virus-specific fingerprinting algorithm.

Cloudmark's zero-hour executable fingerprinting algorithm disassembles executable code to generate fingerprints that identify new worms and virus strains in real time. The algorithm automates and speeds the response process by which suspect emails are evaluated and reported by highly credible reviewers worldwide, in all languages. Cloudmark's worldwide network of "human honeypots" and proven reporters, along with its unique automated data analysis, squelches virus attacks considerably faster than alternative approaches that require time-consuming analysis and new rules creation.

Cloudmark's zero-hour/real-time front line of AV defense detects and halts viruses within moments of first appearance in the Cloudmark Collaborative Security Network™.

Zero-hour/real-time AV protection

In the most effective and intelligent combination of technology and human discretion, Cloudmark's massive installed base of malware reporters instantly responds to threats, corroborating automated fingerprinting to immediately stop a virus.

Ubiquitous, global protection

Micro-updates are provided every minute to instantaneously protect all users when the virus is identified – no need for downloading and installing definitions and rules desktop-by-desktop.

Cannot be deceived

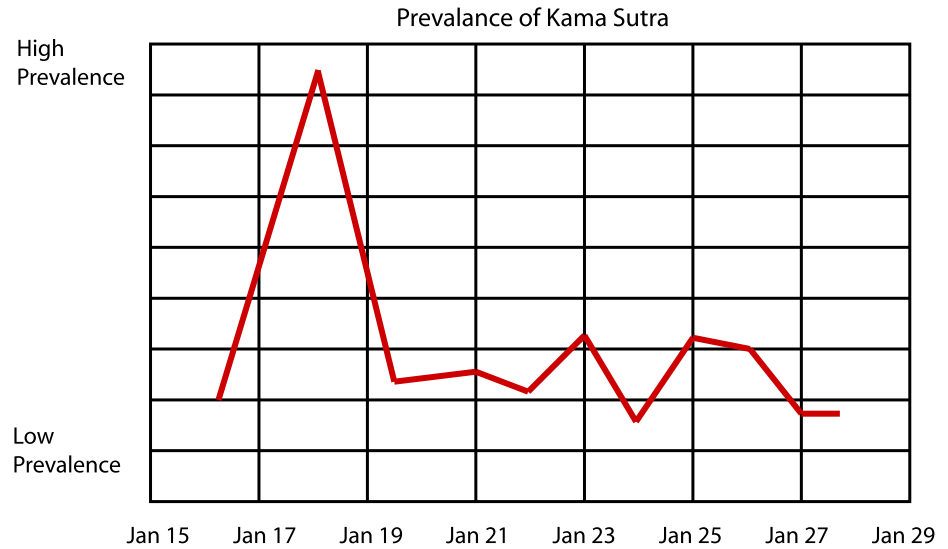
The Cloudmark secure messaging system combines reporters ranked and rated by the global Trust Evaluation System™ (TeS) with highly proficient, automated recognition algorithms.

Normal user interaction

Users simply vote on virus-carrying messages, as they do spam or phishing messages, in the Cloudmark Collaborative Security Network, or they leave messages in the spam folder where they will be automatically deposited, preventing the inadvertent launching of dangerous attachments.

Worldwide data collection by millions of users in every language

Rated, trusted users in 163 countries report on billions of messages a day from more than 100 million mailboxes.



STOPPING KAMA SUTRA: CLOUDMARK'S AV SOLUTION IN ACTION

Cloudmark was first to detect and block the Kama Sutra virus from its users, approximately 15 minutes after its first appearance in the Cloudmark Collaborative Security Network. The next nearest competitor stopped it more than four hours later, and the leading anti-virus giants were a day behind.

For more information visit us at
www.cloudmark.com
128 King Street, 2nd Floor
San Francisco, CA 94107 USA
Ph: +1.415.543.1220
Fax: +1.415.543.1233