



MailFrontier Gateway with MailFrontier Power Protection

MailFrontier Gateway offers

- Anti-Spam
- Anti-Phishing
- DHA/DoS Attack Safeguards
- Compliance Tools
- Policy Management

MailFrontier Power Protection adds

- MailFrontier Time Zero Virus Technology
- Virus Signatures
- Zombie Detection

Fully integrated with MailFrontier Gateway management, quarantine, and reporting, MailFrontier Power Protection provides the best security for email-borne malware.

Virus Outbreaks

More than 100,000 computer virus threats exist today.¹

Viruses are expected to increase in 2005 and combine more frequently with spam and phishing emails to create blended threats that attack recipients on multiple fronts.²

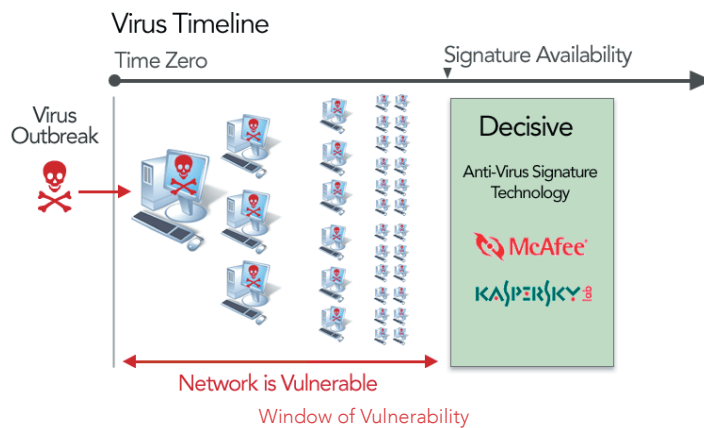
In 2004, viruses caused between \$166 billion and \$202 billion in global economic damages.³

MailFrontier Power Protection Module

MailFrontier Power Protection™ module extends MailFrontier Gateway™ Server and MailFrontier Gateway™ Appliance to deliver protection from viruses and zombies using MailFrontier Time Zero Virus Technology™, anti-virus signatures from Kaspersky and/or McAfee, and Zombie Detection.

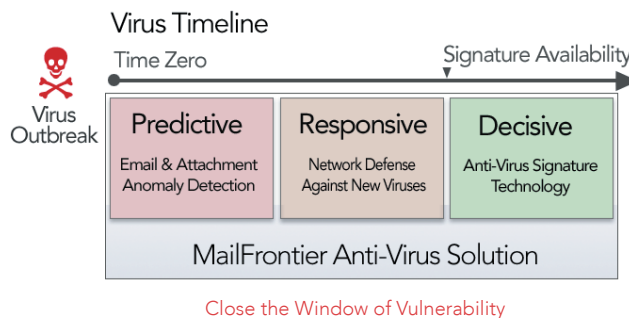
Standard Virus Protection Leaves Enterprises Vulnerable

Most anti-virus products rely primarily on signatures to stop viruses. Signatures are a critical component of anti-virus solutions. However, at the moment the outbreak occurs -- "Time Zero" -- a virus has the opportunity to do significant damage to your computer system before the virus is identified and a signature is developed and deployed. This window of vulnerability is often 24 hours or longer.



MailFrontier Time Zero Virus Technology Protects During Outbreaks

MailFrontier has developed breakthrough anti-virus methods in its MailFrontier Time Zero Virus Technology, which provides the only truly predictive and responsive techniques that stop viruses as soon as they emerge. These techniques are enhanced by MailFrontier's decisive dual-engine signature technology of partners McAfee and Kaspersky.



Predictive Techniques

- **Email and Attachment Profiling** uses statistical and heuristic methods to identify attachments that contain malicious code.
- **Deceptive File Type Detection** finds dangerous attachments that are masquerading as innocuous files.
- **Virus Traffic Analysis** monitors a company's normal email patterns to identify anomalies that may indicate a virus outbreak.

These methods are applied at time zero as the outbreak starts, prior to a virus signature being available. On November 13, 2004, time zero for Sober.J, MailFrontier's predictive techniques immediately stopped 4 out of the 5 virus variants.

¹ Statistic from McAfee Security Headquarters.

² Cox, Mark. "McAfee Warns of Changing Online Threat Patterns." eChannel Line. 9 January 2005.

³ The Mac Observer. "Study: OS X World's Safest OS From Security Attacks." MacNewsWorld. 2 November 2004.

MailFrontier Anti-Virus Partners



Kaspersky is a technology leader and acknowledged expert in the development of anti-virus signature technology. In tests conducted on 24 leading anti-virus vendors, Kaspersky was the fastest to create and deploy signatures.⁴



McAfee is the industry leader in dependable anti-virus signatures, protecting 100 million end users. McAfee Anti-Virus Emergency Response Team (AVERT) researches and provides rapid responses to viruses.

Zombie Consequences

- Corporate domain blacklisting
- Network bandwidth deterioration
- Intellectual property theft
- Costs to purge malicious code

At least one million hosts are compromised and can be controlled by malicious attackers.⁵

⁴ Marx, Andreas. "Anti-Virus Outbreak Response: Testing and Impact." AV-Test GmbH. September 2004.

⁵ "Know your Enemy: Tracking Botnets." The Honeynet Project and Research Alliance, 13 March 2005.



1841 Page Mill Road
Palo Alto, CA 94304
866-3NO-SPAM
www.mailfrontier.com

Responsive Techniques

MailFrontier applies its MailFrontier Self Monitoring Active Response Team (SMART) Network™, a real-time network of over one million global users whose responses enable MailFrontier to quickly identify and react to new email threats. Emails identified by MailFrontier SMART Network™ as containing dangerous attachments are immediately and safely quarantined. The fifth Sober.J variant was stopped by MailFrontier's responsive techniques.

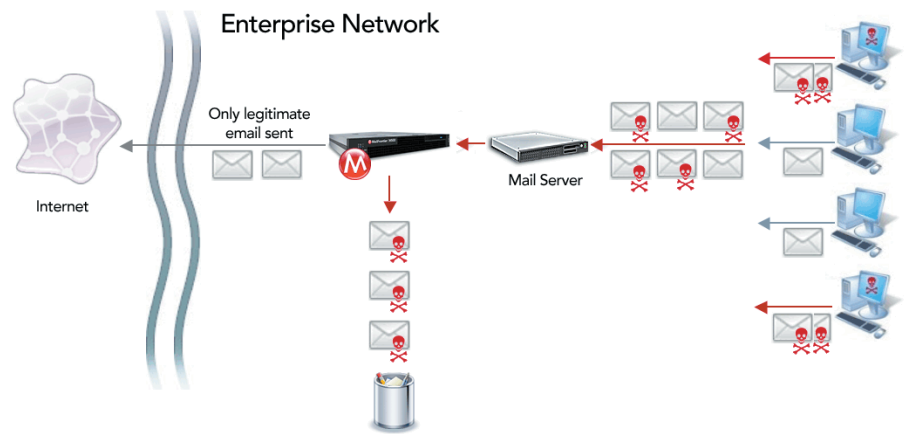
Decisive Virus Signatures

MailFrontier Time Zero Virus Technology is complemented with leading anti-virus signature engines from Kaspersky and McAfee. MailFrontier customers can select one or both of these signature engines, each of which has a comprehensive set of signatures that provide decisive protection against previously identified viruses.

Protection from Zombie, or "Hijacked," Computers

Malicious code can take over a computer on an enterprise's network, which is then used to send out dangerous emails, such as spam, phishing, and viruses, or to conduct Directory Harvest Attacks (DHAs) or Denial of Service (DoS) attacks. This hijacked computer is called a zombie because it has been secretly taken over to do the bidding of the hacker. A computer can become a zombie through any method of downloading a virus or Trojan, such as executable attachments to emails and downloads on Web sites.

MailFrontier Prevents Dangerous Emails Sent by Zombies



Emails from Infected Zombie Machines Are Stopped

MailFrontier provides zombie detection that employs multiple techniques to locate these dangerous machines and stop the transmission of outbound email threats. MailFrontier identifies emails sent from an address not in the corporate LDAP, outbound email spikes above configurable volume levels, and machines sending spam, phishing, or virus emails.

MailFrontier Power Protection: Security Against Malicious Code

The best protection today against malicious code, MailFrontier Power Protection with Time Zero Virus Technology protects from new virus outbreaks and also incorporates leading signature partners to eliminate known viruses. In addition, MailFrontier Power Protection includes zombie detection, which identifies and quarantines hijacked computers.