

WHITEPAPER

MailFrontier Anti-Virus:

A Complete Solution to
Protect Your Network From Outbreaks

Table of Contents

I. Executive Summary	1
II. Viruses: The Threat	2
III. Most Solutions Fall Short—Leaving Networks Vulnerable	4
IV. Extreme Measures During Window of Vulnerability	6
V. Protecting Your Network With Breakthrough Technology	7
VI. Effortless Implementation and Complete Control	10
VII. Conclusion	13
VIII. About MailFrontier	14

I. Executive Summary

Virus outbreaks cause considerable damage to enterprises because most current anti-virus solutions are unable to effectively protect networks at all stages of the outbreak. With most anti-virus products, networks are left vulnerable during the dangerous window between the time a virus first appears and the time a signature is developed and deployed that will remove the virus. Virus outbreaks during this window are known as “zero-day viruses” and although this window can be just a few hours, without time zero protection it can take only minutes to damage your computer network and cause costly clean up.

MailFrontier offers the first holistic anti-virus solution that provides predictive, responsive, and decisive protection to defend against viruses during all stages of the outbreak. MailFrontier combines predictive and responsive techniques in its MailFrontier Time Zero Virus Technology™, which protects computer networks when these systems are most vulnerable—the time between when viruses are first unleashed on the Internet and when a signature is deployed. The MailFrontier Time Zero Virus Technology is complemented by MailFrontier’s decisive approach, which applies the leading anti-virus signature engines of partners Kaspersky and McAfee. This multi-layer defense against viruses protects users from known viruses as well as new, unique outbreaks.

II. Viruses: The Threat

More than 100,000 computer viruses exist today and viruses are expected to increase in 2005.

Email is the primary method of transmitting viruses —through attachments or links provided in the email.

Virus emails are sent out en masse, infecting thousands if not millions of computers in just minutes.

Virus Damage:

- Destroying computer files
- Modifying or stealing files
- Opening security holes
- Crashing networks and systems

Requires costly and time consuming clean-up.

A computer virus is an uninvited malicious program. Viruses began as pranks that programmers played on one another. Since then viruses have grown and are now a threat to all computer users. In 2004 viruses, including Trojans, and worms, continued to spread at an unrelenting pace.¹ Threats specifically targeted at vulnerabilities in operating systems exceeded 380 in 2004, which was approximately a 50 percent increase from 2003. In total, more than 100,000 computer virus threats exist today.³ Viruses are expected to increase in 2005 and more frequently combine with spam and phishing emails to create blended threats that attack recipients on multiple fronts.²

In the early history of viruses, people feared the spread of malicious code through sharing floppy disks. Today, email has become the primary method of transmitting malicious code. The virus is generally in a file attached to the email, which downloads when the attachment is opened, or launched through a link provided in the email.

Spam techniques enable these virus emails to be sent out *en masse*, allowing hackers to infect thousands, if not millions, of machines in just minutes. As early as May 2000, the “I Love You” virus infected millions of machines overnight. The virus was in an email attachment, that when opened, sent itself to everyone in the victim’s address book and then corrupted files on the victim’s computer. Another email threat, the Sober email worm, first appeared in October 2003 has since been sent out in many variants. The Sober version sent out in November 2004 began in Europe, and by the end of the same work day, had spread across North America.

The malicious code in viruses can do extensive damage, including destroying computer files, modifying or stealing files, opening security holes, and crashing networks and systems, which causes severe security, productivity, and financial losses. No matter what the damage caused by a virus, once a network is infected, it requires extensive IT time and effort to purge the network of the virus and minimize the damage. This costly clean, up depletes company funds and IT resources.

¹ “Review of 2004 Shows Malware Continuing at Unrelenting Pace” Kaspersky Labs. 6 December 2004. <<http://www.kaspersky.com/news?id=155897089>>

² Cox, Mark. “McAfee Warns of Changing Online Threat Patterns.” 9 January 2005. eChannel Line. <<http://www.integratedmar.com/ECL.cfm?item=DLY010905-5>>

³ Statistic from McAfee Security Headquarters. <<http://www.mcafeesecurity.com/us/security/home.asp>>

In 2003, each virus incident cost an organization an average of \$213,000.

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

Viruses are able to cause considerable damage because most anti-virus solutions are unable to adequately protect computers. In an article titled, "Fear of Viruses and Poor Protection Grows" the author states, "According to separate research from the FBI, 99 percent of businesses have anti-virus protection. Yet in 2003, 82 percent were attacked by a virus, resulting in more than \$200 billion in losses."⁴ In 2003, each incident of malicious code is estimated to have cost an organization an average of \$213,000 in work hours and related costs.⁵ In 2004, viruses, Trojans, and worms are estimated to have caused between \$166 billion and \$202 billion in global economic damages.⁶

⁴ Sturgeon, Will. "Fear of Viruses and Poor Protection Grows." CNET News.com. 6 July 2004. <http://news.com.com/Fear+of+viruses+and+poor+protection+grows/2100-7355_3-5258497.html?tag=cd.top>

⁵ Gartner Technology Overview "Virus and Malicious Code Protection Products: Technology Overview", Noakes-Fry, Kristen. 24 February 2004

⁶ The Mac Observer. "Study: OS X World's Safest OS From Security Attacks." MacNewsWorld. 2 November 2004. <<http://www.macnewsworld.com/story/Study-OS-X-Worlds-Safest-OS-From-Security-Attacks-37788.html>>

III. Most Solutions Fall Short—Leaving Networks Vulnerable

Signatures are a critical component to an anti-virus system, but when used alone, leave a window of vulnerability.

The majority of anti-virus solutions are based on signatures. Signatures are a critical component of an anti-virus solution because when a new virus is discovered, a signature is created that can identify the virus and safely remove it.

However, it takes time for signatures to be developed and deployed. First the virus must be found, which means that someone may have fallen victim to the virus to first identify its existence. Then the virus must be analyzed and a signature created that works across all applicable platforms. This time ranges from 4 to 16 hours with the average response time at 10 hours.⁷

Yet damage can occur in just minutes. This creates the “time zero” window of vulnerability between the time a new, unique virus is released and when a signature is developed and deployed. If an anti-virus solution relies solely on signatures, its users are unprotected during this window of vulnerability.

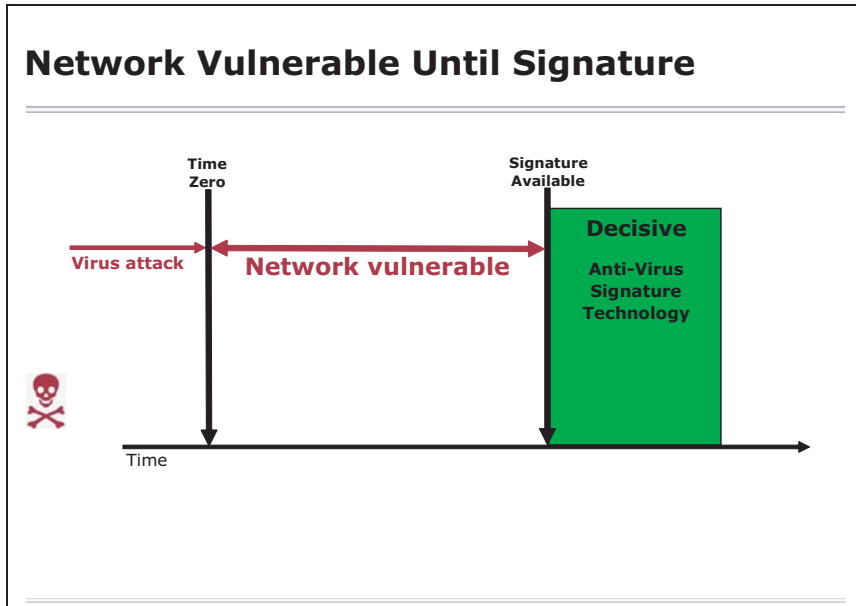


Figure 1: Window of Vulnerability

⁷ Marx, Andreas. "Anti-Virus Outbreak Response: Testing and Impact." September 2004. AV-Test GmbH. <www.av-test.org>

Signature should be provided from multiple engines through timely and easy updates.

Very few anti-virus solutions consider the virus delivery vehicle—the email.

Not only does a signature need to be developed, but it must also be made available to the solution's users. Many anti-virus solutions do not provide updates in a timely manner or instead provide burdensome update procedures. Most solutions which rely on signatures are further limited by only offering protection of signature engine from a single company. The customers may not have the most timely access to a virus signature because they rely on how quickly that one company develops its signature.

In addition, very few anti-virus solutions consider today's most common virus delivery vehicle—the email. Most anti-virus solutions merely focus on the malicious code itself.

IV. Extreme Measures During Window of Vulnerability

During time zero, extreme measures to protect a network damage a company's productivity and are ineffective at stopping viruses.

As already discussed, many anti-virus solutions rely solely on signatures, which leaves an enterprise vulnerable. If a new virus outbreak becomes known and a signature has not yet been deployed, some enterprises have resort to extreme measure to protect their networks, such as:

- Sending out multiple "do not open" emails
- Blocking zip files or all attachments or
- Disconnecting their network from the internet until the virus signature is available

These are drastic approaches that damage a company's productivity and are ineffective at stopping viruses. And these actions are only possible if the enterprise is aware that a new virus has been released. A network with only signature protection is an open target for a new, unknown virus.

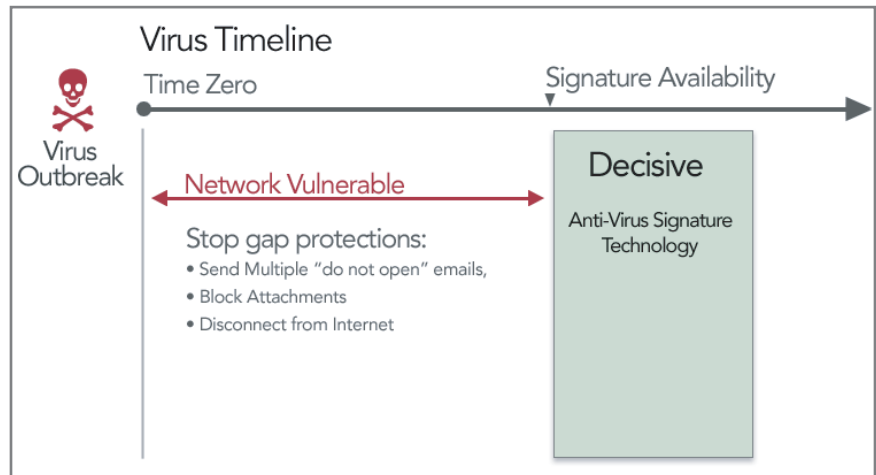


Figure 2: Extreme Measures Taken During Time Zero

Companies need complete protection—both during the critical time zero period and after a signature has been deployed. Predictive and responsive techniques need to be applied during time zero when signature is not available. These techniques must be achieved through the skillful application of analysis supported by large diverse datasets of both emails and attachments and global user feedback to stay on the pulse of the Internet. This approach should be coupled with decisive support from multiple signature engines with timely updates. A combination of methods of this sort in a single solution would provide a company with complete protection during all periods of a virus outbreak—keeping the enterprise secure.

V. Protecting Your Network With Breakthrough Technology

MailFrontier Time Zero Virus Technology adds two new layers of defense—predictive and responsive techniques.

Known viruses are safely removed through MailFrontier's decisive dual-engine signature technology.

MailFrontier has developed breakthrough anti-virus technology presenting the only truly predictive virus defense complemented with responsive techniques to stop viruses as soon as they emerge and decisive signature protection that removes known viruses. MailFrontier leverages its expertise in email threat protection to provide a comprehensive approach that ensures a company's email remains secure before, during, and after a virus outbreak.

MailFrontier Anti-Virus has added two layers of defense with predictive and responsive techniques in its **MailFrontier Time Zero Virus Technology™**. These layers are enhanced by MailFrontier's decisive dual-engine signature technology. With MailFrontier Time Zero Virus Technology, emails potentially containing new viruses are identified and safely quarantined, while known viruses are recognized and removed by virus signatures

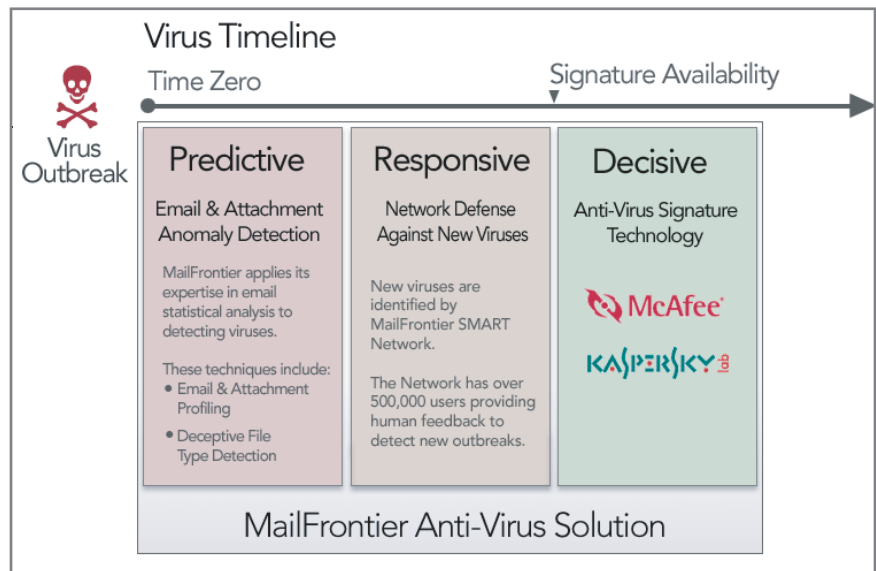


Figure 3: MailFrontier's Complete Anti-Virus Solution

Predictive:

MailFrontier's expertise in statistical analysis is applied to identifying malicious code and detecting deceptive files.

Responsive:

MailFrontier Self Monitoring Active Response Team (SMART) Network of over 825,000 global users provides feedback on millions of emails.

Decisive:

MailFrontier provides signatures from two leading anti-virus signature engines—Kaspersky and McAfee.

Predictive: Email Attachment and Anomaly Detection

The first level of protection employs predictive techniques which are used to discover potentially dangerous emails and attachments. MailFrontier has extensive expertise in applying statistical analysis to stopping email threats. Now Mailfrontier applies this expertise to detecting viruses.

- **Email and Attachment Profiling** uses statistical methods and heuristic rules to identify emails with attachments that contain malicious code. These profiling techniques are highly effective because MailFrontier has access to a diverse dataset of millions of emails which are used to accurately establish the rules and statistical probabilities that are applied.
- **Deceptive File Type Detection** finds dangerous attachments that are masquerading as innocuous files. This technique includes checking MIME exploits to find attachment inconsistencies in the email which can be an indicator of a dangerous attachment.

These predictive methods can identify seemingly innocent attachments that may be harboring malicious code.

Responsive: Network Defense Against New Viruses

The second level of anti-virus protection is a responsive approach that stops new viruses after they have been released into the Internet community but before a signature has been created. This method utilizes MailFrontier **Self Monitoring Active Response Team (SMART) Network™**. This expansive network is comprised of over 825,000 global users who provide feedback on a diverse set of millions of emails. MailFrontier once again utilizes its expertise in statistical methods and heuristic rule development to analyze this real-time user feedback to detect and terminate new threats. Emails identified by MailFrontier SMART Network™ that contain dangerous attachments are immediately and safely quarantined.

These first two levels of anti-virus protection encompassing both predictive and responsive techniques comprise **MailFrontier Time Zero Virus Technology**, delivering real-time protection for the network during the critical time zero window. MailFrontier's anti-virus solution safely contains the potentially infected emails, but allows access to these emails if necessary, similar to a email junk box, ensuring that no email is lost.

Decisive: Anti-Virus Signature Technology

The innovation of MailFrontier Time Zero Virus Technology is complemented with leading anti-virus engines from Kaspersky and McAfee. These anti-virus engines have a comprehensive set of signatures that provide decisive protection against previously identified viruses.



Fastest anti-virus signature engine to create and deploy signatures.



Largest intrusion prevention appliance vendor in 2003.

Kaspersky and McAfee signatures safely remove any previously identified virus.

- **Kaspersky** is a technology leader and acknowledged expert in the development of external threat defenses. In tests conducted on 24 leading anti-virus vendors, Kaspersky was the fastest to create and deploy signatures.⁸ Kaspersky Labs supports one of the largest collections of virus definitions in the world, with over 82,000 records and counting.
- **McAfee** was the largest intrusion prevention appliance vendor in 2003. MailFrontier customers can access this up-to-date detection and prevention anti-virus technology as part of MailFrontier's holistic anti-virus package in a comprehensive email security suite.

MailFrontier customers can select anti-virus protection from one or both of these best-of-breed anti-virus signature engines. Having two leading anti-virus signature engines ensures that customers will receive signatures quickly that safely block and remove viruses.

⁸ Marx, Andreas. "Anti-Virus Outbreak Response: Testing and Impact." September 2004. AV-Test GmbH. <www.av-test.org>

VI. Effortless Implementation and Complete Control

Unparalleled ease in implementation and management.

In addition to offering the best anti-virus protection, MailFrontier's anti-virus solution provides unparalleled ease of implementation and management. The anti-virus module is integrated into the complete MailFrontier solution. MailFrontier's email security solutions are deployed in under an hour and managed in minutes each week.

MailFrontier provides an easy-to-use web interface that allows for unified administration of all email options.

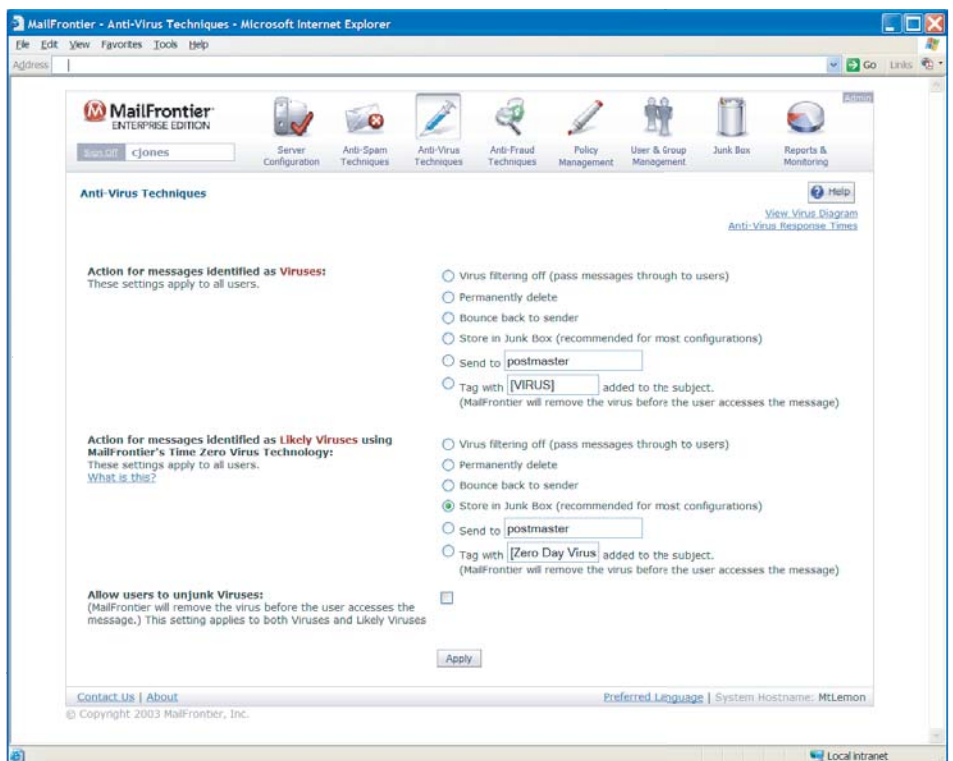


Figure 4: Easy-to-use web interface for unified administration

The administrator's anti-virus user interface is pictured above. The options apply to both viruses identified by the signature engines and likely viruses identified by MailFrontier Time Zero Virus Technology.

The administrator can choose whether to turn virus filtering on for either or both of these filtering methods. If turned on, the administrator can choose whether viruses or likely viruses are permanently deleted, bounced back to sender, stored in the Junk Box, sent to a particular mailbox, or tagged with "Zero Day Virus" or other message at the beginning of the subject line. These options give the administrator the flexibility to manage virus emails in the manner that best meets the needs of the company.

The administrator can also designate how often the system is updated for virus, spam, and phishing with time intervals ranging from 5 minute up to 12 hours. Once the time interval is selected, the virus signature files are automatically updated, eliminating the administrative burden of updating files and ensuring timely protection.

Administrators can:

- Quickly configure virus and likely virus filtering options.
- Designate the time intervals for signature updates.
- Generate informative reports on viruses.

The web-based administrator interface can also be used to generate virus reports. Figure 5 is an example of the Junk Email Breakdown report which shows the daily count for viruses and likely viruses as well as other email threats. In addition, reports specific to viruses can be generated, including Viruses Caught, and Viruses by Name.

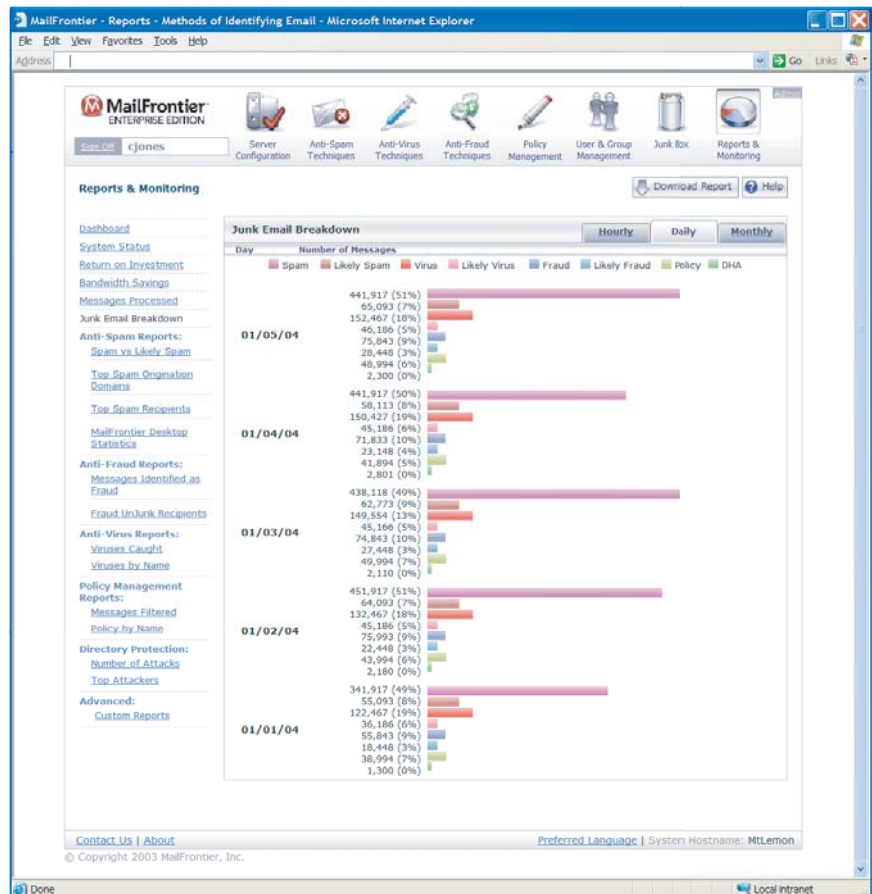


Figure 5: Junk Email Breakdown Report showing daily count for email threats

Administrators can opt to give end users safe access to their quarantined virus emails.

Administrators can opt to give end users independent access to view the list of their quarantined emails, including viruses and likely viruses, through their personal Junk Box Summary. Users can view emails from the Junk Box Summary in Safe Mode by clicking on the email subject line. The email is viewed as text only, ensuring that no malicious code is launched while the email is being read.

Administrators can also allow users to "unjunk" emails designated as viruses or likely viruses, which places the email back into the user's inbox. If a user unjunks a virus, MailFrontier removes the virus before the user can view the message, once again ensuring the network remains safe.

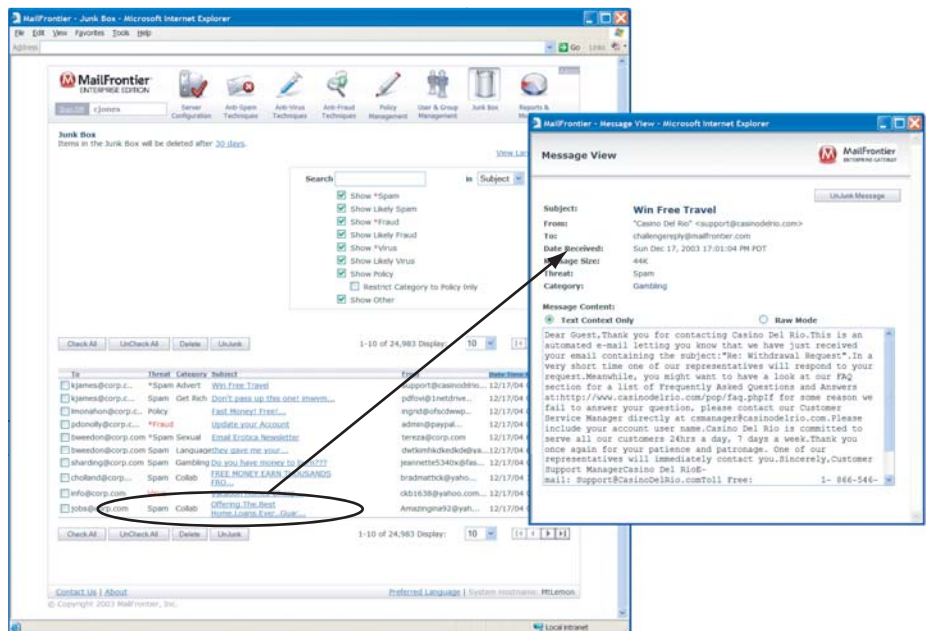


Figure 6: End users can open viruses from their Junk Box summary in Safe Mode

With quick configuration, easy maintenance, informative reports, and optional end-user access, IT administrators need only allocate minimal resources to protect their networks with MailFrontier's anti-virus solution.

VII. Conclusion

MailFrontier Anti-Virus provides the only truly comprehensive protection with a predictive, responsive, and decisive approach to guarding networks against virus outbreaks. MailFrontier Time Zero Virus Technology uses predictive techniques to detect emails that potentially contain viruses and uses a responsive approach through its MailFrontier SMART Network™ to stop viruses released in the Internet community. Both the predictive and responsive approaches safely quarantine emails with viruses while known viruses are safely removed by McAfee or Kaspersky signature engines. This technology safeguards the network during time zero, when other solutions fall short. MailFrontier marries this complete anti-virus protection to effortless management and maintenance to ensure that enterprises can easily secure their networks.

When added to MailFrontier's email security suite, MailFrontier Anti-Virus completes a comprehensive email security solution that can protect against stand alone email threats as well as blended threats such as viruses in spam or fraudulent phishing emails. MailFrontier keeps customers a step ahead of every form of email threat.

VII. About MailFrontier

MailFrontier guards the perimeter of the enterprise against the costly, dangerous, and growing threats to corporate email. Threats are stopped before they infiltrate corporate mail servers and employee inboxes. MailFrontier secures company connections and blocks unwanted email while ensuring timely delivery of all legitimate email. MailFrontier Gateway™ products provide comprehensive protection against phishing, spam, directory harvest attacks, viruses, and email policy violation. The solution is dynamic, self-learning, and self-running, providing IT departments with the hands-off protection they need. MailFrontier Gateway products offer redundancy, comprehensive reporting, and central administration across multiple data centers. The solution scales for enterprises of over 100,000 employees. Fortune 1000 businesses across virtually every industry protect their email with the MailFrontier solution, including media and entertainment, insurance, financial services, utilities, healthcare, manufacturing, high technology and other sectors. MailFrontier has more than 900 customers including Pier 1 Imports, Wyndham Hotels & Resorts, and the San Francisco Giants.



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