

WHITEPAPER

Protecting Your Email: MailFrontier Technology Overview

Table of Contents

I. Executive Summary.....	3
II. View the Lifecycle of an Email Attack.....	4
The Lifecycle of an Attack Is Broader Than the Email.....	4
Email Security Challenges.....	4
III. Apply Technology to Email Threats.....	7
MailFrontier Reputation Service Paired with Authentication.....	7
MailFrontier Content Evaluation.....	7
<i>Adversarial Bayesian</i>	7
<i>Bayesian Fraud</i>	8
<i>Lexigraphical Distancing</i>	8
MailFrontier SMART Network.....	8
Time Zero Virus Technology.....	8
MailFrontier Contact Point Validation.....	9
<i>Browser Exploit Detection</i>	9
<i>Social Engineering Trick Checks</i>	9
<i>Real-Time Phishing List</i>	9
IV. Stop Spam.....	10
V. Protect Against Viruses.....	12
VI. Prevent Phishing.....	14
VII. Safeguard Against DHA/DoS Attacks.....	16
VIII. Stop Infected Zombie Machines.....	17
IX. Comply with Regulatory and Corporate Compliance.....	18
X. Free Up Your Resources with Easy Management.....	19
Quick & Flexible Configuration.....	19
Auto-Updates	19
Flexible Policy and Group Management	19
Centralized, Web-Based Console for Administering All Junk Boxes	20
Personalized End-User Controls	20
Robust Reporting: Visibility into Your Email Flow	21
XI. Achieve High Performance.....	22
MailFrontier Preemptive Scanning MTA.....	22
Redundant High Availability Deployments	22
Infrastructure Consolidation	23
XII. About MailFrontier.....	24
XIII. How Can I Protect My Organization?.....	27

I. Executive Summary

Email threats have increased dramatically over the past several years, from a mere annoyance to an estimated cost to businesses of \$20 billion per year.¹ Email has evolved into a medium for spam, viruses, phishing, and other email threats; any one of which can impose a significant cost on a company. To combat this problem, MailFrontier provides a comprehensive solution in its MailFrontier Gateway™ products which offer the best protection, effortless control, and high performance.

Best Protection

MailFrontier protects networks from all inbound and outbound email threats using MailFrontier Cognite™, an end-to-end email attack monitoring system that identifies and stops email attacks. MailFrontier Cognite tracks the reputation of the email servers, evaluates message content, analyzes the impact on recipients, and checks any embedded URLs. Through MailFrontier Cognite, Mailfrontier Gateway covers all email security needs.

- Anti-Spam
- Anti-Phishing
- Anti-Virus
- DHA and DoS Protection
- Internal Zombie Detection
- Time Zero Virus Protection
- Policy Management
- Compliance Tools
- Blended Threats

Effortless Control

MailFrontier makes managing email security easy. MailFrontier Gateway is designed to ensure simple configuration, easy customization, and automated maintenance, all through an easy-to-use, Web-based administrative interface. MailFrontier Gateway is installed and configured in under an hour and is managed in less than 10 minutes a week, reducing the burden on IT staff.

- **Quick Configuration** in less than an hour, protecting your network as soon as it is installed
- **Auto-Update** of all data and software, reducing the administrative maintenance
- **LDAP Integration**, enabling easy group and user-level flexibility while IT retains complete control
- **Streamlined Group and End-User Management**, creating specific rules for the organization, group, or mailbox with just a few clicks or delegating administrative privileges to groups or end users with ease
- **Personalized End-User Controls** at IT discretion within corporate limits, enabling users to access their junk box without burdening IT administrators
- **Detailed Reporting**, providing easily customizable system-wide and granular reporting including information on attack types, solution effectiveness, and system performance

High Performance

MailFrontier provides high performance through its unique MailFrontier Preemptive Scanning MTA™ that offers breakthrough message analysis and industry-leading message delivery rates that are 40-290% faster than other email security solutions.² Such a solution needs fewer machines to process the email load, resulting in reduced management complexity with lower capital and operating costs.

MailFrontier combines the best protection with effortless control and high performance to ensure that enterprises get a “no compromise” solution that can easily and effectively secure their networks.

¹ National Technology Readiness Survey, Rockbridge Associates, Inc. and the Center for Excellence in Service at Maryland's Business School, 11/2004.

² “Analyzing the Spam Test Results.” *Network World*. 12/20/04.

II. View the Life Cycle of an Email Attack

The complexity and sophistication of email attacks are increasing as email threat types proliferate and blend together. Today a typical email attack is a global event. All email attacks, whether spam, viruses, phishing, or other attack type, follow a similar lifecycle.

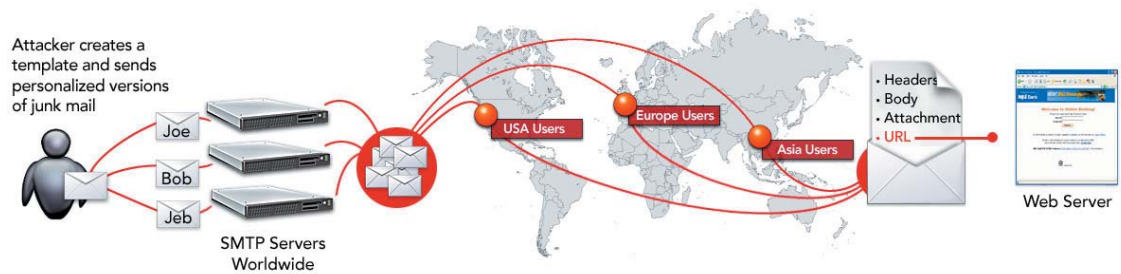


Figure 1. Lifecycle of an Email Attack.

The Lifecycle of an Attack Is Broader Than the Email

To effectively stop email attacks, a solution must look at the entire lifecycle, not just the email itself. The email security solution must consider the sending server; the email content; any attachments; embedded URLs and other contact points; any Web sites to which the embedded URLs link; the recipient; and the effect on the email community. Merely focusing on the email will miss many of the identifiers of an attack and will not consider some of the broader ramifications. For example, does the embedded URL take the recipient to a known fraudulent Web site that can download malicious code? The lifecycle starts with the sender, not the email, and ends with the last effect on the recipient.

In addition to being global in nature, email attacks often contain blended threats. For example, spam and phishing emails can contain viruses. Stand-alone products are a thing of the past as more and more customers turn to complete email security products.

Email Security Challenges

Many email security solutions limit their analysis to the email and do not consider all aspects of the attack, reducing their effectiveness. Email security products tend to fall into the following traps:

Effective
Source Code

Using Open Source or Outsourcing Email Protection

Incorporating a third party's solution, either by using open source code or outsourcing types of threat protection, limits support and can cause significant delays in resolving problems and providing updates. In addition, products that use open source code to stop email attacks (for example, open source anti-spam protection) leave themselves vulnerable to attack. Open source code is also available to spammers, fraudsters, and hackers, making it easier for them to get around the email security defenses. To ensure effective and timely protection, an email security solution must use a secure code system created by the solution vendor.

Threat Type:
Virus

Only Scanning Attachments for Known Viruses

Most anti-virus products are solely based on signature engines which scan emails and attachments in search of known viruses. Although signatures are an important part of virus scanning, users are left vulnerable between the time a virus is discovered and the signature is developed and deployed. Emails need to be scanned using predictive techniques in addition to signatures to ensure that users are safe during all phases of a virus outbreak.

Threat Type:
Virus

Relying on Only One Virus Signature Engine

When anti-virus protection is based solely on a single anti-virus signature engine, customers are not given sufficient options to meet their anti-virus needs. When a virus is released on the Internet, each separate anti-virus signature engine must first identify the virus and then develop and deploy a signature. The response time varies between engines and different viruses. Often customers want more than one anti-virus signature engine to scan their email and secure their networks.

Threat Type:
Phishing

Wrongly Treating Phishing as Spam

Spam and phishing are not the same and should not be filtered using the same techniques. Spam is generally trying to sell a product or service, while phishing emails are designed to resemble legitimate correspondence. Techniques specifically tailored to detect phishing emails must be applied to successfully stop this threat. In addition, because these emails resemble legitimate correspondence, these emails need to be labeled as fraud in the junk box so the user will know that they are dangerous emails even if they look like good mail.

Threat Type:
Zombie

Lacking Zombie Detection

More email security products are offering outbound filtering. But this filtering merely applies to outbound policy filters and does not specifically offer zombie protection. Zombie machines are computers on your corporate network that have been hijacked by malicious code and are used to send out dangerous emails en masse. Emails sent from zombie machines will appear to originate from the victim's computer and will steal computer resources to send the emails. These internally compromised machines can damage a company's reputation and require costly resources to purge the malicious code.

Sending Server
Analysis

Relying on Failed Authentication

Authentication provides an important part of email threat protection by identifying emails that have inconsistencies between the claimed origin and actual origin. However, failing authentication does not indicate whether the email is good or junk. It may be a spam or phishing email lying about its origin, it may be good email that was forwarded through a third party, or it may simply be from a source that has not accurately set its DNS records to support authentication. Therefore, failing authentication does not provide decisive information. However, emails that pass authentication can be paired with a reputation assessment to provide useful filtering information.

Sending Server Analysis

Expecting Sender Reputation to Always Be Clear

Reputation based services, including Realtime Blackhole Lists (RBLs), identify sending SMTP servers that are known for sending junk emails. Reputation services use lists of IP addresses of servers that have sent out email attacks and use these lists to block emails from these servers. Reputation services can be helpful when a server consistently sends large quantities of junk emails. But whether to block or not block a particular IP address is not always clear. Mail servers can have a mixed reputation. While a mail server can have mostly good senders, it may also have a few bad or infected machines sending email through the server causing it unknowingly to send junk emails. A sending server's reputation should not be the only factor that determines whether an email should be blocked.

Content Analysis

Using Insufficient Methods for Content Analysis

Many email security products limit their content analysis to keywords and phrases that are indicative of spam. These methods do not effectively stop email threats because they cannot efficiently identify altered terms. Spammers have made an art form of altering spam words to try to bypass email filters. For example, there are 600,426,974,379,824,381,952 ways to spell Viagra when the word is altered using methods such as switching letters (viarga), adding spaces (v i a g r a), replacing characters with symbols (vi@agra), and many more.³ Of course all of these methods can be combined in various ways (V 1 @ R G A). A content filter must be able to effectively identify the numerous variations of spam words.

Content Analysis

Mistakenly Ignoring Contact Information

Email attacks, especially spam and phishing, usually contain contact information such as URLs and phone numbers in the body of the email. Some email security products do not include this information as part of their analysis. Reputations can be applied to URLs within an email, and inconsistencies in the contact information in the email body can provide valuable information during filtering.

Ease of Use

Making Email Security Difficult

An email security solution that solves one problem (email threats) by creating another (ongoing system administration) is not really a solution. Administrators should not be required to write rules, update virus signatures, upgrade software, or add new users. These tasks should be completed instantly and automatically by the email security solution.

Email security products that fall into these traps do not adequately protect their users. Email security vendors must efficiently combine multiple techniques to effectively analyze the entire email lifecycle and stop email attacks. In addition, email security must protect against both stand-alone and blended threats, which can only be done by using technology that targets the different types of email threats.

³ "There are 600,426,974,379,824,381,952 Ways to Spell Viagra." [Cockeyed.com](http://cockeyed.com). 7 April 2004. Retrieved from <http://cockeyed.com/lessons/viagra/viagra.html>.

III. Apply Technology to Email Threats

MailFrontier Cognite is MailFrontier's technology system that protects networks from all inbound and outbound email threats. Different technologies housed in MailFrontier Cognite are applied to each email threat to ensure that the technology addresses the unique nature of each threat. This specialized targeting of MailFrontier's technology secures networks and protects against both individual and blended threats.

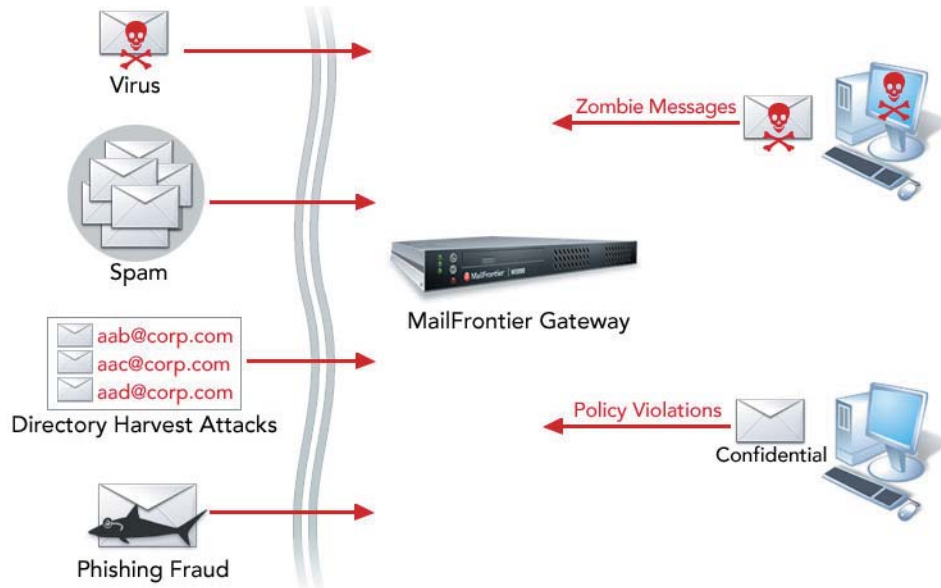


Figure 2. MailFrontier Cognite Technology Protects Against Inbound and Outbound Threats.

MailFrontier Cognite uses numerous technology methods to track the reputation of the email servers, evaluate message content and attachments, analyze the impact on recipients, and assess the destination Web sites linked within the email. Some of MailFrontier's unique technologies are mentioned below.

MailFrontier Reputation Service Paired with Authentication

Authentication with MailFrontier Reputation™ is an important part of MailFrontier's email security filtering. Authentication identifies emails that have inconsistencies between the claimed origin and actual origin. An email that fails authentication originates from a server that is not approved to send mail from the claimed domain. If an email passes authentication, the filter knows that the email actually originated from the claimed sender, allowing the email's reputation to be assessed. The email is sent through MailFrontier Reputation, which determines whether the sender has a good or bad reputation for sending email threats. MailFrontier Reputation is based on the industry's largest proprietary database.

MailFrontier Content Evaluation

Most content filtering techniques do not meet the challenge of today's pervasive email attacker. A combination of content filtering methods must be used to provide effective protection.

Adversarial Bayesian

Spammers use various techniques to bypass content filters that use keyword matches, regular expressions, and Naïve Bayesian to filter spam. MailFrontier Adversarial Bayesian™ analysis was developed to target spammer tricks, preventing these spam messages from entering the inbox. Specific spam indicators based on spammers' adversarial approach are used to determine the probability that an email is spam.

Bayesian Fraud

Phishing emails are not spam. They are designed to imitate legitimate correspondence, making it a challenge for content filters to differentiate between phishing and good email. MailFrontier's patent-pending MailFrontier Bayesian Fraud™ evaluates the indicators unique to phishing emails. MailFrontier identifies phishing emails and labels them as fraud in the junk box.

Lexigraphical Distancing

Spammers purposely modify words in an attempt to bypass content filters. MailFrontier has crafted its patent-pending MailFrontier Lexigraphical Distancing™ to detect this trick. As mentioned earlier, there are 600,426,974,379,824,381,952 ways to spell Viagra by replacing letters with symbols, adding spaces, inserting characters, changing the letter order, et cetera. Lexigraphical Distancing applies edit distance to detect these word variations. Edit distance determines how many edits need to be made to the modified expression (including phrases and words with extra spaces) to change it into a designated spam word or phrase. If it is an acceptably small number of edits (low edit distance), then there is a higher probability that it is an altered spam word.

MailFrontier SMART Network

MailFrontier Self Monitoring Active Response Team (SMART) Network™ is a real-time network of over one million global users whose responses enable MailFrontier to quickly identify and react to new email threats. These are real users receiving real email, not honeypots. Honeypots do not collect email based on actual human behavior. Real users surf the Web, sign up for lists, purchase items on the Internet, and conduct other activities that affect their email. The information received by the MailFrontier SMART Network™ is used to analyze multiple components of an email. In addition, since this network gets real email, MailFrontier SMART Network also understands legitimate email, dramatically reducing the false positive rate. MailFrontier immediately passes the knowledge and value of its collaborative network to its customers through automated updates.

Time Zero Virus Technology

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. MailFrontier Anti-Virus has added two layers of defense with its MailFrontier Time Zero Virus Technology™ which applies predictive techniques and a responsive approach that stops new viruses after they have been released into the Internet community but before a signature has been created. When combined with leading anti-virus engines, MailFrontier Time Zero Virus Technology protects users during all stages of a virus outbreak.

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 applies its extensive expertise in statistical analysis to detecting viruses. Email and Attachment Profiling uses statistical methods and heuristic rules to identify emails with attachments that contain malicious code. 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. In addition, Virus Traffic Analysis detects anomalies in a company's email traffic.

Responsive: Network Defense Against New Viruses

This method utilizes the MailFrontier SMART Network. MailFrontier analyzes this real-time user feedback to detect and terminate new threats. Emails identified by MailFrontier SMART Network as containing dangerous attachments are immediately and safely quarantined.

MailFrontier Contact Point Validation

MailFrontier is the industry leader in analyzing contact points (URLs and phone numbers included in threat emails). MailFrontier offers three levels of contact point review:

Browser Exploit Detection

MailFrontier analyzes emails for items such as port-number inconsistencies, URL redirection, and encoding that exploits vulnerabilities in browsers and operating systems.

Social Engineering Trick Checks

MailFrontier uses techniques such as obfuscated URL identification and MailFrontier Divergence Detection™ which examine the difference between the appearance of a link and the actual result of acting on that link. These tricks are common in phishing emails, but not in legitimate correspondence.

Real-Time Phishing List

MailFrontier cross-checks all contact points against its MailFrontier Real-Time Phishing List™, which assesses the reputation for phishing URL's used in the body of the email.

MailFrontier Cognite is the industry's only end-to-end attack monitoring system. MailFrontier's real-time global view into email attack outbreaks enables MailFrontier to provide the best protection against spam, viruses, phishing, and other emerging and blended threats.

IV. Stop Spam

The lifecycle of an email attack happens in just minutes. Real-time automated statistical consolidation of end-to-end attack information makes it possible to immediately identify the spam attack and take action against it. When MailFrontier Cognite is applied to stopping spam, it processes every email by identifying the sender, analyzing the content, and applying a collaborative review through MailFrontier SMART Network.

Sender Authentication and Reputation

MailFrontier identifies the sending servers, applies authentication, and, if the email passes authentication, assesses the reputation based on the industry's largest proprietary database.

Content Analysis

MailFrontier Adversarial Bayesian is applied to the email message content to determine the probability that an email is spam. For example, if an email subject is "Let Me Help" it may appear to be a good email. However, a closer inspection of the underlying source code may show hidden HTML characters in between the text characters. This email trick is a strong indicator of spam. This example represents one of 200,000 different methods that MailFrontier applies to content analysis.

Spammers often use typographical tricks to disguise content. With MailFrontier Lexigraphical Distancing, sets of characters used to represent words or phrases can be identified as spam.

Community Response

MailFrontier SMART Network provides a collective statistical community response which helps to identify spam. In addition, since this network gets "real" email, it also understands legitimate email, dramatically reducing the false positive rate.

Spam Judgment, Not a Score

Most email security products apply a single spam "score" to email. IT administrators have the burden of determining the score, or threshold, that indicates when an email is spam. And the threshold must be continually adjusted as spam trends change. In addition, rigid scoring often leads to blocking email that customers actually want to receive (increases false positives).

MailFrontier frees IT administrators from adjusting spam scores by using a unique cross-analysis approach that requires that at least two of MailFrontier's independent categories label a message as spam before it is marked as definite spam, thus ensuring no good email is caught.

A judgment that results in Spam, Likely Spam (strong single indicator), or Good Email lets the customer confidently delete unwanted email, securely quarantine suspect email, and accurately receive good email. This approach achieves 98 percent effectiveness at stopping spam.

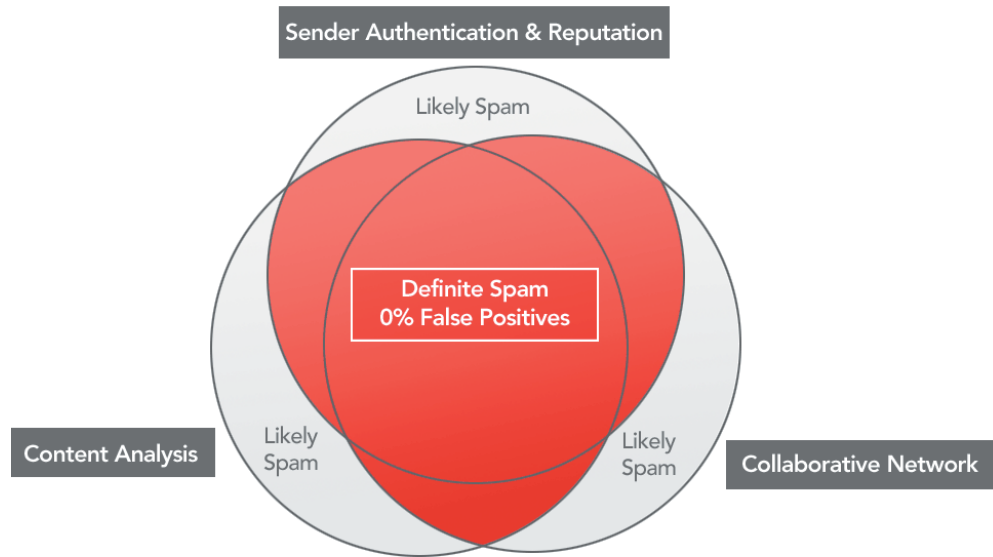


Figure 3. MailFrontier's Cross-Analysis Approach to Fighting Spam.

V. Protect Against Viruses

Most anti-virus products rely primarily on signatures to stop viruses. At the moment the outbreak occurs, called "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.

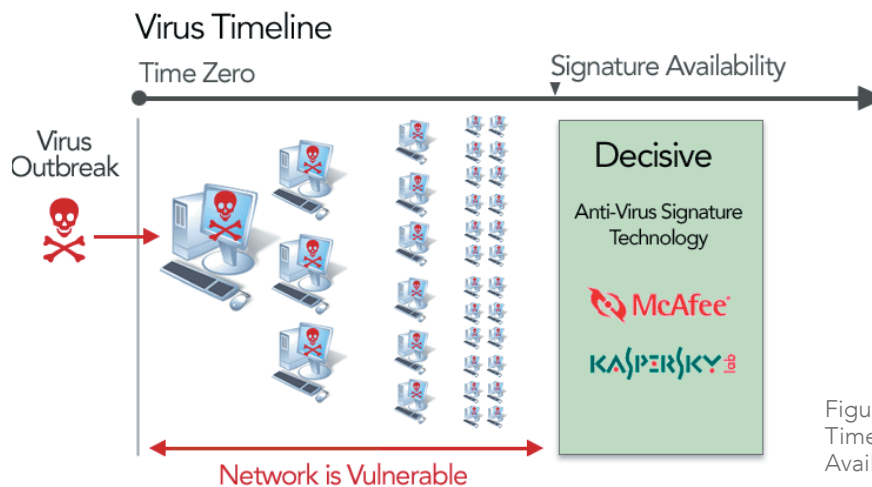


Figure 4. Vulnerable from Time Zero to Signature Availability.

MailFrontier has developed breakthrough anti-virus technology in its MailFrontier Time Zero Virus Technology. This part of MailFrontier Cognite 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.

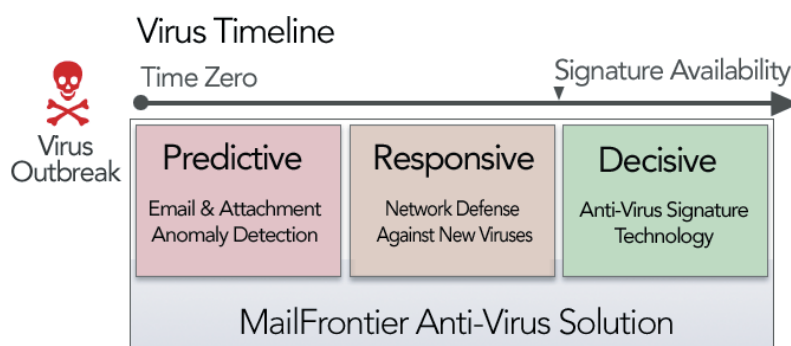


Figure 5. Close the Window of Vulnerability.

Predictive Techniques

MailFrontier applies the intelligence of MailFrontier Cognite to time zero virus protection using predictive anomaly detection methods.

- Email and Attachment Profiling uses statistical methods and heuristic rules 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 email to identify anomalies that may indicate a virus outbreak.

These predictive methods identify and quarantine seemingly innocent attachments that may be harboring malicious code. 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 5 of the virus variants.

Responsive Techniques

The MailFrontier SMART Network provides rapid feedback on viruses as soon as they emerge, providing another early detection mechanism that allows viruses to be identified and quarantined prior to signature arrival. The fifth Sober.J variant was stopped by MailFrontier's responsive techniques.

Decisive Techniques

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.

MailFrontier also applies its breakthrough anti-virus techniques to scanning outbound emails to ensure viruses are not being sent from within the company. MailFrontier anti-virus keeps the network safe and enables the enterprise to maintain a reputation of safe outbound email.

VI. Prevent Phishing

Phishing emails are more insidious and more dangerous than spam. They are also more difficult to identify because they are made to look like legitimate correspondence, consistently eluding spam filters. They require specific analysis, identification, and handling. Billions of phishing emails are sent out every month and can lead to identity theft, security breaches, and financial loss and liability. The latest research estimates that phishing caused more than \$44 billion in damages worldwide in 2004.⁴

What Is the Difference Between Spam and Phishing?

	Spam	Phishing
<i>How does it arrive?</i>	Sneaks in the back door.	Walks in the front door.
<i>How does it make its offer?</i>	Looks bad, seems far-fetched.	Looks plausible, seems credible.
<i>What is it trying to do?</i>	Tries to sell you something.	Tries to steal something from you.

Consumer Phishing

Phishing emails spoof, or imitate, legitimate companies such as banks, ISPs, or Internet retailers, and attempt to defraud recipients of personal information such as logins, passwords, credit card numbers, bank account information, and social security numbers. Generally this information is collected through a form in the email or a URL link which takes users to a fraudulent Web site that appears to be the spoofed company's site. If recipients provide the requested information, they may lose funds or become a victim of identity theft.

Corporate Phishing

Phishing began as a consumer threat but is now moving to the corporation. Corporate phishing attempts to gain access to corporate networks, databases of user or client data, payroll and CRM systems, DNS servers, and other valuable corporate assets.

A Unique Solution for a Unique Threat

MailFrontier has the only solution that uniquely identifies phishing. MailFrontier Cognite analyzes the email header, content, and contact points. MailFrontier Reputation and Authentication are applied to the sending server analysis. The content analysis includes MailFrontier Bayesian Fraud which specifically targets phishing emails. The contact points are processed using MailFrontier Real-Time Phishing List, which determines their reputation; MailFrontier Divergence Detection, which looks for inconsistencies with the email links; and URL Exploit analysis, which identifies when fraudsters attempt to leverage browser or operating system vulnerabilities.

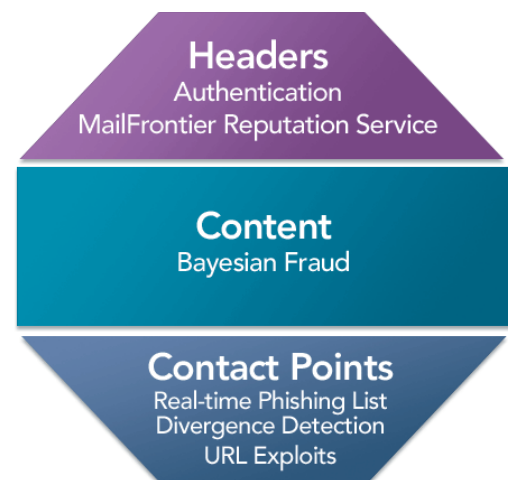


Figure 6. MailFrontier Phishing Analysis.

⁴ "mi2g:Q3 2004: The Rise of Islamist Hacking and Criminal Syndicates." mi2g. 20 October 2004. Retrieved from <http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/201004.php>.

Identifying Fraud in the Junk Box

Phishing emails need to be identified as fraud in the junk box. Because phishing emails resemble legitimate correspondence, users may believe that these emails are good emails that were mistakenly identified as spam, leading the recipients to fall victim to the fraud. MailFrontier research shows that phishing emails marked as spam will be unjunked by users at a rate of 10-40 percent. To protect users, phishing emails are labeled as fraud in the junk box for easy identification. Separation of spam and phishing also makes it possible to automatically route phishing emails to the appropriate IT and security personnel, enabling IT to monitor attacks.

VII. Safeguard Against DHA/DoS Attacks

Email threats come not only in content, but in volume and invasiveness. Directory Harvest Attacks (DHA) and Denial of Service (DoS) attacks can bring down an organization's email infrastructure due to both the sheer quantity of email traffic they generate and the debilitating invasion of the network they infiltrate. These attacks happen every day and can place a significant burden on email infrastructure. They also put employee information at risk and open the door for subsequent unwanted email that is targeted, deceptive, and dangerous. MailFrontier provides unique protection for your email infrastructure with specific features designed to thwart these types of email attacks.

Directory Harvest Attack Defense

An exhaustive "brute force" attack, DHAs bombard mail servers with emails sent to variations of possible email addresses and checks which are bounced back and which are sent through as having legitimate email addresses for that company. The extensive volume of a DHA strains the email infrastructure. In fact, some high-profile companies who find themselves constant DHA targets overbuild their email infrastructures with additional hardware and software just to keep up with the volume from DHAs, especially the spikes in email traffic. In addition, a DHA quickly amasses thousands of email addresses for the company to be used later in follow-up spam, virus, and phishing attacks.

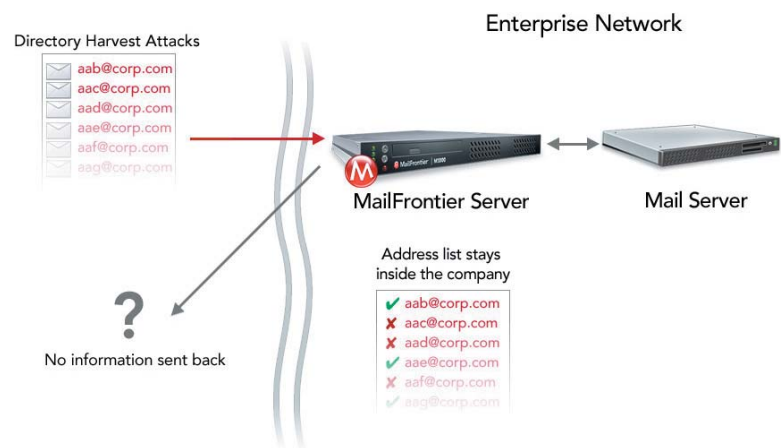


Figure 7. Directory Harvest Attacks Are Blocked at the Perimeter.

MailFrontier Cognite thwarts DHAs by combining email pattern analysis with data collected through synchronization with the corporate directory, preventing the theft of corporate directory information. In addition, by blocking DHAs at the perimeter, MailFrontier reduces the load placed on the entire infrastructure by preventing fraudulent requests from going in through the entire mail system and preventing bounces from flowing back out.

Denial of Service (DoS) Attack

A DoS attack is a malicious attempt to bring down your email infrastructure. By sending an enormous volume of email traffic into an organization at a coordinated time, attackers attempt to overwhelm the network and email infrastructure, bringing email to a complete stop. With MailFrontier Cognite, companies are able to meet the challenge of a DoS attack and keep their email up and running. Through unique email pattern analysis and threat detection tools, MailFrontier determines which mail servers are sending good emails and which are sending bad traffic, and offers a different quality of service to each.

With MailFrontier, companies are able to stop DHA and DoS attacks in real time with no impact on email services.

IX. Comply with Regulatory and Corporate Compliance

Today, internal security breach prevention is a principal concern among CIOs. Research shows that 70-90 percent of information breaches are caused by insiders⁵ and the most common method of stealing information is sending electronic copies of files and documents to personal email accounts.⁶ This makes email a critical focus of policy, regulation, and corporate compliance to prevent security breaches.

In addition to preventing threats such as spam, viruses and fraud, MailFrontier Cognite also prevents confidential and sensitive information from leaving the company.

Content Evaluation

As part of its content evaluation, MailFrontier supports compliance dictionaries such as those used for legislative regulations and to detect harassing or derogatory language. Additionally, MailFrontier Disguised Text Identification™ goes beyond other products in the market that limit their content evaluation to regular expressions and keyword matching. MailFrontier Disguised Text Identification detects information that has been accidentally altered or purposefully modified in an attempt to conceal its transmission. Misspelled and differently formatted text bypasses standard compliance filters, but is caught by MailFrontier. MailFrontier's highly effective content evaluation helps companies prevent inadvertent error and intentional employee sabotage, saving substantial fines, legal fees, and the companies' reputations.

Customized Policies

MailFrontier's easy policy management enables enterprises to define and enforce policies that secure confidential information and stop offensive emails. When a policy is violated, the action can be set to send an alert or delete, quarantine, encrypt, or bounce the email, giving the company the flexibility to apply the appropriate action to each situation. Information can also be limited to specific departments or groups within an organization, helping the company to prevent inadvertent or intentional misuse of information.

Partners

MailFrontier has partnered with PGP Corporation and Voltage Security, Inc., two leading encryption companies. Deploying MailFrontier Gateway with either PGP Universal or Voltage IBE Gateway Server provides an integrated email security solution including encryption, digital signature, anti-virus, anti-spam, anti-phishing, and content filtering—all managed by policies created through MailFrontier's streamlined user interface.



MailFrontier Gateway implements company's security and privacy policies, and provides consistent and effective enforcement to create easy compliance within the organization.

⁵ Gaudin, Sharon. "Security Begins From Within." [eSecurity Planet.com](http://www.esecurityplanet.com). 4 August 2003. Retrieved from <http://www.esecurityplanet.com/trends/article.php/2244131>.

⁶ Jaques, Robert. "IT Fuels Intellectual Property Theft." [Personal Computer World](http://www.pcw.co.uk). 20 February 2004. Retrieved from <http://www.pcw.co.uk/News/1152924>.

X. Free Up Your Resources with Easy Management

MailFrontier’s email security solution is easily managed through MailFrontier’s intuitive Web-based administrative interface, which is designed to ensure simple configuration, easy customization, and reduced maintenance.

Quick & Flexible Configuration

MailFrontier enterprise products can be installed and configured in under an hour. MailFrontier streamlines first-time set-up and enables configuration for all-in-one or split architecture installation, which provides the flexibility to choose greater redundancy; separation between filtering and management; and decentralized, multi-machine arrangements. For customers who choose all-in-one configurations, Quick Configuration enables administrators to complete the five step deployment, all from one screen in less than one hour.

“MailFrontier told me that I would spend less than ten minutes a week managing spam after installing MailFrontier Gateway Server. They were wrong. I only spend five.”

Niall Pariag
Senior Network Administrator
Riverside Healthcare Systems, Inc.

Auto-Updates

Auto-updates provide hands-off maintenance. MailFrontier’s auto-updating system can be set to download data and new releases at any time and frequency set by the administrator.

Flexible Policy and Group Management

MailFrontier policy management allows users to implement email policies through an easy-to-use, Web-based administrative interface. MailFrontier’s streamlined policy management uses an identity-based architecture that is fully integrated with LDAP, Microsoft Active Directory, and other standard directory systems. IT can create global policies or customize policies by geography, department, group, function, user, and/or title to cover inbound or outbound requirements without any need to duplicate directory structures. IT can create specific rules with just a few clicks or delegate administrative privileges to groups or end users with ease.

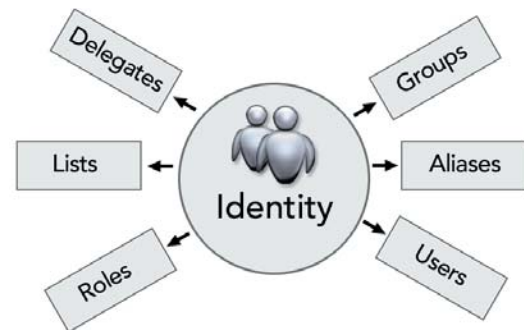


Figure 9. Using Identity-Based Architecture.

	Engineering (Functional)	Japan (Geographic)	Legal (Functional)	IT (Functional)
Remote Administration	✓	✓	✓	✓
Language	English	Japanese	English	English
Allow Delegates		✓		✓
Attachments	No Attachment that is .mov	No Attachment Over 10 Megs	No Attachment that is .exe. or .bat	All types and sizes allowed
Confidential Information	No IP or source	Not Allowed	Allowed	Not Allowed
Allow Newsletters		✓		✓
Separate Quarantine	✓	✓	✓	✓
Encryption			✓	✓

Figure 10. Centralized IT: Example of Possible Policy Configurations by Department and Geography.

Centralized, Web-Based Console for Administering All Junk Boxes

Managing unwanted email is trouble free. A single, consolidated Junk Box for the company and a personal Junk Box for each user enable instant search, sort, review, and retrieval.

Personalized End-User Controls

Administrators can allow users to personalize their protection and their junk box, reducing the IT burden. Administrators also can allow end users to periodically receive an actionable Junk Box Summary, which provides for “safe” viewing and message retrieval. Web-based controls give users access to numerous functions:

- Personalized allowed and blocked lists
- A personal Junk Box
- Junk Box Summary settings (such as preferred language, time, and frequency)
- Delegation options
- And more

Through Personalized Spam Management and individual Junk Box Summaries, MailFrontier delivers extensive user functionality that lets individuals personalize email filtering while still enabling IT to maintain complete control.

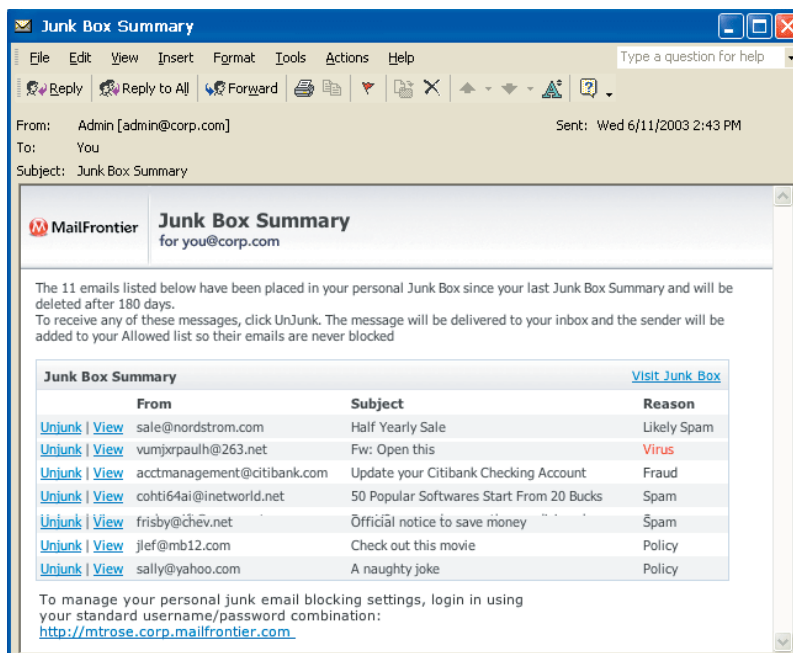


Figure 11. Personal Junk Box Summary.

Robust Reporting: Visibility into Your Email Flow

MailFrontier reporting gives administrators unmatched insight into their email flow and security at both the system-wide and granular levels, including detailed information and statistics about attack types, solution effectiveness, and system performance.

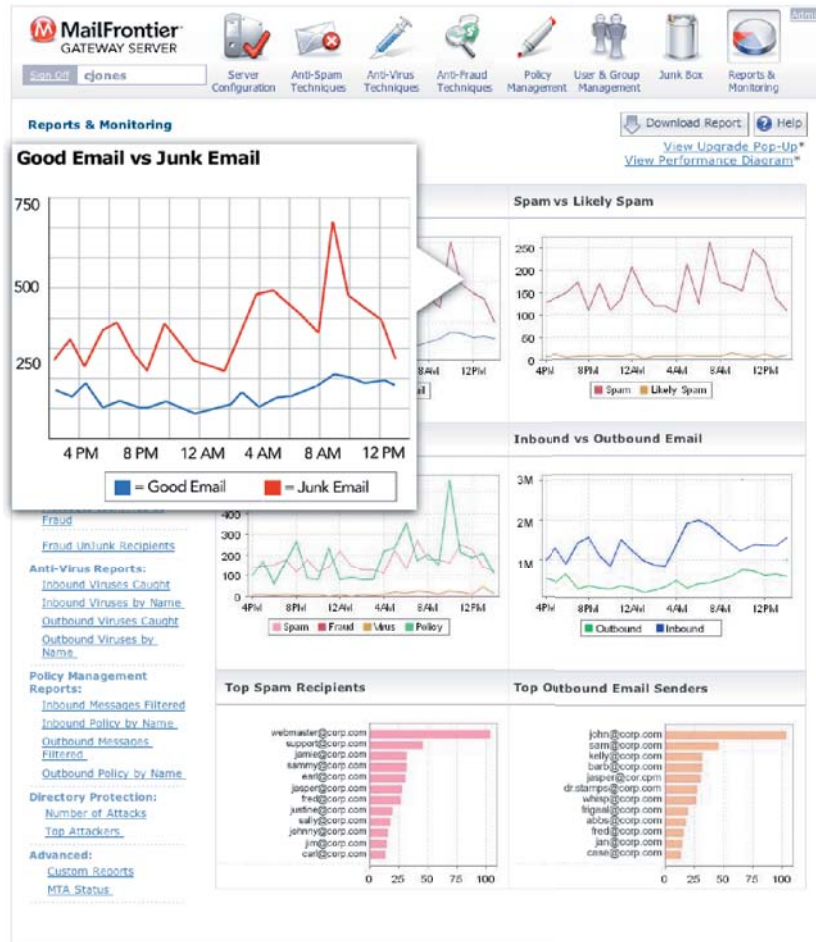


Figure 12. Dashboard Reports.

MailFrontier designs every product to ensure simple configuration, easy customization, and reduced maintenance. The centralized, Web-based management console makes it easy to manage this protection. With just 10 minutes of maintenance a week, customer after customer has found MailFrontier's self-running, self-updating solution the easiest to manage.

XI. Achieve High Performance

Network and email infrastructure proliferation has led to complicated management problems for IT. Sixty-four percent of IT organizations plan to consolidate email security solutions. Seventy percent of those want consolidation to increase their ease of use (simplify management).⁷

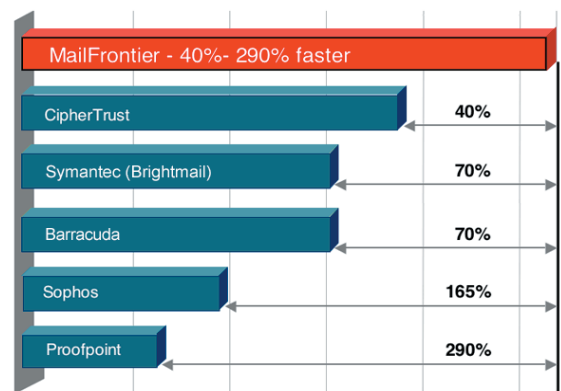
With good mail increasing, junk mail sky-rocketing, and more actions on email being taken, a high performance solution is required to enable fewer machines to process the email load.

MailFrontier Preemptive Scanning MTA

MailFrontier Cognite technology is incorporated into MailFrontier Preemptive Scanning MTA, which provides email scanning and delivery 40-290% faster than other vendors.⁸

MailFrontier Preemptive Scanning MTA uses unique email security-specific architecture in which all messages are scanned prior to being written to disk, delivering a solution that lets organizations consolidate email security while scaling to meet size and performance requirements.

Message Delivery Rate



¹Delivery rate, msg/sec, Network World, Analyzing the Spam Test Results, 12/20/04

Figure 13. MailFrontier Delivers Your Messages 40-290% Faster.

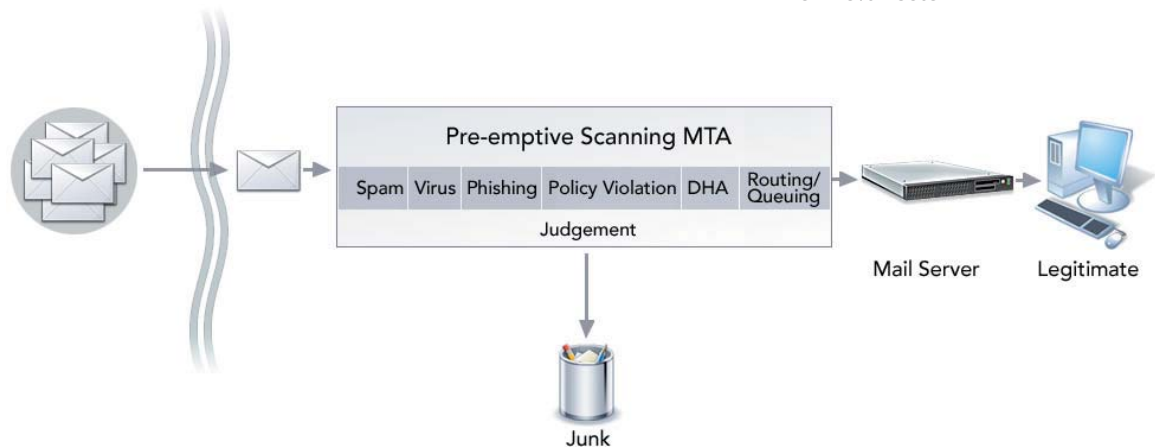


Figure 14. MailFrontier Preemptive Scanning MTA Scans Emails Before They Are Written to Disk.

Redundant High Availability Deployments

MailFrontier can run as a single all-in-one product that easily handles all scanning, quarantining, and management. Alternatively, MailFrontier deploys in high-availability, multi-system environments with its Remote Analyzer option. For the scalability, redundancy, and high availability needs of large enterprises, MailFrontier Remote Analyzers enable distributed processing and management.

⁷ MailFrontier/Insight Express IT Survey, March 2005.

⁸ "Spam in the Wild, The Sequel." *Network World*. 20 December 2004

When using MailFrontier Gateway in a split configuration, all boxes can use the same operating system, or the Linux and Windows boxes can be combined. One unique split deployment option is to use a Linux appliance to handle all security in the DMZ, analyzing email at the perimeter of your organization, while a Windows appliance provides system management, reporting, and a central email quarantine inside your secure corporate network. Whatever your configuration, MailFrontier can provide an option that fits seamlessly into your environment.

Infrastructure Consolidation

MailFrontier's solution needs fewer machines to process the email load. First, MailFrontier provides all of your email protection in one solution. With MailFrontier, one solution receives and scans all of your messages instead of combining different solutions to protect you from spam, phishing, virus, and other inbound and outbound threats. Second, MailFrontier's high performance allows users to have fewer servers. For example, if customers have a redundant and load balanced setup with two MailFrontier servers, they will need 3 to 8 servers from other vendors for equivalent performance.

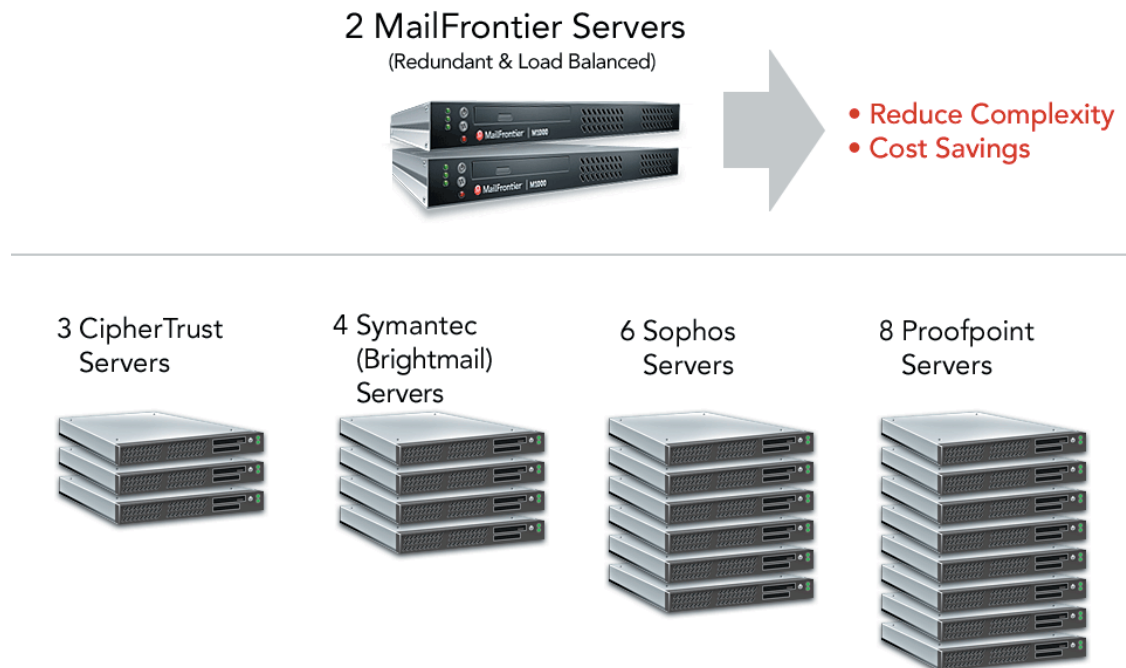


Figure 15. MailFrontier Enables Consolidation of Email Infrastructure.

By consolidating email security infrastructure, customers are able to reduce infrastructure complexity, save time by managing just one solution, and lower the Total Cost of Ownership.

XII. About MailFrontier

MailFrontier is an email security company that protects organizations against threats such as spam, viruses, and phishing, provides control for content compliance, and enables consolidation of email infrastructure. MailFrontier's platform provides power without complexity.

Gartner, a leading technology research and advisory firm, positioned MailFrontier in the visionary quadrant of its E-Mail Security Boundary Magic Quadrant for 1H 2005 (as published on June 30, 2005). In a market with hundreds of vendors, Gartner identified 21 companies to be included in this Magic Quadrant analysis, with three vendors appearing in the Visionary Quadrant.⁹

- Only MailFrontier offers MailFrontier Cognite, an end-to-end email attack monitoring system that identifies and stops email attacks. MailFrontier Cognite tracks the reputation of the email servers, evaluates message content, analyzes the impact on recipients, and checks any embedded URLs.
- Installed in just minutes and configured in under an hour, MailFrontier Gateway is designed to ensure simple configuration, easy customization, and automated maintenance, all through an easy-to-use, Web-based administrative interface.
- MailFrontier continues to evolve its technology, techniques, and tactics to stop new threats as they emerge, delivering cutting edge anti-threat innovations such as MailFrontier SMART Network, MailFrontier Time Zero Virus Technology, and the MailFrontier Phishing IQ Test™. MailFrontier is a proven industry and market leader with one issued patent and 17 pending patents filed in email security. MailFrontier was the first email security company to accomplish the following:
 - ✓ Apply a multi-pronged approach to spam filtering
 - ✓ Design an MTA that prioritizes scanning before message acceptance and queuing
 - ✓ Provide users with a personalized summary of quarantined items
 - ✓ Offer corporate, group, and mailbox-level flexibility
 - ✓ Integrate a spam-filtering solution with LDAP
 - ✓ Enable split configuration filtering at the network perimeter
 - ✓ Offer a unique phishing solution and identify fraud in the junk box

MailFrontier continues to gain high-profile recognition for its technological innovation, its product advances, and its customer service.

MailFrontier Products

MailFrontier Gateway email security solution delivers the most effective email protection available for both inbound and outbound threats, blocking 98 percent of spam, fighting virus outbreaks, eliminating phishing, stopping DHA/DoS attacks, defending against Zombie machines, and detecting policy violations.

MailFrontier Gateway Server

MailFrontier Gateway Server software solution provides easy and flexible deployment on your own hardware.

MailFrontier Gateway Appliance

MailFrontier Gateway Appliance is a pre-configured, pre-hardened solution standardized on IBM xSeries hardware available on Windows and Linux operating systems.

⁹ "Magic Quadrant for E-Mail Security Boundary, 1H05," Arabella Hallawell, June 30, 2005. The Magic Quadrant is copyrighted 2005 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

MailFrontier Customers

MailFrontier is an email security company trusted by individuals and organizations to deliver protection from spam, virus, phishing, and every other form of inbound and outbound email threat, setting the standard for email security protection, control, and performance.

With enterprise customers across industry sectors, MailFrontier is a proven winner in the email security marketplace worldwide.

				
Retail	Finance	Retail	Sporting Goods	Non-Profit
				
Real Estate	Health Care	Technology	Education	Retail
				
Media/Publishing	Transportation	Hospitality	Finance	Technology/ Manufacturing



“The MailFrontier implementation was easy—and actually working in only 30 minutes. And the server has been running smoothly ever since. A solution that delivers and is easy to use—MailFrontier does it all.”

—Tracy Holt
Manager
Enterprise Messaging



“The entire experience with MailFrontier reinforced the product’s ease-of-use... MailFrontier exceeded our expectations.”

—John Tipton
IT Director

MailFrontier Awards

MailFrontier is an acknowledged leader in the industry with a proven track record of recognition and excellence, year after year.



IT WEEK Editor's Choice – 5 out of 5 Stars

"MailFrontier Gateway Appliance m500 setup was easy...and took less than an hour... It really blocks all unwanted email." – June 6, 2005



InfoWorld Rated Excellent

"MailFrontier had the easiest installation...provides lots of control to the admin...[and] provides excellent accuracy." – September 27, 2004



CRN Recommended

"MailFrontier's hands-off approach can help ease the administration burden on IT departments." – June 7, 2004



Red Herring Top 100 Private Companies/Innovators

Recognizing the company for its innovation and strategy – May 2004 and December 2004



NetworkWorld Top-Rated Enterprise Anti-Spam Software

"...MailFrontier's ASG put up some impressive results in terms of blocking spam and letting legitimate mail pass." – September 15, 2003

Recommends MailFrontier be included on "Short List" of products evaluated for large-scale, high-performance anti-spam systems – December 20, 2004



PC Pro RECOMMENDED – 5 out of 6 Stars

"An effective message-security appliance that can be customised to suit a wide range of network scenarios...we found installation easy... It's effective against spam straight out of the box, and it compares well on price with many other enterprise-level options." – October 2005

Partners for Complete Value-Added Solutions

MailFrontier's select set of leading partners combine the strength of their products with MailFrontier to deliver complete value-added solutions to meet the varying needs of MailFrontier's enterprise customers.



XIII. How Can I Protect My Organization?

Contact MailFrontier for a free trial of one of our products:

- MailFrontier Gateway Server (software solution)
- MailFrontier Gateway Appliance

MailFrontier support is provided during your trial to ensure that you can effectively test the product in your environment.

**To Get Started Today
With a *Free* Trial**

Contact Your Local Reseller
Or Go To
www.mailfrontier.com/trial

Install MailFrontier Gateway for trial in under an hour and choose from one of three operating modes:

- Silent mode, which gathers reports and information
- Selected group and user mode, which filters for a subset of users
- Organization wide, which protects the entire organization from email attacks

During your trial you will learn the following:

- How much junk email you get
- How many phishing emails you receive
- The frequency and intensity of your DHA attacks
- Whether emails are being sent to and from your competitors
- How much the above are costing you in bandwidth, storage, and time
- And much, much more

Copyright © 2005 MailFrontier Technology Overview Whitepaper, MailFrontier, Inc. All rights reserved. This whitepaper is a copyrighted work of MailFrontier, Inc. and is owned by MailFrontier, Inc. No part of this document may be reproduced for any purpose without the express written permission of MailFrontier.

This whitepaper is for informational purposes only. MailFrontier makes no warranties, express or implied, as to the information in this document. The information in this document is subject to change without notice and does not represent a commitment on the part of MailFrontier. MailFrontier assumes no responsibility or liability for any errors or inaccuracies that may appear in this whitepaper.

Trademarks of MailFrontier, Inc. include: MailFrontier, MailFrontier Gateway, MailFrontier Cognite, MailFrontier Preemptive Scanning MTA, MailFrontier Reputation, MailFrontier Adversarial Bayesian, MailFrontier Bayesian Fraud, MailFrontier Lexigraphical Distancing, MailFrontier Self Monitoring Active Response Team Network, MailFrontier SMART Network, MailFrontier Time Zero Virus Technology, MailFrontier Divergence Detection, MailFrontier Real-Time Phishing List, MailFrontier Disguised Text Identification, and MailFrontier Phishing IQ Test. Other names of actual companies and products mentioned in this whitepaper may be the trademarks or their respective owners.