

White Paper

# Message Security and Policy Imperatives in the Wake of World Events

January, 2003



## ABSTRACT

The range of issues that need to be covered in basic network security have changed radically as a result of the corporate accounting scandals and terrorist events of the last couple of years. The center of this expanded area of concern is the message network itself. In addition to the longstanding issues of protecting the confidentiality of corporate information, preventing unauthorized network access, managing human resource/harassment issues and defending against internal attacks, e-mail retention and business continuity/disaster recovery issues are now at the forefront of the IT manager's to-do list.

To address these new issues – all centered on the messaging infrastructure itself – enterprises, educational institutions, government organizations and carriers alike must find ways to resolve these new concerns. Working in concert with existing firewalls, the capabilities built into Mirapoint's current and forthcoming message oversight systems provide both the flexibility and scalability needed to secure a message network from external and internal misuse.

## **“PORT PROTECTION” MAY HAVE LITTLE TO DO WITH YOUR FIREWALL**

With the long-term effects of the destruction of the World Trade Center and the massive corporate accounting scandals of the new Millennium continuing to ripple through most of the business world, one very clear result is that message networks are dead center in the review-and-oversight spotlight. Particularly in the United States, government, which was already in a regulatory mindset vis-à-vis e-mail content, has responded with newly found oversight measures. Carnivore – the FBI's e-mail content capture-and-copy technology – now has the new Patriot Act to go with it and the pending TIA systems of the Information Awareness Office. And CALEA, which used to be a mechanism for the legal intercept of PSTN phone calls, has been expanded to require the diversion and discrete archiving of “any random IP stream.” In short, e-mail, VoIP messages and so on. Additionally, in the wake of numerous high-profile corporate bankruptcies and accounting scandals, the US financial community now has GLBA message archiving requirements to worry about. In November 2002 alone, five of the top US securities firms were fined \$8.3M (USD) for “failing to keep e-mails and produce them in regulatory investigations.”

The net effect of this new focus on messages, or, more precisely, networks of messages, is to point out the overriding requirement for IT managers to now view the creation, transmission, security, policy application, archiving and receipt of messages as a business security imperative, not simply as one of a number of applications overlaid on a network infrastructure.

## **THE CLASSIC PARABLE OF NAMING THE BEAST**

The ancient story of the blind wise men attempting to describe an elephant is an all-too-accurate analogy for the messaging network industry today. Messaging, and e-mail in particular, developed quite organically and in a piecemeal fashion – and so did many of the companies involved in its deployment. So it is not all hard to imagine one person holding the trunk and describing what he sees as “wireless Internet messaging,” a second touching a leg and calling it “enterprise e-mail security” or a third touching the tail and talking about “anti-SPAM technology.”

In the new world of message oversight, business continuity and corporate accountability these fractured views of the whole animal – message networks – now represent the evolutionary cul-de-sac of these earlier generation messaging solutions. These first products were – and are – solving real problems, but world events have mandated a new, consolidated, centrally managed approach to message delivery, inspection, retention and disposition that subsumes point solutions for anti-virus, anti-spam and so on.

## **KEEPING YOUR INFORMATION “HEALTHY” IN A LITIGANT AGE**

To ensure that your messaging service remains healthy and efficient, you need a robust system to continuously eradicate threats like viruses and spam, while enabling you to closely control sensitive information. At the same time, your end-users need a tool that can help them organize an ever-growing flood of electronic correspondence. Many organizations have begun to take steps to tackle these issues, but most current approaches are inefficient, and simply do not scale well for customers with growing message volumes and numbers of users. For example, desktop-based anti-virus utilities can eliminate common viruses, but are costly to implement and must be continually updated and fine-tuned by individual users. Optional firewall-based anti-spam and anti-virus products can examine traffic at the packet level, but lack the power needed for sophisticated scanning on a per-message/domain basis. What's more, such applications

are complex, often requiring software upgrades to existing firewalls, and demand considerable technical and management knowledge. In this paper, we will explore some of the challenges inherent in policy-based message filtering and control, and illustrate the benefits of Mirapoint's turnkey integrated system solutions. By centralizing the message filtering process at the messaging infrastructure level rather than dealing with it at the desktop, your organization can overcome these pressing communication issues, optimizing network efficiency and taking charge of the critical information that is the lifeblood of your business.

## **THE REQUIREMENT FOR MESSAGE INSPECTION AND FILTERING**

In today's information age, your company's core data and content are its most important – and valuable -- assets. Maintaining the security and integrity of this information in an intensely competitive environment can mean the difference between success and failure. A single stray virus can quickly destroy years of work and impair critical corporate data. Not only is this information costly to replace, but protecting against viruses can result in an enormous loss of productivity for employees as they waste valuable time scouring their computer files, configuring virus utilities, and rebuilding lost documents. Just as bad, having the IT department "touch" every desktop to upgrade software is an expensive and time-consuming chore that should be avoided whenever possible. Unwanted spam can be a similar time sink, as users wade through reams of get-rich-quick offers and work-at-home schemes, sorting and deleting e-mails. As important as it is to keep unwanted messages out, it's just as important to maintain control of sensitive information within your organization. Without proper policy enforcement measures, confidential or offensive information can be forwarded outside the company in seconds, distributing trade secrets, undermining your competitiveness, or even exposing your organization to legal action. Many industries face stringent regulatory compliance issues, and must be able to prove in audits that they meet regulations concerning appropriate communications. Financial, legal, and health care companies, for example, are well aware of the importance of setting and enforcing policies for employee communications. Policy-based message filtering enables your company to take charge of the e-mail traffic that continuously circulates throughout the network. This filtering process automatically parses message headers, content, and attachments to perform actions on messages based on the rules you define. Some of these actions include message blocking, filing, archiving, quarantining, forwarding, or replying, or moving the message to the trash. Message filtering can also

interact directly with administrators, alerting them about viruses, spam, and information policy violations before they have a chance to do real damage.

Message inspection and filtering is an ideal tool for meeting the challenges of enterprise, university and government environments, because it provides a single point of control for all the information that passes in and out of your company. A well-configured message filtering solution can eliminate viruses in e-mail attachments, block spam from end-users, and help keep users from distributing confidential or offensive information. Message filtering can also help individuals organize their own e-mail content, automatically sorting and filing messages in convenient folders that make sense for the way they work. There are several types of policy-based message filtering, including anti-virus, anti-spam, policy enforcement, regulatory compliance, and end-user filtering. Each type of filtering is optimized to protect the integrity of your organization's information, as well as to enhance productivity.

## **PUTTING MESSAGE INSPECTION AND FILTERING TO WORK**

Many organizations have already begun to implement tools to help them filter and process messages. However, the majority of these methods are unwieldy, time-consuming, and poorly suited to growing organizations. The Mirapoint messaging system is designed specifically to accommodate the challenges of growing messaging operations, enabling organizations to streamline their filtering efforts. Based on a unique three-tier architecture, Mirapoint solutions can scale without limit, splitting message routing, storage and access into separate, dedicated systems.

### *KEEPING A LID ON VIRUSES*

Today, protection is typically handled by individually licensed utility applications installed on the end-user desktop. While adequate for handling common viruses for home and small office users, these utilities cannot scale to practically or cost-effectively accommodate the challenges of a growing, increasingly mobile enterprise environment. Either each end-user must invest time to perform complicated configuration tasks from their desktops, or the IT department must do so —designating which drives to scan and how often, and deciding how to deal with contaminated files. The level of protection provided by desktop products is inconsistent, depending on the skill or knowledge of each user, and does nothing to protect users of mobile devices that are becoming a mainstay of e-business communication. And because new viruses are continually emerging, virus profiles must be frequently downloaded from the vendor,

either by individual users or by network administrators. The end result is costly, inefficient, unreliable virus protection that is often too little, too late. The Mirapoint Message Director is a hardened, carrier-grade system that protects users from viruses at the point at which they enter and exit the organization: on inbound and outbound message routers, and the system presents the IT manager with a unified view of the network's logs and reports. Router-based scanning provides a number of benefits over firewall-based scanning, which some companies are beginning to implement. Although firewall scanning is preferable to desktop scanning, it has serious limitations when compared with router-based scanning. Firewalls simply were not designed to scan for viruses, so the capability is an afterthought. In order to scan a Simple Mail Transfer Protocol (SMTP) message, the firewall must implement an SMTP engine, or mail transfer agent (MTA). These are typically simple implementations that cannot handle complex, though important, situations.

Like viruses, spam is best filtered by the inbound message router, which can detect spam before it consumes valuable server disk space. The Mirapoint Message Director provides a standards-compliant, centralized approach to spam filtering that is compatible for users on both Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) mail systems, helping to optimize vital network bandwidth while improving end-user productivity. Because it's based on Internet standards, the Mirapoint Message Director is fully compatible with most message server environments, including Microsoft Exchange, Lotus Notes, Sun Internet Mail Server, Netscape Message Server, and others.

The integrated Mirapoint anti-spam solution in the Message Director product line also gives each end user discrete control on the anti-spam rules by providing so-called personal "white" and "black" lists. Mirapoint felt that this was an absolute requirement to reach a sub-one percent false positive rate since generic anti-spam solutions tend to block many legitimate electronic newsletters, for example. In the end, these systems will only be as effective as user acceptance allows.

#### *ENFORCING MESSAGING POLICY*

Policy enforcement is now, perhaps, the largest IT challenge that organizations are addressing as they strive to remain competitive while complying with mandatory industry regulations. The stakes are high: e-mail systems enable a single employee to distribute sensitive company information to recipients around the globe instantly, either intentionally or unintentionally. Public examples of this type of illicit activity can readily be viewed on Websites such as

<http://www.internalmemos.com>. Yet little is being done to proactively protect corporate information. Today, policy enforcement in the corporate environment is based largely on educating users. Although well intentioned, this approach provides no consistency of enforcement, no accountability, and little capacity for the collection and management of centralized metrics. For sensitive industries such as legal, medical, and finance, concrete proof of policy enforcement is critical. Like spam and viruses, effective policy enforcement can be efficiently implemented via inbound and outbound message routers. Mirapoint Message Directors provide advanced, standards-based manageability to enable centralized enforcement of policies by management and administrators. Confidential or potentially offensive documents can be flagged and evaluated before they leave your organization's messaging system, and detailed log files provide complete accountability as you keep sensitive corporate and financial data secure. Firewall MTAs are also typically exposed to dangerous SMTP probe commands such as "verify" and "expand," which can open up new security flaws, such as directory harvesting, that enable hackers to learn user names and distribution list contents. Bare-bones MTAs are also prone to denial-of-service attacks, so they can be easily shut down by malicious "mail bombs." Most firewall MTAs also lack detailed logging functionality, making security audits impossible. Because firewalls only scan inbound messages, they are unable to detect viruses that are being sent out. This limitation applies to intra-office communications: if one user gets a virus, he can spread it to his colleagues and the firewall is powerless to stop it. In a matter of minutes, a virus-infected intra-office memo can cause data loss for an entire organization. The Mirapoint solution consolidates and centralizes message filtering processes, enabling the firewall to focus on what it does best: handling remaining network traffic such as HTTP and FTP content. Using this approach, viruses can be scanned for, detected, and eliminated before they have a chance to reach users' desktops. Users are free to focus on their jobs rather than acting as part-time MIS administrators. What's more, under Mirapoint's centralized approach, network managers can easily update virus software and profiles over the network from Mirapoint, ensuring that protection for the entire network is always up to date.

Messaging policy is also at the heart of business continuity planning for unforeseen catastrophic "events." For example, using a Mirapoint messaging system a "mirrored" messaging archive can be set up for a company with Web access for certain executives, departments or entire organizations to prevent business from going "dark" for any length of time.

## BLOCKING SPAM

Protection against spam is typically handled using a similar desktop approach. Individual users configure their desktop clients to create a set of rules and to automatically send spam to the trash. However, like a virus utility, this approach to spam protection is difficult, time consuming, and unreliable. Configuring e-mail client filters is complex, with expertise varying from user to user. And client-based solutions can act as little more than a band-aid, doing nothing to keep spam from circulating throughout the network, filling up mail servers and slowing performance.

## ORGANIZING FOR MESSAGING EFFICIENCY

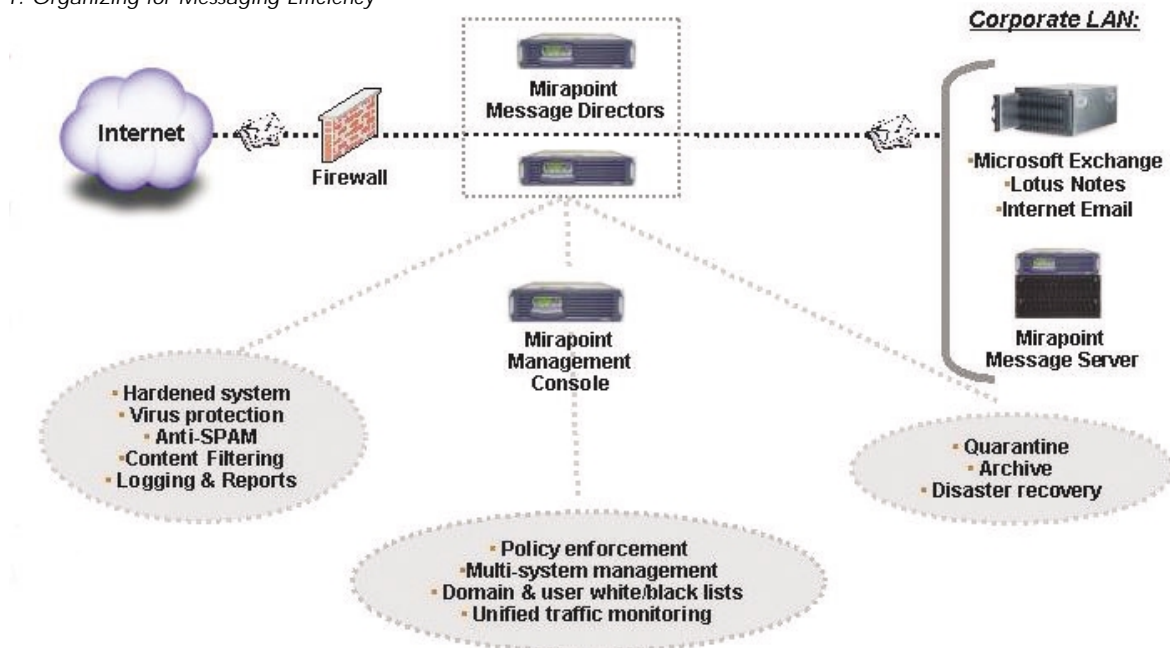
Along with protecting the integrity and security of your organization's information, message filtering can be an effective means to optimize your users' personal productivity as they organize their own electronic correspondence. Individual users using their e-mail client software typically handle message sorting and filing. This approach worked fine in the early days of e-mail, but with today's escalating levels of correspondence, users need a better solution for organizing their mail. In a busy corporate environment, few people have time to spare to sort through and file dozens of e-mails a day, and matters are worse if the network is slow or temporarily disconnected. The Mirapoint Message Server provides a superior alternative. By leveraging an effective filing system directly on the Message Server for IMAP users, individuals can automatically sort and categorize their correspondence. Users can configure the filtering

system to handle messages in the way that works best for them, placing correspondence in appropriate folders as it arrives. And a centralized mail filing system does not require message headers to be downloaded to the client for filtering (followed by users uploading filing commands), so the network benefits from improved use of bandwidth and lower latency. This centralized approach functions even when a user is disconnected, and can automatically forward or reply to messages when the user is away.

## THE MIRAPOINT ADVANTAGE

Armed with a complete set of advanced policy-based message inspection and filtering technologies, your organization can exercise complete control over traffic that passes through its messaging network. Mirapoint solutions enable you to continuously screen and remove inconvenient and potentially disastrous traffic such as viruses and spam, while information policy is better defined and enforced—all by the system, not your end-users. Employees can also gain access to productivity enriching filing tools, enabling them to manage their own correspondence as easily as you manage your company's. Mirapoint offers turnkey solutions to enable your organization to centrally implement this advanced filtering functionality and take charge of mission-critical information. Fully compatible with all of your existing e-mail solution components, Mirapoint's complete messaging systems provide the robust functionality and performance you demand, while keeping management costs to a minimum and freeing end-users from tedious maintenance tasks.

Figure 1: Organizing for Messaging Efficiency



## ACRONYMS

FTP	File Transfer Protocol
GLBA	Graham Leach Bliley Act
HTTP	Hypertext Transfer Protocol
IMAP	Internet Message Access Protocol
MIME	Multipurpose Internet Mail Extension
MTA	Message Transfer Agent
POP	Post Office Protocol
PSTN	Public Switched Telephone Network
SMTP	Simple Mail Transfer Protocol
TIA	Total Information Awareness



### **Mirapoint, Inc.**

909 Hermosa Court, Sunnyvale, California 94085 USA

Tel: 800-494-8965

Tel: 408-720-3700

Fax: 408-720-3725

email: [info@mirapoint.com](mailto:info@mirapoint.com)

[www.mirapoint.com](http://www.mirapoint.com)

For local and international office locations please see [\*\*www.mirapoint.com\*\*](http://www.mirapoint.com)