



# Email Security Requirements Technical Overview

**White Paper**

March, 2004

**razorGATE™**  
A MIRAPoint® APPLIANCE

# Table of Contents

- Introduction ..... 3
  
- Security Requirements ..... 4
  - Security SMTP Connection Management ..... 4
  - Virus Scanning ..... 5
  - Spam Blocking ..... 6
  - Policy Enforcement ..... 6
  - Content Filtering ..... 7
  - Hidden Security Features ..... 8
  - Addressing Other Security Concerns ..... 8
  - Logging and Reporting Features ..... 9
  
- Mirapoint Multi-Layered Security Approach ..... 10
  
- Customer Scenarios ..... 11
  - Centra Health ..... 11
  - ITW ..... 12
  
- Conclusion ..... 14

# Introduction

**It's a war zone out there**—email systems administrators versus hackers, viruses, spam, and who knows what next. Over 450 new viruses are discovered each month, according to IDC Research. Gartner Group estimates that more than 80 percent of computer viruses enter the network through email, and the typical infection costs organizations up to \$500,000 per incident.

Less destructive, but equally disruptive is spam. The average worker receives more than 13 spam messages a day, claims Nucleus Research, which requires six and a half minutes to process, reducing employee productivity. The Radicati Group projects the worldwide cost of spam is \$20.5 billion per year.

Spam-related threats include open relays that can be exploited by unscrupulous senders to route large volumes of spam through an organization's message network without their permission or awareness. Yet another threat is directory harvesting, in which spammers employ public or known email addresses to steal other valid email addresses from a corporate or service provider mail server, and either sell them to other spammers or use the lists themselves.

Beyond viruses and spam are even more menacing security threats. Denial-of-Service (DoS) attacks, sometimes referred to as mail bombs, are designed to bring a network to its knees by flooding it with useless traffic. Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP) ports are subject to the same DoS attacks that impact web servers. While there are software fixes available to limit the damage caused by the attacks, like viruses, new DoS attacks are continually being created by hackers.

Also facing businesses are increasing regulations governing email traffic, requiring vertical industries like finance and healthcare to devise their own requirements to document transactions, archive communications, protect privacy, and ensure honest business practices. Examples include the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Enterprises covered by these regulations must either comply or face possible civil and, in some situations, criminal liability.

Finally, in extreme situations, such as natural disasters or 9/11-like terrorist attacks, companies must disaster-proof their message network so even if a damaging event occurs, key management can continue to communicate and maintain day-to-day operations.

Traditional messaging solutions may not be able to effectively address these security issues. Old-world, software-only messaging solutions were created in an era before security was a problem. Email security solutions are typically assemblies of point product solutions (such as general-purpose servers, virus scanning, and anti-spam applications) integrating hardware and software from multiple vendors that were neither specifically created nor optimized to work together. While subsequent modifications and third-party add-ons try to address some of these issues, correctly configuring these systems or applications can be complicated and error prone, exposing businesses to security threats.

# Security Requirements

In order to address the wide range of messaging risks, next-generation solutions need to take a comprehensive, integrated, multi-layered approach to email security. They must be optimized with hand-selected technology components tailored for security prevention, including features like hardened system design and hacker-proof operating system software. Additionally, these solutions need to be feature-rich and designed for the quick and easy rollout of security services, such as anti-spam, anti-virus, policy enforcement, archival, and other security and protection services.

Smaller businesses face the same threats from viruses, spam, hackers and other security risks as large enterprises, but rarely have the same IT staff or budget as these larger organizations. These next generation security solutions need to deliver enterprise-class features and reliability in a highly effective, simple-to-use appliance that also delivers exceptional value. And since organizations already have existing equipment such as firewalls or legacy mail servers in place, they require a solution that can transparently plug into and leverage their existing infrastructure with minimal complexity. Furthermore, organizations need these next-generation security solutions to provide the 24X7X365 protection against the full range of messaging-based risks.

---

## Secure SMTP Connection Management

Deploying anti-spam and anti-virus applications to secure a mail system is essential—but it's not enough. In addition to whatever filtering engine is used, organizations also need protection at the SMTP layer.

A system should connect via SMTP to a server to determine the acceptability of the sending Internet protocol (IP) address based on block lists, real-time blackhole lists (RBLs), reverse domain name system (DNS) lookup, as well as matches with any other criteria that system administrators may have defined. For example, refuse emails from sites that do not support reverse DNS lookup. By making this determination before accepting data from the sender, the system can eliminate traffic from spammers or hackers and help conserve network bandwidth.

Securing communications with partners or remote employees is critical. STARTTLS should be supported to enable an SMTP session to be encrypted upon request by the server sending the email. Transport Layer Security (TLS), which utilizes Secure Socket Layer (SSL) encryption technology, can provide authentication (i.e., identification of the communication partner), privacy (i.e., ensure the message is not intercepted), and integrity (i.e., make certain the message is not modified).

STARTTLS also allows traveling executives to send email from anywhere securely, including an Internet kiosk, without having to rely on virtual private network (VPN) networks or availability of a local mail server. SMTP AUTH combined with STARTTLS also helps guarantee that any email sent is transmitted securely and not through unknown email servers that could be harvesting userIDs for spam or other information. The SSL encryption additionally secures administrative access into the system.

## **LDAP**

Ideally, in larger environments, edge security systems should be able to utilize Lightweight Directory Access Protocol (LDAP) based databases to manage system security features more effectively. Using class-of-service (CoS) capabilities, administrators can define which users receive anti-virus or anti-spam across multiple systems through a centralized management function.

The system should be able to help ensure password protection and prevent directory harvesting through alerts that advise IT personnel when an external party is using the system as a proxy, when multiple failed logins occur, or when messages are sent to user names that don't exist on the system. In situations where directory harvesting is indicated, the system can progressively slow down SMTP connections until the connection becomes unusable to the external IP address.

## **Denial of Service Attacks**

Denial of Service (DoS) attacks can bring email systems to their knees. Systems should be engineered to resist such attacks and keep on running. They should include high-performance capabilities to provide sufficient traffic handling capacity to absorb many attacks without failing. If the attack is short-lived, system administrators should not need to take any action at all. Ideally, a system should continue to run, even if under attack, and management tools should be available to alleviate the attack.

Systems should address DoS attacks in several ways. When too many SMTP connections are received from a single IP address within a short period of time the system should throttle connections from that IP address. System administrators should also be able to use block lists to filter out known attackers, and even drop

messages from suspected attackers. Of course, the system should generate logs and reports that advise system administrators of attacks as they occur.

## **Virus Scanning**

Integrated virus scanning technology provides powerful protection against viruses. The integrated anti-virus solution should include automatic updates for the latest protection against emerging virus threats and should have the capability to be centrally managed through the system interfaces.

An effective virus-scanning solution uses an intelligent heuristic for finding viruses within Multipurpose Internet Mail Extensions (MIME) attachments. Each incoming email message should be analyzed by disassembling or parsing it into its various attachments according to the request for comment (RFC) (i.e., through RFC-compliant MIME parsing). These attachments are routed to the anti-virus engine, where they are analyzed for viruses. Because most scanners are RFC compliant, many viruses exploit MIME weaknesses. To combat this, the same message should again be disassembled in a way similar to Microsoft Outlook, which does not follow the RFC.

When a virus is found, system administrators should have the option to set various actions to delete, clean, or quarantine a message. Then, unless deleted, the message can be reassembled and sent on to its intended destination—free of viruses.

Industry leading virus protection should be integrated into an appliance, with new engines and virus definition files issued monthly, and virus identity files (VIF) as needed. Your solution provider should continually monitor updates for new virus pattern files and down

load them onto a geographically separated pair of servers that operate in an active, failover mode. The ability to automatically query those servers at regular intervals to update their virus pattern files should also be made available. Customers should update their systems every hour.

## **Spam Blocking**

A truly secure system should provide powerful anti-spam technology that combines effective spam analysis, identification, filtering, and management features to achieve a spam catch-rate of at least 96% with zero false positives. A multi-layered approach should address spam at the email gateway, while giving administrators control to define white and black lists to avoid lost messages and optimize the effectiveness of spam filtering.

Using heuristic rules-based scanning, the system should analyze messages at the server level based on information in the header, envelope, subject, and message, and then score the risk accordingly. The spam engine should also query Vipul's Razor to match suspected spam signatures. If the score exceeds a defined threshold, which can be adjusted by both administrators and end users, the message can be tagged as spam and the appropriate action taken on the message.

Scoring is typically done only once, at the server level, increasing performance and throughput. Evaluation of the scores should be done at both the domain and user levels. In a secure system, tagging and filtering are hierarchical; i.e., domain filtering can be more restrictive than system filtering, and end-user filtering can be more restrictive than system or domain filtering. An end user, for example, can set their spam/no spam threshold to a more restrictive setting than the system threshold, based on their client filtering capabilities.

IT managers should be able to take the most appropriate action based on the magnitude of the filtering score. Possible actions include blocking (bouncing or silently rejecting), forwarding (to a separate folder or email account), discarding, and/or tagging the message in the header or subject line. Text inserted in the subject line identifying a message as spam should be customized on a system basis, by the administrator.

The system should have easy-to-use tools that allow IT managers and end users to identify spam and report newly identified spam characteristics. New spam rules can then be created that are automatically provided to customers via network-based updates. Customers should also be able to create customized rule sets to meet unique requirements. In addition, all spam activity should be logged and easily tracked by the system administrator.

## **Policy Enforcement**

Flexible content filters allow enforcement and creation of corporate policies, and can provide powerful management tools for the end-user. The ideal system should be configurable at the domain level allowing actions to be taken based on content embedded in the header, body, or attachment of a message. Systems should also have pre-defined content filters to make policy enforcement easier for the administrator. Such policy enforcement tools can help companies manage employee email usage, prevent sensitive information leaks, address regulatory compliance requirements, and protect against harassment and other types of email abuse.

## **Content Filtering**

A truly secure system should enable IT staff to define spam and customize spam protection. White and black lists should exist at both the user and domain levels to trigger filter actions just as if the message was not spam. IT managers should additionally be able to adjust the spam threshold to optimize it for their organization's message traffic and develop unique domain or system-level white and black lists based on the email sender.

Content filtering increases the spam catch rate, but at the same time it also helps users manage their mailbox. Users, for example, should be able to manage how incoming messages are handled. Filtering should be done by message body, header, subject, as well as the "to," "cc," "from", and "reply to" fields. Based on that information, users can then initiate a custom action by message, such as sending to a specific folder, deleting, forwarding, or copying.

## **Wiretaps**

Wiretaps give administrators an easy way to copy messages to and from a given user for review. In addition to splitting the message into two streams, a wiretap should provide a method for guaranteeing security. Traditional duplication mechanisms cannot prevent bounces if the storage mailbox fills or becomes unavailable, causing discovery of the wiretap. Systems offering wiretap should be able to rewrite the envelope to prevent this possibility and allow the administrator to specify where bounce messages should go if they are encountered.

## **Blocked Address Filters**

Secure systems should provide blocked address filters that allow administrators to easily create filters that block specific email addresses or domains. Organizations may need this to prevent disgruntled employees from sending out company-wide emails, prevent competitors from sending messages to the company's employees, or prevent employees from contacting competitors.

## **Blocked Message Filters**

In addition to blocking addresses or domains, a system should also enable administrators to easily create blocked message filters that prevent any message that matches any word in a word list from being delivered.

## **Blocked Attachment Filters**

Attachments with file types such as .pif, .scr, and .vbs have been known to contain viruses. A secure system should allow administrators to create blocked attachment filter lists to prevent delivery of known harmful file types. A filter of this type should also enable administrators to prevent employees from sending mail containing file types, such as a .xls Excel spread sheet, that might be considered company confidential or contain sensitive information.

## **Redirected Attachment Filters**

Administrators should also be able to redirect or quarantine email messages with certain file types where a policy exists that requires documents to be reviewed before they are sent out of the company.

### **Corporate Word List Filters**

Administrators should be able to create a policy around confidential information using keywords such as “confidential,” “proprietary,” “NDA,” and internal project names. Corporate word list filters should be capable of quarantining these messages, forwarding them to another address for review, or rejecting or discarding messages containing these words.

### **Objectionable Word List Filters**

Similar to word list filtering, administrators should be able to create a policy around objectionable words that may be the basis of harassment-based lawsuits, allowing human resources departments to enforce corporate policies.

### **Hidden Security Features**

Systems ideally should offer security features that work in the background, notifying administrators only when a problem arises. These features should include directory and password harvesting protection, intrusion detection, and a closed, hardened operating system.

Systems should automatically detect anomalous behavior from a single IP address and act accordingly to protect itself. For example, if an SMTP connection occurs repeatedly from the same IP address, or a login attempt occurs repeatedly and each connection has some anomaly—either as a syntax error in issuing a command, repeatedly sending to unknown recipients (directory harvesting), or a bad password issued—the system should automatically introduce delays or prevent access for that IP address’ connection. The system should also continually increase the amount of delay introduced with each new suspect connection. These events should be additionally tagged in both real-time and in the daily logs for administrative review and alerting.

System administrators often worry that their systems will be the target of a hacker attack or intrusion using security flaws in software they are running. The system should be rigorously tested to ensure that all possible security flaws in the OS are removed. As an added level of protection, the system should also be able to detect a hacker or intruder gaining access to the system. The intrusion detection system should be designed to alert the administrator when a hacker attempts to access or change files and executables in the system. This mechanism should ensure that administrators are running the safest system possible and that undiscovered security flaws cannot be exploited.

### **Addressing Other Security Concerns**

The system should be capable of addressing other security concerns such as email archival and business continuity.

#### **Email Archival**

To meet regulatory compliance requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the Securities Exchange Commission (SEC) and Gramm-Leach-Bliley Act (GLBA), an email solution should address message traffic to outside parties. Archival solutions should complement the email system and automatically archive message traffic as defined by a specific policy. Furthermore, archival solutions should provide advanced search, custom index, as well as security features to ensure the integrity of the archived content

#### **Quarantine**

The system should also serve as a quarantine station or pass email transparently to a quarantine station for any mail identified by policy management and content filter-

ing rules imposed by IT managers. It should have the additional advantage of being tamper free, so as to be able to seamlessly be passed to the recipient without detection of having been quarantined.

### **Business Continuity**

Email, and the information it contains, has become a mission-critical asset for most organizations today. The loss of this information in the event of a disaster (fire, earthquake, or terrorist attack) can have a severe and lasting impact on the viability of companies. Systems should provide a cost-effective, scalable solution for disaster recovery to meet emerging requirements around business continuity planning.

### **Logging and Reporting Features**

Systems should provide detailed, realtime logging and reporting with security alerts and notifications to enable system administrators to determine the nature, scope, and frequency of threats impacting the system or systems in addition to trends such as increasing load from external and internal mail.

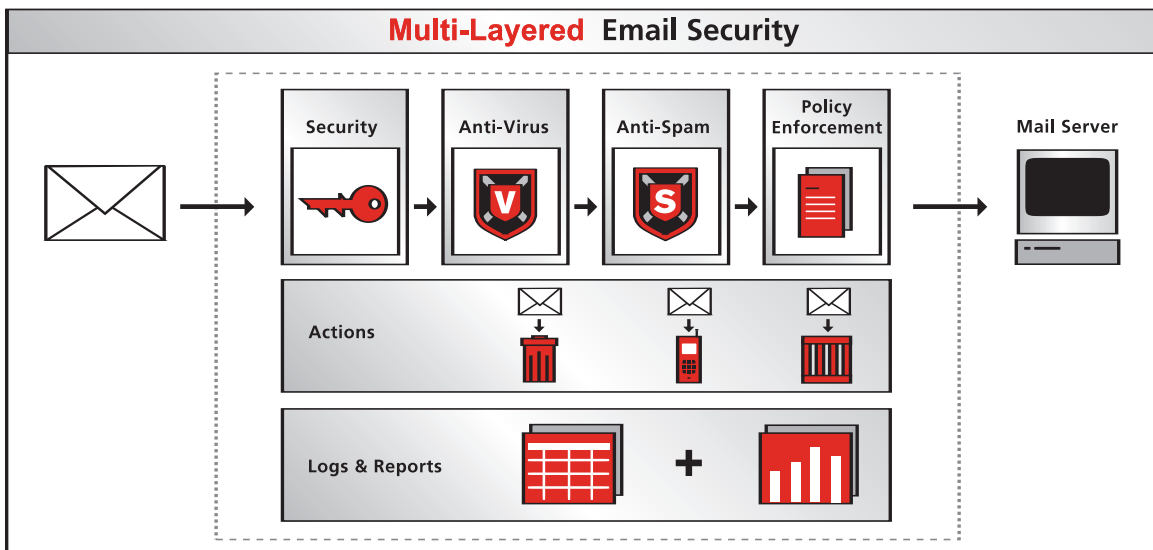
The system should have a mechanism that can be put in place for rapid migration and deployment in the event of a disaster, so business-critical email communications can be quickly restored. The system should provide failover capabilities for handling a queue of email in case of a catastrophic failure. The system should be able to store a copy of another mail server's store, such as Exchange, in the event of a disaster. And it should provide an image backup and restore capability to rapidly backup messages to tape. Finally, the system should be designed to be a robust and highly available appliance with proven 5-9s of reliability.

## Multi-Layered Security Approach with RazorGate

The messaging experts at Mirapoint are proud to introduce the RazorGate email security appliances. Designed for the network edge, RazorGate delivers the industry's best protection against spam, viruses and hacker attacks meeting all of the requirements mentioned above.



Mirapoint has significant expertise in messaging with its first email and security appliances shipping back in 1998. Today, organizations worldwide rely on Mirapoint to secure their message networks with exceptional performance, reliability, and ease of management. The RazorGate appliances are based off of the same customer-proven Full-Spectrum™ email security technology that the Mirapoint Message Director employs which boasts 96% spam catch rates with zero false positives, a hardened operating system with no known exploits for hackers, and superior reliability with proven 5-9s of availability based on real-world deployments.



## Customer Scenarios

Following is a customer benefiting from Mirapoint's full spectrum email security features including anti-virus and anti-spam protection and although they have deployed these features on a Mirapoint Message Director they can also be deployed on RazorGate appliances for the small and medium sized business (SMB) market.

---

### Centra Health

#### **Background**

Centra Health is a regional, not-for-profit healthcare system located in the heart of Central Virginia with more than 3000 skilled healthcare professionals providing comprehensive medical services. The core of their messaging system is an IBM Lotus Notes email server. Until late 2002, they also had a Unix server for message routing and another server running IBM Secure Network Gateway firewall and Symantec virus scanning software.

"The existing four-year-old solution became increasingly unreliable and difficult to manage," said Steve Higgins, Network Engineer at Centra Health. The aging Unix server hardware and software used for message routing and virus scanning required more frequent reboots.

#### **Challenge**

As the demands of keeping the ailing system running increased, spam was also becoming a serious problem. "Most users will at least look at the messages, which takes time that adds up, impacting overall productivity throughout the organization," says Higgins. It was clear that something had to be done. What they needed was a system that was simple, reliable, and secure.

#### **Solution**

In early 2002 they began the search for a replacement that was easy to set up, ease to use, and easy to man-

age; one that could provide effective virus scanning, spam filtering, and the flexibility to add capabilities in the future.

Centra Health considered Mirapoint and Sendmail for Windows. "The complexity of configuring Sendmail was much greater than Mirapoint," says Jody Hobbs, Lead Network Engineer at Centra Health. "One of Mirapoint's key benefits was ease of setup. Mirapoint also provided a broader set of security features at a better value and gave us the flexibility to add features in the future."

Deployed in the fall of 2002 to front-end the existing Notes server, the Mirapoint Message Director consolidated the message routing and virus scanning servers into a single, more manageable solution. It includes Mirapoint's message routing, virus filtering, spam protection, content filters, and domain-level black and white lists to manage email traffic. "Once we migrated everyone to the Mirapoint system, the only thing our users noticed was they had less spam in their mailbox," says Hobbs. "It was a seamless transition."

The virus and spam capabilities have proven very effective. "We've caught over 1300 viruses this year, and we're also blocking between 5500 and 6000 spam messages a day," says Higgins. "That many messages adds up over a month's time, so it saves us money because we don't need as much disk space. Of course, it increases the productivity of our people too."

Not only was the solution easy to deploy, but it has been easy to manage as well. "We can administer the system from any workstation through a web browser," says Hobbs. "Before we had to go to the Unix server and use the command line interface." Overall management has been reduced to less than an hour a day, mostly related to simple questions from users about how the spam protection works. Reliability, too, has improved dramatically over the legacy system. "Overall, I would say it's been excellent," says Hobbs. "Mirapoint has enabled us to consolidate from multiple servers to one appliance. It has also given us the ability to effectively filter spam as well as ease of use and management, which we didn't have before."



## **Background**

Illinois Tool Works, Inc., headquartered in Glenview, Illinois, (ranked 197 on the Fortune 500) is a \$9 billion diversified manufacturer of highly engineered components, industrial systems, and consumables. The company consists of approximately 600 decentralized operations in 43 countries and employs over 50,000 people. Operating autonomously, each business unit selected its own messaging solution. Some have AOL or Hotmail. Others have chosen third-party hosting through Sprint or Quest. Still others have Microsoft Exchange as their in-house solution.

## **Challenge**

While not abandoning its autonomous culture, ITW was driven to provide a higher level of security for its financial payroll and human resource information traveling through email by deploying an enterprise-wide virtual private network (VPN). The company wanted a messaging

solution that would allow business units to retain some autonomy, letting them have control over their domains, add and delete their own users, and enforce their own policies and spam filtering. The solution also had to be scalable, easy to manage, and most important, provide security.

## **Solution**

ITW considered two solutions, Microsoft Exchange and Mirapoint. "We liked Mirapoint's 'all-in-one' solution," says Marc Palano, director of IT for ITW. "It not only offered a message store, but spam and virus filtering as well. It was future-proofed. It was WAP-enabled and had XML applications: all the features we were looking for in a mail server."

Installed in June 2002, the Mirapoint system, consisting of two Message Servers and two Message Directors, now supports about 6000 email users. Another 2000 have retained their existing email servers, but rely on the Mirapoint Message Directors for virus and spam filtering. "We've been able to reduce spam by more than 80 percent," says Palano.

ITW leverages the delegated domain administration feature from Mirapoint that allows its individual business units to administer, manage, and control their own email domains, yet partition system management and service availability to ITW's centralized corporate group. Each business unit, for example, can set its own spam filters and black and white lists. "That's important for us because that's the spirit of ITW: decentralized and autonomous" says Palano. "Yet, at the same time, by centralizing email, controlling all the mail here, it plays right into our VPN strategy."

ITW has many cell phone, PDA, and BlackBerry users that rely on Mirapoint's IMAP capabilities to access their mail from wherever they are. "All they need is Internet access and the user experience on the road is the exact same user experience they have at the office," says Palano. "Because the messages are kept on the server and not on the laptop, the speed of the laptop is increased. And if the laptop is lost, stolen, or crashes, users won't lose their messages. It also enables corporate IT to better enforce mail storage policies."

Business units that have taken advantage of the Mirapoint system have been pleased with the outcome. A survey taken by the IT group prior to deployment of the Mirapoint system revealed that local messaging system administrators were most concerned about daily backups, administrative tasks, and downtime over the weekend. "By bringing them into the central system, we have eliminated their top three headaches," says Palano.

Palano and local systems administrators alike have been pleased with the reliability of the Mirapoint system. "Since it went in, we've had zero downtime. Talk about the 5-9s of availability," says Palano. That level of performance has encouraged a growing number of business units to give up their local systems. "We are not pressuring any business units to come onto the Mirapoint system, but we have actually had units shut down their Exchange servers." That enthusiasm has spread overseas as the first international business unit migrated to the Mirapoint system in June, citing the system's bilingual capability as a key feature.

## Conclusion

**It's time to take control and slam the gates on threats to your message network.**

The RazorGate appliances are built on the same technology as Mirapoint's Message Director. With hundreds of deployed Message Directors, this technology is customer tested and proven to offer the best hacker, spam and virus protection. The feature-rich RazorGate appliances are designed for quick and easy rollout of highly-effective security features, that are highly available, scalable and reliable with world-class performance.

For more information on how RazorGate can improve the security of your message network, visit our Web site at [www.razorgate.com](http://www.razorgate.com), or for larger customer scenarios visit the Mirapoint website at [www.mirapoint.com](http://www.mirapoint.com) to learn more about the Message Director. You can also call us at 408-720-3700.



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) or [www.razorgate.com](http://www.razorgate.com)

© Copyright 2005 Mirapoint, Inc. Mirapoint, RazorGate, MailHurdle, Rapid Anti-Spam, MessageBase, Full-Spectrum, Messaging Operating System, DirectPath, DirectAccess and logo are trademarks or registered trademarks of Mirapoint, Inc. WP-SecStrat-0205