

Meeting the Challenge of Email Security and Regulatory Compliance

A White Paper



Mirapoint, Inc.
909 Hermosa Court
Sunnyvale, California 94085
www.mirapoint.com
Tel. 1 + (408) 720-3700

Executive Summary

With the rising popularity of email, comes an increased scrutiny of email for regulatory compliance. Because email messages make up a significant portion of the daily communications of almost any large organization, email messages have become important evidence in regulatory investigations and lawsuits.

A growing number of industry regulations and national laws explicitly or implicitly require enterprises to better manage, secure, and archive their email messages. Some of these regulations, such as Sarbanes-Oxley, apply to public companies in all industries. Other regulations, such as HIPAA, apply to specific industries, such as a healthcare. Around the world, countries are enacting new laws and regulations to better protect consumers and promote fiscal responsibility. The EU Privacy Directive and Japan's Data Protection Act are two examples recent laws that require businesses to tightly control confidential data about consumers.

While these laws and regulations vary in purpose and scope, they share common requirements for secure data transmission and storage. These requirements include real-time filtering of message headers and content, spam management, anti-virus protection, encryption, hierarchical storage and retrieval, and message quarantine and review. Enterprises must find of way of meeting these requirements without sacrificing the benefits of convenience and cost-effectiveness that email offers for daily communications.

Mirapoint, the leading secure messaging leader, offers secure messaging solutions that enable organizations of all sizes to meet the challenges of regulatory compliance. Mirapoint messaging appliances provide the secure, scalable messaging infrastructure organizations need in order to:

- Provide reliable, highly available messaging services that enforce the authentication and encryption controls required by regulations such as Sarbanes-Oxley and HIPAA.
- Protect networks from viruses, spam, and other unauthorized traffic.
- Provide the policy-based controls for blocking, redirecting, and archiving messages, based on regulatory requirements and internal guidelines.

By deploying Mirapoint messaging appliances, an enterprise can quickly and affordably create a secure, messaging infrastructure for compliance.

Introduction

Over the past decade, email has become the primary communication channel for business—and its growth is continuing at an awe-inspiring rate. Email traffic volumes and storage requirements are rising dramatically. According to the Radicati Group, the average corporate email user sends 84 messages per day, consuming 10 MB of storage. By 2008, the average email user's daily storage requirement will reach 15.8 MB per day. Not surprisingly, the email archiving market is expected to skyrocket over the next few years, growing tenfold from \$465 million in 2005 to \$4.4 billion in 2009. IT departments are scrambling to ensure that email services are continuously available and that adequate servers are provisioned to transmitting and when appropriate archiving messages.

With the rising popularity of email, comes an increased scrutiny of email for regulatory compliance and law enforcement. Because email messages make up such a significant portion of the daily communications of almost any large organization, email messages have become important evidence in lawsuits and regulatory investigations. Organizations of all kinds and sizes, ranging from the federal government to small consultancies, have been asked to produce email as part of an investigation.

Putting in place technology for systemically archiving messages and rapidly retrieving email messages upon request, can be expensive. For example, in an anti-trust case in 1995, Ciba-Geigy was forced to search 30 million email messages to produce required evidence. Ciba-Geigy estimated that this search cost the company \$60,000. Legal infractions involving email can also be costly. Chevron faced a \$2 million lawsuit resulting from an employee's "joke" email that allegedly contained sexist content. Thus, a single user's ill-considered decision to distribute this email message resulted in large expenses and bad publicity for the company.

Because email messages can provide the "smoking gun" in actions ranging from civil lawsuits to accounting scandals to criminal investigations, the number of laws and industry regulations requiring organizations to control, secure, and archive their email have increased dramatically. Some of the regulations are tied to specific industries, such as healthcare, while others are related to the types of information an organization is working with, such as customer data.

While email volumes are surging, management teams and IT departments are coming under increasing pressure to ensure that every email message passing their networks complies with an increasingly strict set of industry regulations, company policies, and best practices.

To avoid criminal and civil penalties, bad publicity, and lost business, it is in the best interest of management teams and IT departments to understand these regulations, to assess the risk exposure of their own email and messaging infrastructures, and to develop policies and plans for addressing regulatory compliances and following best practices for email communications.

This paper presents a survey of the most important regulations regarding email, summarizes email feature and usage requirements across these regulations, and introduces the email compliance solutions available from Mirapoint, the leading secure messaging vendor.

Regulations Affecting All Businesses

Sarbanes-Oxley

No regulatory legislation is receiving more attention these days than the Sarbanes-Oxley Act of 2002. Drafted in response to the corporate accounting scandals of the late 1990's, Sarbanes-Oxley requires the financial leadership of public companies to take full responsibility for the accuracy and security of their financial data and accounting procedures. Access to financial data must be limited to authorized individuals. Communications between executives and accountants must be archived. Communication procedures must be monitored, security controls put in place, and monitoring procedures documented and rigorously followed. Sarbanes-Oxley says little about specific technologies, but since email has become the de facto standard medium for corporate communications, the Act clearly has implications for the secure use and distribution of email messages. Public companies must not divulge financial data inappropriately through email. The regulations call for financial data to be maintained in financial software applications, rather than distributed in ad hoc, uncontrolled spreadsheets like those so commonly emailed around corporations today.

To comply with Sarbanes-Oxley, an organization's email system must authenticate senders, encrypt confidential information, track and log message traffic, and support the indexing, archiving, and retention of messages. Email policy servers (integrated with email servers to monitor communications and to redirect, block, or encrypt messages based on their contents) should be able to filter communications between executive team and accountants and archive those communications for a future review of accounting practices.

Accountability for Sarbanes-Oxley compliance goes right to the top. The CEO and CFO must attest that the organizations financial statements are accurate and that its accounting and information management policies are in order. The penalties for infractions are severe, with fines of up to \$5 million and imprisonment for up to 20 years. Not surprisingly, executive teams and boards of directors have scrambled to achieve and maintain compliance with Sarbanes-Oxley.

Officially, Sarbanes-Oxley applies only to public companies (the law first applied only to companies with a market capitalization of \$75 million or more, but as of April 15, 2005, all public companies must comply). But the effects of Sarbanes-Oxley extend far beyond public companies. Inspired by the broad press the Act has received, and wary of the public's low tolerance for new accounting and mismanagement scandals, many private companies and even non-profits are adopting Sarbanes-Oxley as a model for securing and monitoring accounting processes and for improving information management.

Currently Sarbanes-Oxley is restricted to US companies; however organizations wishing to do business with the United States need to comply with its regulations and other parts of the world, especially the European Union (EU), are looking to implement their own variants of the legislation.

The California Security Breach Notification Act

The California Security Breach Notification Act (SB 1386), which took effect in 2003, requires any business, regardless of its location, to publicly disclose a security breach that could compromise the confidential information of any California resident. The law is remarkable for its focus on disclosure and for its broad scope: if a business has no offices in California, it still must comply with the law if even a single customer is residing in California. Organizations, public or private, that fail to comply with the law face civil penalties and class-action lawsuits.

In June 2006, the California Security Breach Notification Act contributed to Citigroup's decision to disclose that computer tapes containing personal information of 3.9 million customers had been lost in transit.

Such disclosures can be expensive for the companies who make them. Not only does the company's reputation suffer from its admission of carelessness or vulnerability, but the company must also bear the sometimes exorbitant costs of notifying large numbers of customers. According to an industry executive interviewed about Citibank, notifications can cost from \$30 to \$50 per customer, and monitoring customer credit records after a breach costs an additional \$25 per customer. Financial services firms are therefore advised to budget \$75 per customer for communications and monitoring costs overall for a single security breach.¹ A breach affecting 100,000 customers would cost \$7.5 million for communication and monitoring alone. Citibank's tape loss would therefore cost the company over \$292 million dollars in customer care services alone.

Regulations for Specific Industries

Financial Services

A broad range of regulations and standards, some general and other very specific, apply to the email systems of financial institutions.

¹ "The Citi Sleeps," *FinanceTech*, June 7, 2005.

Gramm-Leach-Bliley

Also known as the Federal Modernization Act of 1999, Gramm-Leach-Bliley (GLB) regulates the way that financial institutions manage the private information of individuals. The Gramm-Leach-Bliley legislation refers to this information as Nonpublic Personal Information (NPI). A written information security program should contain administrative and technical safeguards to protect NPI in transit or in storage. Companies must protect NPI from all anticipated threats and hazards, and must ensure that NPI is not carelessly or maliciously divulged.

Two rules within Gramm-Leach-Bliley have special significance for email and email security. The Financial Privacy Rule treats the collection, use, and disclosure of NPI, and calls for institutions to provide opt-out mechanisms and privacy policies to customers.

The Safeguards Rule says that organizations must implement security programs protecting NPI that are appropriate for the size and complexity of the organization and the sensitivity of the NPI.

Companies will have to use authentication and encryption to protect NPI found in email. To support all of Gramm-Leach-Bliley's security mandates, a company will likely require an email solution that provides policy-based filtering and blocking, logging, and reporting.

Basel II

An example of a general guideline is Basel II, a capital investment framework developed by a group of central bankers under the auspices of the Basic Committee on Banking Supervision (BCBS) in Basel, Switzerland. The central bank governors of the Group of Ten nations (G-10) created the BCBS to formulate standards and guidelines for banking supervision. The member authority in each G-10 nation, such as the Security and Exchange Commission in the United States, is expected to enforce these standards and guidelines through their own national laws and organizations.

The Basel II framework recommends “three pillars” of best practices to bring stability to risk management in international banking. The second and third pillars relate to email in a general way. The second pillar calls for the effective supervisory review of bank’s internal assessments of their risks. Internal processes, including processes involving internal communication, must be well designed and controlled to ensure that a bank’s risk management practices are sound. The third pillar calls for banks to properly manage their public disclosures to encourage transparency in accounting. Clearly, mismanaged or duplicitous email communications would run counter to risk management controls and prudent public disclosures.

Member nations are required to implement the Basel II accord by 2008.

NASD Regulations

An example of precise and stringent guidelines for email can be found in the regulations for the National Association of Securities Dealers (NASD). These regulations make fine distinctions between the content, senders, and recipients of email. For example, email to 25 or more prospective retail customers is considered sales literature. As such, it must be approved prior to use by a registered principal of the company, then archived as part of the company’s records for three years from the date of last use. Email to a single customer or to an unlimited number of existing retail customers or to 25 or fewer prospective retail customers is classified as correspondence, which is treated differently. The regulations pay close attention to the content of email messages. For example, regulations stipulate that communications with the public may not predict or project the performance of securities. The sources of any statistical table, chart, graph, or other illustration included in email must be noted and maintained in a record.

To comply with these NASD regulations, a financial services firm must have a messaging infrastructure that can:

- Filter email messages based on header information, such as sender and recipient fields), as well as on message content
- Quarantine messages pending approval, and transmit messages once approved
- Ensure that only authorized users grant approval for message transmission
- Archive messages

- Retrieve messages in a timely fashion for review by compliance officers and regulators

Healthcare

Originally created to enable insurers to transfer patient insurance information among organizations to ensure that workers moving from one job to another received uninterrupted healthcare coverage, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has evolved into a far-reaching bill that calls for the protection and management of all patient health information.

The part of HIPAA most relevant to email communications is the HIPAA Privacy Standard, Section 142.308 of Subpart C, Security and Electronic Signature Standards. This section sets forth requirements for “technical security services that guard integrity, confidentiality, and availability.” Healthcare organizations must implement a secure communications infrastructure that provides:

- Access control (context-based, role-based, user-based, or some combination of these)
- Authorization control (either role-based or user-based) that ensures that only authorized users gain access to patient health information
- Data authentication, ensuring data integrity
- User authentication involving unique user IDs, an authentication feature such as a password or PIN, and automatic logouts
- The optional use of data encryption
- Audit controls that enable email security to be analyzed for compliance

The civil and criminal penalties for HIPAA violations are severe. Civil penalties can reach \$25,000 for multiple violations of a single requirement or prohibition during a calendar year. Criminal penalties for individuals failing to protect patient data range from a \$10,000 fine and up to one year’s imprisonment for the wrongful disclosure of patient data, to a \$250,000 fine and ten years’ imprisonment for wrongful disclosures committed under false pretences for commercial advantage, personal gain, or intent to commit malicious harm.

Healthcare organizations (HCOs) should deploy messaging solutions or email filtering systems that can scan email messages and detect content requiring special treatment. Such content would include all patient health information (PHI), including electronic medical records (EMR) appointment information, prescriptions, invoices and bills, American Medical Association (AMA) treatment codes, and Centers for Medicare and Medicaid Services (CMS) disease codes.

Government

The Federal Information Security Act of 2002 (FISMA), developed by the National Institute of Standards and Technology (NIST) in 2002, requires all federal agencies and their partners to establish, consistent, risk-based security processes. FISMA calls for each federal agency to “develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source.” Because every agency relies on email to support operations and assets, agencies must address email security in order to comply with FISMA. To protect information assets traveling in email, and to protect database servers and other IT assets from malware threats (viruses, worms, and Trojans) introduced by email, agencies need comprehensive email security, including authentication, encryption, spam-filtering, and virus-filtering.

International Regulations

American organizations doing business internationally have additional regulations to comply with whenever they do business outside the borders of the US. In the Americas, Europe and Asia governments have passed legislation to protect the privacy of their own citizens.

Canada’s Personal Information Protection and Electronic Document Act

Canada’s Personal Information Protection and Electronic Document Act (PIPEDA), passed in 2000, applies to all organizations doing business in Canada, unless they are doing business in a province whose local laws more or less replicate the requirements of PIPEDA. This privacy legislation compels organizations to use authentication and encryption to protect personal information.

The European Union's Privacy Directive

The European Union's (EU) Privacy Directive defines the rights of "data subjects," people about whom information is being collected. Whenever an organization in the EU collects information about consumers, the organization must report who is collecting the information, what the information is being used for, and who will have access to the information. The directive stipulates how data can be used for direct marketing and how information can be exchanged between organizations. To comply with this directive, organizations may be asked to demonstrate that no consumer information has been illegally collected or divulged through email. Comprehensive control over inbound and outbound messaging is an essential component of any solution for complying with this directive.

Japan's Personal Data Protection Act

In Japan, the Personal Data Protection Act, which took effect in April 2005, calls for all organizations doing business in Japan to secure personal information and to diligently protect any database that lasts at least 6 months and that contains at least 5000 records. Since viruses and worms can attack databases and database servers, and email is the most common source of viruses and worms in the enterprise, businesses should make email security—specifically email filtering solutions that keep viruses and worms off the network—part of any multi-layered solution for database security. Other Asian governments are likely to adopt legislation similar to Japan's data protection act, so the requirement for protecting databases from email-borne threats is likely to become more widespread.

The United Kingdom's Data Protection Act

The United Kingdom has its own Data Protection Act, which passed in 1998. This Act calls for organizations to securely store all personal data, including data found in email messages. Personal data must be accessible only to authorized users, and the security of this data must be regularly audited. The Data Subjects—the people whose personal information is being stored—have the right to learn how their personal data is being stored and accessed. They also have the right to receive accurate copies of the data, even if it is contained in email messages scattered across multiple servers and archives. Organizations may even have to furnish deleted email messages, if it is remotely possible to retrieve them from archives.

The security measures required by this Act are not commonly found in email systems. Many organizations will be forced to integrate email services with vast, secure storage systems, while ensuring that whenever an employee, ex-employee, or customer asks for his or her data, it can be retrieved in a timely fashion. Most organizations lack such sophisticated archives today. The storage systems will have to be able to delete data that is “no longer necessary,” as the Act prescribes. This is another capability not found in most email systems and archives deployed today.

ISO 17799

Originally published by the International Organization for Standardization and the International Electrotechnical Commission in 2000, the ISO/IEC 17799 security standard describes best practices for information security that apply to organizations of all sizes and purposes. The standard is divided into ten sections, each describing an important aspect of security. The sections include:

- Business continuity planning
- System access control
- System development and maintenance
- Physical and environmental security
- Compliance
- Personnel security
- Security organization
- Computer and network management
- Asset clarification and control
- Security policy

Several of these topics relate to email. For example, system access control involves controlling access to information and providing security to mobile users—both of which relate to email security. It would be difficult, if not impossible, to claim ISO 17799 compliance without an email security solution that enforced rigorous authentication controls and that defended information systems from malware attacks.

That said, few organizations claim or attempt to achieve compliance with the entire standard. As *Information Security Magazine* notes, “For the most part, the standard is used as a checklist for developing security policies. Organizations take only what sections they need to develop a sound framework.”²

Compliance with ISO 17799 is certified by authorized certification body, such as Certification Europe and KPMG. While there are no legal penalties for non-compliance, organizations may lose business if prospective customers or partners are interested in doing business only with other ISO 17799-compliant organizations.

Requirements for a Compliance Solution

While the emphasis and scope of these regulations vary, the requirements for identifying, protecting, and archiving specific types of email communication are common to nearly all of them. From these commonalities, we can derive a set of features that are required for any enterprise messaging system.

Real-time Filtering of Address Information and Content

An email policy engine should be able to filter messages based on criteria such as:

- sender
- recipient
- content, including key words and phrases in the body of a message, as well as key words and phrases in an attachment

For example, to comply with Sarbanes Oxley, enterprises should archive online communications between the executive team and the organization’s accounting firm. Email messages between these two groups can be identified by their sender and recipient fields. Similarly, financial services firms that are required to police communications between securities analysts and broker/dealers could also make use of message header filtering to identify these communications.

Securities firms can also filter message contents for specific content such as ticker symbols and language likely to be used for stock touting.

² “Standard Practice: ISO 17799 aims to provide best practices for security, but leaves many yearning for more,” Lawrence M. Walsh, *Information Security Magazine*, March 2002.

Upon detecting suspicious or illegal activity, the email policy engine should be able to take action, such as quarantining messages and alerting a compliance officer.

Spam Management

Effective spam filtering at the network perimeter can reduce the volume of email entering a network by 98%. Filtering spam is an essential part of deploying any compliance solution involving email archiving and retrieval. It's much easier—and much more affordable—to archive and search through 2% of messages, rather than 100% of messages. Besides saving money on disk space, tape, and other storage costs, smaller archives offer the benefit of faster retrieval times. They make it easier for an enterprise to furnish messages to auditors or a court in a timely manner. Especially in cases where an enterprise is taking the approach of archiving every message on its network in order to assure compliance, reducing the number of messages on that network is an essential step in making a compliance solution workable at all.

Of course, reducing spam has important advantages beyond compliance. It can also reduce fraud. A recent survey by the Radicati Group and Mirapoint of 800 email users, including business users and consumers, found that 11 percent of users had purchased products or services by responding to spam, and 9 percent of users had lost money as a result of an email scam.³ Clearly, cautionary news stories and well-intentioned security guidelines are not enough to prevent users from shunning spam offers. Eliminating spam at the network perimeter protects corporate assets, as well as the personal assets of users.

Anti-Virus Protection

According to Gartner, over 80% of the viruses gain entry to an organization's network through email. As the typical virus infection can cost an organization up to \$500,000, businesses have a strong incentive to deploy email security systems that block viruses and other malware at the network edge.

³ http://www.mirapoint.com/company/news_events/press/20050712.shtml, "Survey Finds That Spam Now Hits Your Wallet," July 12, 2005.

Keeping a network free from viruses and other malware is important for compliance. Many standards, such as HIPAA, call for information systems to be secure and highly available. Because virus and worm attacks can jeopardize network and server availability, preventing virus and worm attacks becomes essential for compliance.

Encryption

Many regulations, such as HIPAA, explicitly call for the use of encryption to protect confidential data. Even when regulations do not mention encryption per se, most organizations will rely on encryption to comply with requirements for confidentiality.

Given the high volumes of email traffic to be encrypted and the large number of senders and recipients working with confidential data, the only effective encryption and decryption solution for an enterprise will rely on automation. Basic email services need to be augmented with encryption technology that automatically detects confidential data requiring protection, encrypts and decrypts confidential messages in real time, and manages cryptographic keys used by senders and recipients.

Enterprises should not try to impose unfamiliar or cumbersome encryption procedures on end users. Most business users have little understanding of encryption. Even if they do understand encryption, most users are reluctant to use special commands or unfamiliar email clients simply to comply with security guidelines. Consequently, encryption capabilities must be built into the enterprise email infrastructure itself, comprehensively protecting confidential messages while altering the end user's typical email experience as little as possible. The encryption solution must also be able to work with the hardware and software being used by partners, customers, and other likely email senders and recipients. The confidentiality of data cannot be compromised simply because senders and recipients are using different email products.

Enterprises need a streamlined, affordable system for deploying and managing cryptographic keys. Because an organization may have to furnish encrypted content to regulatory investigators, the IT organization must ensure that it can decrypt any encrypted message stored in the company's archives.

Hierarchical Archiving and Retrieval

Many laws and regulations, such as the United Kingdom's Data Protection Act and the NASD email regulations, require organizations to archive all email meeting certain requirements, such as email containing personal information or correspondence between a broker/dealer and a customer. These laws and regulations also require organizations to be able to retrieve specific email messages in a timely fashion.

The only way to comply with these requirements is for organizations to implement hierarchical storage systems, probably using a combination of disk storage and tape storage, that keep the messages most likely to be requested close at hand, and that ensure any collection of messages can be located and retrieved within a matter of days.

The type of email archiving systems now used by some financial services companies will need to be adopted by other types of companies in other industries.

Quarantining and Reviewing Messages

To ensure that personal data is not divulged or that suspicious messages that may contain malware are not automatically transmitted, email servers need to be able to quarantine messages for inspection.

Some regulations, such as NASD regulations for sales literature, require that message content be reviewed for compliance before being transmitted. To support this type of review, email systems must include features for automatically routing messages to the appropriate reviewers, ensuring that only authorized reviewers approve or deny the messages, and recording the approval or denial of the message for future audits.

These quarantine and review capabilities are well beyond the means of most corporate email servers today.

The Mirapoint Solution

Mirapoint, the leading secure messaging provider, offers messaging solutions that enable organizations of all sizes to meet the challenges of regulatory compliance. Mirapoint messaging appliances provide the secure, scalable messaging infrastructure organizations need in order to:

- Provide reliable, highly available messaging services that enforce the authentication and encryption controls required by regulations such as Sarbanes-Oxley and HIPAA
- Protect networks from viruses, spam, and other unauthorized traffic
- Provide the policy-based controls for blocking, redirecting, and archiving messages, based on regulatory requirements and internal guidelines.

The Mirapoint solution delivers:

- Proven five-nines reliability
- 60-80% threat block-rates at the SMTP layer reducing overall message traffic
- 98% spam catch-rates with virtually zero false positives
- Collaborative services including calendaring, group scheduling, address book and to-do list
- Integrated virus scanning technology
- Microsoft Outlook synchronization for a seamless end-user transition
- Secure, hardened, non-Windows operating system with no known exploits for extra protection against hackers
- Outbound content filtering for corporate policy enforcement

Unmatched Protection against Viruses and Spam

Eliminating viruses and spam is an important step in meeting regulatory compliance. Messaging filtering and archiving solutions become much more manageable and timely when they have to work with only traffic that is legitimate, instead of torrents of illegitimate traffic and legitimate traffic, as well.

Mirapoint's comprehensive approach to email security comprises best-of-breed virus scanning and multi-layered spam protection, including heuristic rules-based scanning with automatic updates, and controls for managing relay and blocked domains. Additional protection is provided through SMTP connection management features, plus support for RBLs and Vipul's Razor.

Mirapoint's RAPID™ Anti-Spam and RAPID Anti-Virus products offer near real-time protection against spam and virus attacks. By continuously monitoring a worldwide network of email probes, Mirapoint RAPID technology can identify spam and virus attacks as soon as they begin. As a result, Mirapoint appliances can typically begin protecting networks within an hour or two of the appearance of a new threat—giving organizations a 20-30 hour lead over the anti-virus and anti-spam defenses offered by other vendors.

Mirapoint's MailHurdle™ technology provides an industry-leading approach that blocks up to 80% of threats at the network edge before network bandwidth, storage, processor and administration resources are wasted. In combination with other email security technologies such as RAPID™ Anti-Spam and RAPID Anti-Virus, customers can achieve overall catch-rates upwards of 98% with virtually zero false-positives.

Secure, Encrypted Email from Desktop to Server

Mirapoint's RazorGate™ email security and policy management appliance, integrated with PGP Universal's automatic, network-based encryption, provides enterprise customers a full gateway email security solution offering encryption, digital signatures, anti-virus, anti-spam, and content filtering—all managed through a common security policy. The integrated Mirapoint/PGP solution helps enterprises comply with regulatory, partner, and customer security requirements as well as meet the organization's own objectives for security and protection of confidential data.

Key features and benefits of the Mirapoint/PGP solution include:

- **Comprehensive email security**—Mirapoint RazorGate integrates content filtering, spam detection, virus protection, encryption, decryption, digital signatures, and policy management.
- **Industry-leading encryption**—Mirapoint/PGP encryption is gateway-based, automatic, user-transparent, and non-disruptive to deploy. It supports all encryption standards and delivers email securely even if recipients have no encryption solution. Mirapoint/PGP encryption has keys and integrates with PGP Desktop, PGP Command Line, and S/MIME deployments.
- **Granular policy**—Mirapoint/PGP enforce security policies, including encryption, according to individual sender or recipient, groups, domains, specific content, or message format; policies can be applied to header, body, or attachment parameters.

- **Integrated management**—Mirapoint/PGP enables IT to create and manage a full range of email security solutions from a single console, reducing administrative burden, ensuring consistent policies, and streamlining change management.
- **Scalability**—Mirapoint/PGP supports encrypted email services for even the largest enterprises, Mirapoint appliances scale to handle millions of users.
- **Mail flow visibility** — Generate real-time and historical reports that show the effectiveness of email security efforts. Any message can be instantly tracked without parsing logs.

Rapid Deployment and Ease of Integration

Ease of installation and configuration is important for organizations who want to meet the challenges of regulatory compliance, without becoming burdened to complex, time-consuming IT initiatives. Mirapoint's appliance form factor enables enterprises of all sizes to deploy Mirapoint solutions and begin benefiting from Mirapoint's industry-leading messaging technology right away.

Organizations of all sizes can take advantage of the Mirapoint solution, without replacing or redesigning their current messaging infrastructures. Mirapoint appliances support standards such as IMAP4, POP, and LDAP, and work with any standard desktop, and provide Web and wireless access to email. The solution is designed to complement and extend existing messaging technology.

A Proven Track Record

Mirapoint appliances deliver secure messaging infrastructure for leading organizations in both the public and the private sectors, including the Bank of China, National Health Service (NHS), Research in Motion (RIM), British Telecom, the Illinois Department of Public Health, RSA Security, the University of Chicago, and the World Bank Group. Organizations can invest in a Mirapoint solution knowing that Mirapoint products are deployed in some of the largest, most demanding networks in the world today.

Regulations such as Sarbanes-Oxley and HIPAA can make organizations stronger by focusing attention on the processes and controls essential to their success. By helping organizations comply with the messaging requirements of these regulations, Mirapoint enables organizations to communicate more securely and effectively every day.

About Mirapoint

Mirapoint is the market leader in appliance-based solutions for secure message networks in enterprise, service provider, and education organizations, with more than 100 million mailboxes served and secured worldwide. Customers use Mirapoint appliances including the Message Server mail appliance and RazorGate mail security appliance to build the messaging infrastructure that intelligently serves, secures and manages email. Mirapoint is headquartered in Sunnyvale, Calif., with offices throughout North America, Europe and Asia.

Our mission at Mirapoint is simple. We make email work for our customers. For more information on how Mirapoint can help you, contact us today.

Mirapoint, Inc.
909 Hermosa Court,
Sunnyvale, CA 94085 USA
Tel: 800-937-8118
Tel: 408-720-3700
Fax: 408-720-3725
Email: info@mirapoint.com
www.mirapoint.com

For local and international office locations please visit www.mirapoint.com.

©2005 Mirapoint, Inc. All Rights Reserved. Mirapoint is a registered trademark and Mirapoint Message Server, RazorGate, Mirapoint Directory Server, RAPID and MailHurdle are trademarks of Mirapoint, Inc. All other trademarks are the property of their respective owners.