

### About Mirapoint

Founded in 1997, 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 the RazorGate mail security appliance to build the messaging infrastructure that intelligently serves, secures and manages email. Mirapoint is headquartered in Sunnyvale, California, with offices throughout North America, Europe and Asia. For more information on Mirapoint, visit its Website at [www.mirapoint.com](http://www.mirapoint.com).

**“Analysts at IDC say the factors contributing to the growth of email archiving include the growth in email and other electronic records, an increase in regulation and corporate governance and the need to respond to litigation and discovery requests.”**

IDC

# MEETING REGULATORY COMPLIANCE REQUIREMENTS WITH MIRAPOINT

MIRAPOINT DELIVERS PROVEN, APPLIANCE-BASED SOLUTIONS WITH CARRIER GRADE RELIABILITY TO BUILD A SECURE MESSAGING INFRASTRUCTURE WITH CENTRALIZED CONTROL AND SIMPLIFIED MANAGEMENT – ALL AT A DRAMATICALLY LOWER COST.



Mirapoint Inc.  
909 Hermosa Court  
Sunnyvale, CA 94085 USA  
Sales Phone: 1+ (800) 937-8118  
General Phone: 1+ (408) 720-3700  
General Fax: 1+ (408) 720-3725  
Email: [info@mirapoint.com](mailto:info@mirapoint.com)

Mirapoint Europe Ltd  
Mercury Business Park  
Wycombe Lane  
High Wycombe  
Buckinghamshire  
HP10 0HH  
United Kingdom  
Tel: +44-(0)16-2853-1121  
Fax: +44-(0)16-2853-5670  
Email: [dl-europe@mirapoint.com](mailto:dl-europe@mirapoint.com)



# BUILD SECURE MESSAGING INFRASTRUCTURE WITH MIRAPOINT.

## Increased Scrutiny of Email

With the rising popularity of email as a primary means of communication for business 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, they have become the focal point of regulatory oversight and a common form of evidence in litigation of all kinds.

A growing number of industry regulations and national laws explicitly or implicitly requires enterprises to better manage, secure, store and archive their email messages. Some of these regulations, such as Sarbanes-Oxley, apply to public companies in all industries and are even followed by many private companies looking to be acquired or file for an IPO. Other regulations, such as HIPAA, Basel II and FISMA apply to specific industries – in this case healthcare, banking and government, respectively.

## The Cost of Inaction

Neglecting to put in place technology to systemically archive messages so they may later be retrieved upon request, can be expensive. For example, in a 1995 anti-trust case, Ciba-Geigy, a chemical manufacturer 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 was forced to pay more than \$2

million to settle a sexual harassment claim based on sexually offensive emails that were circulated within the company's email infrastructure. Morgan Stanley paid a \$10 million dollar fine for failing to preserve email documents required for an SEC investigation.

*Gartner*

To avoid criminal penalties and civil liability, bad publicity, loss of reputation, 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 processes needed to address regulatory compliances through the implementation of best practices for secure email communications.

## Meeting Regulatory Requirements With Messaging Security and Controls

**Sarbanes-Oxley:** 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 veracity of their financial data and integrity of their accounting procedures. To comply with Sarbanes-Oxley, an organization's email system must authenticate senders of messages, 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 also be able to filter communications between the executive team and accountants and archive those communications for a future review of accounting practices.

**Gramm-Leach-Bliley:** Officially known as the Federal Modernization Act of 1999, Gramm-Leach-Bliley (commonly referred to as GLBA) regulates how financial institutions manage the private information of individuals. Two rules within Gramm-Leach-Bliley have special significance for email and email security.

*Mirapoint enables organizations of all sizes to meet the challenges of regulatory compliance.*

The Financial Privacy Rule treats the collection, use, and disclosure of Nonpublic Personal Information (NPI), and calls for institutions to provide opt-out mechanisms and privacy policies to customers. The Safeguards Rule states 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.

To comply with Gramm-Leach-Bliley companies should employ authentication and encryption functionality to protect NPI found in email. To support all of Gramm-Leach-Bliley's security mandates, a company will also likely require an email solution that provides policy-based filtering and blocking, logging, and reporting.

**Basel II:** 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 a 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.

**National Association of Securities Dealers (NASD):** An example of precise and stringent guidelines for email can be found in various NASD regulations. These regulations make fine distinctions between the content, senders, and recipients of email.

To comply with these NASD regulations, a financial services firm must have a messaging infrastructure that can: filter email messages, quarantine messages, ensure authorized message transmissions, archive messages and retrieve them in a timely manner.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA):** The part of HIPAA most relevant to email communications is the 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, authorization control, data authentication (ensuring data integrity), user authentication, optional use of data encryption and audit controls.

**The Federal Information Security Act of 2002 (FISMA):** Developed by the National Institute of Standards and Technology (NIST) in 2002, FISMA requires all federal agencies and their partners 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 effectively address email security including authentication, encryption, spam-filtering, and virus-filtering in order to comply with FISMA.

## Meet Regulatory Requirements with Mirapoint

While the foregoing laws and regulations vary in purpose and scope, they share common requirements for secure data transmission and storage, robust filtering, logging and reporting. 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.

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

Mirapoint, the leading secure messaging provider, offers messaging solutions that enable organizations of all sizes to meet the challenges of regulatory compliance. Mirapoint protects networks from viruses, spam, and other unauthorized traffic. Policy-based controls allow administrators to block, redirect, and archive messages, based on regulatory requirements and internal guidelines.

**"Criminal sanctions for knowingly misusing or disclosing of patient health information (PHI) carries fines of \$50,000 to \$250,000 and one to ten years imprisonment."**

*HIPAA Penalties*

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.

**"According to Gartner, more than 80 percent of high-cost security incidents occur when data from inside the organization gets out."**

