

Mirapoint Meets the Needs of the Government Agencies

Secure Messaging Simplified

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.

INDUSTRY BRIEF | GOVERNMENT

- Quickly and easily deploy reliable, scalable messaging appliances that enforce the authentication and encryption, per group and per user controls required by FISMA
- Fully integrated technology protects networks from viruses, spam and other unauthorized traffic
- Allow for complete policy-based control of access to the message network by employees, contractors and others, including all directory, storage and archiving systems
- Allow for the comprehensive logging, reporting and forensics examination needed for regulatory and policy auditing and event analysis

Government compliance requires integrated security throughout the network

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 heavily on email to support operations and assets, agencies must address email security throughout their message network – not just at the network perimeter - 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 throughout their message network, including authentication, encryption, spam-filtering, and virus-filtering.

Mirapoint's secure messaging infrastructure provides an integrated defense

Mirapoint, the leading secure messaging provider, offers messaging solutions that provide government agencies a secure, scalable messaging infrastructure to meet the challenges of regulatory compliance. With Mirapoint government agencies provide reliable, highly available messaging services that enforce the authentication and encryption controls required by the FISMA and NIST. Mirapoint also provides policy-based controls for blocking, redirecting and archiving messages, based on regulatory requirements and internal guidelines.

Mirapoint Meets the Needs of the Government Agencies

Secure Messaging Simplified

Mirapoint messaging appliances are the building blocks of an “always-on” messaging infrastructure that addresses security throughout the fabric of the network, not just at the network perimeter. A Mirapoint appliance-based infrastructure can easily scale to meet the growing needs of even the largest government agency while maintaining the lowest TCO in the messaging industry and providing a platform for the provisioning of new services. Mirapoint solutions are designed to meet the demands of government agencies by providing:

- Proven five-nines reliability (less than 6 minutes of downtime per year)
- SMTP-layer edge blocking reducing unwanted message traffic by 60-80%
- 98% spam catch-rates with virtually zero false positives
- Integrated zero hour virus scanning technology
- Outbound content filtering for global policy enforcement and regulatory compliance
- Encrypted transmission of messages from client to the mail server
- Secure, hardened, operating system with no known exploits for extra protection against hackers
- Sender authentication to assure messages from unauthorized sources never enter the network
- Standards-based architecture works with major email clients (Outlook, Eudora, Netscape, etc.), legacy email applications, directory servers and storage options
- Collaborative services including calendaring, group scheduling, address book and to-do-lists
- Microsoft Outlook synchronization for a seamless end-user transition

Integrated, Secure Messaging Appliances

Message Server. Mirapoint’s appliance-based Message Server provides 99.999% availability with exceptionally high performance. Users can access their email from any desktop via a secure, web-based interface, or via any standards-based email client including Outlook. In addition to its email functionality, the Message Server also provides easy-to-use collaboration tools, including group calendaring, scheduling and address book.

RazorGate. Mirapoint’s RazorGate appliance is an award-winning security appliance that incorporates everything you need to ensure the security of your email network. It blocks spam, protects against viruses, and filters content for both inbound and outbound messages. RazorGate is also a powerful router that can be used as a front end to integrate heterogeneous email systems.

Directory Server. The Mirapoint Directory Server appliance is the industry’s first high-performance appliance providing unified user and system management. With proven scalability to millions of entries, the Mirapoint Directory Server simplifies the creation, use and integration of LDAP directories as a common information database for all messaging and related applications. Like the RazorGate and Message Server appliances, the Directory Server is also fully compatible with other directory products, including Active Directory.

Mirapoint serves and secures over 100 million mailboxes worldwide. Here are a few successes in government:



For more information and to request a free 30-day evaluation, call us at (800) 937-8118 or email info@mirapoint.com.