

Email Encryption from the Desktop to the Server

Mirapoint and PGP Corporation

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.

SOLUTIONS BRIEF | EMAIL ENCRYPTION



- Integrated content filtering, spam detection, virus protection, encryption, decryption, and digital signatures
- Create and manage a full range of email security solutions from a single console, reducing administrative burden, ensuring consistent policies, and streamlining change management
- Enforce 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
- Generate real-time and historical reports that show the effectiveness of email security efforts. Any message can be instantly tracked without parsing logs
- Gateway-based, automatic, user-transparent encryption, that is non-disruptive to deploy

Mirapoint and PGP Corporation team up to offer secure, encrypted mail from desktop to server

PGP® Universal's fully automated network-based encryption for email, integrated with Mirapoint's Razorgate™ email security and policy management solution, provides enterprise customers a comprehensive gateway email security solution that provides 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.

Mail is mission critical and under attack

Email has become the key channel of business communication in a world that demands “always available” services with ever-reducing administrative complexity and cost. At the same time, IT groups are struggling to combat viruses, spam and phishing attacks, which threaten the productivity of this critical business tool. Unfortunately, addressing these threats has resulted in complex, fragmented, multi-vendor solutions that are frustrating to use and expensive to maintain. Government and industry regulations complicate matters even more with requirements to scan and secure confidential corporate email.

Enterprises need a centrally managed and secure messaging infrastructure that incorporates email security throughout the fabric of the network to meet today's needs for security, reliability and compliance while satisfying demands for lower complexity and cost.

Email Encryption from the Desktop to the Server

Mirapoint and PGP Corporation

Mirapoint and PGP Corporation offer an integrated solution to deliver mail securely

Mirapoint has partnered with PGP Corporation to offer enterprise customers a secure messaging infrastructure that features a comprehensive, integrated email security and policy-management solution to protect critical enterprise email and encrypt sensitive corporate data. A single management console enables the creation and maintenance of a unified security program that addresses encryption, authentication, anti-spam, anti-virus, and content filtering needs. Policies can be set based on attributes of a message, individual sender or recipient, groups, domains, content, attachments, or message format.

PGP Universal Server

PGP Universal automatically handles all encryption, decryption, and digital signatures for gateway and end-to-end email security.

- Inbound encrypted email is received by the Mirapoint RazorGate appliance, routed to PGP Universal for decryption, and passed back to the RazorGate for further scanning and security processes.
- Outbound mail is scanned by the Mirapoint RazorGate appliance; based on policy, confidential email is sent to PGP Universal for automatic key management, key lookup, encryption, and digital signing.
- Legitimate emails with content that in the past incorrectly triggered quarantine now can be encrypted and delivered without delay.
- Supports users of standard encryption products (OpenPGP and S/MIME), can send securely to recipients without keys, and provides two-way policy enforcement.
- Part of a suite of PGP products that includes security for email, disk, FTP/batch, and instant messaging (IM).

Mirapoint – Secure Messaging Infrastructure

Mirapoint appliances incorporate email security throughout the fabric of the network and are centrally managed to meet today's needs for security, reliability, and compliance.

- Distributed Management & Centralized Administration—Reduces ongoing operational cost of large, complex deployments
- Centralized Policy Management—Policy-based control that can extend across a heterogeneous, multi-vendor message network
- Integrated Email Security—Fully integrated inbound and outbound protection from spam, viruses, and malware

Configuration scenarios

The Mirapoint and PGP solution delivers a secure messaging infrastructure that have passed extensive compatibility testing.

Inbound message encryption

Encrypted inbound messages are received by the Mirapoint RazorGate and routed to the PGP Universal Server, where they are decrypted and authenticated. Messages then return to the RazorGate to be scanned with preventive and reactive measures, including sender reputation, virus outbreaks, spam blocking, virus detection, and content filtering for policy enforcement.

Outbound message encryption

Outbound mail is scanned by the Mirapoint RazorGate for spam, virus, and message content; based on policy, confidential email is identified and sent to PGP Universal for encryption and digital signatures. PGP Universal automatically performs all key management, key look-up, and message delivery to recipients without keys.