Mirapoint Anti-Spam

MIRAPOINT®

Deploy multi-layered protection at the network edge to block spam and unwanted email.

- Reverse DNS lookup, RBL support, UCE block lists and SMTP-based authentication
- Intelligent heuristic and lexical message analysis with automatic rule updates
- Domain-level black and white lists plus configurable actions for message handling
- Personal junk mail folder and end-user controls for black and white lists and content filters
- Integrated Vipul's Razor for spam detection with real-time signature updates
- Unified management with comprehensive reporting and graphs of junk mail activity

The Challenge

An ineffective spam solution threatens employee productivity, creates liability exposure, as well as jeopardizes email service reliability. The financial impact of spam is significant and according to Gartner Group costs the average American business with 10,000 employees about $16 million a year.

The Mirapoint Solution

Mirapoint delivers a powerful set of capabilities for addressing the growing problem of unsolicited email. By using Mirapoint's Full-Spectrum™ multi-layer approach to spam protection, Mirapoint is able to achieve the "industry's best accuracy with 96% catch-rate and zero false positives," according to independent analysis.

Features

Standard Spam Protection: Every Mirapoint appliance includes a basic level of spam protection including support for real-time blackhole lists (RBLs), domain name system (DNS) reverse lookup, closed relay protection and simple mail transfer protocol (SMTP)-based authentication. In order to better manage messaging traffic, Mirapoint systems limit the number of SMTP connections that can be made by remote hosts. Customers can also change the SMTP port number that is used by specific hosts for sending email through the Mirapoint system. To protect against denial-of-service (DOS) attacks, Mirapoint employs a back-off algorithm that manages SMTP connections to a specific IP address in the event abnormal activity is detected. These features drop many unwanted SMTP connections to offload system processing and stop spam before it enters your system.

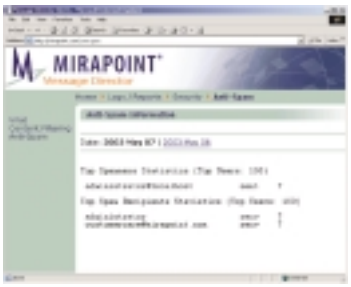
Intelligent Analysis: Mirapoint's advanced features to protect against spam include a junk mail scanner that evaluates incoming messages and applies a set of heuristic rules to the mail headers and body text to determine if it is potentially spam. Mirapoint's junk mail scanner awards points for each rule that is matched and adds a junk mail header to the message if the total number of points exceeds the specified threshold. Administrators have the ability to manually or automatically download new rules for the junk mail scanner from Mirapoint to ensure the latest protection against spam, as well as throttle the junk mail threshold value based on their environment. Messages marked as spam can be tagged in the header or subject line or can be deleted or rejected.

Black & White Lists: In addition to heuristic filters, Mirapoint spam protection includes support for domain-level black and white lists. Both black and white lists can be configured with ease through the existing Mirapoint administration interfaces. Black lists are useful for addressing mail abuse and preventing DOS attacks. White lists are important to reduce false positives and prevent company mail from being classified as junk mail.

End-User Controls: For users that have been granted access to Mirapoint spam protection through class-of service, they can enable junk mail filtering through the existing Mirapoint Webmail interface. End-users also have the ability to create personal black and white lists to block or approve email addresses or domains. An easy-add button is provided within the Mirapoint Webmail interface, so users can quickly add senders to their black or white list, as well as report spam traffic to Mirapoint in order to enhance the rule set.

Content Filtering: To complement the anti-spam protection, Mirapoint supports filtering of message content. Configurable at the domain-level or by the end-user, Mirapoint filtering allows actions to be taken based on content embedded in the body or header of a message. For example, content filtering could be used to automatically move messages with inappropriate language to the trash folder.

Mirapoint Anti-Spam Screen Shot



Class-of-Service Controls: Mirapoint provides class-of-service controls that define what services are offered to individual users or domains. The different class-of-service settings can be stored within the Mirapoint system or in the Lightweight Directory Access Protocol (LDAP). For Mirapoint spam protection, these controls define what messages get scanned for spam, as well as which end-users get access to the junk mail filter and personal white and black list features. Class-of-service also controls which administrators get access to domain-level white and black lists.

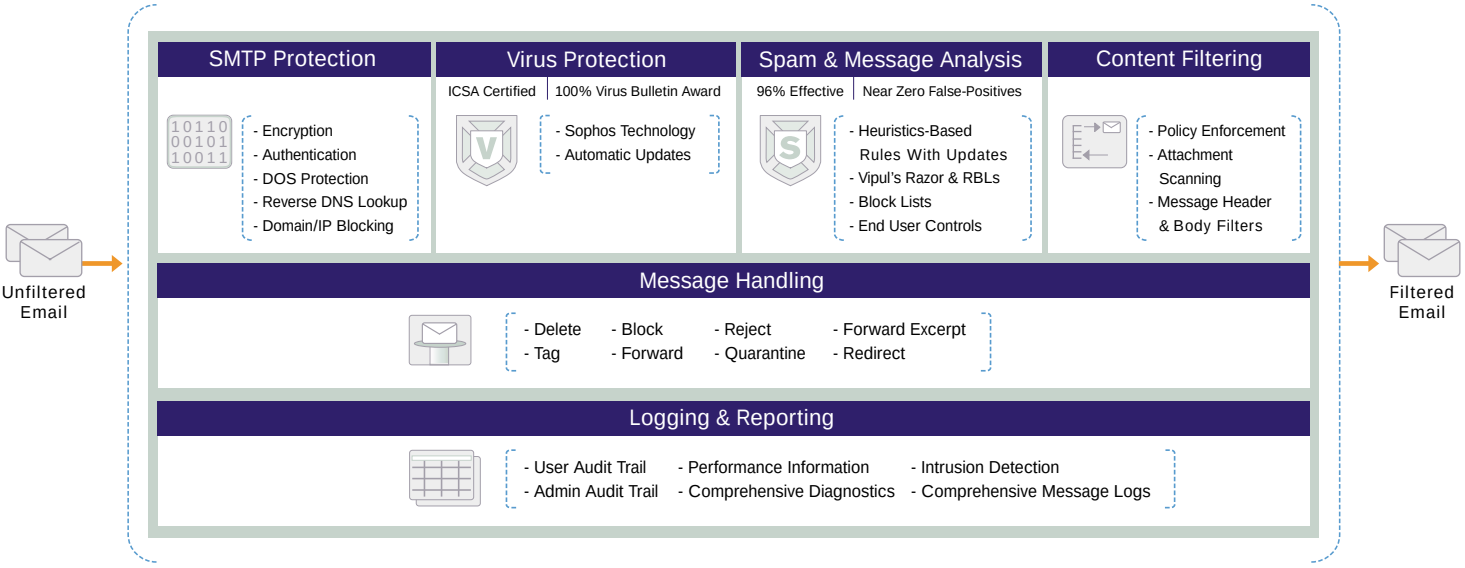
Vipul's Razor Support: Vipul's Razor is a distributed, collaborative, spam detection and filtering network. Through user contribution, Vipul's Razor establishes a distributed and constantly updating catalogue of spam in propagation that is consulted by email clients to filter out known spam. Detection is done with statistical and randomized signatures that efficiently spot mutating spam content. User input is validated through reputation assignments based on consensus on report and revoke assertions that in turn is used for computing confidence values associated with individual signatures.

Simplified Management: Compared with alternative solutions that require separate hardware and software investments, Mirapoint's approach dramatically reduces costs and simplifies deployment of anti-spam protection. Mirapoint spam protection can be deployed on the existing Mirapoint messaging platforms and managed through the same unified management tools used today for other email services. The anti-spam features are also incorporated in Mirapoint's unified logging model. Reporting graphs are provided through the Web-based management interface for viewing junk mail activity.

Flexible Deployment: Mirapoint spam protection is available on the Mirapoint Message Server, Message Director, and RazorGate appliances. For customers with an existing investment in Microsoft Exchange, Lotus Notes or any Internet standards-based server, the Mirapoint Message Director or RazorGate appliances can be deployed to front-end the existing mail system and provide a powerful perimeter layer of network security to block spam, as well as virus threats.

Complementary Virus Protection: In addition to defending against spam, the Mirapoint platform also includes robust protection against email borne viruses. Fully-integrated in the Mirapoint platform, the anti-virus capabilities can be deployed quickly and easily using the same administration interfaces used for the core messaging and anti-spam services. Like Mirapoint spam protection, the virus protection can be configured on a per user or domain basis to scan incoming or outgoing email traffic.

Mirapoint Email Security Diagram



MIRAPOINT®
909 Hermosa Court, Sunnyvale CA 94085
info@mirapoint.com