



## Mirapoint: Securing Message Networks



## Do You Have a Comprehensive Email Security Solution?

The right answer for organizations looking to secure and protect their message networks is an approach that addresses all incoming, outgoing and stationary risks—Mirapoint provides end-to-end email security.

### Threats are Everywhere

Widely recognized incoming message threats are spam, viruses, hackers, directory harvests, and password attacks. But damage can also come from outgoing messages. When email is abused inside a business to propagate pornography, distribute sensitive information, harassment, chain letters, or flame wars between employees, the company may be vulnerable to multi-million dollar lawsuits. Stationary threats can be equally devastating. New federal laws and regulations protecting national security, personal financial and medical information, require businesses to archive and protect a wide range of email communications and prevent information leaks or face dire consequences.

### Email: Vital—Yet Vulnerable

While most organizations understand that email is vital to their operations, many have neglected the fundamental need for securing their message networks—a potentially costly and destructive oversight:

- In January 2003, nearly 20,000 virus and hacker attacks caused \$8 billion in damage—equaling a yearly rate of more than 180,000 attacks and up to \$100 billion in damages. (mi2g Ltd)
- Ferris Research estimates that 15% to 20% of incoming email at U.S. corporations is spam; at that rate, Jupiter Research estimates that an employee will delete 2,600 pieces of spam in 2003 alone, costing organizations billions of dollars in lost productivity and computing resources.
- In January 2003, two employees of an IT outsourcing company filed a \$15 million dollar lawsuit against their employer and a client relating to pornography discovered on a client computer. (Information Week, May 12, 2003)
- Five security firms agreed to pay fines totaling \$8.25 million for failing to archive emails sought by regulators investigating analysts' conflicts of interest. (The Morning Call 2002)

## Yesterday's Solutions Don't Work Today

After years of installing firewalls, spam filters, and other point solutions, many companies are left with a cumbersome patchwork defense to guard against email threats. Now, with increasing messaging volume and complexity and the difficulty of managing all those disparate defenses, companies experience serious performance bottlenecks and gaping security holes in their networks, including vulnerabilities with outgoing message traffic and stationary content.

## The Safe and Secure Solution: Mirapoint's Security CONTINUUM™

With built-in flexibility, the Mirapoint Security CONTINUUM™ architecture provides a wide range of options to secure a Mirapoint or legacy infrastructure such as Microsoft® Exchange. Mirapoint builds highly secure appliances for the sole purpose of messaging, with tightly integrated hardware and software. By strategically placing Mirapoint messaging systems at the edge of your network, you can secure all incoming, outgoing and stationary messages 24/7/365.

**Hacker and Security Protection:** Mirapoint systems use a hardened OS with no known exploits. For added security protection, Mirapoint supports SSL and SSH-level encryption, Kerberos, trusted Internet Protocol (IP) address access and a dedicated administration network interface. Mirapoint systems can encrypt client access to an existing mail server using secure proxy technologies for Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and webmail.

**Virus Protection:** Mirapoint messaging solutions integrate industry-leading Sophos™ virus scanning technology to provide protection over incoming and outgoing message traffic. Mirapoint anti-virus can be rapidly updated to protect against new virus threats—and be deployed and managed through standard Mirapoint administration interfaces.

**Spam Protection:** To conserve system and network resources, Mirapoint systems include comprehensive features for blocking spam. They include support for Real-time Blackhole Lists (RBLs), Simple Mail Transfer Protocol (SMTP)-based authentication, and system-level filters for blocking messages based on sender, originating domain or IP address. Mirapoint also offers spam prevention through powerful heuristics-based spam recognition and tagging with automatic rule updates, as well as administrator-configurable white and black lists to define approved or blocked senders. Mirapoint is one of the only vendors to offer personalized features for spam management, including individual white and black lists and content filters, so that people can better manage their incoming email and define what is and is not spam.

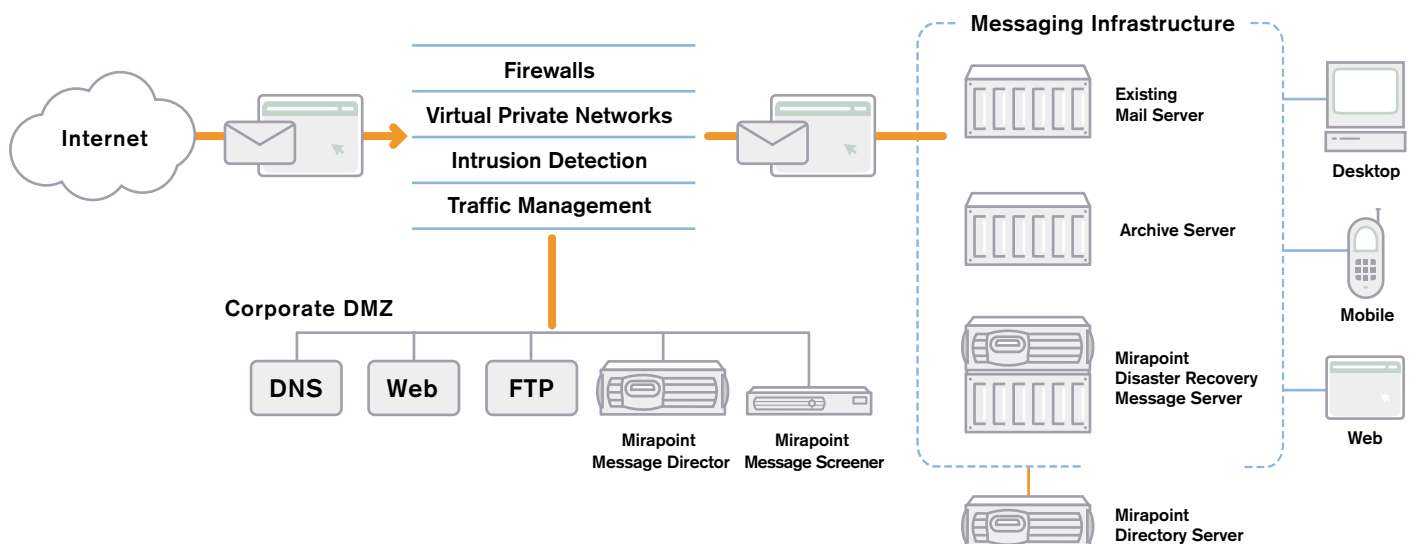
"The university used to receive 50,000 reports on viruses a day. By implementing Mirapoint's solution, that number has decreased by 97 percent."

>Virginia Tech

"With Mirapoint's Message Director, Centra Health now has an email security solution in place that addresses our needs for simplicity and reliability. This system also provides us with all the functionality we need today for spam and virus protection, and can serve as a platform to provide additional security protection in the future, as needed."

>Centra Health

## Mirapoint Security CONTINUUM™



### Mirapoint Facts:

- > Proven 99.999% Uptime
- > 24/7/365 Policy Enforcement
- > Hardened OS—No Known Exploits
- > ICSA Anti-Virus Certified
- > World-Class Performance



#### ELIMINATE INCOMING THREATS

Viruses	✓
Spam	✓
DOS Attacks	✓
Hacker Attacks	✓
Directory Harvests	✓
Password Attacks	✓
Open Relays	✓

#### PREVENT OUTGOING THREATS

Harassment	✓
Pornography	✓
Profanity	✓
Chain Letters	✓
Email Floods	✓
Flames	✓
Sensitive Information Leaks	✓

#### ADDRESS STATIONARY THREATS

Auto-Archive Confidential Information	✓
Quarantine Questionable Content	✓
Regulatory Requirements	✓
Manage Mail to/from Competitors	✓
Manage Mail to/from Any Individual	✓
Disaster Recovery	✓
Unified Logs and Reports	✓

“Mirapoint's approach, with its integrated hardware plus software systems purpose-built for messaging services, addresses key pain points including the need for greater efficiency, security, and consolidation to create a single structured message network that works across a variety of legacy operating environments.”

#### > IDC

“With Mirapoint solutions, we provide our financial customers with hosted disaster recovery services that provide rapid migration from Microsoft Exchange to the Mirapoint Message Server in the event of a disaster, plus integrated features for web and wireless access, as well as spam and virus protection.”

#### > Radianz

**Policy Management:** Mirapoint systems give administrators the flexibility to define and enforce a broad range of corporate policies governing incoming and outgoing email traffic. These policy enforcement tools help companies better manage employee email usage, prevent sensitive information leaks, and meet regulatory compliance requirements like Health Insurance Portability and Accountability Act (HIPAA), and Securities and Exchange Commission (SEC) rule seventeen, or Gramm-Leach-Bliley Act (GLBA), and protect against harassment and other types of email abuse.

**Message Archival:** Mirapoint systems can integrate with archival solutions for storing critical email communications that may be subject to regulation, review or auditing. These archival solutions complement existing Mirapoint messaging systems and provide advanced search, custom indexing, as well as security features to ensure the integrity of archived content. Deployed in conjunction with Mirapoint policy enforcement tools, companies can easily specify which incoming and outgoing messages are archived.

**Disaster Recovery:** Mirapoint systems provide a cost-effective, scalable solution for disaster recovery and business continuity. Regardless of the existing mail system, organizations can put Mirapoint systems in place for rapid migration and redeployment in the event of a disaster, so business-critical email communications are quickly restored.

#### Securing Your Message Networks

Enterprises, government agencies, educational institutions, and service providers everywhere are under increasing pressure to deliver email securely to ever-larger onsite and remote audiences. With incoming, outgoing, and stationary email threats potentially causing billions of dollars of damage every year, it is absolutely imperative to establish and maintain the most secure, scalable, and manageable message network possible. That's precisely what Mirapoint delivers. Where other messaging solutions are focused on part of the problem, Mirapoint is the only vendor that offers simple, secure, and service-oriented solutions to address the complete messaging lifecycle. For more information, visit [www.mirapoint.com](http://www.mirapoint.com). And put the power of Mirapoint email security solutions to work for you.