

Securing the Enterprise from Instant Messaging, Spyware and Peer-to-Peer Threats

Mirapoint and FaceTime

MIRAPOINT AND FACETIME DELIVER COMPREHENSIVE MESSAGING SECURITY TO PROVIDE ENTERPRISES WITH MANAGEMENT AND CONTROL OVER THE AUTHORIZED AND UNAUTHORIZED USAGE OF GREYNET APPLICATIONS ON THE CORPORATE NETWORK.

SOLUTIONS BRIEF | IM SOLUTIONS



FaceTime™

- Spyware Prevention – Stop spyware at the Internet gateway before it infects your network and puts corporate assets at risk
- Instant Messaging Security – Stop data leaks and preserve network integrity by securing the use of public IM against exploitation by hackers, spyware, worms and viruses
- P2P Control – Prevent unauthorized applications from hijacking legitimate protocols to serve as vectors for malware distribution
- Compliance – Log, archive and protect IM conversations and other shared content to meet compliance regulations
- Microsoft LCS Standardization – Enforce use of Microsoft LCS by blocking unauthorized public IM and P2P connections

Mirapoint and FaceTime team up to enable businesses to manage and control the threats caused by IM, Spyware, and P2P networks

FaceTime Communications is the leading provider of security solutions enabling businesses to secure and control greynet applications such as instant messaging, adware/spyware, webmail, P2P file sharing, web conferencing and instant voice. FaceTime's products allow IT professionals to take a comprehensive approach to securing and controlling greynet applications in their organization.

The growing threat of greynet applications

Enterprise IM (EIM) products, public IM (PIM) services, and industry-focused IM communities all provide the ability for employees to communicate with one another as well as with customers, partners, and others external to the corporate network, more quickly and efficiently than ever before. While businesses are adopting IM with increasing confidence, its growing use is causing compliance and technology management challenges for large organizations, especially those subject to government regulations.

Unfortunately for many organizations, the ease of obtaining and installing greynet applications – such as IM, spyware and peer-to-peer file sharing - has resulted in their rapid and disruptive adoption for both authorized and unauthorized purposes. Regardless of their origin, greynet applications pose a myriad of network and information security risks to an organization because they provide vectors for malware, client-side code vulnerabilities, intellectual property loss, and identity theft. While some greynets, especially IM, have legitimate business uses, others such as P2P file sharing, Skype™ and spyware can pose serious security risks to the organization. The ability to implement powerful controls to enable the productive use of greynets, while defending and preventing their malicious use, is a necessity for today's enterprises.

Fortunately, there is an answer for the problems posed by greynet applications. Mirapoint has partnered with FaceTime to enable companies to secure and control authorized and unauthorized greynet usage. By joining together, Mirapoint can offer greynet Defense in Depth — a comprehensive strategy for end-to-end security, compliance and management of greynets. Effective management of greynets helps to prevent spyware infection, block P2P, and manage the legitimate use of IM to:

- Protect technology and intellectual assets
- Comply with corporate and regulatory requirements
- Optimize business value from existing systems
- Increase employee productivity and lower costs

Securing the Enterprise from Instant Messaging, Spyware and Peer-to-Peer Threats

Mirapoint and FaceTime

Compliance

The increased use of workplace IM and P2P brings the risks and challenges of protecting company information. Policies regarding monitoring and protecting confidentiality that began as an industry best practice, are now legally mandated across many industries.

Challenges associated with information sharing occur throughout the enterprise, but effective IM management and P2P control pose a unique set—logging and archiving, unauthorized use, circumvention, and network security risk, are but a few of the issues. Mirapoint's partnership with FaceTime provides TrueCompliance™ solutions to address the most important compliance issues by providing:

- Authorized usage policies
- Monitoring and auditing of information sharing
- Message accuracy and authentication
- Ensuring confidentiality of data
- Restricted access to sensitive data
- Non-repudiation
- Tamper proof environments
- Secure logging
- Enforcement and validation of the audit trail
- Content scanning and keyword matching

Instant Messaging Security

Instant Messaging (IM) usage in business – both sanctioned and not – is growing rapidly. Unfortunately, desktop anti-spyware and anti-virus measures are insufficient to manage IM vulnerabilities, and can cause additional problems through false alarms, resource-intensive scanning, and incomplete cleansing.

Mirapoint has partnered with FaceTime to enable organizations to provide secure and controlled access to IM, in addition to comprehensive logging and reporting functionality to comply with government regulations and corporate policies. The products provided through Mirapoint's partnership with FaceTime provide certified support for the most popular public and enterprise IM protocols, and protects users from viruses, spIM, and other threats that travel over these networks.

Spyware Prevention

The applied Defense in Depth model pulls together strategies that effectively prevent spyware from invading corporate networks through an easy-to-manage approach that:

- Disables access to known spyware infection sites
- Prevents spyware installation
- Blocks downloads and installs of known spyware
- Detects and blocks “phone-home” activities of adware
- Targets remediation for infected PCs with no false alarms
- Prevents spyware on both managed and remote PCs
- “Freezes” existing spyware and prevents re-infection

P2P Control

The protocols used by peer-to-peer (P2P) applications are stealthy, often encrypting themselves or tunneling undetected through open ports. P2P networks can open up back doors into the network, allowing hackers direct access to corporate assets and enabling the unlawful exchange of protected material. Unfortunately, point products such as desktop anti-virus or anti-spyware solutions don't have the range of controls needed to enable the productive use of P2P while protecting against abuse. Through FaceTime, Mirapoint offers a broader and more comprehensive approach supporting the beneficial aspects of P2P without endangering network security.

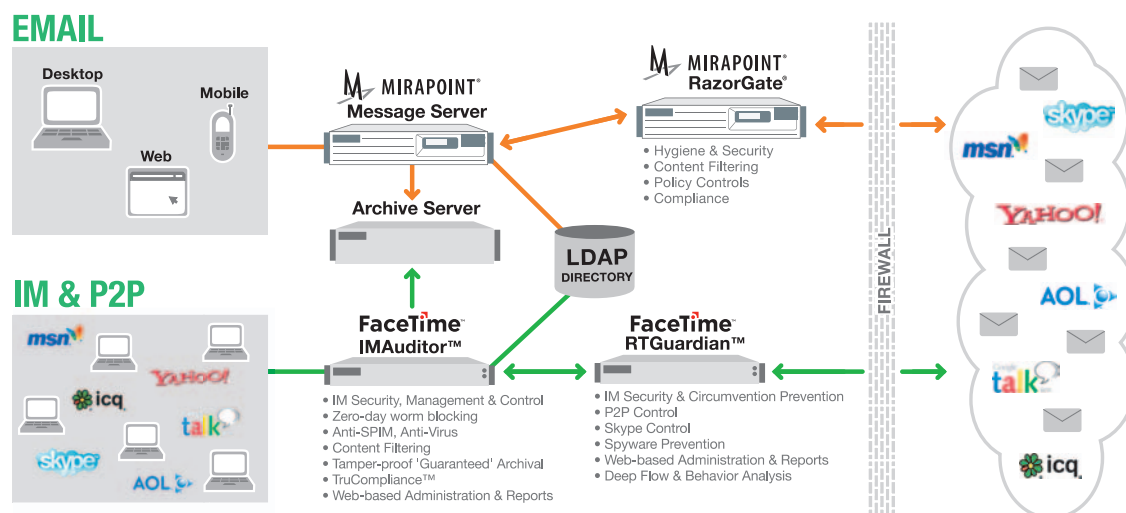


Figure 1 – Example topology of Mirapoint and FaceTime solution