



White Paper

Securing Greynets in the Enterprise:

Control Instant Messaging, Block Peer-to-Peer, and Prevent Spyware

Abstract

Fast, superior execution is a key driver for success in today's fast-paced economy. Real-time access to information, colleagues, customers, and partners creates business efficiencies and sets the real-time organization apart from the rest. Instant messaging, Web conferencing and other real-time communication and collaboration tools have become requirements for strategic and competitive advantage.

IM and Web conferencing programs, as well as their less-well-intentioned cousins P2P and spyware, are part of a category of applications that FaceTime terms 'greynets.' Greynets are network-enabled applications that are installed on an end user's system without the permission or knowledge of the IT department (and sometimes the user) and are largely invisible to the existing security infrastructure.

The productivity benefits reaped from the use of greynet applications have dramatically expanded the use of IM, peer to peer (P2P) file sharing and Voice over IP (VoIP) for many organizations. But because these tools tend to operate below the security radar, their widespread and uncontrolled use brings with it new risks for malware infection, loss of intellectual property, falling out of compliance with government regulations and more. While some greynets, such as IM and Web conferencing, have significant business value, others can pose serious security risks. However, all need to be controlled and managed according to policy set by the enterprise.

Managing the use of real-time communications in business is a major compliance and security concern for information security, human resources, and legal department personnel. Its prevalence and convenience as a business tool must be balanced by the requirement of certain regulations, such as SEC 17a-3 and 17a-4, NASD 3010/3110, HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, Regulation FD, FISMA, and the US PATRIOT Act, to enforce policies and retain reviewable customer records and transaction data. This covers all forms of electronic communications, including email, IM and other chat streams, Web conferencing and other electronic collaboration content.

This paper examines FaceTime's integrated approach to the management, control, and security of greynet applications, an approach which provides defense in depth while ensuring that business can continue to benefit from the advantages of real-time communications and abide by the requirements of information security and privacy legislation.

Content

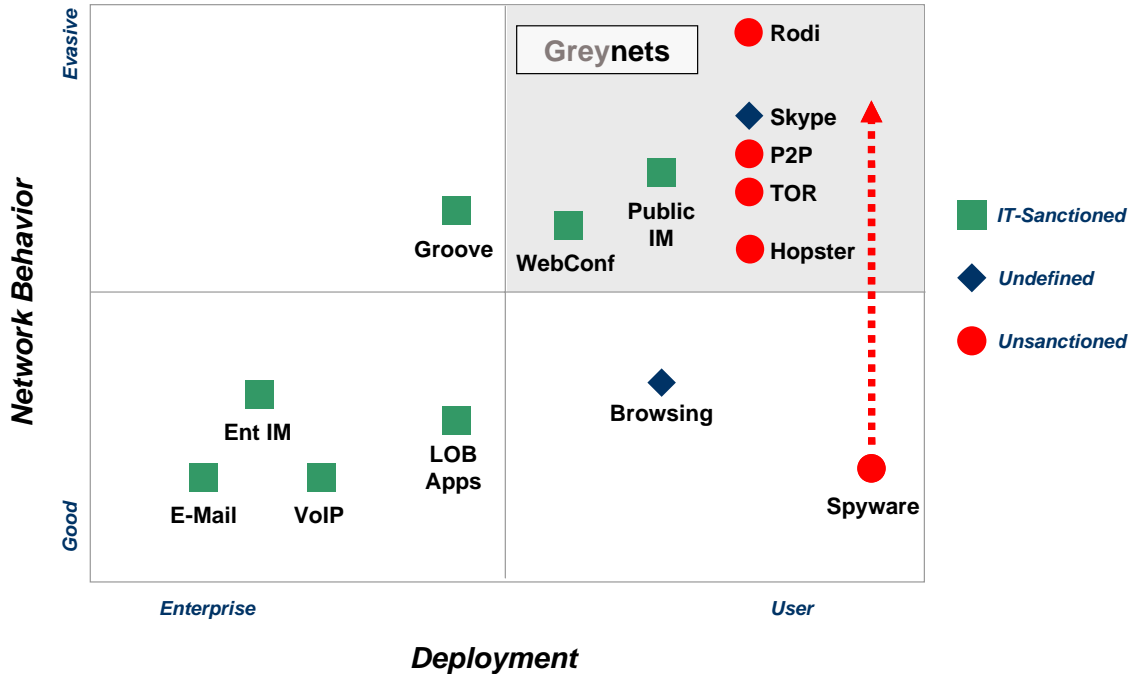
ABSTRACT	2
CONTENT	3
THE GREYNET THREAT	4
THE ORIGINS OF THE GREYNET	4
GREYNET USAGE TODAY.....	5
THE DEFENSE-IN-DEPTH APPROACH.....	6
THE LIMITATIONS OF FIREWALLS AND WEB PROXIES	7
BLOCKING IM.....	7
<i>Port Crawling</i>	7
<i>Changing IP Addresses</i>	7
<i>Constantly Evolving Proprietary Protocols</i>	7
<i>Application Intelligence</i>	8
<i>Complexity of Real-time Communications</i>	8
BEST PRACTICES MANAGEMENT FRAMEWORK FOR GREYNET APPLICATIONS	8
DEFINING THE FRAMEWORK FOR SECURING EMPLOYEE USE.....	8
THE IMPORTANCE OF ZERO-DAY PROTECTION	9
FACETIME ENTERPRISE EDITION.....	10
COMPREHENSIVE	10
RESEARCH-DRIVEN.....	10
IDENTITY-BASED MANAGEMENT & COMPLIANCE.....	10
SECURITY.....	10
PREMIER SUPPLIER.....	10
IMAUDITOR	11
RTGUARDIAN	11
THE IMPORTANCE OF DEFENSE-IN-DEPTH.....	12
COMPREHENSIVE SECURITY, MANAGEMENT AND COMPLIANCE	13
ZERO-DAY DEFENSE SYSTEM.....	13
INTEGRATED ANTI-VIRUS SCANNING	14
PATENT-PENDING ANTI-SPIM.....	14
CONCLUSION.....	15
MORE INFORMATION	15

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of FaceTime Communications, Inc.

©2006 FaceTime Communications, Inc. All rights reserved. FaceTime and the FaceTime logo are registered trademarks of FaceTime Communications Inc. FaceTime Enterprise Edition, FaceTime IMAuditor, FaceTime Real-Time Guardian, RTG and RTMonitor are trademarks of FaceTime Communications Inc. All other trademarks are the property of their respective owners.

The Greynet Threat

FaceTime considers IM, P2P, and spyware part of a large, fast-growing set of unsanctioned applications called “greynets.” Greynet applications are downloaded and installed on end user systems, without expressed permission from, or awareness by IT (and often without even the end user’s awareness - as with spyware) and then use evasive encryption and port agility techniques to traverse the network. Greynet applications include instant messaging, P2P file sharing, web conferencing, SKYPE, web mail and adware/spyware and anonymizers.



Managing the use of greynet applications in business is a major compliance and security concern for information security, human resources, and legal department personnel. Its prevalence and convenience as a business tool must be balanced by the requirement of certain regulations, such as SEC 17a-3 and 17a-4, NASD 3010/3110, HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, Regulation FD, FISMA, and the US PATRIOT Act, to enforce policies and retain reviewable customer records and transaction data. This covers all forms of electronic communications, including email, IM and other chat streams, Web conferencing and other electronic collaboration content.

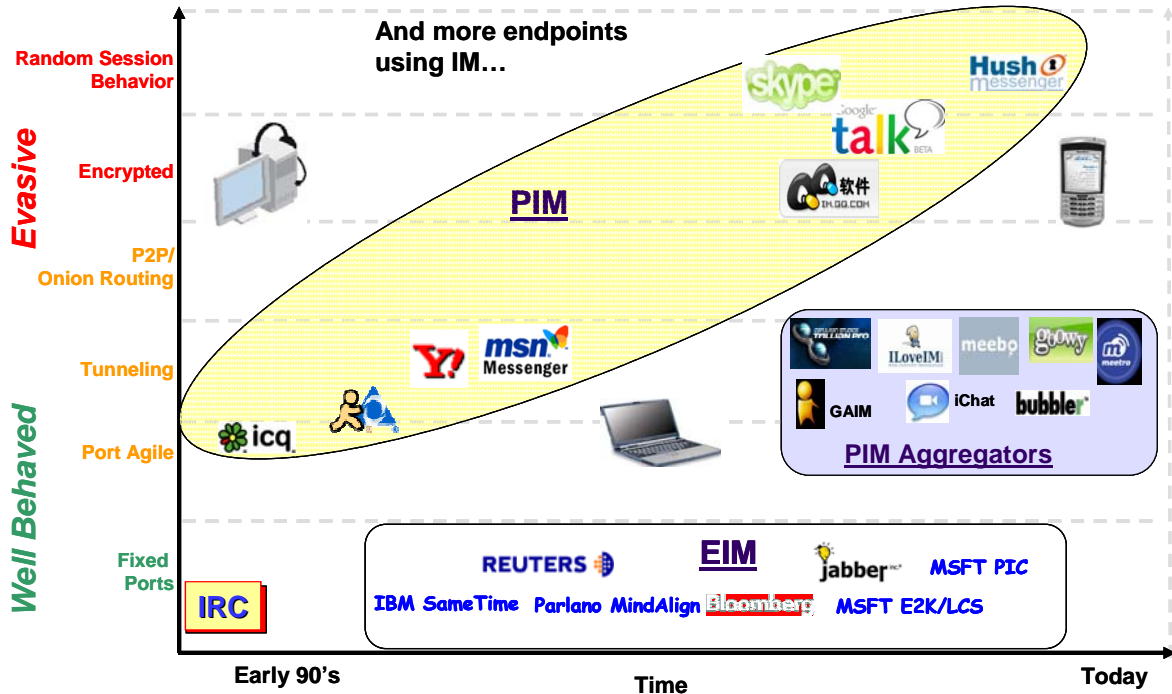
The Origins of the Greynet

Greynets are not new. Back in the early days of the Internet, Internet Relay Chat (IRC) grew from the bulletin board culture to become a widely used communication protocol in the technical community. Even then, there was concern about the IRC channel being hijacked by virus writers as a more ‘efficient’ distribution mechanism than floppy disks.

However, widespread Internet access quickly accustomed users to immediacy, and real-time communications protocols proliferated over the ensuing decade. Instant messaging in particular moved quickly from being a personal communications tool to a valuable business tool – so much so that email is sometimes regarded as being as slow and outdated as postal mail. Once its value as a

business tool became clear, the adoption rate skyrocketed. According to IDC, more than 28 million business users today use IM to send nearly 1 billion messages each day at work, making it the fastest-growing communication system ever.

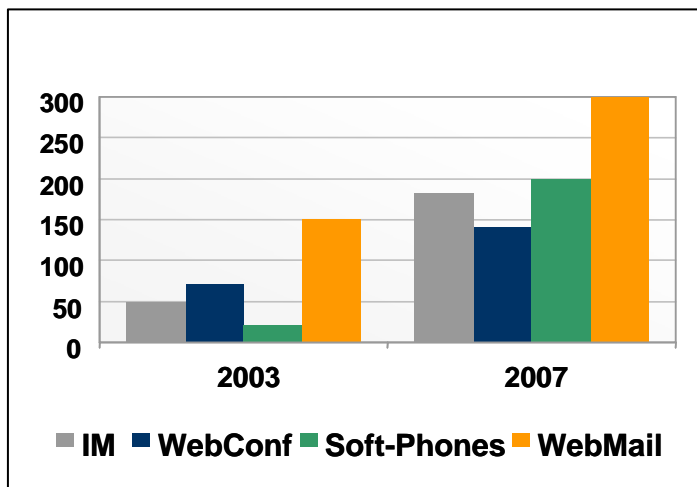
The chart below illustrates the progression from IRC to today's everyday real-time greynet communication tools over a period of less than fifteen years.



Greynet Usage Today

FaceTime Communications and market research company NewDiligence conducted a survey over a three-month period in 2005, compiling data from 622 IT managers and 564 end users across small, medium and large businesses to learn about the corporate use of Greynets and the impact of spyware and virus incidents within organizations. Key findings can be found below.

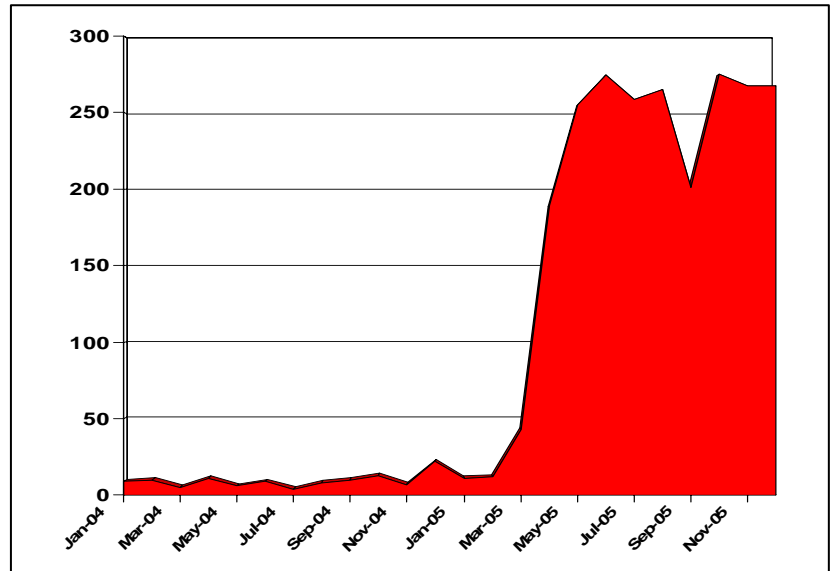
- Companies are spending on average \$130,000 every month in IT time fighting spyware problems.
- End users believe they have the right to install greynet applications and that IT has taken care of whatever security precautions.
- 87% of the same end users reported a spyware or virus problem resulting in slow Internet response times, pop up ads and corrupted files.



- Among IT managers who have rolled out perimeter security (gateway anti-virus, URL filtering and IDS/IDP) 77% have had either a virus or spyware incident in the past six months.
- Within the next 6 months, almost all end users expect to have deployed some type of greynet application, and 8 in 10 end users currently use at least one such application.
- 3 in 10 IT managers who experienced a virus or spyware incident reported that IM had been associated with such occurrences.

FaceTime Security Labs, the greynets research arm of FaceTime Communications, recorded several disturbing trends in greynet-related security incidents for calendar year 2005 when compared to similar data collected during 2004.

- Security incidents involving the use of chat, IM, and P2P up 2200% in 2005 over 2004
- Incident frequency has increased more than 1300% between the first and last quarters of 2005
- By Q4 2005 it was 19 times more likely that individual viruses and other security breaches would make use of two or more



- distribution channels than in the first quarter of 2005
- While the MSN network continued to show the largest number of incidents in 2005, year-on-year growth rates were highest for AOL Instant Messenger (AIM)

Clearly, the threat from uncontrolled greynet applications is real, growing – and largely invisible to traditional security defenses.

The Defense-In-Depth Approach

Greynet applications create and leverage a social network unlike any other category of application in the enterprise, presenting new channels for security threat propagation. The pattern of use and behavior is significantly different than other forms of communication due to the synchronous and real-time exchange of signaling events and data.

Defense-in-Depth is a practical strategy for addressing these threats and behavioral differences to ensure network and information security in today's highly networked environments. FaceTime's approach to Defense-in-Depth for greynets addresses the multiple layers in the network infrastructure which are at risk from use of these real-time communications technologies.

FaceTime Enterprise Edition enables Defense-in-Depth by creating a framework for authorized access to services outside the perimeter, coupled with a mechanism for detecting and preventing rogue or unauthorized access. The result is comprehensive protection without compromise on cost, performance or operational considerations.

By implementing FaceTime Enterprise Edition, enterprises are able to create an environment in which the use of greynet applications can benefit the business without endangering it, enabling legitimate use while preventing unwanted use.

FaceTime Enterprise Edition provides organizations with all the tools required to safely and knowledgeably use real-time communications tools within regulatory compliance requirements:

- Security:** Block worms, protect intellectual property, stop SpIM, prevent spyware
- Management:** Gain complete visibility over all forms of greynet communications and control their use through the application of powerful, granular policies
- Compliance:** Log, audit and archive all message and chat traffic

The Limitations of Firewalls and Web Proxies

Blocking IM

The first response of most companies is to try and block all IM either implicitly by just issuing a notice to employees warning against use or explicitly by using current infrastructure such as firewalls and web filtering proxies.

Unfortunately, the time is long past when employees can be dissuaded from using IM; such an approach will lead only to dissatisfaction among employees and less-efficient communications networks. Besides which, any attempt to explicitly block IM using firewalls and web filtering proxies is manual, laborious, error-prone, and does not guarantee a solution.

Port Crawling

Even though IM and P2P applications typically have a well-publicized port to use, e.g. 5190 for AIM, 1863 for MSN, 5050 for Yahoo, 1214 for Kazaa, it is not as straightforward to block these applications at the firewall. That is because all these applications have the capability to exploit any open port on the firewall, frequently tunneling out through ports primarily designated or intended for use by other applications, such as port 80 (primarily used for HTTP), port 25 (primarily used for email), port 23 (primarily used for telnet) and port 21 (primarily used for ftp). When these applications exchange content directly with each other in peer modes, they negotiate ports randomly. This is commonly known as port-crawling behavior and is highly undesirable.

Changing IP Addresses

Every IM network provider has its own unique set of IP addresses to which clients can connect. These IP addresses change frequently or at random without notice. Firewalls and proxies apply blocking policies on the notion of a "black list" of IP addresses. The steps to block access at the firewall to every single IP address out of hundreds of potential IP addresses are manual, laborious and error-prone, not to mention the fact that the firewall or proxy has to be touched and kept updated on a more frequent basis, which is also highly undesirable.

Constantly Evolving Proprietary Protocols

The rate of innovation for greynet applications far exceeds the rate of innovation in firewalls and proxy infrastructure. The protocols are proprietary and evolve constantly to deliver newer and advanced features to the IM community. Firewall and proxy vendors do not typically have the necessary relationships with IM providers to support the protocols, and most IT organizations prefer not to constantly update the firewall with protocol signatures.

Application Intelligence

Some firewall and proxy vendors claim to support IM and P2P protocols, but as the number and complexity of protocols increases, the firewall/proxy has to do more processing per packet resulting in potentially slowing down the network. Also, the synchronous nature of real-time connections is much different from the asynchronous web browsing and email traffic; standard firewalls and proxies were not designed to inspect and analyze real-time communication traffic.

A standard firewall or proxy only offers a very cursory level of control and inspection of IM traffic. There is no ability to understand application behavior and context by understanding the proprietary application protocol. As a result, it is generally not possible to distinguish between authorized and unauthorized real-time connections. Where firewalls do have application level capabilities, they have a sufficiently serious impact on performance that IT staff are forced to make a trade-off between security and performance.

Complexity of Real-time Communications

As real-time communications expands to Voice over IP (VoIP), the situation becomes even trickier. VoIP sessions use H.323 or Session Initiation Protocol (SIP). H.323 and SIP have separate connections for call control and actual media exchange. Call setup typically happens on one IP port, and then a random high-numbered port, usually above 1024, is selected for the media portion of the call. It is simply not possible to configure firewalls with some ports open and some closed to support these protocols because it is not possible to predict which ports may be requested for the connection.

Best Practices Management Framework for Greynet Applications

Rather than choosing to block all greynet communications channels, FaceTime advocates a more pragmatic approach of managing and securing its use within the organization. This requires an understanding of not only how the applications themselves behave, but how users behave when they interact with real-time communications tools.

Defining the Framework for Securing Employee Use

Probably the biggest problem for IT staff in gaining control of greynet application use is finding out who's using which under-the-radar applications – and the fact that most users of public IM services use personal nicknames or buddy names rather than a name that would be recognized through standard enterprise directory tools only worsens the problem. Knowledge is power, and once IT knows what's being used, they are in a far better position to manage it.

Requirements for securing user behavior require an understanding of:

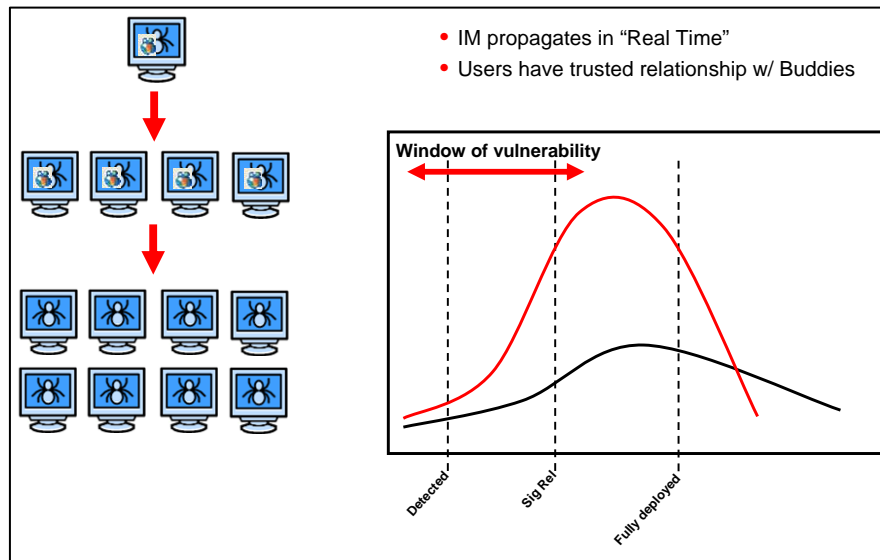
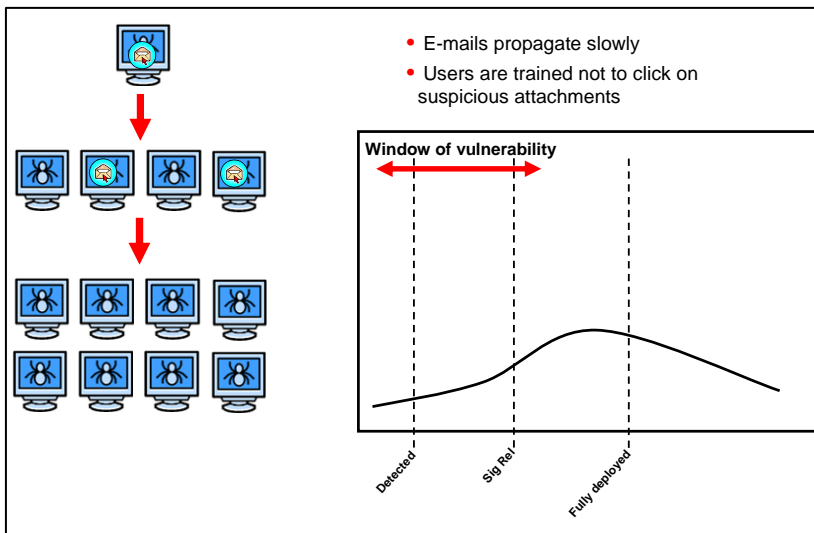
- Who is using greynet applications?
- Which public IM, P2P, and web conferencing services are being accessed?
- What 'buddy names' do employees use while representing the company over IM?
- How can sensitive information be prevented from being disclosed over these channels?
- Does the content of a message violate security policy or compliance requirements?
- How can messaging traffic be archived for regulatory record-keeping?
- Can users be subject to policies selectively based on which group or business unit they belong to?

- Are users being targeted and solicited by SpIM?
- Are users being asked to click on malicious URLs or accept virus-infected files?

A user policy framework that addresses these requirements is best implemented by a dedicated IM proxy solution that provides native connection management for the respective proprietary protocols.

The Importance of Zero-Day Protection

A new IM threat has the greatest propensity to spread and infect organizations immediately after it is released by its creator. IM threats are extremely challenging for IT because they are using the greynet's real-time communications channels, as well as proven social engineering techniques, to propagate significantly faster than email-based attacks. Enterprises forced to wait hours or even days for their security vendor to create, test and distribute an updated signature file are left defenseless for a significant period of time. Effective Zero-Day protection must incorporate behavioral attributes such as message frequency, content matching, and URL identification in addition to the traditional signatures in order to stop these 'real-time' infections before they can impact the network.



FaceTime Enterprise Edition

FaceTime Enterprise Edition provides the most mature and wide-ranging security and compliance management solution for greynet applications available today.

Comprehensive

FaceTime Enterprise Edition supports the widest range of IM applications – public and enterprise instant messaging, community networks such as Reuters and Bloomberg, and the likely next focus for malware distributors – peer to peer VoIP applications such as Skype. Additionally, support is included for emerging greynet applications - web conferencing, less-constructive P2P networks, and spyware. The two-tier, best practices architecture delivers a proven solution that is scalable to large enterprise deployment, incorporates deep integration with Microsoft's Live Communications Server (LCS) and robust directory support with dynamic groups for managing the largest deployments.

Research-Driven

Operating behind the scenes, FaceTime Security Labs is the industry's largest research team dedicated to the collection, analysis, and handling of greynet applications. With facilities on three continents, FaceTime Security Labs employs dozens of dedicated researchers and supports a global network of honeypots as well as a community of more than two million individuals who contribute their own experiences to the research effort. The labs are sponsored by industry leaders including Symantec, McAfee, Sophos, Microsoft, Yahoo, VeriSign, and Webroot. FaceTime Security Labs discovered four of the top ten spyware threats of 2005, including the AOL Rootkit over IM threat.

Identity-based Management & Compliance

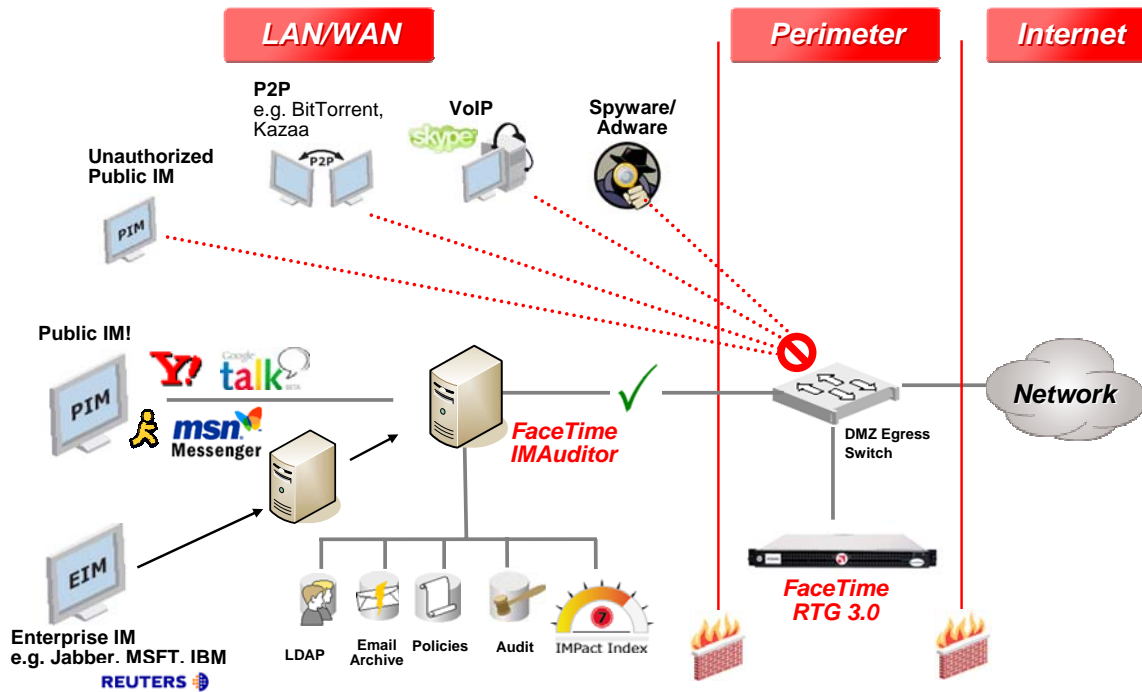
FaceTime Enterprise Edition is the only provider of TrueCompliance™ solutions, offering full compliance with federal regulations through user and group level policy based access control and management, monitoring and auditing of information sharing, and message accuracy and authentication to ensure confidentiality of data. Restricted access to sensitive data, non-repudiation, tamper-proof environments, secure logging, enforcement and validation of the audit trail, and extensive scanning and keyword matching reinforce information integrity. Seamless integration with all major corporate directories, email and WORM storage systems ensures maximum use of existing infrastructure.

Security

FaceTime Enterprise Edition is backed by the industry's only worm-free guarantee, delivering comprehensive malware protection against worms, viruses, spyware, SpIM and other inbound threats, using both behavioral and signature-based models to provide protection in the crucial Zero-Day vulnerability gap before other vendors can update their signature-only defense systems. Support is provided for virus scanning using existing anti-virus tools, and patent-pending anti-SpIM keeps IM networks free of bandwidth-hogging spam. Intelligent, granular content filtering and archiving/logging of all electronic conversations ensures an audit trail for information leak prevention.

Premier Supplier

FaceTime solutions are deployed in eight of the largest ten banks in North America, and the company offers the only certified scalable enterprise IM solution that supports deployments in excess of 100,000 seats. FaceTime Enterprise Edition is ranked #1 for IM Security by SC Magazine, and IDC has made the company its #1 vendor of IM security solutions for two consecutive years.



FaceTime Enterprise Edition Topology Overview

FaceTime Enterprise Edition is comprised of two major components: FaceTime IMAuditor™ to secure and manage IM use, and Real Time Guardian (RTG) to enforce IM standardization and block spyware and peer-to-peer networking.

IMAuditor

The award-winning IMAuditor™ is a scalable, enterprise-class application for the management and control of IM in the enterprise. Addressing the needs of businesses that must adhere to stringent corporate and regulatory compliance regulations, IMAuditor contains specific features needed to meet compliance requirements for electronic messaging. Deployed behind the firewall, IMAuditor supports all major public and enterprise IM clients, WebEx web conferencing, and leading financial services-specific IM systems such as Reuters and Bloomberg, providing a single enterprise-wide IM management solution.

IMAuditor also maintains an integrated trust relationship with RTG for complete end-to-end security, management and compliance of IM in the enterprise.

RTGuardian

The industry's first multi-channel anti-spyware perimeter security solution, RTGuardian™ (RTG) is the most advanced perimeter security solution for blocking the spread of spyware and adware in the enterprise and securing unauthorized IM and P2P usage.

RTG delivers gateway-based spyware detection and prevention to protect corporate networks against security threats to the network on any communications channel.

Detection

- Monitors all possible protocols – HTTP, IM, P2P, and more – so no transmission channels can leak data without the corporation’s knowledge
- Blocks attempts by spyware to ‘phone home’ with unauthorized data, thus preserving the integrity of corporate electronic assets
- Delivers targeted remediation of infected PCs by identifying both machine and spyware application, avoiding the possibility of false alarms

Prevention

- Blocks user access to known spyware sites, preventing accidental infections
- Stops “drive-by” installations of spyware applications through unauthorized P2P and IM communications
- Prevents unintentional downloads of spyware hidden within or co-opted by a seemingly helpful application using a combination of identifying factors, not just a single signature.

The Importance of Defense-in-Depth

Any attempts, internal or external, to circumvent the framework and establish IM and P2P connections leads to policies being ineffective and creates a heightened sense of risk. Hence, it is important to distinguish between authorized and unauthorized connections at the network perimeter and make sure that only authorized connection requests are allowed to be established.

A two-pronged, layered, Defense-in-Depth approach is essential to effective management and security of all IM and P2P communications. Only FaceTime delivers this unique capability through an integrated trust relationship between IMAuditor and RTG.

As shown in the topology schematic in the previous section, the FaceTime "Defense-in-Depth" approach employs IMAuditor for IM user policy management on the internal network, with RTG at the network perimeter to manage application behavior through deep inspection of network traffic for protocol analysis that distinguishes between authorized and unauthorized use. Through a built-in protocol handshake, RTG can automatically detect connection requests coming from IMAuditor deployed anywhere within the company network, as well as rogue connection requests. Any IM traffic that does not flow through IMAuditor is blocked by RTG to ensure all IM usage adheres to set policies.

This helps preserve the integrity of the rich user policy management and security framework that is defined by using IMAuditor.

Comprehensive Security, Management and Compliance

By bringing together two award-winning products and integrating them seamlessly into existing enterprise infrastructure, FaceTime Enterprise Edition delivers the industry's leading solution to the problems of security, management and compliance of greynet applications.

IMAuditor to secure and manage IM use

- Content filtering and worm protection
- Anti-virus and anti-SpIM
- Collects, parses, and logs all messages
- Universal IM policy and configuration engine
- Statistics and reporting

RTGuardian to enforce IM standardization and block P2P and spyware

- Purpose-built, hardened network device with deep packet inspection
- Detect and block all non-sanctioned IM and P2P (including Skype)
- Shut down file transfer and other features
- Detect and block spyware

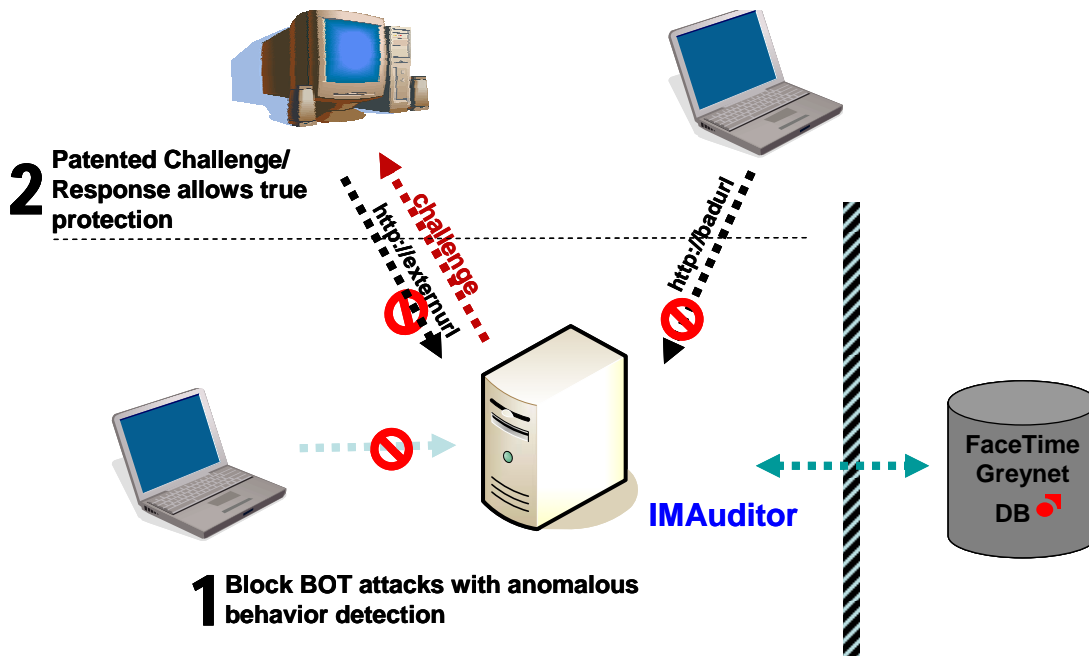
Flexible and manageable

- Multiple deployment modes - software or appliance

Zero-Day Defense System

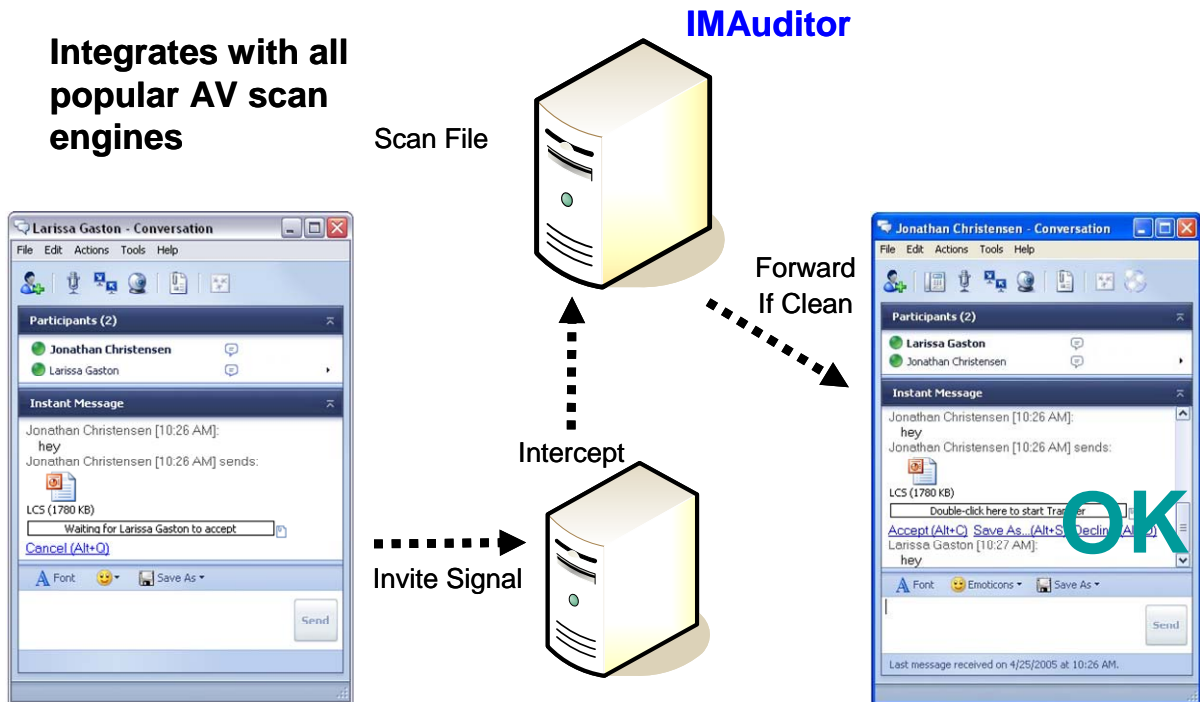
While email-borne malware propagates slowly and users are trained not to click on suspicious attachments, IM-borne malware propagates in real time and users have trusted relationships with their real-time buddies, exacerbating both the danger of the threat and the risk of it propagating.

Importance of Zero-Day Worm Protection



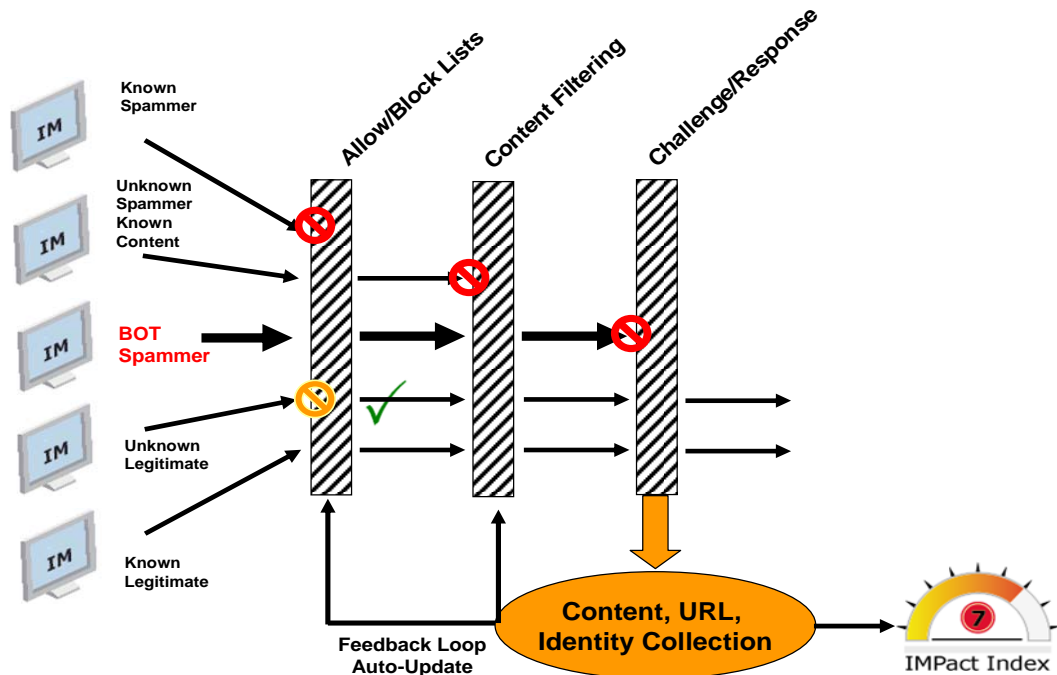
Integrated Anti-Virus Scanning

FaceTime Enterprise Edition integrates directly with all major corporate anti-virus scan engines for seamless incorporation of protection against specific viruses and worms.



Patent-Pending Anti-SpIM

Protect bandwidth and keep communications humming by stopping spammers from infiltrating the IM network.



Conclusion

Instant messaging (IM), Web conferencing and other real-time communication and collaboration tools have become requirements for strategic and competitive advantage in today's real-time enterprises. The productivity benefits reaped from the use of these tools have dramatically expanded the use of IM, peer to peer (P2P) file sharing and Voice over IP (VoIP) for many organizations.

IM and Web conferencing programs, as well as their less-well-intentioned, cousins P2P and spyware, are part of a category of applications that FaceTime terms 'greynets.' Greynets are network-enabled applications that are installed on an end user's system without the permission or knowledge of the IT department (or frequently the user) and are largely invisible to the existing security infrastructure.

Because greynet applications tend to operate below the security radar, their widespread and uncontrolled use brings with it new risks for malware infection, loss of intellectual property, falling out of compliance with government regulations and more. While some greynets, such as IM and Web conferencing, have significant business value, others can pose serious security risks. However, all need to be controlled and managed according to policy set by the enterprise.

FaceTime Enterprise Edition is used by the world's largest firms to secure and manage real-time communications tools, including public and enterprise IM and Web conferencing. It ensures safe, productive use of these applications and compliance with corporate policy and government regulations. It complements collaborative messaging solutions by enabling organizations to benefit from real-time communication tools without the risk of falling out of compliance with regulations.

Used by 11 of the top 15 US banks and 17 of 24 top FIMA banks, FaceTime Enterprise Edition incorporates the award-winning IMAuditor and RTGuardian applications. FaceTime Enterprise Edition was awarded Best Buy in SC Magazine September 2005 issue and in February 2006 received the SC Magazine 2006 Reader Trust Award for Best IM Security.

More Information

For more information about FaceTime Communications and FaceTime solutions please visit <http://www.facetime.com>. You can also contact us by phone at (650) 574-1600 and by email at info@facetime.com.

FaceTime Communications
159 Triton Drive
Foster City, CA 94404
USA
888-349-3223 (FACE) toll-free
650-574-1600 phone
650-574-2700 fax
info@facetime.com