

Ensuring Security and Compliance in an IBM Lotus Sametime Environment

FaceTime Communications, Inc.

Table of Contents

Executive Summary	3
Real-time Communications are Key to Today's Enterprise	4
From Employee-Initiated Tool to IT-Driven Productivity Application	4
Real-time Communications in Today's Workplace	5
EIM and Regulatory Compliance	6
Financial Services	7
Healthcare	7
Corporate Governance	8
E-discovery	8
Gramm-Leach-Bliley Act (GLBA)	8
Sarbanes-Oxley Act	8
EIM Security Challenges	9
Typical IBM Lotus Sametime Implementations	9
Internal use only	9
Federation	9
Public IM connections	10
Meeting the Challenge of IM Security and Compliance	11
FaceTime Enterprise Edition for Sametime	12
Security and Standardization	13
Management and Control	13
Compliance Auditing and Supervisory Review	14
Enterprise-Grade Solution	15
Summary	16
About FaceTime Communications	17
More Information	17

This white paper is for informational purposes only. FaceTime makes no warranties, express or implied, in this document.

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. © 2001 - 2006 FaceTime Communications, Inc. All rights reserved. FaceTime and the FaceTime logo are registered trademarks of FaceTime Communications Inc. FaceTime IMAuditor, RTGuardian, Greynet Enterprise Manager, GEM, RTG and Enterprise Edition are trademarks of FaceTime Communications Inc. All other trademarks are the property of their respective owners.

Executive Summary

IBM Lotus Sametime provides a real-time communications platform for corporate collaborations such as instant messaging, presence, application sharing, online meetings, voice and video. The obvious productivity benefits of Sametime have dramatically expanded the use of IM, peer to peer (P2P) file sharing and voice over IP (VoIP) applications in the enterprise, to the extent that industry analysts expect Enterprise IM (EIM) products, including IBM Lotus Sametime, to reach 100% adoption by 2010, with Public IM (PIM) clients, such as MSN, Yahoo!, GoogleTalk and AOL reaching market saturation even sooner.

However, the increased use of real-time communications in the enterprise today is challenging existing security, network, legal, and compliance policies and infrastructures. The traditional enterprise Internet security infrastructure – designed for well-behaved applications that use standard ports and protocols - is not equipped to manage the new generation of threats that use port hopping, tunneling and masquerading techniques. Enterprise implementations of Sametime are not immune to these new threats and should be appropriately secured, particularly in a federated environment. In organizations where regulatory compliance is required, the effective management of real-time communications should be a vital component of any enterprise security and communications strategy.

In addition to technical security issues, organizations also face operational risks from the disclosure of intellectual property, confidential information leaks, and copyright infringement from illegal file sharing – as hackers turn their attention from the now-well protected email and web channels to the more vulnerable real-time channels. Increasingly, industry watchdog organizations are targeting corporations for illegal file swapping and copyright infringement and the economic impact, as well as the public relations fall-out, can be significant.

Email is ubiquitous today, and users have long since become accustomed to using corporate email resources in a way that's both appropriate to business and compliant with the relevant legislative requirements. The same, however, is not true of IM and other real-time communications. The adoption of IM, be it enterprise or public, as an acceptable business communications medium, needs to mirror the security and usage policies applied to email to ensure uniform behavior and compliance across all communications channels.

This paper provides an overview of security issues related to the use of real-time communications and their impact on corporate, operational and regulatory requirements. It investigates the methods available to avoid the circumvention of Sametime usage and also reviews the desired functionality attributes of a third-party solution - long since acceptable in an enterprise email environment. Finally, we introduce FaceTime Enterprise Edition, which, when used as a complementary addition to Sametime, assists in securing real time communications channels and ensures that the appropriate management, security and compliance requirements are met.

Real-time Communications are Key to Today's Enterprise

Successful business has always been about time-sensitivity and speed in communications. Getting the right information to the right people at the right time to enable them to make the right decisions in a timely fashion is a critical component of effective business leadership. Innovations in computing and communication technologies have been largely responsible for doing business faster and better.

It is this need for speed that is the primary motivator behind the widespread adoption of Instant Messaging (IM) and other real-time communications tools in business – regardless of whether such adoption has been sanctioned by IT. Business users are undertaking virtual conferences, collaborating on projects and documents, augmenting phone conversations, and exchanging documents. Real-time communications build community and collaboration among different corporate locations, remote employees, telecommuters, supply chains, partners, and customers. They're delivering cost savings, lower telecommunication bills, greater accuracy in written transactions, and increased efficiency through rapid decision-making.

IBM Lotus Sametime provides a real-time communications platform for corporate collaborations such as instant messaging, presence, application sharing, online meetings, voice and video. However, while Sametime has emerged as a leading Enterprise IM (EIM) solution, the continued use of public IM networks such as Yahoo and MSN, along with Skype VoIP and other peer-to-peer channels, collectively known as greynets, means that IT is obliged to consider how best to manage and secure these protocols as well as Sametime itself, both for the purposes of security and of legislative compliance with regard to data protection.

These greynets provide potential vectors for malware, client-side code vulnerabilities, intellectual property loss, and identify theft, challenging existing security, policies and infrastructures. The ability to implement powerful granular controls to enable the legitimate use of greynets while defending against and preventing their malicious use is a key requirement for today's enterprises.

Sametime itself, while an enterprise-grade platform for real-time communications, is not immune to these new threats and compliance requirements and should be appropriately secured, particularly when implemented in a federated environment. Additionally, in highly regulated industries where compliance is crucial, the effective management of real-time communications in the enterprise is a legal requirement.

From Employee-Initiated Tool to IT-Driven Productivity Application

Despite valiant attempts to standardize collaboration efforts on Sametime, IT departments continue to be faced with the challenge of employees using consumer IM clients such as AIM, MSN, GoogleTalk, and Yahoo! as well as peer-to-peer file sharing and voice-over-IP applications like Skype. Increasingly bringing their personal communications into the

workplace, employees register themselves on these free services without IT authorization, download and install the applications without IT sanction and embark on a communications spree with no planned security or systems management. This not only presents significant risks, but frequently circumvents the security, management and compliance controls in place for approved network communications traffic.

IT needs to know who's using these tools, what information is being transmitted over real-time communications channels - and what potentially damaging malware might be coming in. The characteristics that make public IM applications so attractive – their ubiquity and ability to work wherever you are, be it behind a firewall, at the airport, at a coffee shop, and so forth - is exactly what renders them threats to corporate security. These applications will do anything to connect; if their destination host's port is blocked at the firewall, they will try tunneling through the Web, telnet or FTP ports, in order to find a way to connect. This evasive behavior is no match for legacy Internet security infrastructure that assumes only port and protocol conformant traffic is entering the company's network via the public Internet.

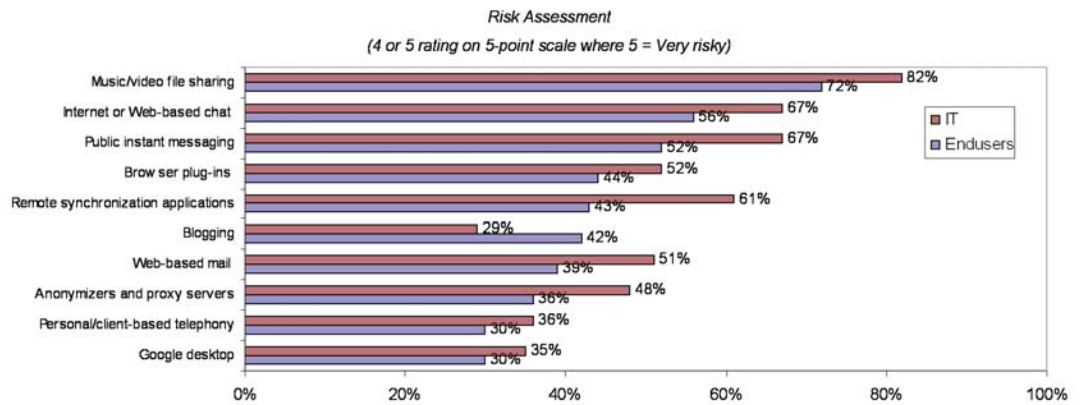
EIMs themselves are increasingly falling victim to new variants of traditional malware, with blended threats hopping from PIM network to EIM network – exposure that is increased by federation with public IM networks and partners. The continuing proliferation of PIM clients on endpoints increases risks and lowers productivity, as well as reducing the return on investment of the EIM network itself. Additional security requirements engendered by federation's heterogeneity and the new modalities in EIM and unified communications and collaboration (UCC) platforms create further complexities. All of which is amplified by an increasingly distributed and mobile workforce.

Compliance with data protection legislation is also a major concern in the form of information leakage potential, as well as the ability of organizations to react swiftly and appropriately to requests for information or transaction records. Compliance regulations largely apply in the same way to IM conversations and chat threads as they do to email records, so Sametime administrators need to be able to “connect the dots” for all types of electronic communications under the same umbrella, particularly when the installation spans multiple sites. Mobile users and telecommuters – as they do in many situations – create their own special set of problems simply by being out of the direct physical control of IT

Real-time Communications in Today's Workplace

Every year, FaceTime conducts a survey in conjunction with New Diligence Market Research to monitor the role and impact of greynet applications on business. The most recent study, completed in October 2006, confirms that employees continue to download and use unsanctioned applications – primarily in pursuit of greater business efficiency - while IT managers continue to voice concern over the potential for these applications to introduce significant security risks.

The chart below clearly indicates the difference in attitudes to risk and the use of greynet application between employees and IT.



Source: FaceTime Communications/New Diligence Greynet Market Survey October 2006

Survey responses from users indicated that they are clearly aware they may be “getting away” with certain behaviors by using instant messaging that would not be permitted under corporate email policies. More than 25% of employees admitted to using IM in order to have “private, unmonitored communications,” and if they were aware that their IM communications were being monitored, almost half (45 percent) acknowledged that they would pay more attention to company guidelines. Seventy percent of end users have sent personal IMs from work, and one in four employees admitted to sending information about company plans, finances or password/login credentials over public IM networks.

Over 80% of IT managers surveyed reported greynet-related attacks within the last six months; the most common attacks continue to be from spyware and adware (75%), viruses and worms (57%), other malware (22%) and rootkits and keyloggers (also 22%).

Such attacks also continue to have a significant effect on the bottom line, with a typical organization spending an average of \$130,000 annually to repair damage from such attacks. Larger enterprises are spending significantly more – upwards of \$350,000 per year, largely due to higher incidence rates from the more widespread use of real-time communications.

EIM and Regulatory Compliance

A key driver in adopting Enterprise Instant Messaging systems such as Sametime is the need to meet compliance requirements, which now embrace all forms of electronic communication – IM, chat threads, even Q&A sessions in online conferences – not just email. Any one of these channels, particularly in an unmanaged environment like public IM, could be causing the enterprise to be in breach of any number of regulations without anyone knowing – until audit trails are required or an eDiscovery request is received. This section of the white paper summarizes some current pertinent US (and some internationally applicable) regulations and where they intersect with real-time communications use; similar legislation exists in most countries with a mature financial and healthcare infrastructure.

Figure 1: The impact of greynets in regulated industries

Banking	Invest. Banking	Broker/ Dealer	Insurance	Life Sciences/ Pharma	Health Care	Energy	Gov.
FDIC Guidance	SEC 204-2, 31 a/b	SEC Rule 17a-4	FDIC, State, SEC 17a-4	21 CFR 11	HIPAA Privacy Regs	FERC Record-keeping	DoD 5015.2, FOIA, GRS 20, NARA
Gramm Leach Bliley	Basel II	NASD Rule 3010		HIPAA			
Public Company, Sarbanes-Oxley							
IRS record keeping requirements							
General Privacy Laws							
Litigation (Corporate Records Discovery)							

Financial Services

The Securities and Exchange Commission (SEC) closely regulates the financial services industry in the US and, in particular, the broker-dealer segment; similar regulatory environments exist in most other nations with a mature financial infrastructure.

Rules, such as SEC 17a-3 and 17a-4, define these regulations. The debate about IM in the financial services industry is related to the books and records requirements of the Securities Exchange Act of 1934 (the "Exchange Act"). IM is a book and record under Exchange Act Rules 17a-3 and 17a-4 if it is a communication related to a broker dealer's "business as such." FaceTime Communications provides hundreds of firms with compliance solutions to preserve IM pursuant to the requirements of the rules of the Exchange Act.

Healthcare

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted on August 21, 1996 to reform the insurance market and simplify health care administrative processes. Security standards for all health plans, clearing houses, and providers proscribe all stages of transmission and storage of health care information to ensure integrity and confidentiality of the records at all phases of the process (before, during, and after electronic transmission). An example of a privacy violation or security breach is any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

The HIPAA rules state that the implementation of privacy and security compliance will reduce the potential overall cost of risk to a greater extent than additional controls will increase costs. Put another way, the potential cost of not reasonably addressing privacy and security risks could substantially exceed the costs of compliance.

Corporate Governance

E-discovery

The Federal Rules of Civil Procedure (FRCP), and in particular the newly amended Rule 26, which govern the production of evidence in most federal court cases, make the efficient management of corporate electronic records (eRecords) more vitally important than ever. Failure to comply with the new electronic discovery (eDiscovery) rules can mean fines, sanctions, executive liability, a drop in stock price, and other risks.

Specific impacts of key FRCP amendments on the availability and accuracy of electronic records include:

- Rule 26(a), which explicitly defines electronically stored information (ESI) as discoverable
- Rule 26(b)(5), which addresses the inadvertent production of privileged information during eDiscovery

For further information on eDiscovery and real-time communications, please consult the FaceTime Communications white paper *The Impact of the New FRCP Amendments on Your Business* by Michael Osterman, available for download at http://www.facetime.com/forms/wp_request.aspx?tyid=OstermanED

Gramm-Leach-Bliley Act (GLBA)

The GLBA data protection provisions require the Regulators (Banking, Insurance, FTC and SEC) to establish appropriate standards for safeguarding financial institutions' customer records and information. GLBA affects a broad range of organizations including banks, insurance companies, securities firms, tax preparers, mortgage brokers and lenders, real estate agents and appraisers, financial planners, and credit card companies. GLBA compliance is mandatory. Companies that do not meet these new information security requirements are subject to enforcement and liability exposure. Consequences for failing to comply include enforcement actions with fines up to \$1,000,000 and other penalties.

Sarbanes-Oxley Act

Sarbanes-Oxley Act (SOX) mandates timely and transparent financial disclosures and that CEOs of public companies certify or “sign off” on their results. SOX mandates that all public companies must demonstrate that they have established, implemented, and evaluated both “disclosure” and internal controls for purposes of certifying reports filed with the SEC and meeting the requirements of SOX. These disclosure and internal controls must satisfy a range of audit tests to provide reasonable assurance that they are operating effectively.

EIM Security Challenges

In order to pinpoint the specific security challenges posed by EIM deployments such as IBM Lotus Sametime, the following sections describe typical implementations. In each case, potentially significant risks to both information security and compliance can be observed, at least in part because users expect to interact with real-time communications networks in the exact same way they interact with email networks.

Typical IBM Lotus Sametime implementations

Internal use only

When Sametime is implemented as an internal-only solution, the goal is usually to improve internal communications and speed up multi-tasking. While this may seem the most secure implementation with the least risk to business, it is highly unlikely that there will be no connection to the Internet or other networks on any machines connected in this fashion. Recent studies by FaceTime Security Labs have shown a predilection of malware authors to create worms that, although designed for public instant messaging networks, have the ability to hop between public and enterprise IM networks, recognizing implementations of Sametime and propagating malware out to an entire organization's networks with a single real-time hop.

Federation

Federation delivers the ability for users on one IM network or one company EIM network to communicate over IM with contacts on a different IM or EIM network in a separate enterprise. This arrangement does not require users to establish separate credentials on each system with which they want to communicate.

In a federated environment, organizations are opening up part of their network to their supply chain in the same way as they did in the 1990's with extranet access, a semi-trusted relationship between two organizations. While providing the potential for significant competitive advantage through presence-based technology, there are downsides.

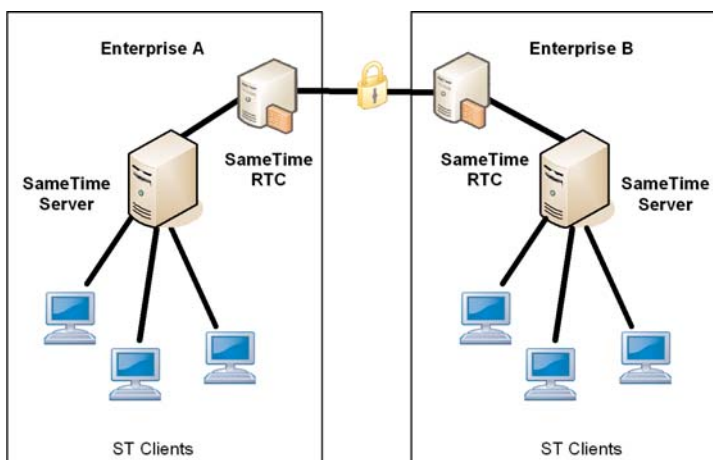
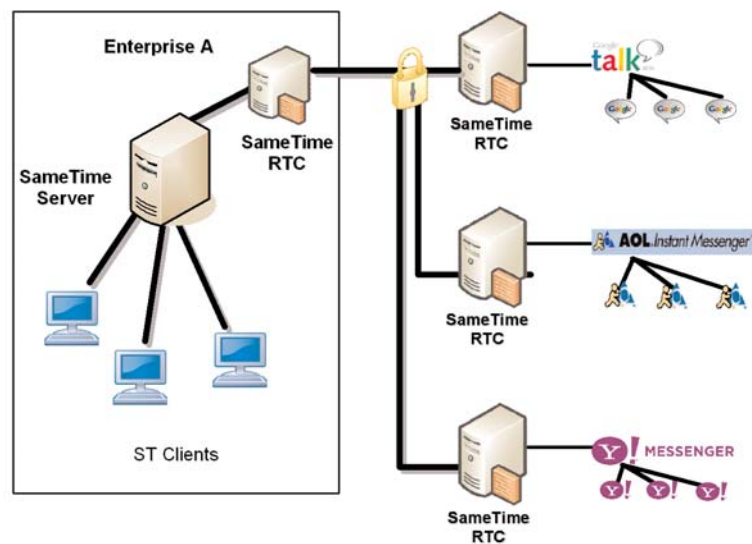


Figure 2: Federation between Sametime deployments

Opening a federated connection with what is in essence an untrusted party (unless you have full control of the security policies, procedures and tools of the organization with which you are federating) is analogous to implementing a new email server while turning off the anti-virus, anti-spam and anti-spyware tools. Quite simply, you wouldn't do it

Public IM connections

In the same way that a federated connection opens up the EIM network to uncontrolled third parties, opening up a public IM connection in a Sametime environment (Figure 3) renders the organization vulnerable to every threat and piece of malware intended for the public IM network with which the organization now has a connection.



In every scenario, the risks are clearly evident. Organizations are exposed to inbound threats, information leakage and compliance risks throughout their real-time communications environments – even those designed for the enterprise, such as Sametime – that they would never consider taking with an email network. Organizations therefore need to ensure that they have policies and tools in place to mitigate the risk involved in opening these new and largely unprotected channels of communication, channels that are increasingly targeted by worms, malware and spyware, as they continue their search for vulnerable systems.

Figure 3: Sametime Federation with Public IM Networks

Meeting the Challenge of IM Security and Compliance

IBM Lotus Sametime provides a solid enterprise communications foundation for the collaborative environment. However, significant operational benefits accrue from the addition of a security layer specifically tailored for the real-time communications environment.

Such functionality should include:

- Redirecting user attempts to communicate over public IM networks to the appropriate secured Sametime channel
- Protection from malware (zero day worms, rootkits, spyware, etc.) propagating over the real-time channels
- Automating virus-scanning of file transfers over IM using existing anti-virus installations
- Providing real-time content filtering with advanced pattern matching, blocking and scanning to prevent information leakage
- Automatic signature and protocol updates to protect against zero-day threats

For compliance purposes, further benefit can be gained from the incorporation of:

- Real-time group-level ethical boundaries (“Chinese Walls”)
- Multi-party chat capture
- Flexible file transfer capture and archival
- Clearly-visible disclaimers
- Single step guaranteed strict recording of communication threads into an SQL database
- Guaranteed strict archiving into email/WORM storage
- Message anti-tampering check sums (non-repudiation)
- Rich reporting, workflow and audit reports

In order to assure smooth integration and operation of any third-party solution alongside Sametime, it's important that the user experience is also integrated – for example, by ensuring that the same window is used to deliver all user-facing messages and other information. Not only does this minimize unnecessary helpdesk calls but it also ensures that user-facing messages required by policies or compliance legislation are always delivered. All disclaimers and policy messages sent to users are logged.

FaceTime Enterprise Edition for Sametime

FaceTime Enterprise Edition for Sametime (FTEE for Sametime) provides organizations with the tools to standardize their IM infrastructure on Sametime, while securing their environment against IM-borne threats such as malware (viruses, worms, Trojans, spyware, rootkits, etc.) and spam over IM (spIM).

FTEE is used by the world's largest organizations to manage and secure IM, P2P, Skype, web conferencing and other greynet applications. It provides user policy management, message hygiene, zero day worm protection, comprehensive compliance, and protection against user circumvention. It also detects and prevents spyware and other malware infections at the Internet gateway – before it impacts the business. Enterprise Edition combines FaceTime's IMAuditor™ in the LAN with Real-Time Guardian™ at the gateway for a complete, end-to-end security, management, and compliance solution. It supports all public and enterprise IM applications.

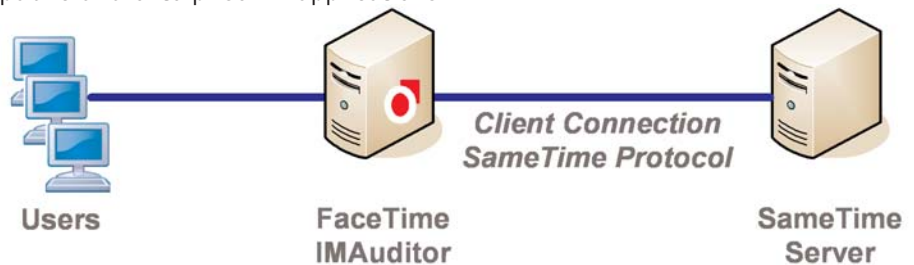


Figure 4: FTEE for Sametime uses simple fault-tolerant architecture

FaceTime IMAuditor secures and manages all Sametime and other allowed IM traffic. IMAuditor, which resides on the LAN, maintains an integrated trust relationship with FaceTime's perimeter product, Real-Time Guardian (RTGuardian), which blocks all IM traffic not specifically allowed and protects against circumvention of policies.

Regardless of complexity or the number of individual clients involved, all real-time communications are accurately and completely logged, including file transfers and event notation such as message blocking. IMAuditor stores the actual file transferred in the database, simplifying the review process and ensuring that all communications are seen in the context of a complete conversation, with accurate message order preserved.

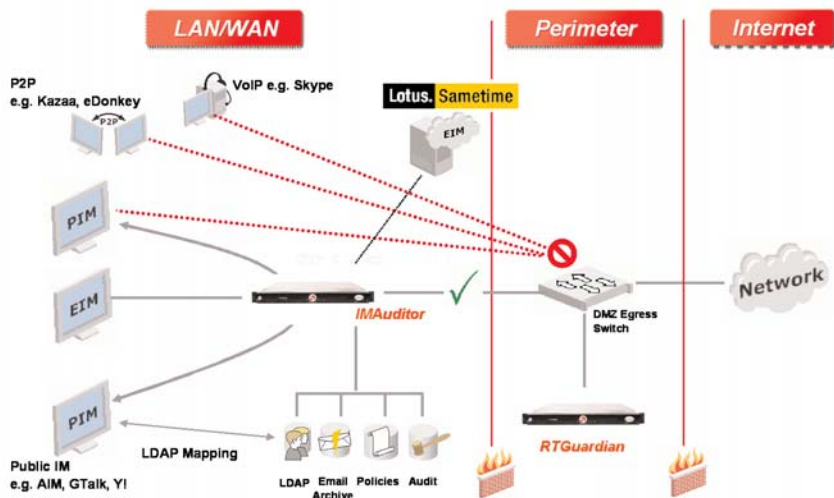


Figure 5: FTEE for Sametime Deployment Technology

Security and Standardization

FaceTime Enterprise Edition for Sametime enforces standardization on the Sametime IM client by blocking all attempts to circumvent the IM security infrastructure. This standardization is achieved by deploying RTGuardian at the gateway to block the use of any unauthorized greynet applications. With this standardization in place, it becomes significantly easier for IT to enforce security policies at company, group and user levels (e.g. allowing IM usage only for mapped buddy names, file transfer over IM, etc.), In addition to policy enforcement, FTEE enhances the security of Sametime deployment by providing real-time content filtering, guaranteed day-zero worm blocking, SpIM protection, and scanning of file transfers over Sametime using existing anti-virus tools.

Security	FaceTime Enterprise Edition
Management	Policies at company, group, user levels <ul style="list-style-type: none">▪ Group level ethical boundaries▪ IP-Address based access controls▪ Policies cover access controls and monitoring options
File Transfer Management	Policies at company, group, user levels <ul style="list-style-type: none">▪ Allow/block at all levels▪ Ability to specify rules for files size, types
AV Scanning of File Transfers	Support for <ul style="list-style-type: none">▪ Symantec, McAfee, TrendMicro, CA, ClamAV▪ Support for Sophos and others in development
SpIM Blocking	Content based: <ul style="list-style-type: none">▪ White/Black lists, Custom Rules, Challenge/Response
URL Blocking	<ul style="list-style-type: none">▪ Domain-configurable and direction-configurable URL policies▪ Challenge/Response to eliminate false positives

Management and Control

FaceTime Enterprise Edition for Sametime provides a hierarchical view of the enterprise network to provide rich policy management at global, group and individual employee levels, with visibility and insight into real-time communications throughout the distributed enterprise and control over IM capabilities at every level. Fine grained control of Sametime client capabilities includes the ability to manage file transfer, collaboration (e.g., audio/video conferencing, VoIP, etc.), and other client privileges at the company, group, and user levels of granularity.

As befits real-time communications protection, FTEE for Sametime supports real-time enforcement of policy changes and delivers real-time usage reports, inter-group reports and graphical monitoring of statistics through a secure, intuitive Web-based interface, with access to configuration functions by authorized personnel only.

Compliance Auditing and Supervisory Review

FaceTime Enterprise Edition is the only solution to offer TrueCompliance™, ensuring strictest compliance with regulatory and corporate policies. With FTEE for Sametime, companies get enhanced capabilities for:

- Real-time group-level ethical boundaries (“Chinese Walls”)
- Flexible and advanced disclaimers
- File transfer archival
- Single step guaranteed strict recordation into SQL DB
- Guaranteed strict archiving into eMail/WORM storage (email, EMC Centera, etc.)
- Message anti-tampering check sums (non repudiation)
- Rich reporting and workflow, including audit reports

FTEE assures exported conversations match recorded conversations at the level of time-stamped messages, storing messages in binary and text format in the order they appear for content accuracy, including accurate capture of multi-party chat threads, and transferring directly to WORM (Write Once Read Many) storage. File transfer management controls include anti-virus scanning, compliance review, and WORM archival. Anti-tampering checksums ensure that archived messages cannot be repudiated.

Customized legal disclaimers are automatically displayed to all parties involved in the IM conversation, reminding them that Sametime is a corporate system which is monitored and audited for compliance with both legal and corporate policy requirements regarding data security. Enterprises also have the ability to turn-off these disclaimers. Ethical usage rules are enforced in real-time by configuring "Chinese Wall" policies to restrict inter-group contact and using "Hair Pinning" to restrict inter-organization contact (for public IM networks).

FTEE also enables Sametime users to more easily review their own IM threads and conversations.

Compliance	FaceTime Enterprise Edition
Disclaimers	<ul style="list-style-type: none"> ▪ Company level and group level configurable disclaimers ▪ Disclaimer display control at the IM network level ▪ Disclaimer display control at company, group, and employee levels
Recording	<ul style="list-style-type: none"> ▪ Group level policy configuration – enables Chinese walls ▪ Policy messages sent to users ▪ Recording of multi-party join/leave events ▪ File Transfers: Capture, AV Scan and archival
Export to Archive	<ul style="list-style-type: none"> ▪ Exports text and files to archive ▪ Export streams are customizable on groups, chat rooms, networks, internal vs. external users ▪ Unlimited number of export streams to multiple email/WORM storage destinations ▪ Export can be scheduled using easy to use UI ▪ User attributes & tamper detection included in export XML
Reports	<ul style="list-style-type: none"> ▪ Reports on IM usage, security violations, compliance violations, transcript reviews ▪ Report generation, scheduling and delivery <ul style="list-style-type: none"> – Instant and scheduled – Browser and email delivery options – HTML, CSV, PDF formats

Enterprise-Grade Solution

FaceTime Enterprise Edition for Sametime co-exists with standard IT infrastructure, including firewalls, load balancers, email systems, and proxy servers; the system itself supports load-balancing among redundant/standby directory, database and corporate proxy servers. The platform-neutral deployment architecture of IMAuditor ensures ease of integration, with flexible, customizable OS and DB connectivity support. Purpose-built hardened RTGuardian appliance enables plug-and-play deployment at the network perimeter, with automated protocol and threat protection updates built in. FTEE for Sametime leverages off-the-shelf load-balancing solutions to ensure five-nines reliability and high availability of security and compliance infrastructure for Sametime installations without the need for additional hardware.

Summary

Real-time communications are here to stay. Their growth within our organizations is set to continue and the adoption rate of technology that provides real competitive advantage is already overtaking the adoption rates enjoyed by email and the web some years previously.

The implementation by organizations of an enterprise grade IM solution, to provide supportable business applications in the same way email services are provided goes a small way towards providing a secure, compliant infrastructure

The combination of IBM Lotus Sametime and FaceTime Enterprise Edition provides a powerful solution to the management, control, and security of these vital business tools. More and more organizations have now realized that blocking greynet applications is no longer a viable solution, and the movement to standardize on Sametime as an enterprise IM system provides the foundation for a productive IM strategy.

Maximizing the benefits of Sametime and ensuring its safe and secure implementation requires the additional security and compliance features and anti-circumvention of policy tools that FaceTime Enterprise Edition provides. Organizations should not contemplate the implementation of any enterprise IM network without an additional security layer, in the same way that new email implementations would not take place without an additional security and management consideration.

FTEE for IBM Lotus Sametime standardizes enterprise IM rollouts by completely eliminating the use of unsanctioned IM clients and rogue P2P applications, in addition to keeping spyware out of the network.

In addition, FTEE for Sametime cost-effectively secures IM communications by supporting the use of existing anti-virus tools to scan file transfers and by blocking spIM. Finally, FTEE for Sametime ensures compliance with US government regulations by archiving all IM traffic in a tamper-proof fashion, blocking spyware, providing rich compliance workflow, and interfacing with email and WORM storage. The rich conversation capture provided by FTEE for Sametime allows for conversation reconstruction depicting exactly what each user saw, including anti-tampering mechanisms to ensure that messages are not altered after capture.

About FaceTime Communications

FaceTime enables the safe and productive use of greynets like instant messaging, VoIP, web conferencing and P2P file sharing. FaceTime Security Labs delivers the industry's first IMPact Index, which assesses "point-in-time" risks posed by viruses, worms and other malware propagating through greynet applications. FaceTime's award-winning solutions are used by more than 800 customers, among them nine of the ten largest U.S. banks. FaceTime supports or has strategic partnerships with all leading public and private IM network providers, including AOL, Google, Microsoft, Yahoo!, IBM, Reuters, Bloomberg, and Jabber.

More Information

For more information about FaceTime Communications and FaceTime solutions please visit

<http://www.facetime.com>

FaceTime Communications

1159 Triton Drive

Foster City, CA 94404

Phone: (888) 349-3223

Email: info@facetime.com