

Security and Compliance for IBM Lotus Sametime

KEY BENEFITS:

- Centralized, tamper-proof environment for logging and archiving UC-based communications, including associated file attachments and metadata
- Auditing and easy retrieval of stored information based on granular searches of keywords, users, time frames, and more to meet e-Discovery requirements
- Integrated with Domino to define permissions at the company, group and user levels to enforce ethical boundaries and acceptable use policies
- Interoperability with existing anti-virus solutions for file attachment scanning
- Integrated anti-spIM ensure productivity and close security holes
- Detection and blocking of malicious URLs within IM or web conferencing chat messages
- Content filtering and keyword blocking to protect confidential information and prevent data loss
- Day zero worm protection that identifies anomalous behavior to protect against new, unknown threats and bots
- Developed for maximum scalability and compatibility
- Warn and coach employees in real-time on acceptable use policies
- Define specific reports based on role or need, such as providing malware violations only to IT security and IM usage only to messaging staff
- Guaranteed TrueCompliance™ features enable organizations to meet the strictest corporate policies and government regulations

FaceTime IM Auditor for IBM Lotus Sametime and IBM Lotus Notes and Domino is a comprehensive solution for the security, management and compliance of unified communications, consisting of user policy management, message hygiene, malware prevention, and archiving for compliance.

What's the Challenge?

Instant messaging (IM) and other real-time communications protocols are a fact of life in today's enterprise, as evidenced by the rapid adoption of unified communications (UC) platforms such as Lotus Sametime; industry analysts expect enterprise IM to reach 100% adoption by 2010.

Despite the availability of enterprise-class instant messaging on the desktop through collaborative environments such as Lotus Sametime, users continue to download and install consumer-based IM networks such as MSN, Skype, and other peer-to-peer channels resulting in a typically heterogeneous enterprise environment consisting of sanctioned and unsanctioned applications.

Enterprises are faced with a number of key challenges in managing and securing the productive use of communications in a heterogeneous UC environment:

- Not only are more attacks entering the network over real-time channels than email, but the attacks themselves are becoming more damaging. Crimeware, rootkits, exploits, and other malware are designed to bypass traditional security measures, and the real-time channel only makes that task easier.
- Just as malware is moving to real-time communications to bypass existing security measures, spam is moving beyond the email inbox into the IM stream, further increasing the risk of accidental malware infection as well as increasing traffic.
- Proprietary information can be transferred outside the company network using unmonitored IM and UC channels

Compliance and e-Discovery

In an integrated, collaborative communications environment it's vital that storage and archiving supports the compliance requirements for all messaging types supported by Lotus Sametime - email, IM, and conferencing chat logs, P2P conversations, and more.

FaceTime's IM Auditor for Lotus Sametime is designed to help companies do exactly this:

- Centralized, tamper-proof recording and archiving of all IM conversations and file transfers
 - Reduce costs from having to piece together conversations from multiple sources
 - Leverages existing storage infrastructure
- Easy retrieval of stored information based on keywords, users, time frames and more
 - Web-based system eliminates need for technical resources to search and sort log files
 - Ensures ability to meet e-Discovery deadlines and minimizes financial exposure

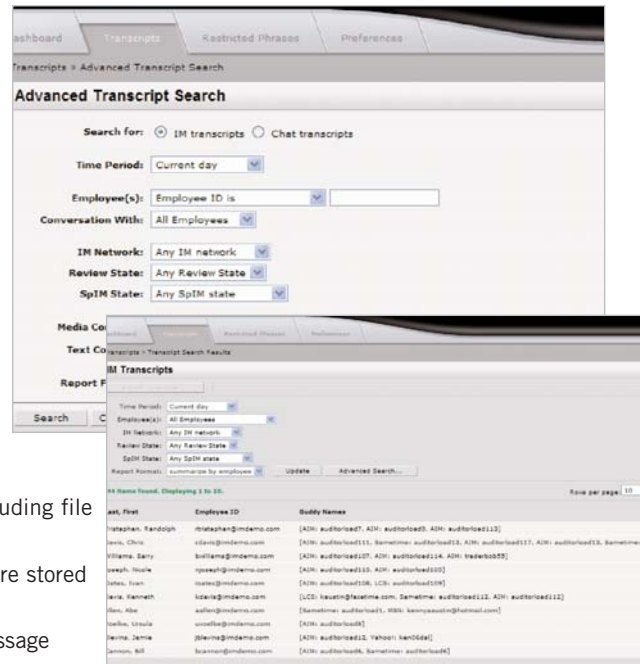
And FaceTime's Unified Security Gateway (USG) appliance can enforce company IM usage policies, preventing the inclusion of inadvertent IM and other chat records as part of e-Discovery.

FaceTime enables enterprises to standardize their IM infrastructure and maximize their investment in UC while securing it against IM-borne threats such as infected file transfers and spam over IM (SpIM).

Key benefits include:

- Files transferred over IM are scanned automatically with existing anti-virus software
- Automatic malware and protocol updates protect against zero-day threats
- Group-level ethical boundaries prevent unsanctioned information-sharing
- Tamper-proof storage of chat threads ensures accurate compliance records
- Flexible file transfer capture and archival for ease of e-Discovery storage and retrieval
- Clearly-visible disclaimers discourage unauthorized use of business channels
- Existing database resources leveraged for storage of all real-time communications

FaceTime IMAuditor accurately and completely logs all real-time communications, including file transfers and events such as message blocking, to ensure compliance with corporate governance, data protection, and e-Discovery regulations. The actual files transferred are stored with the relevant messages, simplifying the review process and ensuring that all communications are seen in the context of a complete conversation, with accurate message order preserved.



FaceTime Complements Lotus Sametime with:	
Granular policy setting	Policies at company, group, user levels: Group level ethical boundaries; IP-Address based access controls; Access controls and monitoring options
Information leak prevention	Allow/block file transfers at all levels; Specify rules for file name/size/ type. Can detect and block words, phrases, and full regular expressions and flag/block and/or alert based on content
Anti-virus and malware control, including bots spreading over IM	Support for Symantec, McAfee, TrendMicro, CA, ClamAV; Sophos; Kaspersky. Automatic updates from FaceTime Security Labs provides day zero worm protection against new, unknown threats.
SpIM blocking	Content-based protection using white/black lists and custom rules.
Malicious URL blocking	Domain-configurable and direction-configurable URL policies detect and block URLs within IM or web conferencing chat messages.
Federation management	Ability to specify explicit partner domain-based rules at company, group, and user levels
Legal disclaimer notifications	Alert employees of policy in real-time. Disclaimers sent inline and audited; disclaimer display controls at the IM network and group levels.
Tamper detection of messages	Guaranteed message order preservation; anti-tamper mechanism validates conversation integrity
File transfer capture	Files archived in database and shown in context in conversation review
Easy retrieval of messages for e-Discovery	Reports on IM usage, security violations, compliance violations, transcript reviews. Report generation, scheduling and delivery.