

## Protect and Secure IBM® Unified Communication and Collaboration (UC<sup>2</sup>)

### Why IBM® UC<sup>2</sup> customers and prospects should purchase FaceTime

- Enforces standardisation of Sametime for Instant Messaging and maximises investment
- Enables safe use of enterprise IM and insight into/control over use of public IM and other real-time communications tools
- Ensures data protection and eDiscovery compliance requirements are met for the full range of electronic communications

### How FaceTime benefits IBM

Organisations will only implement the full IBM UC<sup>2</sup> collaboration features of the Sametime applications once they have adequately secured the platform's basic IM and presence awareness functions. Incorporating FaceTime accelerates adoption timetables and allows additional UC<sup>2</sup> components to be incorporated sooner. FaceTime solutions also drive additional consulting and implementation professional services revenues.

### Key verticals

Financial Services, Utilities, Banking, Insurance, Government, Telecommunications, Transport, Legal Services, Retail, Healthcare, Pharmaceuticals.

### Installed base

900 organisations with 2.6 million users around the world

### What's the challenge?

Collaborative environments such as IBM Lotus Sametime are increasingly falling victim to new variants of traditional malware, with blended threats hopping from public network to enterprise network – exposure that is increased by federation with public IM networks and partners. Additional security requirements engendered by federation's heterogeneity and the new modalities in unified communications and collaboration (UC<sup>2</sup>) platforms create further complexities.

Users continue to introduce public IM networks such as Yahoo and MSN, along with Skype VoIP and other peer-to-peer channels, collectively known as greynets, to the corporate IT environment alongside Sametime. These greynets provide potential vectors for malware, client-side code vulnerabilities, intellectual property loss, and identify theft, challenging existing security, policies and infrastructure.

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.

The ongoing presence of these “under the radar” protocols means that IT must determine how best to manage and secure these real-time communications channels as well as Sametime itself, both for the purposes of security and of legislative compliance with regard to data protection and archiving.

### Key benefits of protecting Sametime investments with FaceTime:

- Ensure all IM communications go through the appropriate secured Sametime channel
- Prevent malware from propagating over the real-time channels
- Automatic scanning of file transfers over IM using existing anti-virus
- Real-time content filtering with advanced pattern matching, blocking and scanning prevents information leakage
- Automatic signature and protocol updates protect against zero-day threats
- Real-time group-level ethical boundaries
- Multi-party chat capture ensures accurate compliance records
- Flexible file transfer capture and archival for easy communication storage and retrieval
- Clearly-visible disclaimers
- Single step guaranteed strict recording of communication threads into an SQL database

Regardless of complexity or number of individual clients, FaceTime accurately and completely logs all real-time communications, including file transfers and event notation such as message blocking, to ensure compliance with corporate governance, data protection, and eDiscovery regulations. The actual files transferred are stored 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.

## Engagement strategy

Engage with FaceTime when prospects are considering, or have deployed Sametime. FaceTime's gateway appliance (RTGuardian) not only ensures standardization of Sametime by blocking access by all unauthorized IM, P2P and VoIP use, but provides justification for the Sametime spend. Use IMAuditor for additional security and management to augment native Sametime functionality:

## Security and Standardization

| Functionality                    | Sametime base capability   | FaceTime additional benefits  |
|----------------------------------|--|---|
| Management                       | Allow/block various features at server level   | Policies at company, group, user levels: Group level ethical boundaries; IP-Address based access controls; Access controls and monitoring options |
| File transfer management         | Allow/block at company, group and user level   | Policies at company, group, user levels: Allow/block at all levels;   |
|                                  | File size and type control at group level  | Specify rules for file size/ type   |
| Virus scanning of file transfers | No built-in a-v support; SameTime 7.5 provides integration with 3rd party a-v on server side | Support for Symantec, McAfee, TrendMicro, CA, ClamAV; Sophos in development   |
| SpIM blocking                    | Not supported natively - "chat-log" API allows third party programs to provide this feature  | Content based: White/black lists, custom rules, challenge/response  |
| URL blocking                     | Not supported natively - "chat-log" API allows third party programs to provide this feature  | Domain-configurable and direction-configurable URL policies; No false positives   |
| Federation                       | Allow/block at company-level only  | Allow/block permissions at company, group and user levels; Specify partner domain-based rules at company, group, and user levels                  |

## Compliance Auditing and Supervisory Review

| Functionality     | SameTime base capability  | FaceTime additional benefits  |
|-------------------|---|---|
| Disclaimers       | No support  | Company and group level configurable disclaimers; Control disclaimer display at IM network level and at company, group, and employee levels   |
| Recording         | Configurable at company and user levels for SameTime meetings; "Chat-log" API allows third party programs | Group level policy configuration enables Chinese walls; Recording of multi-party join/leave events; File transfers: capture, virus scan and archiving   |
| Export to archive | No support  | 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; Export can be scheduled using easy to use UI; User attributes and tamper detection included in export XML |
| Reports           | Only system server events (through Domino); Conversation reports not supported natively                   | Reports on IM usage, security violations, compliance violations, transcript reviews; Report generation, scheduling and delivery; Instant and scheduled browser and email delivery options in HTML, CSV, PDF formats   |

## FaceTime Benefit Overview:

FaceTime enables enterprises to standardize their IM infrastructure and maximize their investment in UC<sup>2</sup> while securing their environment against IM-borne threats such as malware and spam over IM (spIM). Granular filtering and flexible archival ensure that enterprises are able to meet compliance requirements for data protection and eDiscovery across all electronic communications channels.

FaceTime Enterprise Edition for IBM Lotus Sametime combines IMAuditor™ in the LAN with RTGuardian™ at the gateway for a complete, end-to-end security, management, and compliance solution. IMAuditor secures and manages all Sametime and other allowed IM traffic. IMAuditor, which resides on the LAN, maintains an integrated trust relationship with Real-Time Guardian, which blocks all IM traffic not specifically allowed and protects against circumvention of policies.

## Reference Customer Deployments of IBM UC<sup>2</sup> with FaceTime

**INDUSTRY:** Pharmaceuticals  
**ORGANISATION:** Leading research-based pharmaceutical manufacturer  
**REQUIREMENT:** Security  
**IT USERS:** 100,000+

This organisation needed to secure the use of public IM networks while transitioning to a standardised Sametime environment. Following deployment of the Sametime Gateway to provide federation and external public IM connectivity, FaceTime is being deployed to secure these key channels.

**INDUSTRY:** Financial Services  
**ORGANISATION:** Leading reinsurance and financial services provider  
**REQUIREMENT:** Compliance  
**IT USERS:** 4,000

A long term Notes user, this organisation wanted to implement the real-time aspects of IBM's UC<sup>2</sup> strategy, but internal compliance requirements were not met by native Sametime functionality. The company needed all real-time traffic to be incorporated into DB2 Content Manager, which was enabled through the implementation of the FaceTime solution.



FaceTime Communications, Inc. 1159 Triton Drive Foster City, CA 94404  
 (888) 349-FACE (3223) toll free (650) 574-1600 phone (650) 574-2700 fax  
 Information: info@facetime.com Sales: sales@facetime.com www.facetime.com