

## Secure and Enable Unified Communications

IM Auditor™ ensures security, management and compliance for Unified Communications - from presence and instant messaging to conferencing and voice.

### KEY FEATURES

- Support for Microsoft OCS, IBM Lotus Sametime and all major public IM networks
- Support for Blackberry PIN and SMS messaging
- Support for Reuters Messaging and Bloomberg import
- Prevents data leakage over IM and UC platforms through content filtering and regular expressions
- Integrate with corporate directory services to utilize and control communications at global, group and employee level
- Report on total IM usage
- Virus scanning of file transfers using existing AV implementation
- Block zero-day IM-based worm and virus attacks
- Guaranteed 100% accurate binary archiving of all IM for compliance or e-Discovery
- Capture and archive file transfers over IM into email archive
- Advanced text search allows for speedy, simple and efficient retrieval of messages
- Prevent unauthorized communications through ethical walls
- Prevent SpIM to protect bandwidth and close security holes
- Secure, intuitive Web-based administration and reporting, including detailed usage reporting by log in, number of messages, time interval, UC events and more

Instant messaging (IM) and other real-time communications protocols are a fact of life in today's enterprise. From public instant messaging, web based conferencing to the enterprise platforms available in Unified Communications platforms their adoption has been driven by business needs. Organizations looking for ways to increase the speed of decision making, improve productivity, ensure a safe environment for communications and decrease costs – have increasingly turned on these real time communications tools, often with few restraints on usage.

### Security Challenges

Despite the availability of enterprise-class instant messaging, on the desktop through collaborative environments such as Microsoft Office Communications Server (OCS) or IBM Lotus Sametime, users continue to download and install consumer-based IM networks such as Yahoo, AIM, GoogleTalk, Windows Live or Skype resulting in a typically heterogeneous environment consisting of sanctioned and unsanctioned applications.

- Not only are more attacks entering the network over real-time channels than email, but the attacks themselves are becoming more damaging. These infections are designed to bypass traditional security measures, and these real-time channels 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 Unified Communications (UC) channels

### Compliance, Liability and Risk Challenges

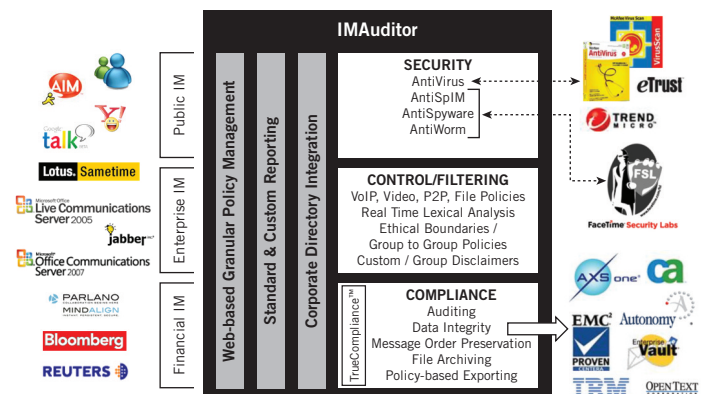
Real-time communications are subject to an increasing number of industry and government regulations. Achieving and maintaining compliance with these regulations and standards is a huge challenge with very clear penalties. Aside from non-compliance fines, the loss of reputation and potential loss of intellectual property, the manpower involved in recovering from any of these issues can be detrimental to ongoing business.

### IM Auditor™: Securing and Enabling Unified Communications

IM Auditor™ supports the full range of public IM clients, leading UC platforms, professional community networks, and Web conferencing applications, meeting the security, management and compliance requirements of organizations and guaranteeing compliance support for all major federal and industry regulations.

IM Auditor protects real-time communications channels against viruses and other malware through integral support for existing anti-virus installations, effectively closing the zero-day gap. Patent-

pending anti-SpIM (Spam over IM) keeps IM networks free of bandwidth hogging spam, and intelligent, granular content filtering and logging of all electronic conversations ensures an audit trail for information leak prevention, compliance and e-Discovery.



**IMAUDITOR FEATURES**

**Security**

- Day-zero worm blocking of virus attacks that use real-time communications channels
- Virus Scan file transfers, including those over OCS and Sametime using existing AV installations
- Block external threats and SpIM at the gateway with perimeter deployment options for OCS and Sametime
- Block file transfer or allow (archiving if required) with imposed file size limits
- Patent pending anti-SpIM technology protects bandwidth
- Stealth proxy operation prevents malware from disabling protection and cloaks IP addresses
- Prevent loss of intellectual property and confidential information by:
  - Routing employee communications over public IM networks internally,
  - Blocking messages using keyword watch list, advanced keyword patterns and full regular expressions
  - Content scanning of file transfers of popular file types, including Microsoft Office and other applications
  - Protecting and blocking encrypted files and controlling what file types can be sent internally or externally

**Compliance**

- 100% guaranteed accurate binary archiving of all real-time communications, including user sign on/off history, multi-party chat participation and file transfers
- Supports Microsoft OCS Group Chat
- Monitors PIN and SMS messages through Blackberry Enterprise Server
- Reuters Messaging and Bloomberg import capability.
- Automatic display of customizable chat disclaimers to all parties involved in a conversation
- Assign and enforce regulatory compliance features at the company, group and individual employee levels
- Facilitate segregation of roles and tasks based on functional responsibilities of an individual
- Configure ethical boundaries to restrict inter-group and inter-organization contact
- Sophisticated workflow process with content monitoring, review cycles and custom search queries
- 360-degree audit of all users including system administrators and content reviewers
- Advanced text search for easy and efficient retrieval of IM transcripts for e-Discovery
- Seamless integration with common email archive and WORM storage systems

- File transfer archival support, includes OCS and Sametime
- Prevent data tampering with a checksum of time-stamped messages, ensuring exported conversations match recorded conversations
- Email alerts and notifications to ensure records retention and facilitate ease of retrieval
- Facility for reviewer to delete personal messages from transcripts
- Reporting of public IM conversations conducted over enterprise IM clients
- MindAlign 2007 persistent chat transcript import capability

**Management**

- Manage file transfer, collaboration (e.g., audio/video conferencing, games, VoIP), and other client privileges at the company, group and user levels for all real-time communications services
- Associate employee IDs in the corporate directory with IM buddy names
- Unique support for AOL Identity Services (including Triton) allows businesses to own corporate domain name use in buddy names and match buddy names to company directories
- IP-based controls enforce policies based on endpoint IP addresses
- Real-time usage reports and graphical monitoring
- Secure, intuitive Web-based access to configuration functions by authorized personnel
- Advanced controls for AIM business client for end-to-end policy enforcement and better user experience
- Detailed usage trend reporting on unique logins, number of messages, number of UC events, and more
- Full management, security and compliance support for Blackberry users within an Sametime environment
- Audit within both OCS and Sametime environments
- Microsoft Live Meeting event and activity support

**Extension and Integration**

- Integrates with corporate database applications, email compliance, archiving, and WORM storage systems
- APIs for extending real-time event management capabilities to:
  - Enable corporate applications with IM and presence capabilities
  - Manage IM from other corporate applications

**Enterprise-Grade Deployment**

- Flexible Operating System and Database deployment architecture
- Flexible deployment options:
  - On premise
  - Multi-tenancy, with hosting management through common infrastructure and delegated administration
- Support to capture any language.
- Double byte support
- Fail-over with load-balance available among redundant and corporate proxy servers
- VMware deployment capabilities
- High availability for multi-site deployment

**Supported Applications**

- **Unified Communications:** Microsoft LCS 2005, OCS 2007 and 2007 R2, IBM Lotus Sametime v8.0.2, Cisco Jabber XCP, MindAlign
- **Professional Community Networks:** Bloomberg, Reuters, Communicator Inc., Pivot
- **Public Instant Messaging:** Windows Live Messenger, MSN, AIM, Yahoo!, GoogleTalk, iChat and others
- **Web Conferencing:** WebEx

**License Modules**

**Basic License**

- Includes Unified Communications & Public Instant Messaging

**Additional License Options**

- Financial and Professional Community Networks
- Blackberry SMS & PIN Messaging

**Recurring Fees:**

- Annual Maintenance & Support
- Security Subscriptions

**Software Requirements**

- Microsoft Windows 2000/2003/2008 Server or RedHat Enterprise Linux 3.0 or ES 4.0
- Microsoft SQL Server 2000, SQL Server 2005, SQL Server 2008, or Oracle 9i, 10g or 11g (on a separate machine)
- Also supported on VMware

**Hardware Requirements**

- Pentium 4, 2 GHz CPU or higher recommended
- Network Interface Card (10/100BaseTx or Gigabit)
- 2 GB of RAM
- 40 GB of available hard disk space



**FaceTime Communications, Inc.**  
 (888) 349-FACE (3223) *toll free*  
 (650) 598-2820 *fax*  
 info@facetime.com

**Worldwide Headquarters**  
 1301 Shoreway, Suite 275  
 Belmont, CA 94002 USA  
 (650) 631-6300 *phone*  
 sales@facetime.com

**EMEA Headquarters**  
 400 Thames Valley Park  
 Reading, Berkshire, RG6 1PT UK  
 +44 (0) 118 963 7469 *phone*  
 emea@facetime.com