

The Industry Standard for Security, Management and Compliance of IM

About FaceTime IMAuditor

IMAuditor addresses the security, management and compliance needs of enterprises that must enforce corporate messaging standards and adhere to government regulations that require all electronic communications, including IM, to be properly secured, managed and archived.

KEY FEATURES

- Creates a standardized profile of all real-time communications use
- Implement powerful policy controls at global, group and employee levels
- Prevents loss of intellectual property and confidential information over IM
- Scans file transfers using existing antivirus installation
- Blocks zero-day IM-based worm and virus attacks
- Automatically protects against greynet threats identified by FaceTime Security Labs
- Guaranteed 100% accurate binary archiving of all IM
- Archives file transfers over IM into WORM storage
- Sophisticated workflow process for regulatory compliance monitoring
- Advanced text search allows for easy and efficient retrieval of messages for e-discovery
- Prevents 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

IMAuditor is used by the world's largest firms to secure and manage real-time communications and ensure that instant messaging and Unified Communications platforms can be safely used to enhance business productivity and responsiveness without endangering the organization's information security or compliance requirements.

Instant Messaging is Embedded in the Business Process

IM is the fastest growing electronic communications medium in history; presence is today's dial tone, and enterprises are clearly deriving significant benefit from fast, effective communication. Enterprise IM (EIM) is just one component of a Unified Communications (UC) platform that integrates a wide range of real-time communications tools for increased productivity and cost savings in the enterprise. Along with public IM services and industry-focused communities, they provide the ability for employees to communicate with one another as well as with customers, partners and others outside the corporate network. Industry analysts expect EIM to reach 100% adoption by 2010.

Liability Risks of IM for the Organization

However, IM applications, as well as their less-well-intentioned cousins P2P, Web chat, and VoIP, are part of a category of applications FaceTime terms 'greynets.' Greynets are network-enabled applications installed on an end user's system without the permission or knowledge of the IT department and are largely invisible to the existing security infrastructure. While frontline productivity may be increasing through the use of these invisible communication channels, so is the security risk, with the potential to more than cancel out the productivity gains.

IM conversations and attachments, along with the chat threads created through the use of web conferencing and VoIP applications such as Skype, as well as any files transferred across these networks, are subject to the same legal controls and compliance requirements as email and web traffic.

Enterprises need to secure this traffic to protect the network from malicious threats, prevent loss of confidential information and intellectual property, enforce corporate policy, and monitor and archive conversations for regulatory compliance and e-Discovery requirements. Furthermore, despite the efforts by many companies to standardize on an enterprise IM client or UC platform, employees continue to download and use freely available public IM clients and P2P applications so implementing a comprehensive IM security and management solution to prevent unauthorized use and enforce policy is vital.

A Proven Solution

IMAuditor is the most mature and wide-ranging security and compliance solution for IM applications available today, supporting the full range of public IM clients, leading UC platforms by Microsoft and IBM, professional community networks, and Web conferencing applications. Backed by FaceTime Security Labs, IMAuditor delivers TrueCompliance™ - guaranteed compliance support for all major federal and industry regulations through multi-layered policy-based access control, monitoring, and insight into the use of real-time communications tools.

IMAuditor 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.



IM AUDITOR FEATURES

Security

- Scan file transfers, including those over OCS and Sametime using existing anti-virus installations
- Block file transfers or allow them with imposed file size limits
- Stealth proxy operation prevents malware from disabling protection and cloaks IP addresses
- Day-zero worm blocking of virus attacks that use real-time communications channels
- 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 all 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 and multi-party chat participation
- Automatic display of customizable legal audit 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 conversations for e-Discovery
- Seamless integration with common email compliance and WORM storage systems
- File transfer archival support, including for 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
- Reporting of public IM conversations conducted over enterprise IM clients

Management

- Manage file transfer, collaboration (e.g., audio/video conferencing, 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 IM buddy names
- Unique support for AOL Identity Services (including Triton) and MSN Connect 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 of statistics
- 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 log-ins, number of messages, number of UC events, and more
- Full management, security and compliance support for Blackberry users within an IBM Lotus Sametime environment

Extension and Integration

- Integrates with corporate database applications, email compliance, archiving, and WORM storage systems
- APIs for exploiting and 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 OS and DB deployment architecture
- Flexible deployment options:
 - On premise
 - Multi-tenancy, with hosting management through common infrastructure and delegated administration
- Multi-language support
- Fail-over with load-balance among redundant and corporate proxy servers
- High availability for multi-site deployment

“FaceTime is still the best fit for organizations looking for an IM hygiene product that can also offer spyware security.”



Supported Applications

- UC and Enterprise Instant Messaging: Microsoft LCS and OCS, IBM Lotus Sametime, Jabber
- Professional Community Networks: Bloomberg, Reuters, Communicator, Inc.
- Public Instant Messaging: Windows Live Messenger, MSN, AIM, Yahoo!, GoogleTalk and others
- Web Conferencing: WebEx

Software Requirements

- Microsoft Windows 2000/2003/2008 Server or RedHat Enterprise Linux Operating System
- Microsoft SQL Server 2000 or Oracle 9i version 9.0.1 or 9.2

Hardware Requirements

- Pentium III 800 MHz CPU, Pentium 4, 2 GHz CPU or higher recommended
- 2 GB of RAM
- 30 GB of available hard disk space