

About FaceTime IMAuditor

IM Auditor 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, be properly secured, managed and archived.

KEY FEATURES

- Automatically protects against greynet threats identified by FaceTime Security Labs
- 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
- Guaranteed 100% accurate binary archiving of all IM
- Archives file transfers over IM into WORM storage
- Sophisticated workflow process for regulatory compliance monitoring
- Prevents SpIM to protect bandwidth and close security holes
- Blocks zero-day IM-based worm and virus attacks
- Secure, intuitive Web-based administration and reporting
- Platform-neutral architecture with flexible deployment options
- High availability and load-balancing deployment increases security and reliability of existing IM infrastructure

IM Auditor is used by the world's largest firms to secure and manage real-time communications and ensure that both public and enterprise instant messaging networks can be safely used to enhance business productivity and responsiveness without endangering the organization's information security.

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. Industry analysts expect two thirds of enterprise organizations to choose an Enterprise Instant Messenger (EIM) solution by 2007. EIM products are moving rapidly towards becoming unified communication and collaboration platforms integrating a wide range of real-time communications tools. Along with PIM services, and industry-focused IM communities, they provide the ability for employees to communicate with one another as well as with customers, partners, and others outside the corporate network.

Liability Risks of IM in the Enterprise

However, IM applications, as well as their less-well-intentioned cousins P2P, Web Chat, and VOIP, are part of a category of applications that 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 information channels, the security risk is also increasing, with the potential to more than cancel out the productivity boost.

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

Enterprises need controls in place to protect the network from malicious threats, prevent loss of confidential information and intellectual property, enforce corporate policy, monitor and archive conversations for regulatory compliance. Furthermore, despite the efforts by many companies to standardize on an enterprise IM client, employees continue to download and use freely available public IM clients and P2P applications.

Implementing a comprehensive IM security and management solution is vital.



Full visibility into IM usage and policy violations

Granular permissions and monitoring controls



A Proven Solution

IMAuditor is the most mature and wide-ranging security and compliance management solution for IM applications available today, supporting the full range of PIM and EIM applications, professional community networks, and Web conferencing applications. It's backed by FaceTime Security Labs, the industry's largest greynet research team. When used in conjunction with FaceTime's Real-Time Guardian as part of the FaceTime Enterprise Edition, IMAuditor delivers TrueCompliance™ - guaranteed compliance support for all major federal and industry regulations through multi-layered policy-based access control, monitoring, and management 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 archiving/logging of all electronic conversations ensures an audit trail for information leak prevention and compliance. IMAuditor enhances the security and compliance capabilities of EIM networks like Microsoft Live Communications Server (LCS), IBM Lotus SameTime, Jabber and others, as well as improving their reliability and availability.

FaceTime solutions are deployed in nine of the ten largest banks in North America, and the company offers the only certified scalable enterprise IM solution that supports deployments in excess of a hundred thousand seats. IDC has named the company its #1 vendor of IM security solutions for two consecutive years.

IMAUDITOR FEATURES

Security

- Scan transferred files, including LCS file transfers, using existing anti-virus installations
- Stealth proxy operation prevents malware from disabling protection and cloaks IP addresses
- Block zero-day worm and virus attacks using real-time communications channels
- Block SpIM using a combination of allow/block lists, rich content filtering and patent-pending challenge-response
- Block file transfers, or allow file transfers with imposed file size limits
- Prevent loss of intellectual property and confidential information by:
 - Routing employee communications over public IM networks internally, and
 - Blocking messages using keyword watch list, advanced keyword patterns and full regular expressions

Compliance

- File transfer archival support for EIM networks
- Reporting of PIM conversations conducted over EIM clients
- 100% guaranteed, accurate binary archiving of all real-time communications, including user sign on/off history and multi-party chat participation history
- Automatic display of customizable legal audit disclaimers to all parties involved in the conversation
- Assign and enforce regulatory compliance features at the company, group, and individual employee levels
- Configure "Chinese Wall" policies to restrict inter-group contact and use "Hair Pinning" to restrict inter-organization contact
- Sophisticated workflow process with content

monitoring, review cycles and custom search queries

- Seamless integration with common email compliance and WORM storage systems
- Prevent data tampering with a checksum of time-stamped messages, ensuring exported conversations match recorded conversations
- 360-degree audit of all users including system administrators and content reviewers

Management and Control

- 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 employees ID in the corporate directory with 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 access 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

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

Supported Applications

- Enterprise Instant Messaging: Microsoft LCS, IBM Lotus Sametime, Antepo, Jabber, Parlano MindAlign
- Professional Community Networks: Reuters, Bloomberg, Communicator Inc.,
- Web Conferencing: WebEx
- Public Instant Messaging: MSN, AIM, Yahoo!, GoogleTalk, and more

Software Requirements

- Microsoft Windows 2000 Server, Windows 2003 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
- 1 GB of RAM