

### About FaceTime IM Auditor

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

- Create a standardized profile of all public and enterprise IM use
- Block SpIM to reduce the spread of viruses and worms
- Block Zero-Day IM-based worm and virus attacks
- Automatically protect against IM and P2P threats identified by FaceTime Security Labs
- Identity management with policy control at global, group and employee levels
- Prevent loss of intellectual property and confidential information over IM
- Scan file transfers using existing antivirus software
- Guaranteed 100% accurate binary archiving of all IM
- Sophisticated workflow process for regulatory compliance monitoring
- Intuitive Web-based administration and reporting
- Platform-neutral architecture with flexible deployment options

IM Auditor is the leading solution used by the world's largest firms to secure and manage real-time communications and ensure that IM communications are conducted in a safe, productive, and effectively-managed environment.

### The Emergence of Instant Messaging for Business

IM, in enterprises that rely on real-time communication and instant information, is the fastest growing electronic communications medium in history. Enterprise IM (EIM) products, public IM (PIM) services, and industry-focused IM communities all provide the ability for employees to communicate with one another as well as with customers, partners, and others outside the corporate network.

However, IM applications, as well as their less-well-intentioned cousins P2P and spyware, are part of a category of applications that FaceTime terms 'greynets.' Greynets are network-enabled applications that are 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 businesses are adopting IM with increased confidence, managing this growing use is challenging for security-conscious organizations.

### Liability Risks of IM in the Enterprise

With the increased use of IM for critical real-time business communications, Compliance Officers, Security Officers, and IT managers can no longer disregard the use of IM. They 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 download and use freely available public IM clients and P2P applications. Implementing a comprehensive IM management solution is a necessity.

Organizations in financial services, healthcare, and other industries must comply with federal, state, and industry-specific regulations that require all correspondence—including electronic communications such as email and IM—be captured and stored for auditing purposes. Rules such as SEC17a-3 and 17a-4, NASD 3010 and Sarbanes-Oxley Act, HIPAA and others define these regulations.



Granular permissions and monitoring controls



Full visibility into IM usage and policy violations



## A Proven Solution

IMAuditor provides the most mature and wide-ranging security and compliance management solution for IM applications available today, supporting PIM, EIM applications as well as professional community networks and Web conferencing applications. It's backed by FaceTime Security Labs, the industry's largest greynet research team. IMAuditor, in conjunction with FaceTime's Real-Time Guardian, is the only provider of TrueCompliance™, offering full compliance with federal and industry regulations through multi-layered policy-based access control, monitoring, and management of these applications.

IMAuditor offers comprehensive protection against worms, viruses, spyware, and other inbound threats to close the zero-day gap. Support is provided for virus scanning using existing anti-virus tools, and patent-pending anti-SpIM keeps IM networks free of bandwidth-hogging spam. Intelligent, granular content filtering and archiving/logging of all electronic conversations ensures an audit trail for information leak prevention.

FaceTime solutions are deployed in eight of the largest ten banks in North America, and the company offers the only certified scalable enterprise IM solution that supports deployments in excess of 2M seats. IDC has named the company its #1 vendor of IM security solutions for two consecutive years.

## IMAUDITOR FEATURES

### Security

- Block Zero-Day IM-based worm and virus attacks
- Block SpIM using a combination of allow/block lists, rich content filtering and patent-pending challenge-response
- Automatic protection against IM and P2P threats identified by FaceTime Security Labs
- Block file transfers, or allow file transfers with imposed file size limits
- Prevent IP address exposure by blocking direct IM client-to-client connections
- Scan transferred files using leading anti-virus engines, without incurring additional cost
- 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

- 100% guaranteed, accurate binary archiving of all IM use, 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 IM 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

- Seamlessly integrate 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 IM services
- Associate employees ID in the corporate directory with IM buddy names
- Unique support for AOL Identity Services (including secure Local Authentication) and MSN Connect allows businesses to own corporate domain name use in buddy names and match buddy names to company directory
- Real-time enforcement of policy changes
- Real-time usage reports and graphical monitoring of statistics
- Intuitive Web-based access to configuration functions by authorized personnel

### Extension and Integration

- Interfaces with existing anti-virus, firewalls and proxies
- 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
- True multi-tenancy, with hosting management through common infrastructure and delegated administration
- Multi-language support
- Fail-over with load-balance among redundant/stand-by directory servers, database servers and corporate proxy servers

### Supported Applications

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

