

### About FaceTime Enterprise Edition

FaceTime Enterprise Edition is a comprehensive solution for the security, management and compliance of real-time communications, consisting of user policy management, message hygiene, spyware prevention, archiving for compliance, blocking unauthorized usage, and protecting the network against sophisticated user workarounds.

### KEY FEATURES

- Enable, secure and manage the use of public and enterprise IM applications
- Ensure safe use of Web conferencing and other real-time chat applications
- Automatic protection against threats identified by FaceTime Security Labs
- Identity management with policy control at global, group and individual employee levels
- Guaranteed TrueCompliance™ to meet corporate policies and government regulations
- Zero-Day blocking of IM-based worm and virus attacks
- Anti-SpIM controls to reduce spread of worms and malware
- Advanced content filtering and keyword blocking to prevent loss of confidential information
- Targeted remediation and inoculation of spyware-infected endpoints without deploying client software

FaceTime Enterprise Edition is the leading solution used by the world's largest firms to secure and manage real-time communications and ensure that the use of instant messaging and other tools complies with corporate policy and government regulations.

### Real-time Communications in the Enterprise

Instant messaging (IM), Web conferencing and other real-time communication and collaboration tools have become requirements for strategic and competitive advantage in today's real-time enterprises. The productivity benefits reaped from the use of these tools have dramatically expanded the use of IM, peer to peer (P2P) file sharing and Voice over IP (VoIP) for many organizations. According to IDC, more than 28 million business users today use IM to send nearly 1 billion messages each day at work, making it the fastest-growing communication system ever.

IM and Web conferencing programs, 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 (or frequently the user) and are largely invisible to the existing security infrastructure.

### An Emerging Security and Management Challenge

Because greynet applications tend to operate below the security radar, their widespread and uncontrolled use brings with it new risks for malware infection, loss of intellectual property, falling out of compliance with government regulations and more. While some greynets, such as IM and Web conferencing, have significant business value, others can pose serious security risks. However all need to be controlled and managed according to policy set by the enterprise.

Managing the use of greynet applications in business is a major compliance and security concern for information security, human resources, and legal department personnel. Its prevalence and convenience as a business tool must be balanced by the requirement of certain regulations, such as SEC 17a-3 and 17a-4, NASD 3010/3110, HIPAA, Sarbanes-Oxley, FISMA, and others, to enforce policies and retain reviewable customer records and transaction data.

### FaceTime Enterprise Edition

FaceTime Enterprise Edition provides the most mature security, control and compliance management solution for real-time communication applications available today, supporting public and enterprise IM applications, WebEx web conferencing, P2P networks such as Skype, and professional community networks such as Reuters. It's backed by FaceTime Security Labs, the industry's largest greynet research team, providing total threat protection coming over these new channels of communication.

FaceTime Enterprise Edition is the only provider of TrueCompliance™, offering full compliance with federal and industry regulations through multi-layered policy-based access control, monitoring, authentication and management of real-time communications. Through its defense-in-depth architecture, it offers comprehensive protection against worms, viruses, SpIM and other inbound threats, and targets existing spyware installations with patent-pending Targeted Remediation to clean and inoculate infected endpoints. 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.

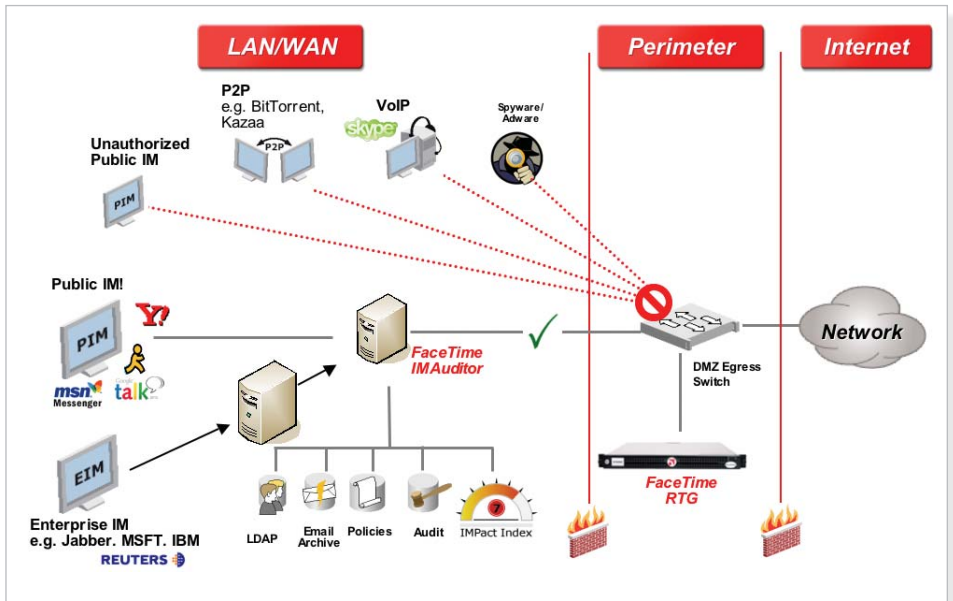
Used by eleven of the top fifteen US banks and seventeen of twenty-four top FIMA banks, FaceTime Enterprise Edition incorporates the award-winning IMAuditor™ and Real-Time Guardian™ applications. FaceTime Enterprise Edition was awarded Best Buy in SC Magazine September 2005 issue and in February 2006 received the SC Magazine 2006 Reader Trust Award for Best IM Security.



## KEY BENEFITS

- Single solution to secure, manage and control usage policy for major public and enterprise instant messaging, web conferencing and professional community networks
- Secure and enable the safe use of real-time communication applications
- Prevent spyware with targeted remediation and inoculation of infected endpoints
- Avoid loss in productivity from inbound threats and content leakage from outbound threats from these new channels of communication
- Meet corporate policies and government regulatory requirements
- Minimize IT administration costs with flexible deployment and enhanced management features

FaceTime Enterprise Edition brings together the benefits of IMAuditor and RTGuardian to deliver a fully-integrated solution to the problem of security, management and compliance for greynet applications.



## FACETIME ENTERPRISE EDITION FEATURES

### Security

- Creates a standardized profile for public and enterprise IM use
- Distinguishes between authorized and unauthorized IM connections
- Blocks potential infections by SpIM through a combination of rich content filtering mechanism and challenge/response algorithm
- Zero-day blocking of IM-based worm and virus attacks
- Automatic protection against new and emerging threats identified by FaceTime Security Labs
- Delivers targeted remediation of spyware-infected endpoints without client software deployment
- Sets granular level user policies for the transfer of files over IM
- Scans file transfers using existing anti-virus applications
- Blocks unauthorized P2P and VoIP applications

### Management and Control

- Provides visibility and insight into real-time communications throughout the distributed enterprise
- Control IM capabilities at global, group, and individual employee levels
- Automatically associate employees' email addresses with IM buddy names
- Real-time enforcement of policy changes
- Real-time usage reports, inter-group reports and graphical monitoring of statistics
- Web-based access to configuration functions by authorized personnel

### Compliance

- 100% auditing across major public and enterprise IM, web conferencing and professional community networks
- TrueCompliance™ blocks attempts to circumvent established compliance workflow
- Automatic display of customizable legal disclaimers
- Blocks messages depending on severity of breach, with real-time alerts
- Prevents data tampering by assuring exported conversations match recorded conversations at the level of time-stamped messages
- Stores messages in binary and text format in the order they appear for content accuracy
- Ensures authorized communications between groups use "Chinese Walls"
- Establishes compliance workflow with custom search queries for tracking and managing review of conversational content

### Ease of Deployment and Operations

- Flexible OS and DB platform-neutral deployment architecture in the LAN
- Co-exists with standard IT infrastructure, such as firewalls, load balancers, email systems, and proxy servers
- Load-balances among redundant directory, database and corporate proxy servers
- Plug-and-play deployment at network perimeter with purpose-built hardened configuration
- Automated protocol and threat protection updates

### Enterprise-grade Solution

- Cost-effective support for complex, distributed data centers
- Multi-language support
- Manage and extend IM into other corporate applications through published APIs and SDKs
- Multi-tenancy capability

### Supported Applications

- Enterprise Instant Messaging: Microsoft LCS, IBM 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, Microsoft Windows 2003 Server, or Linux
- Microsoft SQL Server 2000

### Hardware Requirements:

- Pentium IV 2 GHz CPU or higher recommended
- 1GB RAM
- 30GB available hard disk space