

KEY BENEFITS

- Enforce standardization on LCS by blocking access to unauthorized IM and P2P networks
- Mitigate security risk by blocking file transfers and scanning files using existing anti-virus software
- Prevent spread of viruses and malware by automatically blocking SpIM
- Block spyware at the Internet gateway and enable targeted remediation of infected desktops
- Block “Day-Zero” IM-based worm and virus attacks
- Receive automatic protection against IM and P2P threats identified by FaceTime Security Labs
- Simplify regulatory and corporate compliance monitoring through sophisticated workflow and reports
- Preserve investment in existing compliance systems by seamlessly integrating with a wide variety of e-mail and WORM storage systems
- Minimize IT administration burden with ease and flexibility of enterprise deployments and enhanced management features
- Archive file transfers over LCS into WORM storage
- Increase reliability of IM security with high availability and load balancing

“Dedicated IM hygiene products are the best way to protect and manage IM usage.”

- Gartner, 2006



FaceTime Enterprise Edition for Microsoft Office Live Communications Server (LCS) is used by the world's largest firms to secure and manage real-time communications and ensure that the use of instant messaging and other real-time communication applications comply with corporate security policies and government regulations.

Challenges of Enterprise Instant Messaging

Microsoft LCS provides a real-time communications platform for corporate communication, such as IM, presence, application sharing, collaboration, voice and video. The benefits of Microsoft LCS have dramatically expanded the use of IM, peer to peer (P2P) file sharing and voice over IP (VoIP) applications in the enterprise. Enterprise Instant Messaging (EIM) products are moving rapidly towards becoming unified communication and collaboration platforms integrating a wide range of real-time communications tools, and enabling federation with Public IM (PIM) services and industry focused IM communications.

However, the increased use of real-time communications in the enterprise today creates its own set of challenges:

- Increases exposure to malware over IM with federation;
- Opens channels for information leakage with use of unauthorized IM/P2P applications;
- Lowers return on investment in EIM when it is not secured and managed.

Risks of IM and P2P in the Enterprise

Implementation of LCS often leads employees to believe that all IM use is sanctioned and the dangerous practice of downloading and using freely available consumer IM clients and P2P file sharing applications continues. This unauthorized IM and P2P use can introduce viruses, worms and other security threats to the network, and put organizations at risk of non-compliance.

In addition to technical security issues, organizations also face business risks from disclosure of intellectual property, confidential information leakage, and copyright infringement from illegal file sharing. Increasingly, industry watchdog organizations are targeting corporations for illegal file swapping and copyright infringement and the economic impact, as well as the public relations fall-out, can be significant.

Many public organizations must also comply with detailed regulations requiring all correspondence—including electronic communications—between employees and clients to be captured and stored for auditing purposes.

About FaceTime Enterprise Edition

More organizations choose FaceTime Enterprise Edition as an essential complement to Microsoft Office Live Communications Server deployments because it provides:

- Standardization on LCS by blocking unauthorized public IM & P2P connections;
- Enterprise-wide security, management, and control of all IM traffic;
- Day zero worm protection and SpIM blocking.
- Gateway spyware prevention and targeted remediation;
- Real-time content filtering and keyword matching to prevent disclosure of proprietary information;
- Compliance with corporate policy and government regulations;
- Enhanced IM management functions and reporting tools beyond those provided by LCS;
- Enterprise-class performance, scalability, and flexibility.

KEY FEATURES

Security

- Enforce standardization by blocking all attempts to circumvent the IT policy of using only the sanctioned LCS 2005 IM client
- Blocks SpIM using a combination of allow/block lists, rich content filtering mechanism and patent-pending challenge/response
- Block day-zero worm and virus attacks using real-time communications channels
- Continuous protection against greynet threats identified by FaceTime Security Labs
- Scans file transfers, using existing anti-virus tools
- Delivers targeted remediation of spyware-infected endpoints without client software deployment
- Sets granular level user policies for file transfers over IM
- Blocks unauthorized P2P and VoIP applications

Compliance and HR

- 100% auditing across major public and enterprise IM, web conferencing and professional community networks
- Achieve 100% accurate binary archiving across all IM usage in the enterprise, including user sign-on/off history and multi-party chat participation history
- File transfer archival support to WORM storage
- TrueCompliance™ blocks attempts to circumvent established compliance workflow
- Automatic display of customizable legal disclaimers to all parties involved in the IM conversation informing them that LCS is a corporate not a personal messaging system
- 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

- Enforce ethical rules in real-time by configuring "Chinese Wall" policies to restrict inter-group contact and using "Hair Pinning" to restrict inter-organization contact
- Establishes compliance workflow with custom search queries for tracking and managing review of conversational content
- 360-degree audit: Audit all users (end users, system administrators, content reviewers) - in addition to capturing IM traffic

Management and Control

- Hierarchical view of enterprise to provide rich policy management at global, group and individual employee levels
- Fine grained control of LCS 2005 client capabilities including the ability to manage file transfer, collaboration (e.g., audio/video conferencing, VoIP, games), and other client privileges at the company, group, and user levels of granularity
- Provides visibility and insight into real-time communications throughout the distributed enterprise
- Controls IM capabilities at global, group, and individual employee levels
- Real-time enforcement of policy changes
- Real-time usage reports, inter-group reports and graphical monitoring of statistics
- Secure, intuitive Web-based access to configuration functions by authorized personnel

Enterprise-Grade 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/standby 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

- Ease and flexibility of enterprise deployment means minimal IT administration
- Cost-effective support of global scaling for complex distributed data centers
- Support for multiple languages
- High level of fault-tolerance provides support for normal operations in the unlikely event of a critical infrastructure resource failure
- Maximize IT and compliance productivity with intuitive Web-based administration and reporting

Software Requirements

- Microsoft Windows 2000 Server or Windows 2003 Server
- Microsoft SQL Server 2000

Hardware Requirements

- Pentium 4 2 GHz CPU or higher recommended
- 1 GB of RAM
- 30 GB Available Hard Disk Space