

Security and Compliance for Microsoft Solutions

KEY BENEFITS

FaceTime Enterprise Edition for Microsoft Office Live Communications Server (LCS) is used by the world's largest firms to secure, manage and ensure that the use of instant messaging and other real-time communication applications comply with corporate security policies and government regulations. More organizations choose FaceTime Enterprise Edition as an essential complement to Microsoft LCS deployments because it provides:

- Standardization on LCS by blocking access to unauthorized IM and P2P networks
- Software upgrade to secure OCS deployment
- 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
- Interoperability with existing anti-virus solutions
- Zero-day blocking of IM-based worm and virus attacks
- Anti-SpIM controls protect bandwidth and close security holes
- Archival of file transfers over LCS into WORM storage
- Advanced content filtering and keyword blocking to prevent loss of confidential information
- High availability and load-balancing deployment increases security and reliability of existing real-time communications infrastructure
- Targeted remediation and inoculation of spyware-infected endpoints without deploying client software



FaceTime Enterprise Edition provides organizations with the tools to standardize their instant messaging (IM) infrastructure on the Microsoft LCS unified communications (UC) platform while ensuring compliance and securing their environment against IM-borne malware and spam over IM.

Real-time Communications in the Enterprise

Instant messaging (IM) and other real-time communications protocols are a fact of life in today's enterprise, as evidenced by the rapid adoption of unified communications (UC) platforms; industry analysts expect Enterprise IM to reach 100% adoption by 2010.

IM, web conferencing, and other real-time UC tools have become requirements for strategic and competitive advantage in today's real-time enterprise. Despite widespread access to enterprise-ready IM networks such as LCS and regardless of corporate policy, users continue to communicate through public IM networks such as Yahoo and MSN. Unfortunately, IM, both public and enterprise, is increasingly becoming the threat vector of choice for malware attacks; add client-side code vulnerabilities and the potential for intellectual property loss, compliance breach and identity theft, and it is clear that IM channels are a major risk factor for existing security, policies and infrastructures. Additional security requirements arise when the edge of the corporate network effectively moves out into the broader community of trading partners through the UC environments.

Specific challenges

Enterprises are faced with a number of key discrete challenges in managing the use of IM in a unified communications environment:

- Collaborative environments such as Microsoft LCS are increasingly targeted by malware, with blended threats (viruses, worms, spyware, and more) hopping from public to enterprise network—federation with public IM networks and partners only adds to the risk.
- Not only are more attacks entering the network over IM than email, but the attacks themselves are becoming more damaging. Crimeware, rootkits, exploits, and other malware are designed to bypass traditional security measures, and the IM channel only makes that task easier.
- Just as malware is moving to the real-time communications platform to bypass existing security measures, spam is moving beyond the email inbox into the IM stream, further increasing the risk of accidental malware introduction as well as increasing the traffic load.
- Compliance regulations, including eDiscovery, largely apply to IM conversations and chat threads just as they do to email records. Enterprises must be able to “connect the dots” for all types of electronic communications, particularly when the installation spans multiple sites.
- In the same way that malware can hop across peer-to-peer connections unchallenged, proprietary information can be transferred, redirected, or hijacked both inside and outside the company networks using unmonitored IM channels.
- Communications that can't be seen can't be monitored. Unverified identities such as “buddy names” prevent appropriate corporate policies from being applied to public IM communications, and the ort-hopping behavior exhibited by these applications renders simple blocking controls unusable.

“As IM traffic becomes increasingly higher in volume and potentially higher in value, organizations will need to adopt ‘enterprise class’ IM technologies as well as IM hygiene services to ensure efficient, integrated, reliable and secure use of IM technologies.”

— Gartner: Business Use of Instant Messaging

KEY BENEFITS

- Single solution to secure, manage and control the use of instant messaging, web conferencing, VoIP, and other LCS communications tools
- Leverage existing investment in LCS and anti-virus to apply the same high level of security and compliance across all real-time communications channels
- Prevent spyware with targeted remediation and inoculation of infected endpoints
- Minimize administration overhead with flexible deployment and enhanced management capabilities
- Mature, proven solution backed by world class research and used by leading corporations around the world

FaceTime Enterprise Edition brings together the benefits of IMAuditor and RTGuardian to deliver the first fully-integrated solution to unified security, management and compliance for Microsoft LCS.

Security

- Enforce standardization by blocking all attempts to circumvent policies to use only LCS 2005 communications channels
- Block SpIM using a combination of allow/block lists, rich content filtering mechanism and patent-pending challenge/response
- Block zero-day worm and virus attacks using LCS communications channels
- Continuous protection against malware threats identified by FaceTime Security Labs
- Scan file transfers over real-time channels using existing antivirus tools
- Symantec, McAfee, TrendMicro, CA, ClamAV, Kaspersky, Sophos
- Granular level content leakage control policies for file transfers over IM
- Targeted remediation of spyware-infected endpoints without client software deployment
- Blocks unauthorized P2P and VoIP applications
- Manage web access through dual filters:
 - FaceTime WebFilter with over 21 million sites in 54 predefined categories
 - Secure Computing SmartFilter with over 7 million URLs in 73 predefined categories

Compliance

- Full auditing across major public and enterprise IM, web conferencing and professional community networks
- 360-degree audit of all users (end users, system administrators, content reviewers) in addition to IM traffic
- 100% accurate binary archiving across all IM usage in the enterprise, including user sign-on/off history and multiparty 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 messaging system
- Block messages depending on severity of breach, with real-time alerts
- Data tampering prevented by assuring exported conversations match recorded conversations at the time-stamped message level
- Store 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
- Establish compliance workflow with custom search queries for tracking and managing review of conversational content

Management and Control

- Hierarchical view provides rich policy management at global, group and individual employee levels
- Fine grained control of LCS 2005 client capabilities includes the ability to manage file transfer, collaboration, and other client privileges at the company, group, and user levels of granularity
- Integration with Active Directory to enforce web access policies at user and group levels using single sign-on for end users
- Visibility and insight into real-time communications throughout the distributed enterprise
- Control 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