

Ensure Security and Compliance for Microsoft Unified Communications

Why Microsoft UC customers and prospects should purchase FaceTime:

- Enforces standardisation on authorised real-time communications channels to maximize investment
- Reinforces and strengthens existing UC security and oversight controls to enable administrators to effectively monitor and secure real-time communications
- Ensures data protection and e-Discovery compliance requirements are met for the full range of electronic communications

How FaceTime benefits Microsoft

Incorporating FaceTime accelerates adoption timetables and allows additional UC components to be incorporated sooner. Organisations will only implement the full Microsoft UC platform once they have adequately secured the basic IM and presence awareness functions. FaceTime solutions also drive additional consulting and implementation professional services revenues.

Key verticals

Financial Services, Utilities, Banking, Insurance, Government, Telecommunications, Transport, Legal Services, Retail, Healthcare, Pharmaceuticals.

Installed base

900 organisations with 2.6 million users around the world.



What's the challenge?

Despite the availability of enterprise-class instant messaging on the desktop through collaborative environments such as Microsoft Live Communications Server (LCS) and its successor, Office Communications Server (OCS), users continue to make use of public IM networks. MSN, Skype VoIP, and other peer-to-peer channels - collectively known as greynets - are widely deployed throughout enterprises today, and their use is growing.

These greynets are vectors for malware, client-side code vulnerabilities, intellectual property loss, and identity theft, challenging existing security, policies and infrastructures. When users access these unmanaged greynets, they're using identities that can't be verified, so authentication and content filtering policies can't be applied to any information - conversation or files - traversing that channel. Public IM network connections port-hop for the next available connection, so firewalls can't see what connections are being made and anti-malware can't check the traffic stream for malicious code.

Greynets are also increasingly falling victim to new variants of traditional malware, with blended threats hopping from public network to enterprise network - exposure that is increased by federation with public IM networks and partners. The edge of the corporate network is moving outwards at high speed, but security and oversight controls are not keeping pace.

Compliance issues

Compliance regulations for data protection, archival, and retrieval largely apply in the same way to IM conversations and chat threads as they do to email records. Microsoft UC administrators therefore need to be able to "connect the dots" for all types of electronic communications under the same umbrella, particularly when the installation spans multiple sites. Ideally, administrators should be able to leverage their existing investments in security, policy management, and data storage to ensure the secure, productive use of all real-time communications.

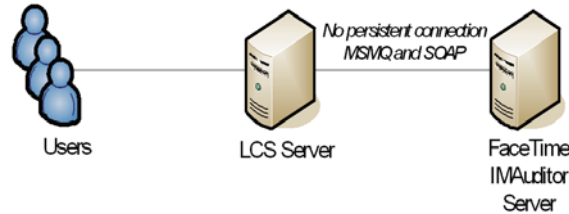
Key benefits of protecting Microsoft UC investments with FaceTime:

- Ensure all IM communications go through secured, authorised Microsoft channels
- Prevent malware from infecting the enterprise through real-time channels
- Files transferred over IM are scanned automatically with existing anti-virus infrastructure
- Highly granular real-time content filtering prevents information leakage
- Automatic malware and communication protocol updates protect against zero-day threats
- Group-level ethical boundaries prevent unsanctioned information sharing in real time
- Tamper-proof storage of chat threads ensures accurate compliance records
- Flexible file transfer capture and archival for ease of e-Discovery storage and retrieval
- Clearly-visible disclaimers discourage unauthorized use of business channels
- Leverage existing SQL database resources for storage of all real-time communications

Regardless of complexity or number of individual clients, FaceTime solutions accurately and completely log all real-time communications, including file transfers and events such as message blocking, to ensure compliance with corporate governance, data protection, and e-Discovery regulations. The actual files transferred are stored with the relevant messages, simplifying the review process and ensuring that all communications are seen in the context of a complete conversation, with accurate message order preserved.

Engagement strategy

Engage with FaceTime when prospects are considering, or have deployed, a Microsoft UC platform. FaceTime's RTGuardian gateway appliance not only ensures standardisation on Microsoft UC by blocking access of all unauthorised IM and VoIP use, but provides justification for the UC investment. IMAuditor provides additional security and control for native Microsoft functionality:



Function	Microsoft LCS	Microsoft OCS	FaceTime additional benefits
Authentication & Authorisation Services	Allow/block at company and user levels only	Allow/block access at company, group, and user levels	Policies at company, group, user levels: Group level ethical boundaries; IP-Address based access controls; Access controls and monitoring options
File transfer management	Allow/block at company and user levels only	Granular file transfer settings at company level only	Policies at company, group, user levels: Allow/block at all levels; Specify rules for file name/size/ type. Can detect and block words, phrases, and full regular expressions and flag/block and/or alert based on content
Anti-virus and malware control, including bots spreading over IM	Antigen for IM	No controls (Antigen for IM will not ship for OCS at launch)	Support for Symantec, McAfee, TrendMicro, CA, ClamAV; Sophos; Kaspersky. Greynet database protection. Zero-day worm blocking
SpIM blocking	Blocks messages from non-LCS clients	Enhanced presence can filter on presence information	Content-based protection using white/black lists and custom rules
URL blocking	Inflexible: blocks all messages containing URLs	URL rewrite to remove hyperlink and/or add warning	Domain-configurable and direction-configurable URL policies
Federation	Allow/block at company level and user level only	Allow/block at company and user levels only	Allow/block permissions at company, group and user levels; Ability to specify explicit partner domain-based rules at company, group, and user levels
Unsanctioned IM (including tunneled IM) usage controls	No solution for user circumvention	No solution for user circumvention	RTGuardian detects and blocks more than 40 IM protocols and 65 P2P protocols
Legal disclaimer notification	Disclaimers presented only to external users in federated/PIC scenarios	Disclaimers presented only to external users in federated/PIC scenarios	Disclaimers sent inline and audited; disclaimer display controls at the IM network and group levels
Tamper detection	No tamper proofing or detection mechanism	No tamper detection mechanism	Guaranteed message order preservation; anti-tamper mechanism validates conversation integrity
File transfer capture	Captures names of transferred files only, not actual files	Captures names of transferred files only, not actual files	Files archived in database and shown in context in conversation review
E-discovery retrieval	Not supported	Messages sent to logging database, but no search interface	Reports on IM usage, security violations, compliance violations, transcript reviews. Report generation, scheduling and delivery

FaceTime Benefit Overview:

FaceTime enables enterprises to standardise their IM infrastructure and maximize their investment in UC while securing it against IM-borne threats such as infected file transfers and spam over IM (SpIM). Granular filtering and flexible archival ensure enterprises are able to meet compliance requirements for data protection and e-Discovery across all electronic communications channels.

FaceTime Enterprise Edition for Microsoft UC combines IMAuditor™ in the LAN with Real-Time Guardian™ at the gateway for complete, end-to-end security, management, and compliance. IMAuditor secures and manages all Microsoft and other allowed IM traffic and maintains an integrated trust relationship with Real-Time Guardian, which blocks all IM traffic not specifically allowed and protects against circumvention of policies.

FaceTime is a Managed ISV Microsoft partner, a ranking achieved by less than 1% of Microsoft ISVs and one of only ten vendors participating in the official OCS launch. Close cooperation between the two companies ensures smooth deployment and integration of FaceTime solutions into Microsoft network infrastructures.

Reference Customer Deployments of Microsoft LCS with FaceTime

INDUSTRY: Retail
ORGANISATION: Broadline retailer
REQUIREMENT: Compliance
IT USERS: 300,000+

This organisation was rolling out Microsoft LCS. As part of the rollout, they had to meet legal requirements for archival and quick and easy retrieval of messages for e-Discovery purposes. FaceTime was deployed to ensure these requirements could be met within the LCS environment.

INDUSTRY: Air freight service
ORGANISATION: Supply chain management
REQUIREMENT: Policy management
IT USERS: 12,500

This organisation had deployed Microsoft LCS and was concerned that users would circumvent the LCS infrastructure with unsecured communications. FaceTime was deployed to ensure all real-time communications were directed through authorised LCS channels.



FaceTime Communications Europe Ltd

+44 (0) 1908 561 659 EMEA

Info: emea@facetime.com

EMEA VP: nsears@facetime.com EMEA Partner Relations: scarter@facetime.com www.facetime.com

QRC 0807 MS LCS