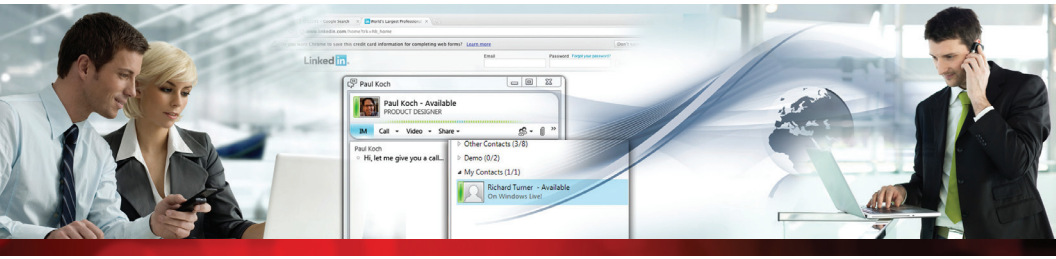
actiance™

Upgrading from Microsoft OCS to Lync

The Ideal Time to Address Your Social Business Needs



Executive Summary

Microsoft Unified Communications (UC) users are migrating from Office Communications Server (OCS) to Microsoft Lync to take advantage of the many new features incorporated into Lync, especially new voice features such as support for common area phones, enhanced emergency service (E-911), new VoIP support that makes Lync a suitable replacement for PBX, and new voice features for select public instant messaging platforms. Where Microsoft OCS delivered federation for different consumer UC platforms so users could connect in real-time using instant messaging and chat, Microsoft Lync adds Public IM Connectivity (PIC), giving users integrated voice with public instant messaging (IM) platforms such as Live Messenger which now supports more than 300 million users. Microsoft's acquisition of Skype, which now boasts about 700 million users, promises to extend Lync access even further.

At the same time, enterprises are seeing a growth in other social media applications. LinkedIn now has more than 160 million users, making it one of the most valuable online destinations for business research and contacts, and something that IT managers need to be concerned about as part of their UC strategy. Similarly, Facebook now has more than 900 million users and continues to gain momentum with business users as well as consumers, and soon you will be able to send messages and even initiate voice contact and even Skype video chat from within the Facebook environment.

With enhanced PIC support with Live Messenger and other clients, the promise of Skype integration and social media access, Lync users now have the potential to connect to more than one billion consumers with a single mouse click. These advances make Lync UC more valuable to corporations, putting sales in real-time contact with potential customers, enhancing support for existing customers, enabling hiring managers to contact prospects and work with new hires, and allowing marketing to engage with prospects in a new way. As UC value and access expands beyond the enterprise to embrace public networks, so do the concerns over managing access for security and compliance.

As enterprises deploy Lync to take advantage of richer communications with public IM networks and UC clients, it creates a need for more robust security. Migration from Microsoft OCS to Lync is the ideal time to assess the security of your unified communications, especially as it relates to an open federation strategy and access to public networks. This white paper will discuss potential weaknesses in enterprise security and compliance that can accompany Lync migration and federation and will offer some strategies to address those weaknesses.

The Case for Lync Migration and UC Federation

Organizations looking to hone their competitive edge are relying more on Unified Communications (UC) to support collaboration both within their enterprise networks and through UC federation. Migrating to Lync offers an even richer communications experience with greater productivity and cost savings thanks to new and enhanced UC features. Deploying UC enables real-time communication using instant messaging/chat, group conferencing, file transfer, whiteboard applications, mobile conferencing, and voice and video.

As an organization begins to benefit from UC, the circle of real-time collaboration typically expands to encompass additional UC platforms, such as Microsoft OCS or Lync, IBM Sametime, and Cisco Unified Communications Manager. UC federation extends to both private and public UC platforms to make it easier to communicate with partners, suppliers, customers, and third parties. According to the latest sixth annual research report produced by Actiance, "The Collaborative Internet: Usage Trends, End User Attitudes & IT Impact," organizations that have chosen to federate their UC platforms are doing so with business partners (66%), customers (46%) and IT vendors (45%), as shown in Figure 1.

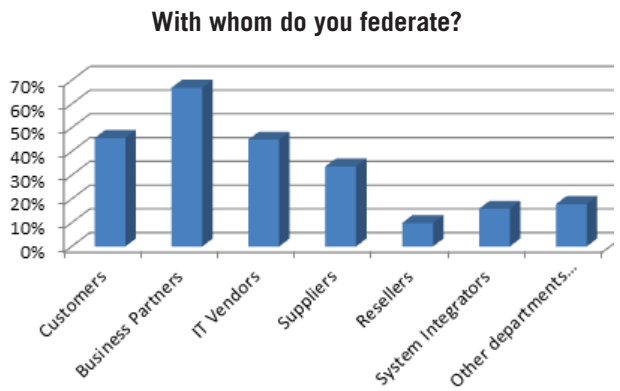


Figure 1. Corporate Usage of UC Federation for Realtime Collaboration

Lync 2010 and recent add-ons such as Microsoft XMPP Gateway and third-party federation products such as NextPlane offer more integration and more connectivity options to accommodate federation and integration with public IM and UC platforms. What makes Lync 2010 attractive to many users is enhanced support for integrated voice communications. Microsoft is promoting Lync 2010 as the UC solution that works across platforms and devices, encompassing PC, Macintosh, browsers, mobile platforms, and even desk phones so users can make the same voice-over-IP (VoIP) calls from their phone or workstation. Lync also enables integrated conferencing services so workstation users have full audio, video, and web conferencing.

Lync also can interoperate with PSN, SIP trunks, and PBXs from vendors such as Cisco, Siemens, Avaya, and Mitel so Lync can deliver real savings to PBX users. Centralizing administration of a few centrally located Lync pools for VoIP versus managing individual PBX systems in each branch office makes it possible to leverage SIP trunking, which is much less expensive than legacy PSTN T1/E1 links. And Lync has the added advantages of providing a common platform for email, IM, voice, video, application sharing, and conferencing.

A recent report in *IT Knowledge Exchange* indicated that:

"Sprint has saved $2.5 million in avoidance of PBX upgrade costs, $6.7 million in recurring circuit costs and $4 million in cost avoidance for conferencing since the installation of Lync. The company has even been able to earn some green savings – $700,000 annually because it doesn't have to power and cool old PBXs anymore."

Lync mobile clients also extend telecommunications support further to handheld devices such as Windows Phone, Apple's iPhone, the Android, and Nokia mobile devices.

And Lync 2010 features much more robust support for public IM connectivity, providing interoperability with AOL Instant Messenger (AIM), .NET Messenger Service, Live Messenger, Yahoo! Messenger, and Google Talk. By design, Lync breaks down the barriers between enterprise and public communications, making it as easy to connect with external IM users as it is to chat with contacts within the enterprise. And Lync Server has an Extensible Messaging and Presence Protocol (XMPP) gateway that can federate with external XMPP servers such as Google Talk and Jabber.

And there is the promise of Skype. Microsoft has committed to extend Lync support for Skype. Microsoft has not disclosed how tightly it will integrate Lync and Skype, but it seems likely integration will be on a par with Live Messenger. Full integration with Skype would extend the reach for Lync users worldwide. Integration with Skype also would clearly give Lync users ready access to almost anyone they need to connect with immediately.

The good news is that all these new Lync 2010 capabilities deliver a richer UC experience and promote seamless connectivity to platforms and partners beyond the enterprise. The bad news is that this same seamless connectivity opens new channels for a potential malware attack or data leaks. The technology that enables creation of an open UC platform to promote better real-time communications is the same technology that creates new vulnerabilities. The challenge facing IT management is finding the right solutions to manage this new open UC infrastructure, to promote better security against malware from an unmanaged or public source, and to filter and archive all the UC data traffic for regulatory compliance.

Considerations for UC and Federation Security

Lync was designed to provide a rich, easy-to-use unified communications experience, and federating Lync with partner, suppliers, customers, and public networks is where users realize more productivity and achieve real ROI from their Lync investment. Enterprise infrastructures tend to standardize on a single UC system and then recoup their investment by adding other UC platforms for specialty applications (e.g., public IM systems, VoIP, and Web 2.0 applications). And with the enhancements in Lync 2010, that list now includes more public IM and communications platforms.

According to Actiance's research report, there has been a significant spike in corporate UC adoption. According to the 2011 survey, 63% of respondents have a UC platform deployed in 2011, compared with 34% in 2009 and 29% in 2008 (see Figure 2). And many of these UC systems are rapidly extending their reach outside the enterprise through federation with other private and public UC infrastructures.

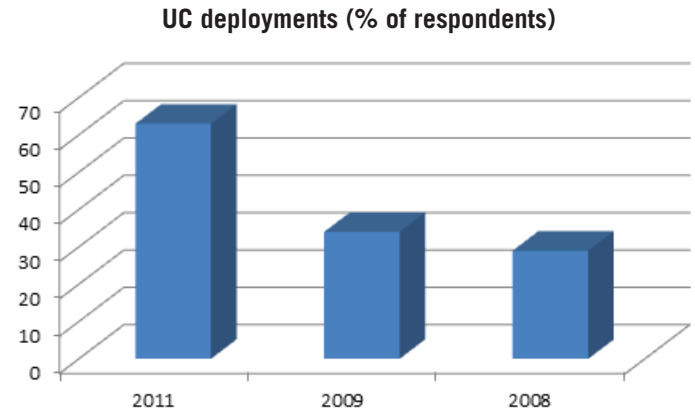


Figure 2. Increase in UC deployment for Corporations

Federating multiple UC platforms to create an open communications architecture is good for business and challenging for network administration. Organizations are susceptible to both inbound threats from viruses, malware, and phishing attacks and outbound threats from data breaches and inappropriate use of federated UC links. With greater connectivity to outside platforms comes greater risk, particularly from public and uncontrolled network sources.

According to Irwin Lazar, vice president for communications and collaboration research at Nemertes Research, most enterprise users see UC and VoIP as closed systems and therefore not subject to attacks. However, new trends in SIP trunking, cloud adoption, and employee BYOD (bring your own device) are increasing the security risks for UC platforms. In a recent article published in Search Unified Communications, Lazar writes:

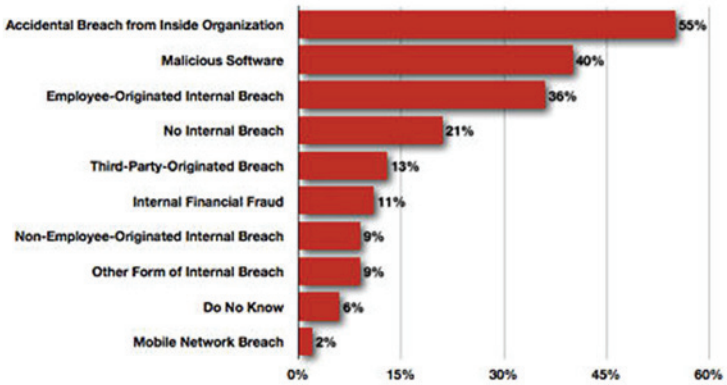
"IT managers can no longer afford to hide behind the PSTN-as-a-fire-break approach to UC security. In order to minimize the risk of data loss or service disruption, it's important to have a proactive strategy that addresses emerging security threats, integrates UC security with the broader overall enterprise security architecture, and leverages specific tools and/or services to mitigate threats from SIP trunking, cloud services and mobile devices."

Increased use in social media platforms for business is stretching IP security even further. There are several reasons for businesses to leverage social media. For example, new survey from CareerBuilder shows that 37 percent of businesses are using social media to research job candidates. According to Actiance research, social media use is found in 100 percent of the organizations surveyed, and more than 90 percent of users reported maintaining profiles on one or more social networks. What's more, 66 percent said they log into their social media site at least once a day, and 20 percent log in from their work location. The same survey shows that 79 percent of respondents indicated their organization maintains a corporate Facebook web page, 61 percent are on LinkedIn, 61 percent are on Twitter, and 46 percent are on YouTube.

However, training users to be safe online is an ongoing challenge. Employees are bringing their bad home computing habits to the office. In a culture increasingly dominated by photo and file sharing and open online conversation, it's no wonder that employees put corporate data and intellectual property at increasing risk from data leaks and malware. According to a report by Deloitte-NASCIO, among state workers, 55 percent of data breaches were accidentally generated from within the organization, and 40 percent were due to malware (see Figure 3).

Sources of Internal Breaches of State Networks

Accidental acts by employees and malicious software caused the greatest number of internal breaches with state organizations and more than 20% of state CIOs say they have had no internal breaches.



Source: 2010 Deloitte-NASCIO Cybersecurity Study

Figure 3. Sources of security breaches

The cost of the damage from data leaks, whether inadvertent or malicious, continues to rise. Recent research from PGP Corporation and the Ponemon Institute released in the annual "U.S. Cost of a Data Breach Study" reveals that corporations paid an average of $5.5 million per data breach last year.

And then there are the issues concerning regulatory compliance. According to Actiance's latest study, use of public networks and social media in regulated industries is on the rise (see Figure 4). Those surveyed indicated that there is a steady increase in the use of social networking in regulated industries such as banking, healthcare, energy and government. The result is a higher risk for regulated organizations that are not taking steps to secure their federated UC channels for compliance. Guidelines issued by Sarbanes-Oxley (SOX), the Financial Industry Regulatory Authority (FINRA), and the Financial Services Authority (FSA) indicate that all electronic communications, including those over enterprise UC, federated UC channels, and public UC channels, need to be preserved and archived.

What's interesting is that the same Actiance survey also found that in regulated industries, social media, collaboration tools, and UC channels are not applying the same level of compliance procedures as traditional forms of electronic communications, such as email. All electronic communications, including chat, instant messages, web conferences, social media posts, and Tweets, all fall under compliance mandates set by industry regulators. However, the research indicates that these are not being monitored or archived for regulatory compliance.

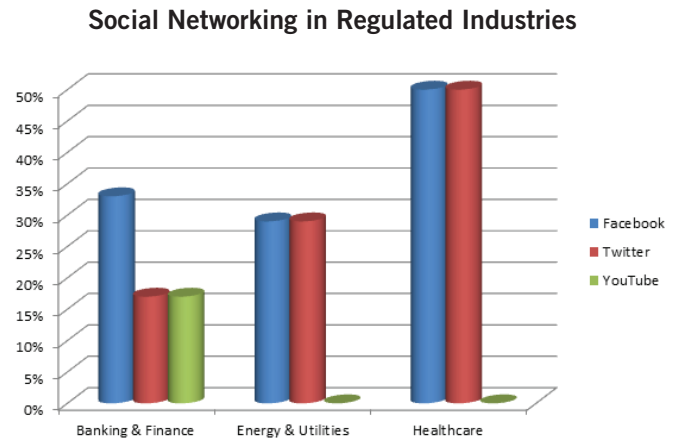


Figure 4. Use of Social Networks in Regulated Industries

Securing UC as Part of Lync Migration

New features in Microsoft Lync provide compelling reasons to expand the enterprise infrastructure and UC deployments, including federation with strategic partners and expansion to include public UC networks. The new capabilities added for voice and video over Live Messenger (and soon for Skype) as well as support for public networks means that data traffic will transit your enterprise network from any number of unmonitored sources. Now is the time to review your UC security strategy.

Security needs to be established at the enterprise perimeter to filter both inbound and outbound data traffic. We recommend a centralized approach to monitor all UC collaboration and social media/Web 2.0 content to provide granular security and policy controls over all real-time

communications traffic. This allows you to monitor conversations within the enterprise for data leaks and regulatory compliance.

Microsoft has its administrative management console, including basic support for managing Lync federation. Lync 2010 provides controls for Microsoft Lync Online users to communicate with other Lync users, including control over which domains to federate with, which domains to block, and enabling or disabling domain federation. However, you still need to monitor and archive the data traversing those federated and PIC connections.

With federation, there are more possibilities built into the infrastructure for a richer real-time communications experience. For example, now you can make audio and video calls to a Windows Live contact. You can call from a SIP-enabled handset or your desktop system, share screens, exchange files, or add other parties via VoIP or chat.

While Microsoft's management utilities make it easier to manage connections, e.g., blocking certain lines from making long-distance calls, controlling call routing and VoIP access, blocking calls from specific domains, or managing bandwidth and quality of service (QoS), you still need to manage content and access at global, group, and user levels. As part of your security strategy, you need to be able to manage Active Directory, IP, and domain-based policies as well as control VoIP, voice, IM, group chat, and data conferencing. You also need to add a solution that supports policy setting, limits file uploads, and supports data loss prevention (DLP), content filtering, and malware protection. A strong security and compliance system will enable you to apply role-based access controls and policy management across multiple UC platforms beyond Lync.

More malware is making its way into real-time communications channels, bypassing conventional antivirus and anti-malware security measures. With more access to IM public networks such as Yahoo!, AIM, Google Talk, Windows Live, and Skype, there are more potential risks from inbound threats such as malware. SpIM (spam over IM) is also becoming more prevalent in the data stream, creating new risks for federated enterprise users. Lync migration is a perfect time to fortify your UC malware protection against real-time threats. The same proliferation in the use of communications through public IM channels, either through the Lync client with PIC or directly through public IM clients, increases the risk of outbound data leaks. Unmonitored IM and UC channels can open up new channels to leak sensitive proprietary corporate information and competitive data, so data monitoring to prevent outbound leaks and threats also needs to be part of your Lync migration strategy.

Regulatory compliance also has become part of federated UC environments. There are more than 10,000 laws relating to electronic and real-time communications overseen by agencies such as the Securities and Exchange Commission (SEC), FINRA, Sarbanes-Oxley, the Federal Rules of Civil Procedure (FRCP), and the Federal Energy Regulatory Commission (FERC). The penalties for non-compliance can be costly, up to millions of dollars in fines, not to mention the loss of intellectual property and corporate reputation. To protect your organization in the event of a regulatory audit, you need the means to archive and search IM chat and UC conversations. Depending on your industry and UC environment, you may also need the means to establish ethical walls between departments and configure "poison room" policies for federated Lync chat and web conferencing to prevent ethical breaches. And you want to be able to add disclaimers and other legal protections to outbound IM communications.

And you will need tools to monitor UC traffic as well as manage it. Where are the potential threats originating from? Are there employees who habitually try to violate security and compliance policies? You need tools that provide visibility into your overall UC infrastructure, including the ability to generate regular reports to identify potential weaknesses and choke points and to bolster your case in the event of a regulatory audit. Without adequate visibility, you cannot effectively manage your federated UC infrastructure, nor can you demonstrate to regulatory auditors that you are both secure and compliant.

Adopting Actiance to Manage Lync Traffic as Part of Migration

As part of Lync migration, you want to filter for all of your federated UC traffic for both security and compliance. You need a central point in your federation architecture that gives you visibility over all collaborative applications and conversations; allows you to filter traffic for malware and data leaks; and that allows you to enforce acceptable usage policies both within your enterprise network and with external, public UC systems.

Actiance Vantage and Unified Security Gateway (USG) have been designed to integrate into a typical Microsoft Lync-enabled network to control, monitor, and maintain all IM conversations, collaboration, and Web 2.0 traffic.

Actiance's Vantage provides granular security and compliance features and policy controls for Microsoft Lync Server 2010, OCS, and other unified communications platforms, such as alongside public instant messaging and community networks. Vantage provides granular content filtering and archiving of all conversations, ensuring an audit trail for data leak prevention, compliance and e-Discovery. Actiance Vantage is used by the world's largest firms to secure, manage, and ensure that the use of instant messaging and other real-time communications applications comply with corporate security policies and government regulations. Organizations choose Actiance Vantage because it provides a number of benefits:

- Built-in support for both Microsoft Lync Server and OCS allows for flexible migration paths
- Identity management with policy control at global, group, and individual employee levels
- Guaranteed TrueCompliance™ to meet corporate policies and government regulations
- Archival of file transfers over Lync Server 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
- Export to third-party email archiving systems
- Centralized reporting and customizable reports
- Enforcement of ethical walls
- Comprehensive solution for preventing user circumvention of Lync

When combined with USG, users can gain total control over enterprise IP traffic. USG is the only Secure Web Gateway to combine feature and content controls of social networks with the monitoring, management, and security of Web 2.0 applications. USG provides granular control of not only websites and applications but also the content posted to blogs, wikis, webmail, and social networking sites such as Facebook, LinkedIn, and Twitter.

In a typical Lync management configuration, Vantage runs on Microsoft Windows Server and connects directly to the Lync Front End Servers to monitor all data traffic, both inbound and outbound, including conversations originating inside and outside the enterprise (see Figure 5).

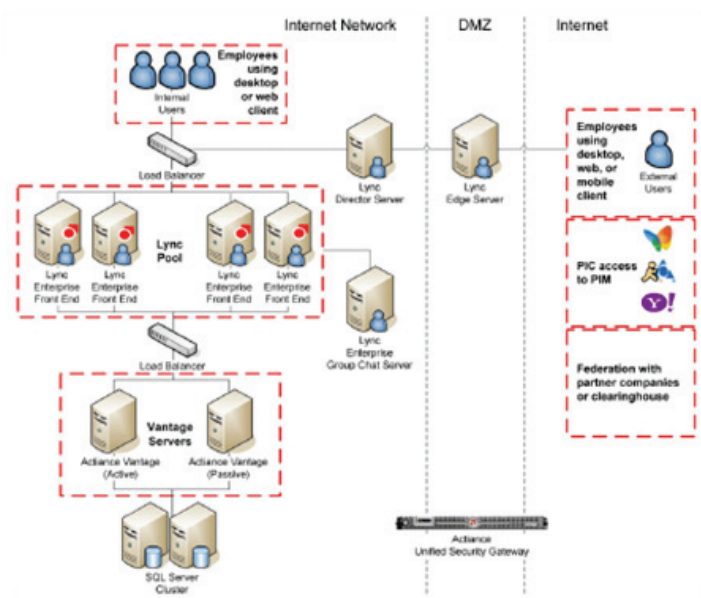


Figure 5. A typical UC architecture secured by Vantage and USG

(You can configure your UC traffic manager at the Lync Edge Server, but such an architecture only allows you to monitor external conversations, which leaves the organization vulnerable to internal abuse.) Vantage manages all policies, storing backend data in a Microsoft SQL database and using queries to Active Directory to apply policies to users and groups. Actiance Lync Connector is installed on the Lync Front End Servers as a small Connector Agent service. Content filtering and archiving is provided by pushing messages for archiving using Microsoft Message Queuing.

Policies are defined within Vantage and regularly pulled from the Lync Front End Servers. Once the baseline policy and global defaults are configured, exceptions can then be defined for different individuals and groups of users, including which groups can intercommunicate. Vantage integrates with Active Directory; thus, policies leverage user information mapped from Active Directory such as user names, SIP uniform resource identifiers (URIs), and phone numbers. Once conversation transcripts are received by Vantage, they are parsed and written into the backend SQL database.

Actiance USG can be integrated into the infrastructure with a Web/FTP proxy server, such as Blue Coat or a Squid proxy, through an ICAP-based connector. It also can be installed in simple passby mode – a plug-and-play deployment that requires no change to network configurations. Any applicable Vantage polices are applied to the user, and any unauthorized applications will be blocked by USG.

Using Vantage with USG, you can manage and monitor all data traffic flowing through internet connections, including federated and PIC UC systems. When internal Lync users communicate with users inside or outside the enterprise through a Lync Edge Server, all the traffic is routed through the Front End Server running the Actiance Connector Agent. That means all traffic is scanned:

- Viruses, malware and other file types are filtered or blocked
- Policies are applied using settings for individual users or using Active Directory, such as:
  - Allow or block Lync functions such as Live Meeting, Voice, or Video
  - Allow or block text or regular expressions in an IM conversation, such as a credit card pattern or a phrase
- Disclaimer messages can be added to IM messages
- Conversation and UC event transcripts can be sent to Vantage for handling, such as:
  - IM content, including disclaimers
  - File transfers
  - Call detail records for voice calls and Lync conference sessions and other communications

Since the Actiance Agent is deployed on the Lync Front End server, Vantage has visibility into all user activity and communications and can monitor and report on overall Lync usage. Some of the reports include the number of users currently online, number of sessions by modality, and usage trend reports – information that can help you measure Lync adoption and identify points of weakness. Vantage also lets you filter on usage by employee groups, time period, and modalities used for more granular results and to provide ROI metrics.

With respect to social media, Actiance offers the Socialite platform to enable the use of networks like Facebook, LinkedIn, and Twitter safely within the organization. Socialite helps organizations protect their brand and ensure compliance while allowing employees to share relevant content, measure impact, and increase engagement to grow their business. Socialite controls access to more than 200 features across the above three networks but can also moderate, manage, and archive any of their traffic routed through the solution.

Best Practice in Securing Lync

By filtering all your Lync traffic from both sides of the firewall, you not only secure your federated UC systems today, but you are also ensuring that your infrastructure remains relevant in the future.

Choose a platform that allows you to monitor Lync traffic and that can monitor additional UC traffic in case users access Live Messenger and Skype directly. It also is important to choose a security and compliance platform that supports collaboration from applications like SharePoint and Jive, as well as communications and collaborations from social applications such as Facebook, LinkedIn, and Twitter.

As Lync continues to evolve with deeper integration into enterprise and public messaging platforms, embracing more UC features and even adding support for potential integrations (e.g., Skype conversations over Facebook), you will have an infrastructure in place that is ready to secure new Lync capabilities.

Remember that while most businesses are seeking a single platform on which to standardize their UC, some of the real value of UC is federating with partners and third-parties or accommodating other UC platforms such as IBM Sametime or Cisco Unified Communications Manager (i.e., accommodating multiple UC platforms). And it is becoming increasingly difficult to head off BYO UC, where employees adopt their own IM, Skype, or Facebook. In fact, the number of Web 2.0 applications being used by business has been rising steadily every year since Actiance started tracking corporate usage of Web 2.0 applications in 2005.

Adding new services and extending reach through federation bring additional security challenges to any enterprise. With the right filtering technology in the right location within your network architecture, you can filter content, inject disclaimers where needed, effectively manage data access and traffic, and archive conversations that may be essential in case of an audit. So as you migrate to Lync 2010 and are considering ways to manage and secure your infrastructure, consider this three-step process:

1. Gain visibility over the entire infrastructure, including all conversations across the entire UC spectrum – those supported by Lync and within the enterprise, those between Lync and public networks, and even public IM to public IM.

2. Create acceptable usage policies that control the flow of conversation, both inside and outside the organization, and have the technology in place to monitor and enforce those policies.

3. Deploy the means to block unauthorized access, prohibited applications, and inappropriate conversations, while enabling those collaborative connections that are in line with your organization's communications objectives.

Enterprises are looking to adopt platforms like Microsoft Lync to enable users to improve productivity and the company to realize cost savings. As Microsoft Lync showcases its value for collaboration, enterprise managers are seeking to expand that value by federating with other private and public UC platforms. Real-time communications and collaboration, including rich presence, IM, Voice, Video, application sharing and conferencing across the enterprise, partners, suppliers, customers and consumers, is the most dramatic change to enterprise communications since email. However, with the added complexity of supporting multiple modalities and applications comes more concern over enterprise security. Just as with the expansion of email, enterprises need to maintain vigilance to protect their UC infrastructures. Actiance Vantage and USG enable enterprise users to realize the benefits of UC communications and online collaboration without compromising security.

About Actiance

Actiance enables the safe and productive use of Unified Communications and Web 2.0, including blogs and social networking sites. Actiance's award-winning platforms are used by more than 1,600 customers for the security, management, and compliance of unified communications, Web 2.0, and social media channels. Actiance supports or has strategic partnerships with all leading social networks, unified communications providers, and IM platforms, including Facebook, LinkedIn, Twitter, AOL, Google, Yahoo!, Skype, Microsoft, IBM, and Cisco.

Actiance is headquartered in Belmont, California. For more information, visit www.actiance.com or call 1-888-349-3223.

actiance™

Worldwide Headquarters
1301 Shoreway, Suite 275
Belmont, CA 94002 USA
(650) 631-6300 phone
info@actiance.com

EMEA Headquarters
400 Thames Valley Park
Reading, Berkshire, RG6 1PT UK
+44 (0) 118 963 7469 phone
emea@actiance.com