actiance®

Securing Microsoft Lync Server

Contents

Executive Summary

Deploying Microsoft Lync is a great first step in leveraging the benefits of unified communications (UC). However, in heterogeneous environments where Lync operates alongside other communications channels, overall information governance becomes more complex.

In practice, it is rare that Lync is used exclusively. Enterprises likely will utilize other productivity tools such as Salesforce Chatter or SharePoint to collaborate with colleagues, partners, and suppliers. Further complications arise when users themselves download unauthorized real-time communications tools such as Yahoo! Messenger or Twitter. Regardless of company policy, because of their pervasive nature and employees' reluctance to do without, these applications are often extensively used in most organizations.

Aside from the obvious hazard of malware using unauthorized channels to enter the network, deploying Lync without the means to monitor or manage other communication channels increases the risk of data leakage in the organization. Without the ability to consistently enforce disclaimers, monitor content, or establish ethical walls, it will be very difficult to meet the security requirements necessary to unleash the full potential of Lync.

Actiance Vantage augments Lync's native security features, enabling enterprises to maximize their investments in Lync while enhancing their overall information governance capabilities.

Lync Can't Do It All

Microsoft Lync is extremely effective in delivering UC, but it does not natively provide the capabilities to meet all of today's security requirements. In addition, it does not prevent employees from using public real-time communications tools like Twitter and Yahoo! Messenger. Securing and controlling this heterogeneous environment is a multi-faceted challenge. Security policies need to be applied consistently across all platforms, both consumer and enterprise, enabling the enterprise not just to deploy Lync, but to embrace a wide spectrum of communications channels.

Lync Security Risks

The main risks for enterprises deploying Lync are very similar to those of other electronic communications such as email: malware, data leakage, and non-compliance with government and industry regulations. Just like email, the principles for applying policies and securing UC remain the same.

However, unlike email, because UC covers such a wide range of modalities, consideration should be given to types of applications, their individual capabilities and the associated risks. At the same time, because Lync is rarely used in isolation, consideration must also be given to the security of other enterprise and public communications applications.

Malware

It is no secret that Internet applications, public IM, peer-to-peer file sharing and social media introduce risk to the enterprise. The productivity advantages of collaboration are quickly lost when malware infections send the IT staff into the equivalent of search-and-rescue mode to clear malware from endpoints and protect the company from sensitive data loss.

Unsurprisingly, social engineering tactics are used extensively by malware writers who hijack IM buddy lists to trick users into thinking a link on their IM screen is actually from a trusted friend on the system. Once introduced to the network, multi-protocol malware can quickly jump from the public IM system to the internal Lync environment.

Zero Day Attacks

A new, and as yet unknown, IM threat has the greatest propensity to spread and infect organizations immediately after it is released by the creator. Products that rely on signatures alone and require organizations to wait hours or even days for a new signature to be created, tested, and distributed are virtually ineffective in defending against IM threats.

Enterprises need to secure against IM threats by preventing new infections before they get started. Vantage's Zero Day defense system protects against worms delivered over public IM and Lync chat using anomaly-detection techniques that measure several attributes of IM conversations against normal behavior.

Data Leakage

Data leak prevention is a crucial piece of Lync management and security. The return on investment of Lync is lost if the result is another security hole from which confidential information can be leaked. Beyond basic text correspondence, file attachments can contain sensitive information and, unless their content can be detected and evaluated, data can be lost unknowingly.

In defending themselves against malicious and inadvertent data leakage, organizations must be able to control access, limit file-sharing capabilities accordingly, and filter content of all electronic communications. With Vantage, enterprises have the ability to provide granular control over an employee's actions on Lync.

Federation

The rewards of federation are clear: it provides interoperability between users similar to the ease with which they enjoy email communications today. However, just like email, it increases the risk of malware infection, data leakage, and the potential to interact with another person outside of an ethical or regulatory boundary.

Vantage allows organizations to control which external parties can communicate with which users, groups, or networks. The enterprise may be subject to a regulation that requires the companies to monitor and/or prohibit communications between different business groups or divisions.

Actiance Vantage

Actiance Vantage is the de facto platform for granular security and policy controls for real-time communications, providing management for the broadest set of applications and modalities, including Microsoft Lync, public IM networks, collaboration, enterprise social, and community-focused networks. It integrates with existing Microsoft enterprise infrastructure including Active Directory, SQL, archiving systems, and more.

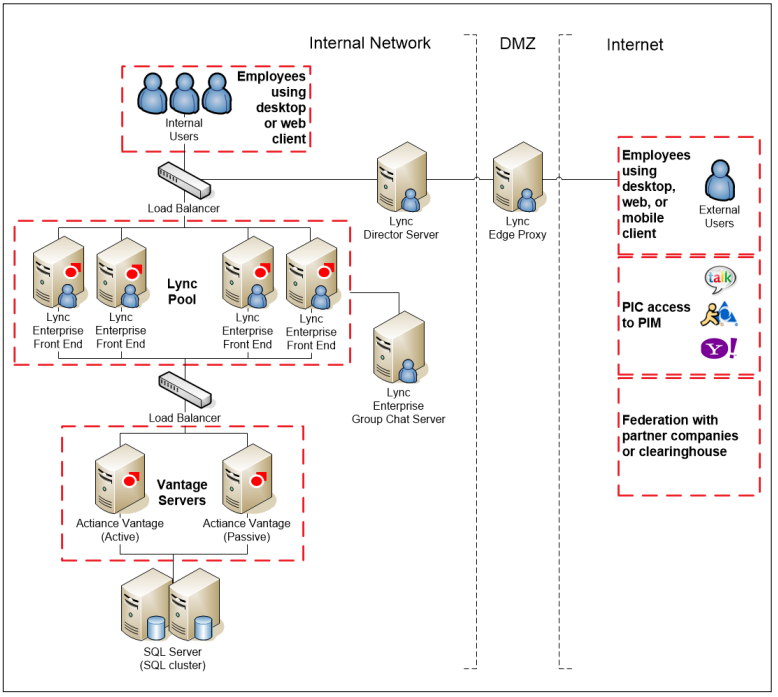
With Vantage, organizations can protect their investment in Lync while meeting strict security requirements for real-time communications. Because Vantage delivers additional security benefits on top of native Lync, enterprises can reduce their risk exposure.

Additional Benefits Over Native Lync

Function	Microsoft Lync	Additional Benefits Provided by Vantage
Anti-virus and malware control, including bots	None	Support for Symantec, McAfee, TrendMicro, CA, ClamAV, Sophos, and Kaspersky. Zeroday worm blocking. Files are not scanned on Lync Server front end so no additional load
SpIM blocking	Enhanced presence can filter on presence information	Content-based protection using white/black lists and custom rules
URL blocking	URL rewrite to remove hyperlink and/or add warning message	Domain-configurable and direction-configurable URL policies
IM client support	None	Support for all native, major public IM clients, including Google Talk, Windows Live, AIM, and Yahoo!
Federation management	Allow/block at company level and user level only	Allow/block permissions at company, group, and user levels; Ability to specify explicit partner, domain-based rules at company, group, and user level

Vantage Technical Architecture

The following diagram shows how Actiance Vantage integrates into a typical Microsoft Lync-enabled network. Vantage is connected via the Lync Front End Servers, enabling it to control, monitor, and retain all Lync and federated conversations, both internal and external. Although it is possible to install Vantage on the Edge Server, it is then only possible to monitor external conversations, thus leaving the organization susceptible to internal abuse.



Installation Environment

Vantage runs on Microsoft Windows Server, storing backend data and policies in a Microsoft SQL database. Active Directory is queried so policies can be applied to users and groups. In accordance with Microsoft recommendations, a small service, Actiance's Lync Connector, is installed on the Lync Front End servers. This Connector periodically pushes messages for retention using Microsoft Message Queuing on TCP port 1801 and pulls policy updates using TCP port 8090 from the Vantage system, thus providing hygiene, content filtering, and retention capabilities.

Information Flow

When internal Lync users communicate with internal or external users (through a Lync Edge server), their traffic is first routed through the Front End server, which has a small Actiance Connector Agent running on it. The Actiance Connector Agent:

- Applies virus scanning and other file type and blocking
- Applies policy to the Lync users or by Active Directory Group, which can include the following:
  - Allow/Block aspects of Lync functionality, including Web conferencing, Voice, and Video
  - Allow/Block/Alert certain text or regular expressions in IM conversations or file transfers, e.g., matching of bank account or credit card number patterns
- Adds corporate disclaimers to messages
- Sends Lync events and conversation transcripts to Vantage, which contains:
  - IM conversation content, including disclaimers
  - File transfers
  - Call Detail Record (CDR) information for voice calls, Web conferencing sessions, etc.

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 groups of users (and/or individuals), including which groups can intercommunicate. Vantage integrates with Active Directory and enables a user's buddyname to be mapped to their Active Directory account in the internal database. Once conversation transcripts are received by Vantage, they are parsed and written into the backend SQL database.

The Actiance Agent deployed on the Lync Front End server has visibility into user activity and communications on Lync, providing a way to monitor and report on overall Lync usage. Available reports include the number of users currently online, the number of sessions by modality, and usage trend reports.

Conclusion

Businesses are looking to Lync to provide a standard platform for exploiting the benefits of these collaborative applications, but in practice, it does not prevent the use of software that employees are already using. In fact, the number of Internet applications in use in the enterprise has been steadily rising since Actiance began tracking these trends in its annual survey.

In addition, deploying Lync or extending its use to include other capabilities, such as federation, brings additional security challenges to the enterprise, such as a lack of disclaimer messages or content filtering. Nor does Lync provide detailed, easy access to archived conversations and file transfers that may end up as key evidence in lawsuits.

With Actiance, organizations can immediately reap the cost and productivity benefits of Lync without exposing the enterprise to security risks.

About Actiance

Actiance® is a global leader in communication, collaboration, and social media governance for the enterprise. Its governance platform is used by millions of professionals across dozens of industries. With the power of communication, collaboration, and social media at their fingertips, Actiance helps professionals everywhere to engage with customers and colleagues so they can unleash social business. The Actiance platform gives organizations the ability to ensure compliance for all their communications channels. It provides real-time content monitoring, centralized policy management, contextual capture of content and smart archiving which improves the efficiency and cost-effectiveness of eDiscovery and helps protect users from malware and accidental or malicious leakage of information. Actiance supports all leading social media, unified communications, collaboration, and IM platforms, including Facebook (FB), LinkedIn (LNKD), Twitter, Google (GOOG), Yahoo! (YHOO), IBM, (IBM), Jive (JIVE), Microsoft (MSFT), Cisco (CSCO), and Salesforce.com (CRM).

Worldwide Headquarters

1400 Seaport Blvd.
Building B, 3rd Floor
Redwood City, CA 94063 USA
(650) 631-6300 phone
info@actiance.com

EMEA Headquarters

Asmec Centre, Merlin House
Brunel Road
Theale, Berkshire RG7 4AB
United Kingdom
Tel: +44 (0) 1189 026 468
emea@actiance.com

More information

actiance.com

sales@actiance.com

Follow us

facebook.com/Actiance

linkedin.com/company/actiance-inc

twitter.com/actiance

youtube.com/actiance

slideshare.com/actiance

actiance®