

# Actiance for Skype

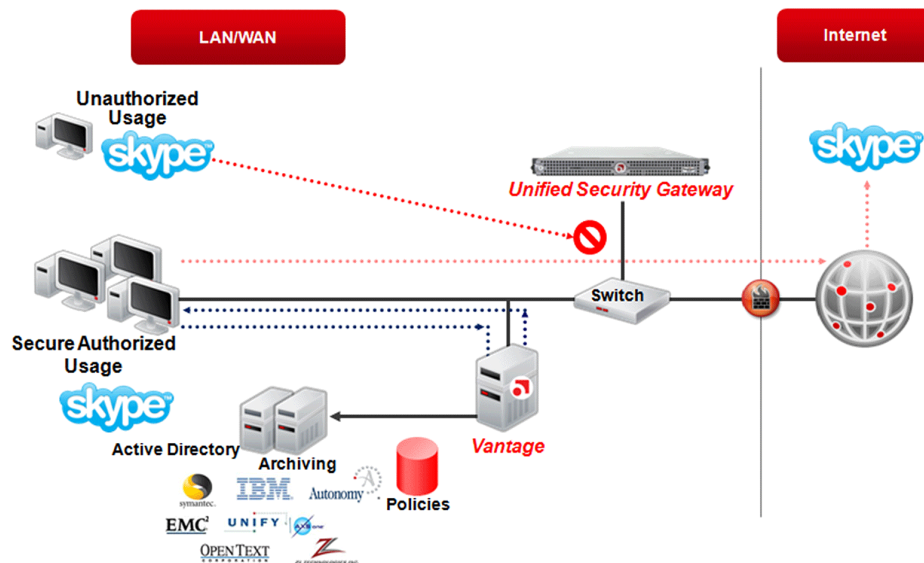
## Securing and Managing Skype Usage

### Risks of Skype in Today's Real-Time Enterprise



Although mostly known and used as a VoIP application, Skype is a complex peer-to-peer (P2P) network that has many Web 2.0 characteristics. It constantly scans for open ports on the network through which it can re-route traffic. Any computer running Skype with a routable IP address can become a “supernode” and route other users’ Skype traffic through it, increasing both bandwidth consumption and the potential for exposure to threats. Uncontrolled use introduces serious risk to the enterprise via inbound malware threats and outbound data leakage.

Skype communications are all classified as “electronic communications” for the purposes of data protection, eDiscovery, and other compliance-related requirements. Because all communications over Skype are encrypted, monitoring with traditional tools is virtually impossible.



### The Actiance Advantage

Actiance provides a comprehensive gateway-to-endpoint approach to managing and securing the use of Skype and other real-time communication applications within the enterprise. Visibility at the gateway is the first step in gaining control over Skype usage. Actiance’s Unified Security Gateway (USG) provides IT with complete visibility into unauthorized Skype traffic on the network. It is purpose-built for the security of real-time communications. Once visibility is obtained, Actiance’s Vantage enables the enforcement of Skype usage policies at the client and blocks any malicious URLs coming in over Skype chat sessions. This robust combination allows IT managers to set and enforce policies that ensure Skype traffic on their network is secure and meets compliance requirements.

### AT A GLANCE

Actiance for Skype enables the safe and productive use of Skype, including mapping buddy names to employees, authorizing/blocking usage, and monitoring file transfers through the Skype network. It also protects enterprise networks from a range of security threats, including inbound malware and data leakage. Additionally, it addresses organizations’ compliance requirements by logging all IM messages sent through the Skype network and issuing inline disclaimer messages whenever appropriate.

### KEY FEATURES

- Enable or block Skype access
- Log IM messages sent
- Map Skype buddy names to employees
- Control whether file transfers are allowed
- Control whether VoIP and Video can be used
- Insert disclaimer message into IM conversations
- Mitigate content leakage by scanning IM messages for words, phrases, and expressions
- Protect employees from malicious content and worm attacks
- Filter URLs sent by employees
- Protect enterprise networks via controls such as preventing Skype clients from becoming a supernode

A-DS-011-SKYPE-0111