

### Security and Compliance for Cisco Unified Presence

Actiance Vantage™ for Cisco Unified Presence addresses the security, management, and compliance of Unified Communications (UC), including user policy management, message hygiene, malware prevention, and archiving for compliance. Enterprise communications environments are heterogeneous, consisting of the “enterprise” UC platform and typically several public instant messaging (IM) networks – requiring corporate UC platform security, federated connections with external parties and networks – alongside those publicly available networks that do not connect with the corporate messaging platform.

#### UC Management Challenges

Businesses increasingly require role-based access control; manage at global, group and user levels; differentiate between group and federation policies; monitor LDAP, IP-, and domain-based policies; and control IM and group chat usage. Vantage enables role-based access control and policy management of VoIP, Video, IM, group chat, disclaimers to end users, ethical walls, reporting, workflow, and audit reports.

#### Data Leakage and Inbound Security Threat Challenges

Within collaborative environments such as CUP, users continue to utilize publicly available real-time communications tools, such as Yahoo!, AIM, Google Talk, and Skype, which results in a heterogeneous environment requiring a security and compliance solution that addresses the whole real-time communications spectrum. However, doing so presents some challenges.

- Malware has begun to appear in real-time communications channels. Increasingly, more damaging attacks are spreading to real-time communications in order to bypass existing security measures. Spam is also moving beyond the email inbox into the IM stream, further increasing the risk of inadvertent malware infection.
- Valuable proprietary information is often transferred outside the corporate network using unmonitored IM and UC channels.

#### Compliance, Liability, and Risk Challenges

In the U.S. alone, there are more than 10,000 laws relating to electronic and real-time communications. There are clear penalties for non-compliance with these regulations. Aside from fines, damaged reputations, and potential loss of intellectual property, the effort involved in recovering from these setbacks can be detrimental to ongoing business.

#### Actiance Vantage™ Enhances CUP Deployments

Vantage™ provides granular security, compliance, and policy controls for CUP, alongside publicly available IM networks and industry-focused IM communities such as Thomson Reuters Messenger, Bloomberg, Pivot, and YellowJacket. Designed to meet an organization's security, management, and compliance requirements for real-time communications, in addition to supporting all the key government and industry regulations (e.g., FISMA, FINRA, SEC, FRCP, Sarbanes-Oxley, MiFID, and FERCA), Vantage™ delivers additional benefits to native CUP implementations.

#### AT A GLANCE

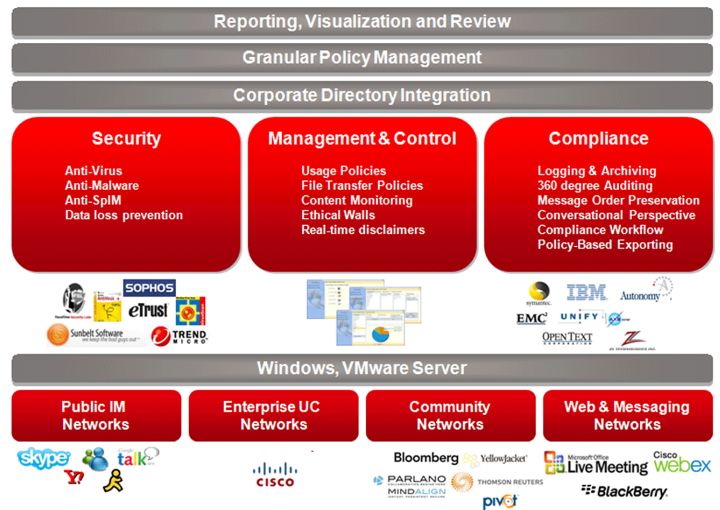
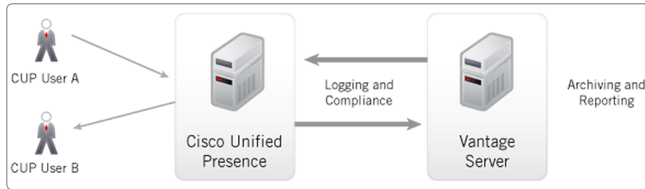
Vantage™ ensures security, management, and compliance for real-time and unified communications – from presence to instant messaging to group chat.

#### KEY FEATURES

- **Support for Cisco Unified Presence (CUP) as well as public IM networks for flexible deployment**
- **Provides policy setting, real-time monitoring, compliance, application of DLP/content filtering rules and enforcement of ethical walls for group chat**
- **Prevents data leakage over CUP and public IM platforms through content filtering and regular expression**
- **Integrated with Lightweight Directory Access Protocol (LDAP) to define permissions at the company, group, and user levels to enforce ethical walls and acceptable use policies**
- **Supports BlackBerry PIN and SMS Messaging**
- **Secure, intuitive Web-based administration and reporting, including detailed usage reporting by log in, number of messages, time interval, and unified communications events**
- **Auditing and easy retrieval of tamper-proof stored information based on granular searches of keywords, users, and time frames to meet eDiscovery requirements**
- **Existing database resources (e.g., SQL Server, Oracle) can be leveraged for storage of all real-time communications**
- **Enterprise reporting for ROI, departmental cross-charge, and usage analysis**

## for Cisco Unified Presence

Actiance Vantage™ accurately and completely logs all real-time communications, including blocked messages, to ensure compliance with corporate governance, data protection, and eDiscovery regulations.



### ADDITIONAL BENEFITS OVER NATIVE CISCO UNIFIED PRESENCE

Function	Additional Benefit Provided by Vantage
Central policy and logging for IM, Group Chat	UC policy is defined centrally and applied across all communication modalities; captured data is stored in a single location to provide a comprehensive view of system usage and a single integration point for data archival systems
Public IM client support	Support for all native, major public IM clients including Google Talk, AIM, and Yahoo!
Authentication & Authorization Services	Policies at company, group, and user levels: Group-level ethical boundaries; IP address-based access controls; Access controls and monitoring options
SpIM blocking	Content-based protection using white/black lists and custom rules
URL blocking	Domain-configurable and direction-configurable URL policies.
Legal disclaimer notification	Disclaimers sent inline and audited; disclaimer display controls at the IM network and group levels
Tamper detection	Guaranteed message order preservation; anti-tamper mechanism validates conversation integrity
eDiscovery retrieval	Reports on IM usage, security violations, compliance violations, transcript reviews. Scheduling and auto-delivering available.

A-DS-021-VANTAGE-CUP-0211