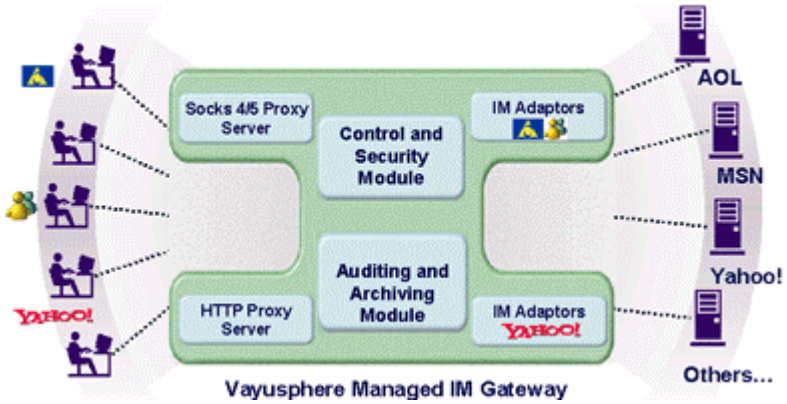
Vayusphere Managed IM Gateway (MiG)

Vayusphere
Instant Response for the Real-Time Enterprise



Instant Messaging in the enterprise

Instant Messaging (IM) is changing the way people work and communicate. IDC, a research firm, predicts the number of global corporate IM users will increase more than tenfold from 18.4 million in 2000 to 229.2 million in 2005.

IM is on its way to becoming an enterprise's lifeblood for collaboration. Your employees and customers are increasingly using it to communicate with their friends and colleagues, inside and outside the enterprise.

Today, IM usage in the enterprise is:

- **Uncontrolled**: IM is behind the firewall and often a mission critical application that cannot be selectively shut off without affecting business. Yet it is used without the control of the IT organization.
- **Unmonitored**: IT organizations have no means to find out the extent of IM usage.
- **Anonymous**: Your employees chose screen names regardless of their identity within the organization. Any misrepresentation subjects an organization to liability.
- **Unaudited**: Unlike email, IM conversations are not centrally logged. No audit trail is available.
- **Insecure**: There are no means for the IT organizations to prevent company secrets from being transmitted across the insecure public IM networks. Additionally, public IM systems bypass existing file transfer security checks, such as virus checking.

Like email in your enterprise, IM usage needs to meet your requirements for compliance, control, reporting, and security.

Vayusphere IM Gateway

Vayusphere Managed IM Gateway (MiG) is the only cross-platform enterprise-scale Instant Messaging management solution. It supports all major platforms in an enterprise and all major public IM servers: AOL Instant Messenger, MSN Messenger, Yahoo! Instant Messenger. You can now control, secure, and report on instant messaging in your workplace, while allowing your enterprise to access the largest instant messaging communities in the world.

Benefits

- **Control and secure IM usage**: Control access to each public IM service and permitted actions.
- **Protect against Viruses**: Restrict file transfer while allowing users to continue to use IM.
- **Monitor IM usage**: Find out who is using IM, what service they are using, and how active they are.
- **Comply to regulations**: SEC, NASD, and HIPAA regulations require conversations be archived.
- **Protect sensitive information**: Make sure that company secrets or sensitive information is not being communicated outside the organization.

Features

- **Multiple levels of control for IM policies**: Control access to each IM service at the enterprise or individual user level.
- **IM feature level control**: Control individual features, such as file transfer.
- **Disclaimer message**: Warn users not connected that their messages are logged.
- **Active filter technology**: Setup filters that can process messages in real-time and modify messages or send warnings within a conversation.
- **Logging and archiving**: Logs can be stored locally in XML files or stored in a database for easier searching and reporting.
- **Web administration portal**: Manage MiG settings and IM policies through a web-based portal.
- **Map public identities to corporate identities**: Trace public IM identities to LDAP identities.
- **IM usage reports**: Identify usage statistics by IM service and message activity through the web portal.
- **Bulk provisioning**: Use files for easier provisioning.
- **Cross platform**: Use any major enterprise platform and database.
- **High-performance and scalability**: The MiG architecture is clusterable to provide linear scalability.

System Requirements

- Operating Systems: Solaris, Windows 2000, or Linux
- Minimum Hardware: SPARC or Intel 450Mhz CPU, 384MB RAM, 1 GB free Disk Space

How to Proceed

Call 1-650 960 2900 or email sales@vayusphere.com.

Vayusphere, Inc.
www.vayusphere.com