

# Symantec™ IM Manager

Secure instant messaging (IM) management and policy enforcement of public and enterprise IM for enterprise risk management

Symantec IM Manager seamlessly manages, secures, logs, and archives corporate IM traffic with certified support for consumer IM services and enterprise IM platforms, with granular policy controls for text messaging, file transfers, audio, video, VoIP, application sharing, and other real-time communication capabilities associated with IM. Symantec IM Manager secures corporate networks against external threats such as IM viruses, worms, and malware through usage of real-time content filtering, worm and virus signature detection, behavior-based threat protection, and file-based antivirus scanning. Symantec IM Manager also protects organizations against the loss of sensitive information or intellectual property over IM through granular policy controls for internal IM usage, including internal message routing, regular expression pattern matching, and real-time user monitoring.

Integrated with the Symantec™ Security Response, Symantec IM Manager offers the industry's first zero-day threat protection from IM-borne viruses and worms.<sup>1</sup> Utilizing a patent-pending behavior- and signature-based system, Symantec IM Manager provides automatic protection for new and emerging IM viruses.

In addition, Symantec IM Manager provides a tool to enforce content and regulatory compliance policies for all aspects of IM, including the ability to selectively log messages based on user, group, or domain attributes; selectively insert customer message disclaimers; and capture 100% of message traffic for internal or external third-party archiving.<sup>2</sup>

## Key features

### *Manage instant messaging to drive business results*

- **User management and access control**—Manage and control IM user, group and domain access to disparate IM systems, including integration with enterprise directory structures.
- **Priority-based policy enforcement**—Establish consistent IM usage policy enforcement, including real-time content filtering, granular file transfer, and advanced client feature controls.
- **Real-time analytics and reporting**—Obtain visibility into IM usage and growth patterns with real-time altering, trend reporting and custom monitoring.

### *Protect the organization with security and usage control*

- **Zero-day protection**—Patent-pending technology for detection and protection against zero-day attacks.
- **Automatic threat updates**—Automatically update virus and spam signatures from the industry-leading Symantec Security Response Team.
- **Virus scanning and file transfer control**—Scan file transfers leveraging Symantec AntiVirus™ Scan Engine to prevent infected or confidential files from traversing your network.

<sup>1</sup> See the *Symantec Real Time Threat Protection System (RTTPS)* press release, July 2005

<sup>2</sup> Message queue technology is a transacted system that ensures high performance and message integrity by acting as a persistent networkable buffer between the point of capture and the archive. If a message is not accepted by the queue it is not sent.



### **Comply with legal and corporate accountability standards**

- **Rich message archive**—Selectively capture and retain IM conversations with direct links to employee data from the corporate directory for enhanced retention and discovery.
- **Real-time content filtering**—Block messages and/or notify administrators when messages containing restricted phrases or inappropriate content is sent.
- **Integration with Symantec Enterprise Vault™**—Out-of-the-box, transactional integration with Symantec Enterprise Vault provides delivery of IM conversations to Enterprise Vault. This allows customers to review IM and email conversations in one centralized store.

---

### **System requirements**

#### **Minimum recommended hardware requirements**

- 1.8 GHz Pentium III dual-processor
- 512 RAM
- 30+ GB Hard Disk
- 1 GB Virtual Memory

#### **Minimum recommended software requirements**

- Windows® 2000 with SP3 or Windows 2003
- MDAC 2.5 or later
- Internet Explorer 5.5 or later
- MSXML Core Services 4.0 SP2
- Microsoft® IIS Web Service
- Access to Oracle® (Oracle 9i v 9.2.0.5 with ODBC drivers 9.2.0.63, Oracle Enterprise Client 9.2.01), MS-SQL 2005, MS-SQL 2000 SP4 or MSDE installed database

### **More information**

#### *Visit our Web site*

<http://enterprise.symantec.com>

#### *To speak with a Product Specialist in the U.S.*

Call toll-free 1 (800) 745 6054

#### *To speak with a Product Specialist outside the U.S.*

For specific country offices and contact numbers, please visit our Web site.

#### *About Symantec*

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

#### *Symantec World Headquarters*

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

[www.symantec.com](http://www.symantec.com)

