

Antigen for Instant Messaging

Instant Messaging Protection Against the Latest Threats

Antigen[®] for Instant Messaging helps businesses protect their Live Communications Servers and public IM clients against the latest viruses, worms, and inappropriate content.

Evolving Threats

New viruses, worms, and blended threats are increasing in sophistication, speed, and frequency. These threats are also finding new ways to propagate within corporate networks.

Instant Messaging (IM) has become a corporate staple, helping to improve productivity and rapid collaboration between employees, customers, and partners. Unfortunately, the ubiquitous use of instant messaging and its collaborative nature make it a target for malicious code writers. Instant messaging threats are rapidly on the rise, with 1379 unique IM/P2P threats reported in the first half of 2005 alone (*IMLogic Threat Center*).

Real-time Messaging Protection with Antigen for Instant Messaging

Antigen for Instant Messaging allows users to communicate without the risk of sending or receiving malicious code or undesirable content. Antigen for Instant Messaging provides comprehensive protection using layered defenses, corporate content policy

enforcement, and optimization of messaging server resources to ensure messages and file transfers are secure at all times.

Layered Defenses

Antigen for Instant Messaging protects organizations against the latest threats by managing multiple antivirus scan engines to scan all IM and file transfers.

This approach allows Antigen for Instant Messaging to minimize the average window of exposure for emerging threats by providing and managing frequent signature updates from multiple antivirus labs around the world.

Antigen for Instant Messaging's layered defenses also protect against downtime. If one engine fails or goes offline to update, other engines remain active to provide

protection, ensuring your IM service is not interrupted and user security and compliance are not compromised.

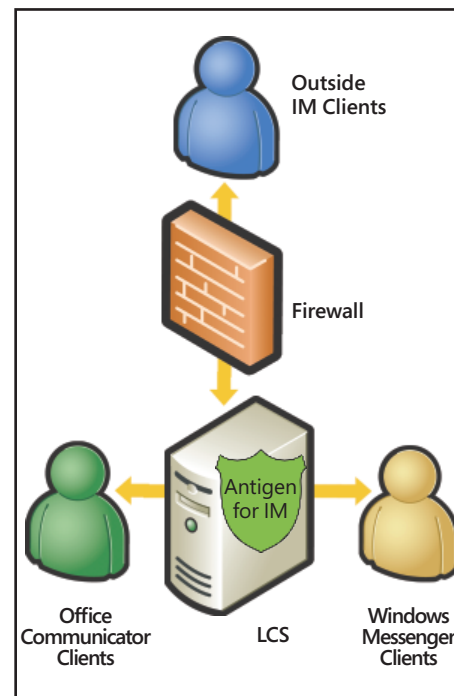
Content Control

Protecting IM conversations does not end with detecting and removing viruses. IM users need to be protected from inadvertent or intentional instant messages or file transfers that contain inappropriate content, such as offensive language, legally or ethically questionable material, or confidential company information, as well as instant messaging spam (spim).

Through administrator-defined content filtering rules, Antigen for Instant Messaging helps enforce compliance with corporate policy for language usage and confidentiality within IM conversations and file transfers. Antigen for Instant Messaging also has configurable file filtering rules that help customers ensure that file types known for carrying viruses (for example, .exe) or opening organizations to legal exposure (for example, .mp3) are blocked.

Server Optimization

Antigen for Instant Messaging provides tight integration with Microsoft Live Communications Server, optimizing server performance and ensuring protection that doesn't overtax server resources. With features like in-memory scanning, multi-threaded scanning processes, and performance bias settings, businesses can achieve the benefits of multiple engine scanning without introducing additional processing time or server performance degradation.





How Antigen for Instant Messaging Works

Antigen for Instant Messaging is a server-based antivirus solution that provides comprehensive protection for Live Communications Server and its Windows Messenger and Office Communicator clients. Real-time scanning ensures conversations and files are safe before they are sent or received.

To protect public IM clients that may be in use within an organization, Antigen for Instant Messaging can also be installed on IMLogic IM Manager servers to provide virus scanning and content filtering.

Multiple Engine Management

Antigen for Instant Messaging manages four scan engines from industry leading security companies, including Computer Associates, Norman Data Defense, and Sophos

Performance Bias Settings

In order to deliver more flexibility and control over security and server performance, Antigen for Instant Messaging provides bias settings that allow administrators to configure how many engines are used for a given server. Administrators can choose from settings like "Maximum Certainty" that scans with all available engines or "Neutral" that scans with approximately 50% of available engines.

In-memory Scanning

Instead of spooling data to disk for virus scanning, Antigen for Instant Messaging dynamically allocates available application memory to scan messages. This process provides real-time protection, while maintaining server efficiency.

Multi-threaded Scanning

Antigen for Instant Messaging also helps improve scanning performance with the ability to create multiple, simultaneous scanning threads.

Content and File Filtering

Antigen for Instant Messaging provides extensive content filtering, blocking messages and file transfers that contain inappropriate content. Antigen for Instant Messaging includes a set of predefined, customizable keyword dictionaries to target spam, profanity, and other unwanted content. Administrators also have the ability to build or import additional lists.

Content filtering can also be used to block URLs, preventing phishing attacks and links to sites that download malicious code.

File filtering allows administrators to block files based on attachment file extension, type, name, and size. This enables organizations to set and manage policies for file sharing. In many cases, this capability can also be used to block new malicious attacks for which there is not yet an available signature.

Whitelisting

Antigen for Instant Messaging allows administrators to create whitelists based on IM screen names and addresses. These "whitelisted" users are exempted from content and file filtering of conversations and file transfers.

Automatic Updates

To ensure that engines have the latest signature files, Antigen for Instant Messaging's Rapid Update Process automatically downloads updates from scan engine partners as soon as they are available and tests them against a virus database. Within minutes, these engines and signatures are tested, confirmed, and posted. Antigen for Instant Messaging can be configured to automatically download the latest updates without stopping IM traffic.

User Notification

Antigen for Instant Messaging provides unique user notification for viruses and inappropriate content. Notifications are sent via an IM message to both users and administrators when a content policy has been violated or infected documents have been sent.

Centralized Management

Antigen for Instant Messaging integrates with Sybari® Enterprise Manager™ (SEM), a browser-based management console for all Antigen products. SEM provides central deployment, centralized updating, hot upgrades, comprehensive reporting, and SMTP/SNMP alerting.

Antigen for Instant Messaging System Requirements

Features and functionality described require Microsoft® Windows Server™ 2003; Microsoft Live Communications Server 2003 or 2005 or IMLogic IM Manager; an SMTP server (for SMTP notifications); 64MB of available RAM; and 100MB of available disk space. Workstation requirements for the Antigen Console include Windows 2000 Professional or later, 10MB of available memory, and 10MB of available disk space.

For more information about Antigen for Instant Messaging, visit <http://www.microsoft.com/antigen>.