Microsoft

Microsoft® Antigen for Exchange

Server-level Protection Against the Latest E-mail Threats

Microsoft® Antigen for Exchange helps businesses protect their Exchange 2003 and 2000 servers against the latest viruses, worms, and inappropriate content.

Evolving Threats

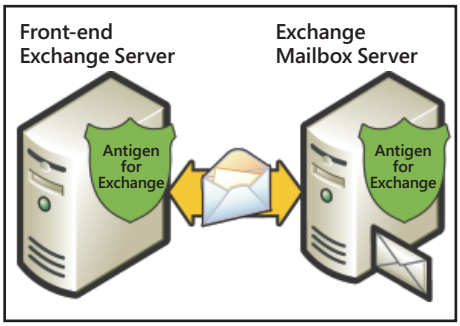
New viruses, worms, and blended threats are increasing in sophistication, speed, and frequency. Yet e-mail remains the delivery mechanism of choice for virus writers to propagate threats throughout the enterprise. The ability for new threats to evade traditional detection methods is clear – 78% of businesses experienced virus infections in 2004, despite 98% having antivirus protection installed (CSI/FBI 2004 Survey). One oversight that often contributes to these infections is the reliance on products that use a single antivirus scan engine to provide protection on all clients, servers and perimeter devices throughout the IT infrastructure. If this single antivirus engine fails to detect a new threat or the scan engine fails for any reason, the enterprise immediately becomes vulnerable at all points in the infrastructure.

E-mail Protection with Antigen for Exchange

Antigen for Exchange helps protect your e-mail infrastructure from infection and downtime through an approach that emphasizes layered defenses, optimization of Exchange Server performance and availability, and enforcement of corporate content policies. Combining these protection technologies at multiple layers throughout the infrastructure helps stop the latest e-mail threats before they impact business and users.

Protect Against the Latest Threats

Antigen for Exchange protects organizations against the latest threats by managing multiple antivirus scan engines at multiple layers throughout the e-mail infrastructure. This approach allows Antigen for Exchange to minimize the average window of exposure for emerging e-mail threats by providing continual signature updates from multiple antivirus labs around the world. Dual scanning at both the SMTP stack and the Exchange Information Store provides a further layer of protection.



Antigen for Exchange's layered defenses also protect against downtime. If one engine fails or goes offline to update, other engines remain active to provide protection, ensuring mail delivery is not compromised or delayed.

Ensure Availability and Control

Antigen for Exchange provides tight integration with the Microsoft® Exchange platform, optimizing server performance and ensuring e-mail protection that doesn't overtax server resources – even during outbreaks. With features like in-memory scanning, distributed, multi-threaded scanning processes, and performance bias settings, businesses can achieve the benefits of multiple engine scanning without introducing additional mail processing time or server performance degradation.

Antigen for Exchange also reduces demands on server workload and disk space by immediately detecting and purging known worms, significantly reducing traffic to mail servers during outbreaks.

Prevent Unsafe Content

Protecting e-mail does not end at virus and worm remediation. E-mail can also contain inappropriate and undesirable content – such as pornography, legally or ethically questionable material, or confidential company information.

Through administrator-defined content filtering rules, Antigen for Exchange helps enforce compliance with corporate policy for language usage and confidentiality within subject lines and message body text.

Antigen for Exchange also offers 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 preemptively blocked, regardless of origin or destination.

How Antigen for Exchange Works

Antigen for Exchange is a server-based antivirus solution that provides comprehensive protection across Exchange 2003 and Exchange 2000 environments. It can be deployed on front-end and back-end Exchange servers, protecting against perimeter threats as well as providing internal incident containment. Inbound and outbound scanning is performed at the SMTP stack and real-time scanning at the Exchange Information Store. Antigen for Exchange can also be configured to perform on-demand or scheduled scans of the Exchange Information Store.

Multiple Engine Management

Antigen for Exchange manages five scan engines from industry-leading security companies, including Microsoft, Computer Associates, Norman Data Defense, and Sophos. Antigen for Exchange can also manage additional engines from AhnLab, Authentium, Kaspersky Labs, and VirusBuster*.

Cluster Support

Antigen for Exchange ensures that both active and passive nodes in Exchange clusters are updated with the most up-to-date configuration information and signatures. Antigen for Exchange associates configuration data and signature engine update files with an Exchange Virtual Server, eliminating the need for nodes to be separately configured.

Performance Bias Settings

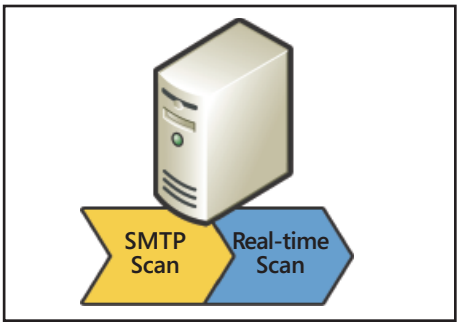
In order to deliver more flexibility and control over e-mail security and server performance, Antigen for Exchange provides bias settings that allow administrators to configure how many engines are used for a given scan job. Administrators can choose from settings like "Maximum Certainty" that scans with all available engines or "Neutral" that scans with approximately 50% of available engines. Different settings can be defined for SMTP scanning and mail store scanning.

In-memory Scanning

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

Distributed, Multi-threaded Scanning

Antigen for Exchange scans at both the SMTP stack and the Exchange Information Store. Administrators have the ability to distribute scanning tasks between the SMTP scan job and real-time scanning of the Information



Store. Process-intensive scanning (like content and file filtering) can be done at the SMTP stack, while scanning processes that require less overhead can occur at the Exchange Store. This helps reduce the performance burden on mailbox servers.

Antigen for Exchange also helps improve the performance of mail throughput with the ability to create multiple scanning threads.

Worm Removal

Antigen for Exchange's WormPurge feature uses a continually updated list of worm signatures to identify and instantly purge messages that match known worm signatures. Since there is no legitimate content in a worm message, there is no reason to quarantine it. Purging worm infected messages reduces unnecessary mail traffic on the network and frees up storage. WormPurge also eliminates help desk calls generated by users who would otherwise confuse worm notification messages with real worm threats.

Content and File Filtering

Antigen for Exchange provides content filtering for message body and subject line, blocking or logging messages that contain keywords for inappropriate content. Administrators can choose from pre-defined Antigen keyword lists, populate their own lists, or import external lists. 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 e-mail attachments. In many cases, this capability can also be used to block new malicious attacks for which there is not yet an available signature.

Secure, Automatic Updates

To ensure that engines have the latest signature files, Microsoft's signature update process automatically downloads updates from scan engine partners as soon as they are available and tests them against a virus database. Within minutes, the engines and signatures are tested, digitally signed by Microsoft, and posted. Antigen for Exchange can be configured to automatically download the latest updates without queuing or stopping mail traffic.

To ensure successful scan engine and signature file updates, Antigen for Exchange can be configured with redundant update paths if primary network connections are not functioning properly.

Centralized Management and Monitoring

Antigen for Exchange integrates with Antigen Enterprise Manager (AEM), a browser-based management console for all Antigen e-mail security products. AEM is a web-based console that provides centralized deployment, quarantine management, signature updating, SMTP/SNMP alerting, and reporting. Antigen for Exchange also provides integration with Microsoft Operations Manager 2005 for availability and performance monitoring.

**These additional four engines are available as part of the Messaging Security Suite. Contact your Microsoft partner or sales representative for more information.*

Antigen for Exchange System Requirements

Features and functionality described require Microsoft® Windows Server™ 2003 or Windows® 2000; Microsoft Exchange Server 2000 or 2003; 128MB of available RAM; and 100MB of available disk space. Antigen for Exchange supports Exchange running on Microsoft Cluster Servers.

For more information about Antigen for Exchange, visit: http://www.microsoft.com/antigen

© 2006 Microsoft Corporation. All rights reserved. This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, Windows,Windows Server, and Antigen are registered or unregistered trademarks of Microsoft Corporation.