

Microsoft Forefront Security for Exchange Server

Multi-Engine Protection Against the Latest E-mail Threats

Microsoft® Forefront™ Security for Exchange Server integrates multiple scan engines from industry-leading security firms in a single solution to help businesses protect their Exchange messaging environments from viruses, worms, and spam.

Microsoft Forefront Security for Exchange Server ships with and integrates multiple scan engines to provide comprehensive, layered protection of Exchange messaging servers, while optimizing server performance and simplifying security management. Formerly known as Antigen for Exchange, this highly regarded product is in its tenth iteration. Forefront Security for Exchange Server with Service Pack 1 (SP1) now includes support for Exchange Server 2007 with SP1 and Windows Server® 2008. It also provides content filtering and manageability enhancements, including:

- Seamless support for organizations running IPv6.
- Installable keyword lists that can be used to eliminate profanity and discriminatory e-mail content in eleven languages.
- Improved integration with Microsoft System Center Operations Manager.

Today, e-mail viruses remain the single most costly threat to businesses in time and productivity losses.* Viruses, worms, spam, and other malware can cripple communications, glut server resources, crash systems, and grind work to a halt. And although nearly 97 percent of businesses used antivirus software in 2006, 65 percent of them suffered from attacks from viruses.*

Why? One reason is that businesses try to protect all mission-critical servers using software that has only one antivirus scan engine. If the engine fails to recognize

the latest risk quickly, a virus can rapidly breach every network node that uses the same vulnerable engine.

Overly restrictive defense practices create their own setbacks. Blocking an entire message when only a part of it is suspect leaves users without vital mail. Scanning every message at every server delays delivery and wastes resources. Installing and managing multiple, nonintegrated antivirus products compounds administration headaches. Redundant scanning of old e-mail, regardless of age, drains server resources.

It all adds up to greater vulnerability to a single point of failure, slower e-mail delivery, and hefty management costs.

Increase the Odds without Increasing the Overhead

Forefront Security for Exchange Server helps solve these problems by providing comprehensive layered antivirus protection while maintaining server uptime, optimizing server performance, and simplifying the security management of Exchange Server systems.

Comprehensive protection against the latest threats

Forefront Security for Exchange Server ships with several antivirus engines from leading security vendors. IT can run up to five scan engines at once on many layers throughout the Exchange Server environment. When one engine goes offline for an update, the others continue to scan mail at Exchange 2007 Edge, Hub, and Store servers—even mail coming from mobile devices. Signature updates for all engines are rapid and automated, helping guard against new threats as they occur.

For spam protection, Forefront Security for Exchange Server enables the premium

antispam and content filters within Exchange 2007 and helps keep them current automatically. Its heuristics and file-filtering technologies help protect enterprises against new threats by detecting viruses based on behavior and by catching dangerous files, such as executables, even with altered extensions.

Optimized performance to keep mail moving

Forefront Security for Exchange Server integrates with Exchange 2007 to help eliminate needless repeat scanning of messages after they've safely passed the first server. Without redundant scanning in transit, mail flows faster and servers don't stall from overload.

To enhance performance at Store servers, IT can selectively scan mailboxes for only the most likely virus candidates. Such incremental background scanning releases servers from re-scanning megabytes of old mail unnecessarily.

Simplified management to ease the IT burden

Automated signature and engine updates, migration protection to Exchange 2007 servers, and centralized control and management all lead to greater cost efficiencies and ease. Forefront Security for Exchange Server can be centrally configured, deployed, and updated in multi-server environments using the Microsoft Forefront Server Security Management Console. Forefront Security for Exchange Server with SP1 offers improved integration with Microsoft System Center Operations Manager (formerly MOM) through new health monitoring logs and alerts that enable administrators to proactively monitor the state of their Exchange 2007 protection.

How Microsoft Forefront Security for Exchange Server Works

Provides comprehensive protection

- **Multi-engine scanning, no single point of failure.** Provides ability to automatically apply and manage up to five antivirus scan engines at a time and use different combinations for Exchange 2007 Transport (Edge and Hub) and Store (Mailbox/Public Folder) servers. Even if one engine is offline or overlooks a threat, mail is scanned by the others, so there's no single point of failure. The product ships with engines from Ahnlab, Authentium, CA, Kaspersky Labs, Microsoft, Norman Data Defense, Sophos, and VirusBuster.
- **Premium spam protection.** Enables the premium antispam services within Exchange 2007, including Microsoft IP Reputation Service, Intelligent Message Filters (IMF) for content filtering, and antispam signature files. These antispam tools are enabled during install and automatically updated multiple times each day.
- **Layered protection.** Installs and enables scanning at different checkpoints, so that if a scan fails at the Edge, mail is still scanned at the Hub. This layered protection is a vital backup to help stop malicious attacks before they impact the network or end-user productivity.
- **Protection against new and hidden threats.** Blocks malicious code based on behavioral characteristics using built-in heuristics technology. Also configures file filtering rules to eliminate file types that are known for carrying viruses (for example, .exe), even if the file extension has been changed. Forefront Security for Exchange Server can also unpack and selectively repack compressed attachments, such as .zip files, after removing an infected or unwanted item. Forefront Security for Exchange Server with SP1 provides increased flexibility for scanning or blocking high-compression .zip files and RAR archives.

Optimized performance

- **Performance optimization settings.** Improves server performance and mail throughput with in-memory scanning (to avoid spooling data to disk) and

multiple scanning threads (to process more mail at once). Forefront Security for Exchange Server also helps IT strike the right balance of server performance and level of security with performance controls that can dynamically manage the number of engines used for a given scan job.

- **More efficient scanning in Transport and at the Store.** Eliminates redundant scanning of mail. Forefront Security for Exchange Server attaches a secure antivirus header stamp to each e-mail as it is first scanned at an Exchange 2007 Edge or Hub server. The mail is delivered without additional scanning, saving processing load at the Hub and Store. Also stops re-scanning weeks- or months-old mail at the Store by limiting the range of a background scan. Incremental background scanning can be scoped to inspect only messages that are most likely to be infected, such as those that are a few days old.
- **Uninterrupted mail flow during updates.** Keeps scan-engine signatures current without queuing or stopping mail. The multi-engine solution of Forefront Security for Exchange Server means that even when one engine is taken offline for an update, other engines continue to inspect mail.
- **Effective mail cluster support.** Keeps e-mail secure when a server fails and mail switches to another node. Forefront Security for Exchange Server helps ensure that both active and passive nodes have up-to-date configuration information and signatures. Its support for cluster configurations includes Exchange 2007 CCR Clusters.

Simplified management

- **Forefront Server Security Administrator.** Provides a built-in management console to fully configure Forefront Security for Exchange Server locally or remotely.
- **Centralized Web-based control.** Enables administrators to easily manage servers remotely, generate comprehensive reports, and receive outbreak alerts from across the infrastructure using Microsoft Forefront Server Security Management Console. This browser-based console provides central configuration, deployment,

and updating for all Forefront server security products.

- **One-stop, automated updates.** Updates multiple scan engines without IT effort. Microsoft constantly monitors its antivirus vendors for new signatures and engine updates. Within minutes, these updates are tested against a virus database, confirmed, and posted for automatic download by Forefront Security for Exchange Server or Forefront Server Security Management Console systems.
- **Migration protection.** Helps keep the entire messaging environment protected during migration to Exchange 2007. Customers who purchase Forefront Security for Exchange Server will also be licensed to use Microsoft Antigen for Exchange, Microsoft Antigen for SMTP Gateways, and Antigen Spam Manager to help protect their Microsoft Exchange Server 2003 and Microsoft Exchange 2000 Server environments.
- **Localized in 11 languages.** Manages messaging server security in English, Chinese (Simplified), Chinese (Traditional), French, German, Italian, Japanese, Korean, Portuguese (Brazil), Russian, or Spanish.
- **Integrated monitoring.** Enables administrators to monitor the health of Forefront Security for Exchange Server environments as part of corporate operational management practices using a management pack for Security Center Operations Manager.

Microsoft Forefront Security for Exchange Server with SP1 System Requirements

Features and functionality described require Windows Server 2003 or Windows Server 2008, Microsoft Exchange Server 2007 or Exchange Server 2007 with SP1, an x64 architecture-based computer, 512MB of RAM per server (1GB recommended), and 300MB of disk space. Forefront Security for Exchange Server with SP1 supports Exchange running on Microsoft Cluster Servers.

For more information about Microsoft Forefront Security for Exchange Server, visit <http://www.microsoft.com/forefront>