

Microsoft Forefront Security for Exchange Server

Multi-Engine Protection Against the Latest E-mail Threats

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

Microsoft Forefront Security for Exchange Server is one of several products in the Forefront security portfolio from Microsoft. Formerly known as Antigen for Exchange, this highly regarded product is in its tenth iteration as it comes under the Forefront brand. It ships with and integrates multiple scan engines to provide comprehensive, layered protection of Exchange messaging servers, while optimizing server performance and simplifying security management.

E-mail viruses remain the single most costly threat to businesses today 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 speed through the organization by breaching 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 slower e-mail delivery, greater vulnerability to a single point of failure, hefty management costs, and lost productivity.

Increase the Odds Without Increasing the Overhead

Microsoft 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 to maximize threat protection. IT can run up to five scan engines at once at multiple 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 with automated updates. And 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 if their extensions have been altered.

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 server resources from unnecessarily re-scanning megabytes of old mail.

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. It also supports Microsoft Operations Manager (MOM), for corporate-wide monitoring of Exchange servers.

* CSI/FBI 2006 Survey.

How Microsoft Forefront Security for Exchange Server Works

Comprehensive protection

- **Multi-engine scanning, no single point of failure.** 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.** Enable the premium antispam services within Exchange 2007, including Microsoft IP Reputation Service, Intelligent Message Filters (IMF) for content filtering, and antispam signature files, through Forefront Security for Exchange Server. These antispam tools are enabled during install and automatically updated multiple times each day.
- **Layered protection.** Install and enable 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.** Block malicious code based on behavioral characteristics using built-in heuristics technology, and configure 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.
- **Multi-vendor response to new threats.** Increase the odds for a quick resolution to new attacks. With Forefront Security for Exchange Server, multiple vendors are busy working on your behalf to block the latest virus outbreaks, and automatic downloads help ensure the first valid solution gets loaded as soon as it's available.

Optimized performance

- **Performance optimization settings.** Improve 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.** Eliminate 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 stop 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.** Keep 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 are available to continue inspecting mail.
- **Effective mail cluster support.** Keep 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.** Use this built-in management console to fully configure Forefront Security for Exchange Server locally or remotely.
- **Centralized Web-based control.** Easily manage servers remotely, generate comprehensive reports, and receive outbreak alerts from across the

infrastructure by managing Forefront Security for Exchange Server 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.** Update 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.** Help keep the entire messaging environment protected during migration to Exchange 2007. Customers who purchase Forefront Security for Exchange Server to help protect Exchange 2007 servers 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 Server 2000 environments.
- **Localized in 11 languages.** Manage messaging server security in English, German, French, Japanese, Italian, Spanish, Korean, Chinese (Simplified), Chinese (Traditional), Portuguese (Brazil), or Russian.
- **Integrated monitoring.** Monitor the health of Forefront Security for Exchange Server environments as part of corporate operational management practices using a management pack for Microsoft Operations Manager (MOM).

Microsoft Forefront Security for Exchange Server system requirements

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

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