McAfee Security for Email Servers

Robust content security for your Microsoft Exchange and Lotus Domino servers

McAfee® Security for Email Servers detects and filters viruses, worms, Trojans, and other potentially unwanted programs. Compatible with Microsoft Exchange or Lotus Domino servers, it blocks spam and filters messages to guard against inappropriate or sensitive information entering or leaving your network, helping you meet policy and compliance requirements.

McAfee connects content inspection, reputation analysis, and malware protection to secure your email. We offer businesses multiple layers of defense and deployment options for email security—a security Software-as-a-Service (SaaS) solution in the cloud, appliances, or virtual appliance gateways at the network perimeter along with protection on the email server.

Key Advantages

Keep your system up and running
Prevent viruses and worms from entering via email or propagating internally via Microsoft Exchange and Lotus Domino.

Keep your employees productive
Block spam and phishing attacks.

Single-console management
McAfee ePolicy Orchestrator provides a powerful, single management console to control, manage, and view reporting.

Protect critical data
Filter incoming and outgoing emails to preserve information security and reduce corporate liability.

Intuitive graphical user interface
Simple-to-use interface provides rich reporting, charts, and real-time email traffic statistics.

Regardless of which configuration you choose, Software-as-a-Service delivered in the cloud or as a software deployment, McAfee Security for Email Servers provides multilayered protection for incoming and outgoing email—from on-demand malware scanning to policy enforcement for preventing loss or abuse of sensitive data.

- *Industry-leading protection*—Uses award-winning McAfee in-memory and incremental on-demand scanning to remove viruses, worms, Trojans, and other threats from incoming and outgoing email
- *Strong internal safeguards*—Detects threats that may have either slipped past your perimeter defenses or entered your network via infected laptops and internal email. It also blocks spam with the anti-spam module.
- *Powerful content filtering*—Enforces corporate policies for email use by filtering for banned file types, offensive content, and plugging leaks of sensitive data
- *Single console management*—Uses the McAfee ePolicy Orchestrator® (McAfee ePO™) platform to deploy, manage security, and display detailed graphical reports

Features

Comprehensive malware protection

McAfee Email Security for Servers relies on real-time file reputation anti-malware that significantly reduces exposure to emerging threats. Using cloud-based, McAfee Global Threat Intelligence™, McAfee sends a fingerprint of any suspicious file for instant reputation analysis at McAfee Labs™. If the fingerprint is identified as known malware, an appropriate response is sent back in milliseconds to block or quarantine the file.

Protect your servers 24/7

Check incoming and outgoing email messages for viruses, worms, Trojans, and other malware. Additionally, scan all internal emails to block a worm propagating internally. Automatically download the latest virus definitions (.DAT files) via HTTP, FTP, network file share, or the McAfee ePO centralized management console.

Enforce compliance

Filter messages based on size, message content, or attachment content. Block or quarantine messages that contain controlled content in the subject, message body, or attachments.

Save time and resources

Pre-built content filters simplify policy creation and enforcement. Create rules on a global basis, with exceptions as needed for individuals and departments. Manage via the built-in HTML interface or the McAfee ePO platform.

Filter spam and boost productivity

Catch more than 99 percent of spam and phishing emails with the anti-spam module to maintain employee productivity and reduce wasted email server storage. Users may create their own whitelists and blacklists. A single quarantine solution shared with the McAfee gateway email solutions provides an easy way for users to access a single quarantine.

Specifications

With exponential growth in email and shared data on email servers, McAfee Security for Email Servers supports both the Microsoft Exchange and Lotus Domino environments to keep employees productive and organizations up and running 24/7.

Minimum requirements for Microsoft Exchange 2003

- Microsoft Exchange 2003, with Service Pack 1 (SP1) or later running
- Microsoft Windows Server 2003 Standard or Enterprise Edition (32-bit)

Minimum requirements for Microsoft Exchange 2007

- x64 architecture-based processor with EM64T or AMD64 support
- Microsoft Exchange 2007 with SP1 or higher
- Microsoft Windows 2003 Server, 2003 R2 Standard or 2003 Enterprise, with latest SPs (64-bit)
- Microsoft Windows 2008 Server with SP2 (64-bit)

Minimum requirements for Microsoft Exchange 2010

- x64 architecture-based processor with EM64T or AMD64 support
- Microsoft Windows 2008 Server or 2008 R2 Server (Standard or Enterprise) with SP2 (64-bit)

Minimum requirements for Lotus Domino on a Microsoft Windows server

- Microsoft Windows 2003 Server, Microsoft Windows 2003 Enterprise Server with SP2 or later, Microsoft Windows 2008 Server with SP2
- Supported Lotus Domino versions: 6.0.2 or later, 7.0.2, 8.0.x, 8.5 (32-bit and 64-bit)

Minimum requirements for Lotus Domino on Linux servers

- Novell SUSE Linux Enterprise Server (SLES) 10, 10 SP1 and 10 SP2 (32-bit and 64-bit)
- Red Hat Enterprise Linux (RHEL) 5.0, 5.2 and 5.3 (32-bit and 64-bit)
- Lotus Domino 8.5 (32-bit and 64-bit)

Minimum requirements for Lotus Domino on IBM AIX servers

- System: IBM AIX v5.3
- Power 4 and higher
- Other software: Lotus Domino 6.0 and later (including 6.0, 6.5, 7.0, 8.5 (32-bit only))

Stay updated with less effort

Count on automatic updates to keep you current with the latest security intelligence from McAfee Labs, the world's top threat research center.

Centralize and consolidate your email quarantines

Included in McAfee Security for Email Servers, McAfee Quarantine Manager (MQM) consolidates quarantine and anti-spam management functionality in a single solution. MQM is easy to manage, allows sample submission to McAfee Labs, and provides fine-grained administrative controls, automatic user synchronization from LDAP servers, management of user or global blacklists and whitelists, and granular reporting—all managed from the McAfee ePO platform.

Network connection reputation

As the most precise and comprehensive reputation system available, the McAfee network connection reputation technology provides active, global threat intelligence based on the behavior of every type of entity on the Internet. McAfee scores for IP addresses, messages, domains, URLs, and file attachments are integrated into McAfee email security solutions, providing real-time analysis of more than one-third of the world's enterprise messaging traffic. This intelligence blocks up to 80 percent of connections based purely on reputation data while maintaining a false positive rate of less than one in one million.

Support all your servers

Ensure protection for your email servers on major operating systems, including Microsoft Windows, Linux, and IBM AIX, on 32-bit and 64-bit platforms.

Scan and protect email stores

Support for on-demand scanning (for example, archive scanning).

Filter spam, and manage via SaaS

McAfee Security for Email Servers is bundled into our endpoint suites, including McAfee SaaS Endpoint and Email Protection Suite. With a subscription to McAfee Saas Endpoint and Email Protection, you can deploy McAfee Security for Email Servers and reduce management infrastructure by having McAfee host the platform offsite. Setting email policies and reviewing new email traffic reports is easily achieved by accessing the web-based management console, available 24/7.

Figure 1. The simple-to-use interface provides rich reporting, charts, and real-time email traffic statistics.

McAfee, Inc.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee, the McAfee logo, McAfee ePolicy Orchestrator, McAfee ePO, and McAfee Labs are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright ©2010 McAfee, Inc.
9608ds_security-for-email-servers_1110_fnl_ASD