McAfee Security for Email Servers

Provide robust content security for your Microsoft Exchange servers

McAfee® Security for Email Servers detects and filters viruses, worms, Trojans, and other potentially unwanted programs. Compatible with Microsoft Exchange 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.

As a part of the McAfee product offering, 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 our award-winning in-memory and incremental on-demand scanning to remove viruses, worms, Trojans, and other threats from incoming and outgoing email.
- **Advanced threat detection**—Tight integration with McAfee Advanced Threat Defense through McAfee Threat Intelligence Exchange enables in-depth analysis and identification of potential zero-day threats within email attachments.
- **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 antispam 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.

Multilayered Email Protection

Comprehensive malware protection

McAfee Security for Email Servers relies on real-time file reputation anti-malware that significantly reduces exposure to emerging threats. Using our cloud-based Global Threat Intelligence (GTI), we send a fingerprint of any suspicious file to McAfee Labs for instant reputation analysis. If the fingerprint is identified as known malware, an appropriate response is sent back in milliseconds to block or quarantine the file. Files that remain suspicious are automatically sent to McAfee Advanced Threat

McAfee connects content inspection, reputation analysis, and malware protection to secure your email. We offer multiple layers of defense and deployment options for email security—edge transport at the network perimeter, hub transport server, and mailbox server.

Connect With Us

Defense for in-depth sandbox analysis. Integration through McAfee Threat Intelligence Exchange enhances protection by enabling McAfee Security for Email Servers and all connected solutions throughout the ecosystem to take action on malicious attachments.

Message reputation

McAfee GTI message reputation is our comprehensive, real-time, cloud-based message and sender reputation service that enables our products to protect customers against both known and emerging message-based threats such as spam. Message reputation combines with factors such as spam sending patterns and IP behavior to determine the likelihood that the message in question is malicious. The score is based not only on the collective intelligence from sensors querying the McAfee cloud and the analysis performed by McAfee Labs, but also on the correlation of cross-vector intelligence from web, email, and network threat data.

IP reputation

Detect threats from email messages based on the sending server's IP address. IP reputation prevents damage and data theft by blocking the email messages at the gateway.

URL reputation

Protects from known and emerging web-based threats based on reputation of the URL embedded in the email.

Protect your servers 24/7

Check incoming and outgoing email messages for viruses, worms, Trojans, and other malware. Additionally, you can scan all internal emails to block a worm from propagating internally. McAfee Security for Email Servers automatically downloads 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.

Less time and resources

Prebuilt 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.

Content filtering

Scans content and text in the subject line or body of an email message and email attachment. Create your own content filtering rules based on regular expressions (Regex).

Data loss prevention and compliance

Data loss prevention (DLP) ensures that email sent (in motion) or at rest is in accordance with your organization's confidentiality and compliance. Prebuilt dictionaries for enterprise and country-specific compliance rules provide quick setup. The built-in workflow automatically forwards quarantined emails to auditors for review.

Key Advantages

- **Keep your system up and running:** Prevent viruses, worms, and advanced threats from entering via email or propagating internally via Microsoft Exchange.
- **Keep your employees productive:** Block spam and phishing attacks.
- **Single-console management:** McAfee ePO software 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 using DLP and reputation technologies (IP, message, URL, and file reputation).
- **Intuitive graphical user interface:** Simple-to-use interface provides rich reporting, charts, and real-time email traffic statistics.

Filter spam and boost productivity

Catch spam and phishing emails with the antispam 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 our gateway email solutions provides an easy way for users to access a single quarantine.

Product health alerts

McAfee Security for Email Servers sends notifications to the specified administrator regarding the product's status. It monitors the time taken to scan each file. In case of any problem, it takes corrective action to avoid adverse impact on exchange server performance.

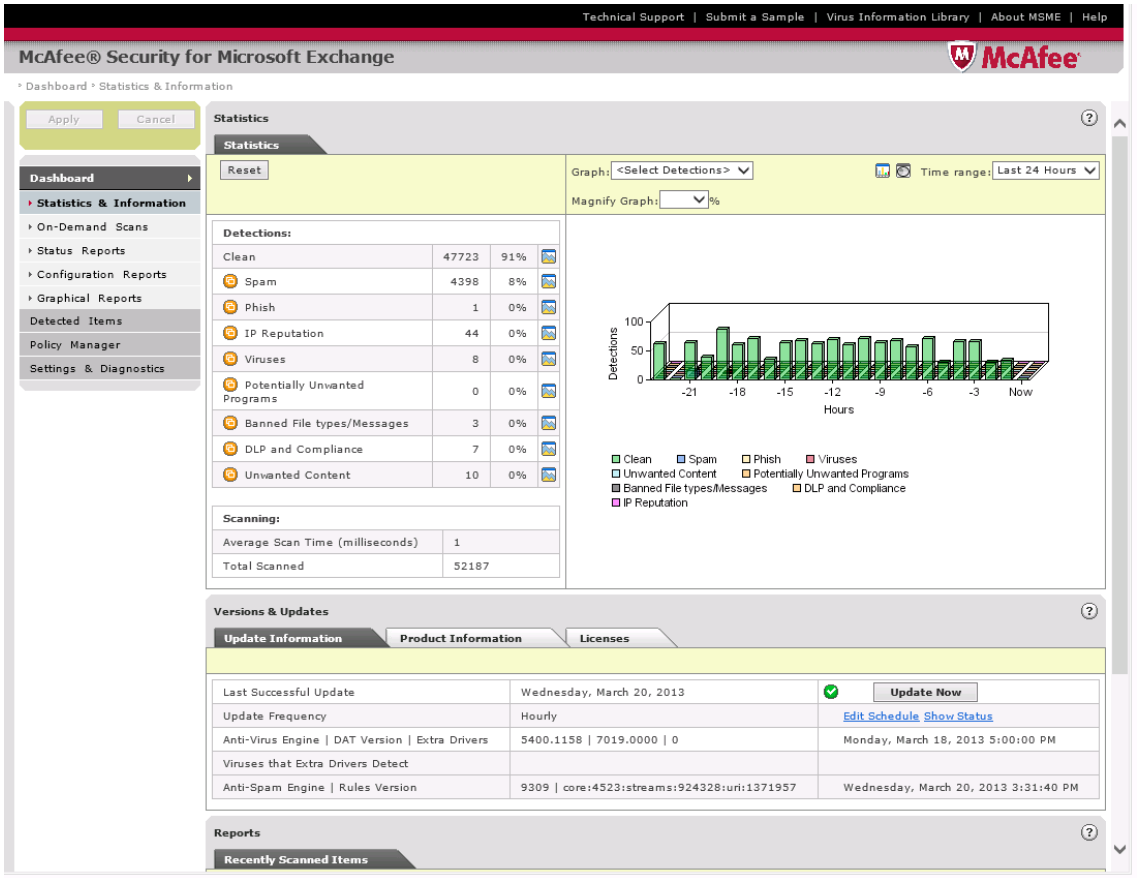

Figure 1. The simple-to-use interface provides rich reporting, charts, and real-time email traffic statistics.

Specifications

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

Requirements for McAfee Security for Microsoft Exchange

Operating system requirements

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Microsoft Exchange server requirements

- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013
- Exchange Servers with cluster are supported

Updates easily

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 the solution, McAfee Quarantine Manager consolidates quarantine and antispam management functionality in a single solution. McAfee Quarantine Manager 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.

Scan and protect email stores

McAfee Security for Email Servers supports scheduled on-demand scanning with granular configuration options to quickly complete scanning as compared to traditional full scans. It includes an option to scan only emails with attachments, unread emails, subject, sender, recipient, CC, message ID, and received within a certain period and of a certain size.

For more information visit **McAfee Security for Email Servers**.

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