Symantec
A Division of Broadcom

Product Brief

Symantec Mail Security for Microsoft® Exchange 7.10

At A Glance

Secure

- Scanning service that provides safe or unsafe verdicts to the Exchange server as it requests a scan
- Repairs, deletes, or quarantines infected files
- Proactively secures email at the distribution point before attacks can spread to multiple users
- Supports MS Exchange Server 2013, 2016 and 2019

Protect

- Sends incoming or outgoing email to the Mail Security Engine to scan email and its attachments
- Exchange mailbox store can also be protected by scheduled or manual scans

Adapt

- Secures email stored on both small/large-scale email platforms
- Detects known existing threats
- Prevents zero-day attacks
- Examines email attachments to find potential threats
- Blocks spam and detects phishing attempts against users

Overview

Superior protection with unparalleled performance

Symantec Mail Security for Microsoft Exchange (Mail Security) combines Symantec anti-malware technology with advanced heuristics and file reputation to provide real-time protection for email against viruses, spyware, phishing, and other malicious attacks.

For additional protection, Mail Security offers Symantec Premium AntiSpam[1], technology. Together, these protections help to stop 99 percent of incoming spam with less than one false positive per million.

Mail Security enforces content filtering policies on Microsoft Exchange Server 2013, 2016 and 2019, while supporting hosted, Microsoft Hyper-V®, and VMware® virtualized Exchange server environments.

Mail Security complements other layers of protection by preventing the spread of email-borne threats and enforcing data loss prevention (DLP) policies.

Key Features

Protect against threats

Symantec engineers track reported outbreaks of threats (such as viruses, Trojan horses, and worms) to identify new risks. After a threat is identified, information about the threat (a signature) is stored in a definition file. This file contains information to detect and eliminate the threat. When Mail Security scans for threats, it searches for these signatures.

Identify spam email

Spam is unsolicited bulk email, which most often advertises messages for a product or service. It wastes productivity, time, and network bandwidth. Symantec Premium Antispam provides continuous updates to the premium antispam filters to ensure that your Exchange server has the most current spam detection filters.

Optimized for Microsoft® Exchange

Edge and hub-focused scanning leverages anti-virus stamping to eliminate redundant scanning and minimize impact to the email store. Mail Security supports Microsoft Exchange 2013, 2016, and 2019 Microsoft Hosted Exchange, 64-bit Windows, VMware®, and Microsoft Hyper-V® Virtualized environments.

Mail Security can protect one or more Exchange servers from the same console. By switching between the server view and group view, you can manage the configuration settings for individual servers or all servers in a specific location. You can also define policies to detect potential risks to your Microsoft Exchange email system and process email messages and attachments that contain threats.

Mail Security provides flexible, real-time, scheduled, and manual scanning that provides efficient protection. Utilizing In-memory scanning and effective multi-threading improves performance. Consolidated security reporting enables customers to view and analyze the security posture of their Microsoft Exchange environment in detail.

[1] AntiSpam activation requires purchase of additional license.

Key Features

Manage outbreaks

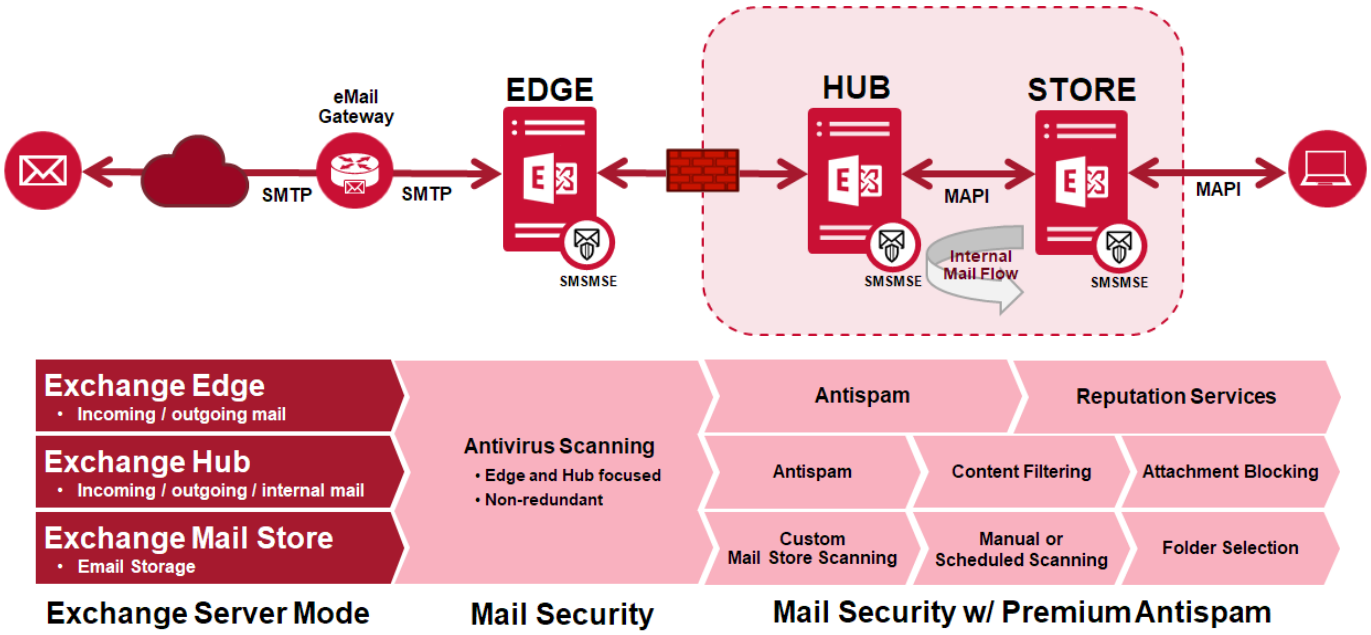
Mail Security lets you manage outbreaks quickly and effectively by setting outbreak rules and sending notifications when an outbreak is detected. You can also select an action to take when an outbreak is detected, such as the following:

- Delete the entire message.
- Delete the attachment or the message body.
- Quarantine entire message and replace with text.
- Quarantine the attachment or the message body.
- Log the event.
- Add a Tag to the beginning of the subject line.

You can set rules to define an outbreak based on event. For example, the same threat occurs a specified number of times within a specified time period. You can also configure Mail Security to send notifications and alerts in the case of an outbreak.

Flexible Implementation

Mail Security can run on different Exchange server roles. Under each role protection is provided in either real-time, scheduled, and/or manual scanning processes to efficiently protect email at rest and in motion. From a high-level view focusing on the Exchange roles, when Mail Security is deployed on a specific role it supports the following protection services:



- Edge Transport Role: This role routes incoming and outgoing messages destined to the public Internet or received from the public Internet and intended for internal recipients. Mail Security for MS Exchange scans messages that are in motion for both malicious content such as viruses, malware, spyware, or spam. Also the sender of the message is evaluated against Symantec's reputation database to insure that no messages are received by bad senders.
- Hub Role: This role routes incoming and outgoing messages within the private network. Typically if messages need to be sent to partner domains within the same network the Hub is used to route that message. Mail Security scans messages that are in motion and provides antivirus protection, antispam protection, content filtering, and attachment filtering.
- Mail Store: This role stores messages that have been routed by the Hub or Edge server. Mail Security scans messages at rest within the mail store database. Mail Security provides the ability to scan the message store to ensure that no threats have bypassed the real-time scanning enforced within the Edge or Hub. In addition if content has later been identified that should not be stored in the mail store database, Administrators can use Mail Security to search and remove that message.

Key Features

Monitor, Report and Notify

Mail Security logs extensive report data on threats, security risks, violations, spam, and server information to the reports database. You can use this data to generate summary or detailed reports based on different subsets of the data.

Scan data is collected from your Exchange servers and generates reports. Mail Security provides the preconfigured report templates that you can modify. You can also create your own report templates.

Several options are provided for notifying administrators, internal senders, and email recipients of threats and violations. Mail Security lets you define the conditions in which to send an alert as well as the alert message text for each alert condition that you define.

Filter undesirable message content and attachments

Mail Security lets you create the filtering rules that you can use to filter email messages and attachments. Mail Security provides the predefined file name and file type filtering rules that you can use to enforce email attachment policies. Mail Security uses match lists to filter email messages and attachments for specific words, terms, and phrases.

Mail Security provides the predefined content filtering policy templates that help prevent data leakage. You can also block active content by enabling features that remove DDE, JavaScript, Macros, and Embedded Files from Office and PDF documents where the original file is quarantined for later retrieval as needed.

A local quarantine feature is provided that can store the infected message bodies and attachments that are detected during scans. You can configure Mail Security to quarantine threats and security risks, and file filtering violations in the local quarantine.

Keep your protection up-to-date

Mail Security relies on up-to-date information to detect and eliminate risks. One of the most common reasons computers are vulnerable to attacks is that definition files are out-of-date. Symantec regularly supplies updated definition files.

Using LiveUpdate, Mail Security connects to a Symantec server over the Internet and automatically determines if definitions need to be updated. If they do, the definition files are downloaded to the proper location and installed. You must have a valid license to update definitions.

Additional Information

Learn More:

https://www.broadcom.com/products/cyber-security/network/messaging/mail-security-exchange

Documentation:

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/symantec-mail-security-for-microsoft-exchange-server/7-10.html

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com