

Kaspersky Security 8.0

для Microsoft®
Exchange Servers

Kaspersky Security 8.0 для Microsoft® Exchange Servers – это решение для защиты пользователей корпоративной почтовой системы от вредоносных программ и спама.

Электронная почта сегодня стала одним из основных каналов распространения вредоносных программ и спама. Вирусные эпидемии наносят компаниям значительный финансовый ущерб, приводя к потере данных, а поток спама вынуждает сотрудников компании тратить рабочее время на удаление из своих почтовых ящиков десятков и даже сотен нежелательных писем. Kaspersky Security 8.0 для Microsoft® Exchange Servers обеспечивает всестороннюю антивирусную проверку сообщений и избавляет пользователей почтовой системы от нежелательной корреспонденции, используя интеллектуальные технологии распознавания спама.

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Интеллектуальное распознавание и эффективная защита от спама

Интеллектуальные технологии распознавания спама. Приложение проверяет все сообщения на наличие признаков спама, используя фильтрацию по формальным признакам (e-mail и IP-адрес отправителя, размер письма, заголовок). Кроме того, содержимое каждого письма и его вложений анализируется с помощью интеллектуальных технологий, в том числе уникальных графических сигнатур для распознавания спама, присылаемого в виде изображений.

НОВШЕСТВО! **Дополнительная проверка сообщений.** Для дополнительной защиты от спама используется проверка сообщений по спискам DNSBL, содержащим спамерские адреса, а также технология SURBL, распознающая спамерские URL в тексте письма.

Классификация сообщений. Администратор может задавать отдельные правила обработки для каждой категории нежелательной корреспонденции, что исключает потерю важной информации: однозначно нежелательные сообщения могут быть заблокированы, подозрительные письма – доставлены в папку «Нежелательная почта», а формальные сообщения (например, подтверждения о доставке и прочтении сообщений) – в папку «Входящие».

НОВШЕСТВО! **Белые и черные списки.** В приложении предусмотрена возможность создания собственных доверенных (белых) и черных списков, которые формируются по SMTP- или по IP-адресу отправителя. Белый список можно также сформировать по SMTP-адресу получателя.

Если адрес занесен в белый список, то такое письмо не проверяется и доставляется непосредственно получателю; если адрес находится в черном списке, письмо маркируется специальным заголовком и далее обрабатывается согласно установленным администратором правилам.

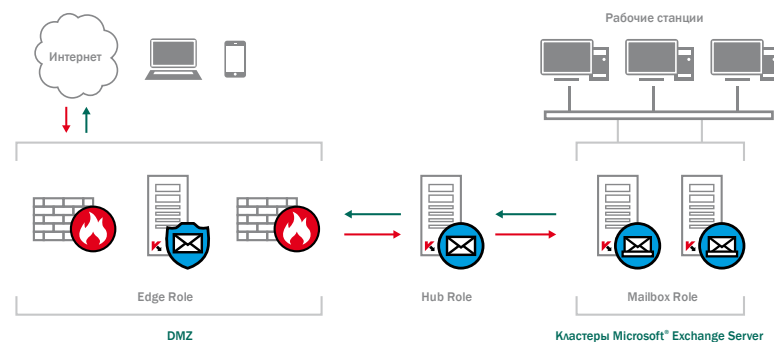


Схема работы Kaspersky Security 8.0 для Microsoft® Exchange Servers

ОСОБЕННОСТИ ПРИЛОЖЕНИЯ

НОВШЕСТВО!

Новое ядро для распознавания спама. Обеспечивает повышенную производительность и устойчивую работу приложения при низких требованиях к объему оперативной памяти.

НОВШЕСТВО!

Новое антивирусное ядро. Гарантирует более высокую скорость проверки и меньшее потребление ресурсов системы.

НОВШЕСТВО!

Защита Microsoft® Exchange Server 2010, включая DAG-конфигурацию. Приложение совместимо с DAG (Database Availability Group) – системой обеспечения высокой доступности сервиса.

НОВШЕСТВО!

Гибкие настройки. Продуманная система настроек защиты от спама и вирусов позволяет учитывать все особенности бизнес-процессов компании.

НОВШЕСТВО!

Проверка сообщений на всех языках. Приложение проверяет на наличие спама сообщения, написанные на разных языках, в т.ч. на языках азиатской группы.

НОВШЕСТВО!

Сертификат VMware Ready. Приложение защищает почтовый трафик, проходящий через серверы Microsoft® Exchange, установленные как на физических, так и виртуальных (гостевых) машинах.

Эффективная защита от вредоносных программ

Проверка в режиме реального времени. Программа осуществляет поиск и удаление всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения практически любых форматов. Приложение выявляет и удаляет не только однозначно вредоносные, но и потенциально опасные программы.

Фоновая проверка по запросу или по расписанию. Приложение проверяет общие папки и сообщения, хранящиеся на сервере, в фоновом режиме, что гарантирует обработку всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер.

Резервное копирование. Приложение сохраняет копии сообщений в резервном хранилище перед их лечением или удалением, что позволяет восстановить важную информацию в случае некорректного лечения объекта или ошибочного отнесения письма к категории «спам». Для удобства нахождения объекта в резервном хранилище предусмотрен широкий набор параметров поиска.

Гибкое администрирование

НОВШЕСТВО! Тонкая настройка. Администратор может настраивать работу приложения в зависимости от политики безопасности организации и возможностей оборудования – например, исключить из проверки определенные типы файлов или настроить уровень интенсивности антиспама. Также можно настраивать сценарии поведения антивируса и антиспама для разных категорий писем, создавать белые и черные списки, формируя их по отправителям или получателям, и многое другое.

Обновления баз. Обновление антивирусных баз может производиться по запросу или автоматически по расписанию с серверов «Лаборатории Касперского» в интернете или с заданных локальных серверов компании. Обновления антивирусных баз и баз для распознавания спама могут производиться независимо друг от друга.

Управление через MMC. Настройка и администрирование (в т.ч. удаленное) приложения осуществляются через единую консоль управления, встраиваемую в Microsoft® Management Console (MMC) – удобный и привычный для администратора инструмент управления.

Подробные отчеты. Администратор может контролировать работу приложения и состояние антивирусной защиты, используя наглядные HTML-отчеты или просматривая журнал событий Windows®. Периодичность формирования отчетов и их содержание задаются администратором. Отчеты могут храниться на диске или рассылаться по электронной почте.

Система оповещений. В приложение встроена удобная система оповещения администратора – по электронной почте или через журнал событий Windows®, где администратор может просматривать сообщения о работе программы наряду с сообщениями приложений Windows®.

ЗАО «Лаборатория Касперского», Россия, Москва, 123060, 1-й Волоколамский пр-д, 10, стр. 1
Тел.: +7 (495) 797-8700, +7 (495) 956-7000
www.kaspersky.ru | info@kaspersky.ru | www.securelist.ru

© ЗАО «Лаборатория Касперского», 1997-2010. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей. Microsoft, Windows Server и Windows – зарегистрированные товарные знаки или товарные знаки Microsoft Corporation в США и/или других странах.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Минимальные аппаратные требования

Соответствуют требованиям
Microsoft® Exchange Server

Поддерживаемые ОС

- Windows Server® 2008 R2
- Windows Server® 2008 x64
- Microsoft® Small Business Server 2008
- Microsoft® Essential Business Server 2008
- Windows Server® 2003 R2
- Windows Server® 2003 x64 SP2

Подробная информация на сайте:

www.kaspersky.ru

Kaspersky Security 8.0 для Microsoft® Exchange Servers можно приобрести в составе линейки Kaspersky Open Space Security и в составе решения Kaspersky Security для почтовых серверов. Для выбора подходящего продукта обратитесь к ближайшему к вам партнеру компании (подробнее см. на сайте www.kaspersky.ru)

Октябрь 2010

СЕРТИФИКАТЫ и НАГРАДЫ

