

# McAfee Security for Email Servers

## Надежное средство защиты содержимого для серверов Microsoft Exchange

McAfee® Security for Email Servers обнаруживает и отфильтровывает вирусы, черви, трояны, а также иные потенциально нежелательные программы. Решение совместимо с серверами Microsoft Exchange, блокирует нежелательную почту и выполняет фильтрацию сообщений для защиты от проникновения в вашу сеть информации неподобающего характера и предотвращения утечки конфиденциальных данных, помогая обеспечивать соответствие политикам и нормативно-правовым требованиям.

Составная часть спектра продуктов McAfee, решение McAfee Security for Email Servers обеспечивает многослойную защиту входящих и исходящих сообщений, начиная со сканирования сообщений на наличие вредоносных программ по запросу, до принудительного применения политик с целью предотвращения утечки данных или несанкционированного использования конфиденциальной информации.

- **Лучшая в отрасли защита.** Решение использует наши передовые технологии для сканирования в памяти и добавочного сканирования по запросу, позволяющие удалять вирусы, черви, трояны, а также иные угрозы, относящиеся к входящей и исходящей электронной корреспонденции.
- **Обнаружение сложных угроз.** Тесная интеграция с McAfee Advanced Threat Defense

посредством McAfee Threat Intelligence Exchange позволяет проводить глубокий анализ и выявлять потенциальные угрозы «нулевого дня» внутри вложений в сообщениях электронной почты.

- **Мощная внутренняя защита.** Обнаруживает угрозы, способные проникать сквозь защиту периметра или попадать в сеть через зараженные ноутбуки и внутреннюю электронную почту. Решение также блокирует нежелательную почту с помощью модуля защиты от нежелательных сообщений.
- **Мощные средства фильтрации содержимого.** Решение обеспечивает применение корпоративных политик защиты электронной почты с помощью фильтрации запрещенных типов файлов и содержимого оскорбительного характера, а также блокирования каналов утечки конфиденциальной информации.

Для защиты вашей электронной почты McAfee объединяет средства проверки содержимого, анализа репутации и защиты от вредоносных программ. Мы предлагаем несколько слоев защиты и вариантов развертывания, включая пограничный транспортный сервер на периметре сети, транспортный сервер-концентратор и почтовый сервер.

### Ключевые преимущества

- **Постоянная доступность и работоспособность ваших систем.** Предотвращайте проникновение вирусов, червей и сложных угроз через электронную почту и их распространение внутри ваших систем через серверы Microsoft Exchange.

Подписаться



## ЛИСТ ДАННЫХ

- **Управление через единую консоль.** В решении используется платформа McAfee ePolicy Orchestrator® (McAfee ePO™) для развертывания, управления системой безопасностью и просмотра подробных графических отчетов.

### Многослойная защита электронной почты

#### Комплексная защита от вредоносных программ

Защита от вредоносных программ в решении McAfee Security for Email Servers обеспечивается с помощью средств анализа репутации файлов, работающих в режиме реального времени и значительно снижающих уязвимость электронной почты к новым угрозам. После обнаружения подозрительного файла его отпечаток посредством облачной службы Global Threat Intelligence (GTI) направляется в McAfee Labs, где сразу же проводится анализ его репутации. Если отпечаток будет распознан как известная вредоносная программа, то соответствующий ответ для блокирования файла или помещения его в карантин последует в течение миллисекунд. Оставшиеся подозрительные файлы автоматически направляются в McAfee Advanced Threat Defense для проведения углубленного анализа в изолированной среде («песочнице»). Эта интеграция осуществляется посредством McAfee Threat Intelligence Exchange и дает McAfee Security for Email Servers и всем взаимосвязанным решениям во всех точках экосистемы возможность принимать необходимые меры реагирования при обнаружении вредоносных вложений.

#### Репутация сообщений

Технология оценки репутации электронной почты с помощью технологии McAfee GTI — наш комплексный облачный сервис, который в реальном времени анализирует репутацию электронных сообщений и их отправителей. Благодаря этому сервису наши продукты могут защитить клиентов от известных и новых угроз, исходящих от электронных сообщений, в том числе от спама. Для оценки вероятности вредоносного характера сообщения решение применяет технологию анализа репутации электронных сообщений, а также такие факторы, как шаблоны рассылки нежелательных сообщений и поведение IP-адресов. Получаемый рейтинг основан не только на совокупной информации датчиков, направляющих запрос в облако McAfee, и на анализе, выполненном в лаборатории McAfee Labs, но также на корреляции информации о различных угрозах, включая веб-трафик, электронную почту и сети.

#### Репутация IP-адресов

Используя IP-адрес передающего сервера, решение обнаруживает угрозы, содержащиеся в электронных сообщениях. Оценка репутации IP-адресов предотвращает ущерб и хищение данных благодаря блокированию электронных сообщений у шлюза.

#### Репутация URL-адресов

Анализ репутации URL-адресов, включенных в сообщения электронной почты, позволяет обеспечивать защиту от известных и новых веб-угроз.

- **Поддержание уровня производительности труда ваших сотрудников.** Блокируйте нежелательные сообщения и фишинговые атаки.
- **Управление через единую консоль.** Программное обеспечение McAfee ePO предоставляет мощную единую консоль управления, обеспечивающую контроль и администрирование систем, а также функцию просмотра отчетов.
- **Защита критически важных данных.** Выполняйте фильтрацию входящих и исходящих сообщений, направленную на защиту информации и снижение уровня корпоративной ответственности с помощью технологий защиты от утечки данных (DLP) и оценки репутаций IP-адресов, сообщений, URL-адресов и файлов.
- **Интуитивно понятный графический пользовательский интерфейс.** Удобный интерфейс обеспечивает подробные отчеты, таблицы, а также статистику почтового трафика, получаемую в режиме реального времени.

### Круглосуточная защита ваших серверов

Решение выполняет проверку входящих и исходящих сообщений электронной почты на наличие вирусов, червей, троянов и иных вредоносных программ.

Кроме того, вы можете сканировать всю внутреннюю электронную корреспонденцию, чтобы блокировать

червей и предотвратить их распространение внутри системы. McAfee Security for Email Servers автоматически загружает самые последние антивирусные базы (DAT-файлы) через HTTP, FTP, общий доступ к файлу в сети или централизованную консоль управления McAfee ePO.

### Спецификации

Объем электронной почты и совместно используемых данных, находящийся на почтовых серверах, растет в геометрической прогрессии. Решение McAfee Security for Email Servers поддерживает среды Microsoft Exchange, обеспечивая продуктивную работу сотрудников, а также работоспособность и доступность систем в режиме 24/7.

### Требования для установки решения McAfee Security for Microsoft Exchange

Требования к операционной системе

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

Требования к серверу Microsoft Exchange

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Поддерживаются серверы Microsoft Exchange Server с кластером

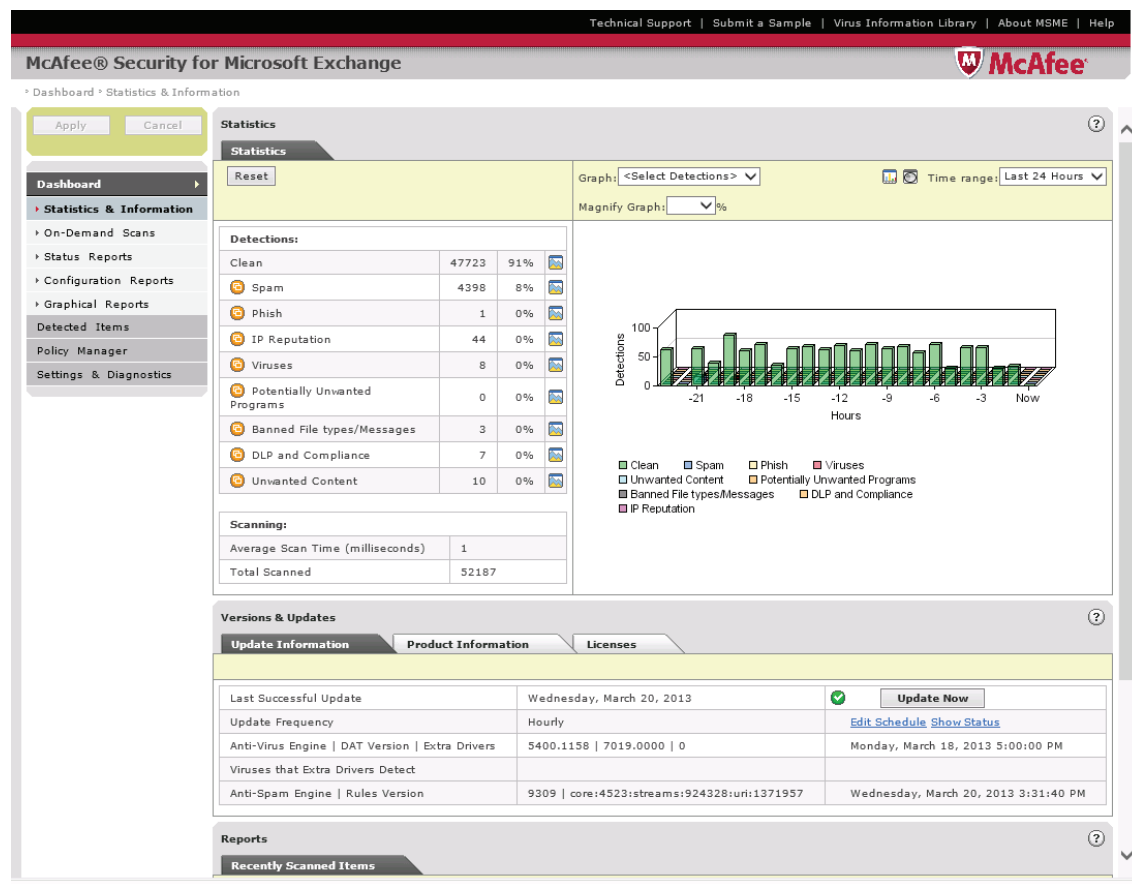


Рис. 1. Удобный интерфейс обеспечивает подробные отчеты, таблицы, а также статистику почтового трафика, получаемую в режиме реального времени.

### **Обеспечение нормативно-правового соответствия**

Фильтрация сообщений осуществляется путем анализа размера сообщения, содержания текста и содержания вложений. Решение блокирует или помещает в карантин сообщения, содержащие контролируемое содержимое в теме сообщения, в тексте письма или во вложениях.

### **Экономия времени и ресурсов**

Встроенные фильтры содержимого упрощают создание политик и их принудительное применение. Возможно создание глобальных правил с исключениями, необходимыми для отдельных сотрудников и структурных подразделений. Управление осуществляется через встроенный HTML-интерфейс или платформу McAfee ePO.

### **Фильтрация содержимого**

Решение сканирует содержимое и текст в строке темы, в тексте электронного сообщения и вложения. Возможно создание ваших собственных правил фильтрации содержимого на основе регулярных выражений (Regex).

### **Предотвращение утечки данных и обеспечение нормативно-правового соответствия**

Механизмы предотвращения утечки данных (DLP) обеспечивают соответствие отправленных (находящихся в процессе отправки) или хранимых электронных сообщений политикам и правилам защиты конфиденциальной информации, принятым

в вашей организации, а также нормативно-правовым требованиям. Встроенные словари, которые включают правила обеспечения нормативно-правового соответствия, специфические для каждой компании и каждой страны, обеспечивают быструю настройку фильтров содержимого. Встроенный бизнес-процесс автоматически направляет электронные сообщения, помещенные в карантин, на аудиторскую проверку.

### **Фильтрация нежелательной почты и повышение производительности**

Модуль защиты от нежелательной почты позволяет отфильтровывать нежелательные и фишинговые электронные сообщения, способствуя поддержанию производительности сотрудников и экономии дискового пространства на серверах электронной почты. Пользователи могут составлять свои собственные «белые» и «черные» списки. Концепция единого карантина, используемого совместно с нашими решениями для защиты шлюзов, позволяет пользователям без труда получить доступ к единому карантину.

### **Уведомления о техническом состоянии продукта**

McAfee Security for Email Servers направляет указанному администратору уведомления о состоянии продукта и отслеживает, сколько времени занимает сканирование каждого файла. В случае возникновения проблем решение принимает меры, необходимые для поддержания требуемого уровня быстродействия серверов Exchange.

### Простое автоматизированное обновление

С помощью автоматической рассылки обновлений вы всегда будете получать самые последние данные об угрозах от крупнейшего в мире центра исследований угроз McAfee Labs.

### Централизация и консолидация карантинных для вашей электронной почты

Включенный в решение диспетчер McAfee Quarantine Manager объединяет в едином решении функции помещения в карантин и управления программами защиты от нежелательной почты. Диспетчер McAfee Quarantine Manager удобен в управлении и позволяет направлять образцы угроз в McAfee Labs. Решение обеспечивает детальный административный контроль, автоматическую синхронизацию пользователей через серверы LDAP, управление пользователями или глобальными «черными» и «белыми» списками, а также формирование настраиваемых отчетов. Управление всеми этими операциями выполняется с помощью платформы McAfee ePO.

### Сканирование и защита хранилищ электронной почты

McAfee Security for Email Servers поддерживает функции планового сканирования по запросу, а также функции выборочной настройки, что позволяет выполнять сканирование быстрее, чем с помощью традиционного метода полного сканирования. Например, решение позволяет выполнять сканирование только электронных писем с вложениями или непрочитанных писем. Кроме того, вы можете сканировать сообщения по темам, отправителям, получателям, получателям копий писем, кодам сообщений. Далее можно установить настройки для сканирования писем, полученных в течение определенного периода времени или имеющих определенный размер.

Более подробная информация находится на сайте **McAfee Security for Email Servers**.



McAfee Ireland Ltd.  
Building 2000, City Gate  
Mahon, Cork, Ireland  
[www.mcafee.com/ru](http://www.mcafee.com/ru)

McAfee, логотип McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2020 McAfee, LLC. 4446\_0420 АПРЕЛЬ 2020 г.