Dr.Web для MIMEsweeper



Dr.Web для MIMEsweeper устанавливается на те же компьютеры, что и контентный фильтр MIMEsw

Продукт подключается к MIMEsweeper в качестве антивирусной и антиспам-политики проверки содержимого почтовых сообщений и осуществляет фильтрацию почты от вирусов, спама и прочей нежелательной корреспонденции. При обнаружении угроз Dr.Web для MIMEsweeper классифицирует нежелательную почту согласно назначенным политикам ClearSwift MIMEsweeper и обезвреживает обнаруженные вредоносные объекты.

Ключевые функции

- Проверка почтовых сообщений и их вложений, включая архивы, до их обработки почтовым сервером
- Лечение инфицированных объектов
- Изоляция инфицированных и подозрительных файлов в карантине
- Фильтрация почты на спам, в том числе с использованием чёрных и белых списков
- Ведение статистики работы комплекса
- Автоматические обновления

Простота установки и настройки

Встроенные в Dr.Web для MIMEsweeper средства конфигурации – мастера создания сценариев – позволяют автоматизированно создавать наиболее современные сценарии проверки сообщений (тип 1 по классификации ClearSwift).

Гибкие настройки

При обнаружении инфицированного объекта плагин пытается вылечить его или сразу удаляет, если опция лечения не выбрана. Если к почтовому сообщению прикреплено несколько файлов или архивов, плагин обезвреживает только зараженные вложения. При обнаружении вируса в теле письма контентный фильтр перемещает письмо в карантин. «Чистые» письма, файлы и архивы передаются получателю без изменений. Вредоносные письма, которые плагин Dr.Web не может нейтрализовать, помечаются и по умолчанию перемещаются в карантин.

Совместимость с DEP

Dr.Web для MIMEsweeper поддерживает технологию предотвращения выполнения данных (Data Execution Prevention, DEP), которая позволяет дополнительно проверять память и предотвращать запуск вредоносного кода. Благодаря этому пользователям не нужно менять режим работы DEP – вредоносные программы не смогут воспользоваться механизмом обработки исключений Windows.

Регистрация событий

Плагин Dr.Web регистрирует ошибки и происходящие события в журнале регистрации событий (Event Log) и текстовом журнале. В эти журналы заносится информация о запуске и остановке плагина, о параметрах модулей, сообщения об обнаружении вирусов для каждого зараженного письма и для каждого вируса в отдельности, сообщения об обнаружении спама. Плагин Dr.Web поддерживает английский и русский языки сообщений в журналах событий.

Карантин

Инфицированные и подозрительные файлы могут перемещаться в карантин. Впоследствии возможна дополнительная обработка этих файлов, в том числе извлечение необходимой информации, лечение или удаление.

Система оповещений

В зависимости от настроек сценария в заголовок и тело обезвреженных писем контентный фильтр может добавлять оповещение о результатах проверки и предпринятых плагином действиях.

Уникальные возможности ядра

- Проверка архивов любого уровня вложенности.
- Высочайшая точность выявления упакованных вредоносных объектов (даже тех, которые упакованы неизвестным Dr.Web методом), разбор их на компоненты и детальный анализ с целью обнаружения скрытых угроз.
- Детектирование и нейтрализация сложных вирусов, таких как Shadow.based (Conficker), MaosBoot, Rustock.C, Sector – в этом Dr.Web нет равных.
- Интеллектуальные технологии проверки памяти позволяют блокировать активные вирусы до появления их копий на жестком диске компьютера, что снижает вероятность использования вредоносным ПО уязвимостей установленных программ или операционной системы.
- Обнаружение и нейтрализация вирусов, которые действуют в оперативной памяти и никогда не встречаются в виде отдельных файлов (например, Slammer и CodeRed).

Борьба с неизвестными угрозами

- FLY-CODE – не имеющая аналогов технология универсальной распаковки файлов, запакованных неизвестными Dr.Web способами.
- Уникальная технология несигнатурного поиска Origins Tracing™ позволяет Dr.Web с высокой долей вероятности распознавать вирусы, еще не внесенные в вирусную базу.

- Эвристический анализатор Dr.Web эффективно детектирует все распространенные типы угроз, определяя их класс по результатам проведенного разбора и характерным признакам.

Преимущества антиспама Dr.Web

- Не требует обучения и настройки перед использованием. В отличие от обучаемых антиспам-систем, построенных, например, на анализе по Байесу, он начинает автоматически действовать с приемом первого сообщения. Таким образом, антиспам Dr.Web не требует ежедневной работы системного администратора
- Не зависит от языка, на котором написано сообщение
- Практически не увеличивает время приема почты
- Фильтрует почту в режиме реального времени
- Сочетает высокую скорость фильтрации с низким потреблением системных ресурсов
- Умеет разбирать объекты любой степени вложенности
- Может буквально на лету выбирать подходящую технологию обработки того или иного объекта в зависимости от конверта обрабатываемого письма или обнаруженных блокирующих объектов
- Не удаляет отфильтрованные письма, а перемещает их в специальную папку почтовой программы, где их можно проверить на предмет ложных срабатываний
- Позволяет полностью отказаться от черных списков – компанию невозможно скомпрометировать через злонамеренное внесение в них
- Абсолютно автономен: для его работы не требуется постоянной связи с внешним сервером или доступа к какой-либо базе данных, что позволяет существенно экономить трафик
- Нуждается в обновлении не чаще одного раза в сутки – уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил избавляют от необходимости скачивать частые и громоздкие обновления

Плагин vaderetro

В продуктах Dr.Web за проверку на спам и нежелательные сообщения отвечает плагин vaderetro, который осуществляет фильтрацию через собственную библиотеку (Vade Retro). Эта библиотека постоянно обновляется, обеспечивая непрерывное повышение качества фильтрации. Высокая продуктивность отсева почтового «мусора» сочетается с

низким потреблением системных ресурсов. Поэтому антиспам Dr.Web эффективно работает и на устаревшем оборудовании.

В зависимости от результатов анализа каждому письму, обработанному библиотекой Vade Retro, дается оценка – целое число в диапазоне от -10000 до +10000. Чем выше оценка, тем больше вероятность, что письмо является спамом.

Пороговое значение задается в параметре SpamThreshold конфигурационного файла плагина. Если оценка, полученная сообщением, равна значению параметра SpamThreshold или превышает его, то письмо классифицируется как спам.

Закончив анализ письма, библиотека Vade Retro может добавить в него (в зависимости от настроек плагина) соответствующие заголовки.

Технологии антиспам-фильтрации

Антиспам Dr.Web анализирует письма на основе нескольких тысяч правил, которые условно можно разбить на ряд групп.

- **Эвристический анализ**

Чрезвычайно сложная высокоинтеллектуальная технология эмпирического анализа всех частей сообщения: поля заголовка, тела сообщения и т.д. Анализируется не только само сообщение, но и, в случае наличия, вложение к нему. Эвристический анализатор постоянно совершенствуется, к нему непрерывно добавляются новые правила. Он работает «на опережение» и позволяет распознавать еще неизвестные разновидности спама нового поколения до выпуска соответствующего обновления.

- **Фильтрация противодействия**

Это одна из наиболее передовых и эффективных технологий антиспама Dr.Web. Она заключается в распознавании уловок, к которым прибегают спамеры для обхода антиспам-фильтров.

- **Анализ на основе HTML-сигнатур**

Сообщения, в состав которых входит HTML-код, сопоставляются с образцами HTML-сигнатур в библиотеке антиспама. Такое сравнение, в сочетании с имеющимися данными о размерах типичных для спама изображений, защищает пользователей от спам-сообщений с HTML-кодом, в которые часто включаются онлайн-изображения.

- **Технология детектирования спама по конвертам сообщений**

Детектирование подделок в «штемпелях» SMTP-серверов и в других элементах заголовков почтовых сообщений – новейшее направление развития методов борьбы со спамом. Адресу отправителя электронного сообщения нельзя доверять, так как злоумышленники могут с легкостью его подделать. Фальшивые письма содержат далеко не только спам. Это могут быть мистификации или средства давления на персонал, например, анонимки и даже угрозы. Специальные технологии антиспама Dr.Web позволяют выявлять поддельные адреса и не пропускать такие сообщения. Соответственно, обеспечена не только экономия трафика, но и защита сотрудников от получения поддельных писем, которые могут подтолкнуть их к непредсказуемым действиям.

- **Семантический анализ**

С его помощью слова и словосочетания в сообщениях сравниваются с типичной для спама лексикой. Сравнение производится по специальному словарю, причем анализу подвергаются как видимые, так и скрытые для человеческого глаза специальными техническими уловками слова, выражения и символы.

- **Антискамминг-технология**

Скамминг-сообщения (а также фарминг-сообщения – один из видов скамминга) – пожалуй, самая опасная разновидность спама. К их числу относятся так называемые «нигерийские письма», сообщения о выигрышах в лотерею, казино, поддельные письма банков и кредитных учреждений. Для их фильтрации в антиспаме Dr.Web применяется специальный модуль.

- **Фильтрация технического спама**

Автоматические уведомления электронной почты – bounce-сообщения – предназначены для информаирования пользователей о сбое в работе почтовой системы (например, о недоставке письма адресату). Аналогичные сообщения могут использовать и злоумышленники. Так, под видом технического уведомления на компьютер может проникнуть компьютерный червь или обыкновенный спам. Специальный модуль антиспама Dr.Web определяет такие нежелательные сообщения.

Всегда актуальный

- Процесс обновления происходит незаметно для пользователя — при подключении к сети Интернет, по запросу или по расписанию.
- Загрузка осуществляется быстро (даже на медленных модемных соединениях).
- Всегда имеются доступные серверы обновлений.
- По завершении обновления в большинстве случаев не требуется перезагружать компьютер: Dr.Web сразу готов к работе с использованием самых свежих вирусных баз.

- Обновления отличаются небольшими размерами — в пределах 50–200 КБ.

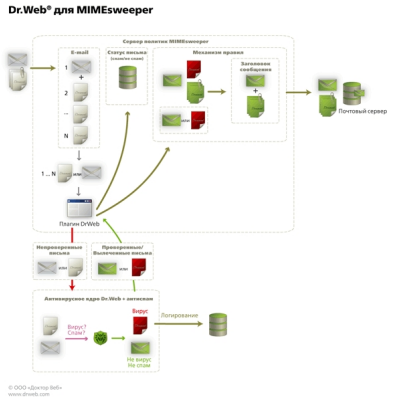
- Для экономии трафика можно настроить прием только обновлений вирусных баз. Включать эту опцию не рекомендуется. Dr.Web с целью противодействия новым киберугрозам постоянно совершенствуется. Новые возможности включаются в обновленные модули антивирусного пакета и автоматически загружаются с серверов компании при очередном обновлении.
- Скачивать обновления можно в виде заархивированных файлов — тем самым трафик экономится. Для уменьшения размеров скачиваемых обновлений компания «Доктор Веб» использует специальный алгоритм сжатия передаваемых данных. При незначительном исправлении или дополнении в вирусных базах или модулях программы применяются файлы-патчи, что сокращает объем передаваемых данных в десятки раз.

Служба вирусного мониторинга

- Служба вирусного мониторинга компании «Доктор Веб» собирает по всему миру образцы вредоносных объектов, изготавливает к ним противоядия и выпускает «горячие» обновления по мере анализа новой угрозы — до нескольких раз в час.
- С момента выпуска такие обновления сразу становятся доступными для всех пользователей Dr.Web с нескольких серверов обновления в разных точках земного шара.

- С целью избежать ложных срабатываний обновления перед выпуском тестируются на огромном массиве чистых файлов.
- Интеллектуальная система автоматизированного добавления родственных вирусов позволяет максимально оперативно нейтрализовать вирусные атаки.

Схема действия



Виды лицензий

- По числу защищаемых пользователей.
- Посерверная лицензия – для проверки неограниченного объема корреспонденции на одном сервере, с числом защищаемых пользователей не более 3 000.

Варианты лицензий

- Антивирус
- Антивирус + Центр управления

Также Dr.Web для MIMEsweeper доступен в составе экономичных Комплектов Dr.Web для малого и среднего бизнеса.

Системные требования

- Windows 2000 Server (SP4) или выше.
- Windows Server 2003 или выше.