

Dr.Web для почтовых серверов Lotus



Dr.Web для IBM Lotus Domino



Лицензии и сертификаты

Dr.Web для IBM Lotus Domino можно использовать в организациях, требующих повышенного уровня безопасности – продукт полностью отвечает требованиям российского законодательства и обладает сертификатами соответствия ФСТЭК России и ФСБ.

Ready for IBM Lotus software

Dr.Web для IBM Lotus Domino внесен в каталог решений IBM Lotus Business Solutions Catalog и имеет знак Ready for IBM Lotus software. Этот знак подтверждает совместимость продукта с системой Lotus Domino и свидетельствует о выполнении всех требований на соответствие IBM.

Исключительная вирусоустойчивость

Продукт может быть установлен на уже инфицированный сервер Lotus Domino и способен вылечить его без помощи дополнительных утилит. Все почтовые и другие базы данных могут сканироваться по требованию немедленно после установки. Для

повышения надежности такого сканирования предусмотрена возможность заблаговременного обновления вирусных баз, что позволяет повысить актуальность средств защиты.

Высокая скорость сканирования

Организация системы **Dr.Web для IBM Lotus Domino**, особая реализация метода проверки и возможность гибко управлять этим процессом позволили добиться высокой скорости сканирования при малом потреблении системных ресурсов. Благодаря функции многопоточной проверки антивирус способен обрабатывать одновременно большой объем почтовых сообщений. Это преимущество позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.

Простота установки и гибкость настроек

Предусмотрено автоматизированное и легко контролируемое развертывание **Dr.Web для IBM Lotus Domino**

. Программа поддерживает административные скрипты и имеет подробную документацию. Удобство управления комплексом обеспечивается благодаря возможности гибкого конфигурирования через консоль администратора. Средства «тонкой» настройки алгоритмов действий антивируса по результатам проверки позволяют отсылать уведомления об обнаруженных вирусах отправителю, получателям и администраторам системы, сохранять заголовки полученных почтовых сообщений и вложения к ним и т.д.

Удобство администрирования

Механизм группирования и управление группами значительно упрощают администрирование антивирусной защиты. Для каждой группы могут быть заданы индивидуальные установки. Также одни и те же установки могут быть заданы для нескольких групп при помощи редактирования соответствующего профиля.

Эффективная фильтрация почтового «мусора» без необходимости обучения антиспама

Встроенный антиспам существенно снижает нагрузку на сервер и увеличивает производительность труда сотрудников компании. Механизм черных и белых списков адресов позволяет исключать из проверки определенные адреса и увеличивать эффективность фильтрации.

Ключевые функции

- Проверка и фильтрация почтовых сообщений и всех их компонентов на вирусы, спам и нежелательные сообщения «на лету» или по заданию администратора.
 - Фильтрация почты на спам, в том числе по черным и белым спискам адресов
 - Проверка документов в заданных nsf-базах на наличие вирусов
 - Проверка объектов по требованию при помощи функции ручного запуска и остановки задач сканера
 - Разбор почтовых сообщений с выделением всех компонентов письма для последующего анализа
 - Лечение инфицированных почтовых сообщений и вложенных в них файлов
 - Детектирование вредоносных объектов в многократно заархивированных файлах
 - Использование механизма обнаружения вредоносных программ, скрытых неизвестными упаковщиками
 - Использование дополнительной технологии обнаружения неизвестных вредоносных объектов, которая увеличивает вероятность обнаружения вирусов новейших типов
 - Хранение инфицированных и подозрительных объектов в карантине (доступ к перемещенным в карантин объектам осуществляется через клиент Lotus Notes)
 - Уведомления о результатах проверки при помощи шаблонов, описанных в системе, что позволяет адресатам, администраторам и другим лицам получать информацию в максимально удобном виде
 - Ведение статистики работы системы
 - Защита работы собственных модулей от сбоев
 - Автоматические обновления
-

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.

- Антискаминг-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 информирования 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.

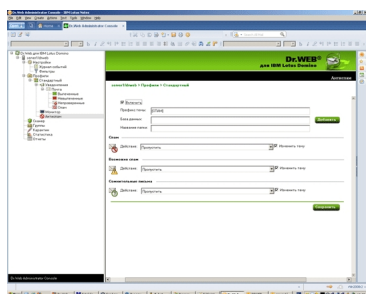
- Скачивать обновления можно в виде заархивированных файлов — тем самым трафик экономится. Для уменьшения размеров скачиваемых обновлений компания «Доктор Веб» использует специальный алгоритм сжатия передаваемых данных. При незначительном исправлении или дополнении в вирусных базах или модулях программы 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.

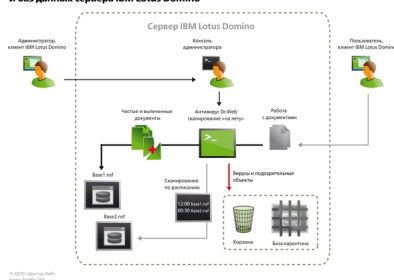
- С целью избежать ложных срабатываний обновления перед выпуском тестируются на огромном массиве чистых файлов.
- Интеллектуальная система автоматизированного добавления родственных вирусов позволяет максимально оперативно нейтрализовать вирусные атаки.

Галерея



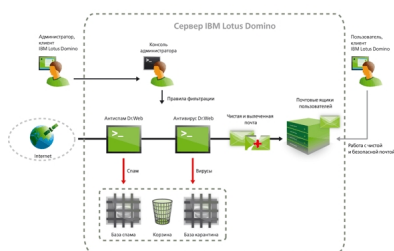
© ООО «Доктор Веб»
www.drweb.com

Антивирусная защита приложений и баз данных сервера IBM Lotus Domino



© ООО «Доктор Веб»
www.drweb.com

Антиспам и антивирусная защита электронной почты сервера IBM Lotus Domino



© ООО «Доктор Веб»
www.drweb.com

Виды лицензий

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

Программный продукт Dr.Web для IBM Lotus Domino можно приобрести отдельно или в составе комплекса Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются [Центр управления Dr.Web Enterprise Security Suite](#) и Антиспам.

Кроме того, в качестве дополнительного компонента Dr.Web для IBM Lotus Domino может выступать SMTP проху. Совместное использование обоих продуктов не только существенно повышает общую безопасность сети, но и снижает нагрузку на внутренние почтовые серверы и рабочие станции.

Варианты лицензий

- Антивирус
- Антивирус + Центр управления
- Антивирус + SMTP проху
- Антивирус + Центр управления + SMTP проху
- Антивирус + Антиспам
- Антивирус + Антиспам + Центр управления
- Антивирус + Антиспам + SMTP проху
- Антивирус + Антиспам + Центр управления + SMTP проху

Также Dr.Web для IBM Lotus Domino доступен в составе экономичных [Комплектов Dr.Web](#) для малого и среднего бизнеса.

Версия для Windows

- Операционная система: Windows Server 2000/2003/2008/2008R2 (32- и 64-битные)

версии);

- Lotus Domino версии R6.0 и выше (32- и 64-битные версии);
- Процессор Intel Pentium 133 и выше;
- RAM 256 MB (рекомендуется 512 MB);
- Свободное дисковое пространство: 60 MB.

Версия для Linux

- Операционная система: Red Hat Enterprise Linux (RHEL) 4 и 5 версии, Novell SuSE Linux Enterprise Server (SLES) 9 и 10 версии (только 32-битные);
- Lotus Domino версии 7.x или 8.x;
- Lotus Notes 6.5 (или более поздний) для Windows
- Процессор Intel Pentium 133 и выше;
- RAM 64 MB (рекомендуется 128 MB);
- Свободное дисковое пространство: 90 MB.