Dr.Web для почтовых серверов Unix



Системные требования

- Linux (ядро 2.4 или выше), FreeBSD версий 6.x, 7.x, 8.x, Solaris 10 (только для платформы In
- CommuniGate Pro, Courier MTA, Exim, Postfix, QMail, Sendmail, ZMailer.

Соответствие требованиям российского законодательства

Dr.Web для почтовых серверов Unix обладает сертификатами соответствия ФСТЭК России и ФСБ. Это позволяет использовать продукт в организациях, требующих повышенного уровня безопасности, в том числе в составе подсистемы антивирусной защиты информационных системах персональных данных (ИСПДн) класса К1. Возможность архивации всех почтовых сообщений позволяет также применять продукт в составе информационных систем кредитных учреждений.

Возможность гибкой настройки под потребности пользователей

Для настройки **Dr.Web для почтовых серверов Unix** можно применять правила. Это значительно повышает гибкость продукта и выгодно отличает его от конкурирующих аналогов, для настройки которых применяются статические параметры конфигурационного файла. Фильтрация и изменение сообщений происходят в зависимости от имеющихся политик. При этом администратор может задавать отдельные правила обработки не только для различных пользователей и групп, но и фактически для каждого письма. Благодаря этому продукт способен отвечать любым корпоративным требованиям к уровню информационной безопасности, что особенно важно в условиях вступления в силу Закона о защите персональных данных.

Нетребовательность к квалификации администратора

Несмотря на богатство функциональных возможностей, **Dr.Web для почтовых серверов Unix** не требует длительной настройки перед введением в строй. Кроме того, он поставляется не только в виде программного продукта, но и в составе программно-аппаратного комплекса Dr.Web Office Shield – сервера, спроектированного для работы по принципу «поставил и забыл».

Нетребовательность к системе

Dr.Web для почтовых серверов Unix отличается низкими системными требованиями, что позволяет ему идеально функционировать на почтовых серверах практически любой конфигурации. Это особенно актуально для тех предприятий, которые не имеют возможности постоянно обновлять свои серверы под растущие системные требования большинства антивирусных продуктов.

Минимальная совокупная стоимость

В отличие от многих конкурирующих решений, **Dr.Web для почтовых серверов Unix** имеет максимально гибкую и мультивариантную систему лицензирования. Клиент приобретает только те компоненты защиты, которые ему нужны, и не переплачивает за ненужные ему элементы или даже целые решения, которые он никогда не будет использовать.

Отличная масштабируемость

Dr.Web для почтовых серверов Unix способен удовлетворить запросы как небольшой компании с одним почтовым сервером, так и безграничные потребности по сканированию почтового трафика транснационального поставщика телематических

услуг. Это стало возможно благодаря способности продукта обрабатывать гигантские массивы информации в режиме реального времени, надежности его работы и гибкости настроек.

Возможность динамического распределения нагрузки позволяет оптимизировать загрузку сервера без необходимости проведения серии ручных тестов. Использование интерфейса тестирования настроек и контроля за состоянием сервисов позволяет вносить изменения в их правила работы практически «на лету», что значительно упрощает сопровождение системы и снижает сроки введения ее в строй.

Настройки сервисов фильтрации и базы карантина могут храниться в хранилищах самого различного типа – от простых файлов до баз данных типа Oracle. Использование для хранения настроек сервисов, поддерживающих протоколы LDAP, значительно упрощает их администрирование благодаря возможности интеграции в структуру корпоративной службы каталогов.

Высокая скорость отклика

Технология многопоточной проверки обеспечивает высокую скорость отклика системы. Проверка сообщений в каждом случае производится «на лету», параллельно с обработкой ранее принятых файлов. Это позволяет конечным пользователям получать корреспонденцию практически мгновенно.

Эффективная фильтрация нежелательных сообщений

Антиспам Dr.Web поставляется в составе единого решения (а не в виде отдельного продукта) и устанавливается на одном сервере с продуктом для фильтрации вирусов. Это упрощает администрирование комплексной защиты и обеспечивает более низкую совокупную стоимость, чем при покупке решений конкурентов.

Dr.Web для почтовых серверов Unix использует для своей работы уникальные

технологии фильтрации спама, которые позволяют полностью отказаться от черных списков, что делает невозможным компрометацию компаний через злонамеренное внесение их в такие списки.

Dr.Web для почтовых серверов Unix может изменять свое поведение в зависимости от конверта обрабатываемого письма или обнаруженных блокирующих объектов.

Дополнительные преимущества антиспама Dr.Web:

- не требует обучения и начинает эффективно работать с момента установки – в отличие от антиспамов, построенных на использовании алгоритма Байеса
- вынесение вердикта спам/не спам не зависит от языка сообщения
- позволяет задавать различные действия для разных категорий спама
- использует собственные черные и белые списки, что делает невозможным компрометацию компаний через злонамеренное внесение их в списки нежелательных адресов
- допускает рекордно малое количество ложных срабатываний
- 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

Повышенная безопасность корпоративной почты

Модульная структура **Dr.Web для почтовых серверов Unix** позволяет не только интегрировать этот продукт в различные почтовые системы, но и использовать его в качестве SMTP proxy – фильтра, обрабатывающего сообщения до их попадания на почтовый сервер. Совместное использование
Dr.Web для почтовых серверов Uni
x и дополнительного компонента SMTP proxy:

- существенно повышает общую безопасность сети;
- значительно улучшает качество фильтрации за счет отсутствия ограничений, накладываемых почтовыми серверами;
- снижает нагрузки на внутренние почтовые серверы и рабочие станции;
- повышает стабильность работы системы проверки почты в целом

Защита конфиденциальной информации

Продукт позволяет восстанавливать сообщения, случайно удаленные пользователями из своих почтовых ящиков, а также проводить расследования, связанные с утечкой информации. Этому способствует управление карантином как через веб-интерфейс, так и через специальную утилиту, а также возможность архивации всех проходящих сообщений.

Гарантированная доставка почты

Даже если пользователь длительное время недоступен и не может получать письма, они не удаляются, а сохраняются в специальном каталоге и в любой момент доступны адресату. Это позволяет упростить настройки почтового сервера и избавиться от приобретения для этих целей специальных продуктов.

Удобство администрирования

Возможность использования веб-интерфейса для настройки и управления продуктом позволяет с легкостью осуществлять администрирование защиты из любой точки мира.

Открытость

Dr.Web для почтовых серверов Unix может интегрироваться в решения других производителей. Кроме того, благодаря открытому API в него можно добавить новые функциональные возможности.

Возможность подключения неограниченного количества плагинов

Dr.Web для почтовых серверов Unix позволяет неограниченно наращивать функциональность, причем любой разработанный плагин работает сразу со всеми поддерживаемыми MTA.

И это далеко не все преимущества **Dr.Web для почтовых серверов Unix!** Изучить все сильные стороны этого продукта можно с помощью сервиса онлайн-тестирования Dr.Web LiveDemo.

Описание

Dr.Web для почтовых серверов Unix обладает встроенной возможностью балансировки нагрузки между серверами и способностью обрабатывать гигантские массивы информации в режиме реального времени. Благодаря этому, а также с учетом надежности работы и гибкости настроек продукт способен удовлетворить запросы как небольшой компании с одним почтовым сервером, так и безграничные потребности по сканированию почтового трафика транснационального поставщика телематических услуг.

Технология динамического распределения нагрузки позволяет эффективно использовать ресурсы каждого сервера без необходимости проведения серии ручных тестов.

Интерфейс тестирования настроек и контроля состояния сервисов позволяет вносить изменения практически «на лету», что значительно упрощает сопровождение системы и ускоряет сроки введения ее в строй

Настройки сервисов фильтрации и базы карантина могут помещаться в хранилища различного типа – от простых файлов до баз данных типа Oracle.

Для хранения настроек используются службы каталогов LDAP. Это значительно упрощает администрирование системы фильтрации благодаря возможности интеграции в структуру корпоративной службы каталогов.

Dr.Web для почтовых серверов Unix – это группа взаимосвязанных программных модулей. Круг задач, которые способен решать этот комплекс, определяется набором подключаемых к нему плагинов – библиотек, отвечающих за непосредственную обработку сообщений.

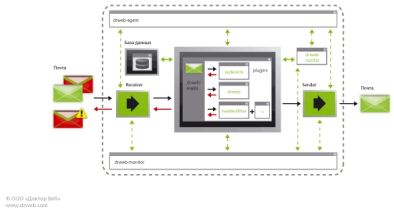
Плагины почтового демона обрабатывают письма по следующему алгоритму: поступающие сообщения принимает модуль Receiver, который передает их модулю Checker (исполняемый файл drweb-maild), отвечающему за проверку. Модуль Checker по очереди вызывает плагины, которые проводят всесторонний анализ сообщений.

Письма, успешно прошедшие проверку плагинами почтового демона, отсылаются почтовой системе модулем Sender. В процессе работы плагины могут создавать различные отчеты о результатах проверки сообщений. Эти отчеты формируются модулем Notifier (исполняемый файл drweb-notifier) и могут рассылаться отправителям писем, их получателям и администратору системы. Обработка писем почтовым демоном может гибко регулироваться с помощью правил.

При использовании соответствующих политик отфильтрованные сообщения можно поместить в карантин. При необходимости системный администратор может проводить различные действия с этими сообщениями (поиск, удаление старых писем из карантина, перемещение их в хранилище) через веб-интерфейс, специальную утилиту или управляющие письма. Возможность контроля карантина через управляющие письма доступна и для обычных пользователей.

В конфигурационный файл почтового демона записываются правила – это одна из полезнейших возможностей программы. Правила позволяют гибко варьировать параметры работы почтового демона в зависимости от содержания обрабатываемых почтовых сообщений. В текущей версии почтового демона можно настраивать правила по отношению к адресам отправителя и получателя почтового сообщения, а также к вредоносным объектам, найденным в сообщениях.

Dr.Web для почтовых серверов Unix позволяет архивировать все входящие и исходящие сообщения, благодаря чему можно восстановить случайно удаленные письма, а также проанализировать пути распространения вирусной эпидемии.



Компоненты

- **Receiver**

Компонент Receiver отвечает за получение почты, либо напрямую от почтовых систем, либо по протоколам SMTP/LMTP, и последующую их передачу компоненту *drweb-maild*. В зависимости от используемых почтовых систем и протоколов функции компонента *Receiver* выполняют разные модули (*drweb-receiver, drweb-milter, drweb-cgp-receiver и т.д.*), причем поддерживается одновременная работа нескольких модулей компонента *Receiver* , что позволяет получать и обрабатывать почту сразу из нескольких источников. Некоторые модули компонента *Receiver* поддерживают возможность модификации/отправления полученных сообщений, принимая результаты проверки писем от компонента *drweb-maild* . Например, такой возможностью обладает модуль *drweb-milter* , что позволяет ему возвращать почтовой системе *SendMail* результат проверки писем до окончания smtp-сессии.

- **drweb-maild**

Основной компонент системы обработки почты. Модуль *drweb-maild* производит

mime-разбор сообщений, передает письма на обработку плагинам и, кроме того, отвечает за хранение писем в базе данных. Обработка писем производится плагинами, подключаемыми к модулю
drweb-maild
. Плагины могут запускаться и выгружаться пользователями в произвольные моменты времени, без остановки модуля
drweb-maild
. Обработка писем плагинами осуществляется в порядке, определяемом пользователем системы. Плагины распределяются по двум очередям –
BeforeQueueFilters
и
AfterQueueFilters
.

Сразу после получения письма обрабатываются плагинами из очереди *BeforeQueueFilters*, после чего, если очередь *AfterQueueFilters* пуста, результаты обработки письма возвращаются компоненту
Receiver
. Если же в очереди
AfterQueueFilters
указаны какие-либо плагины, то письмо, после обработки плагинами из очереди BeforeQueueFilters поступает в базу данных, а затем отправляется во внутреннюю очередь модуля
drweb-maild
, при этом компоненту Receiver возвращается код успешной проверки письма. Затем письмо проверяется плагинами из очереди
AfterQueueFilters
.

Результаты проверки отправляются либо компоненту *Receiver* (если существует такая возможность, например, еще не истек таймаут на ожидание результата проверки), либо компоненту *Sender*. Через компонент
Sender
также отправляются все письма сгенерированные плагинами. Некоторым плагинам для работы необходима поддержка базы данных, такие плагины не могут быть помещены в очередь
BeforeQueueFilters
.

- **drweb-notifier**

Модуль отвечает за создание всех отчетов, формируемых в процессе работы комплекса. Дополнительно установленные плагины могут добавлять свои собственные типы уведомлений. Запрос на отправку отчетов могут отправлять как плагины (например, при обнаружении вируса), так и другие компоненты системы. Например, модуль *drweb-maild* может посылать запрос на создание общего отчета со статистикой работы всех подключенных плагинов, а компонент
Sender
может посылать запрос на формирование отчета DSN о невозможности отправить письмо. Реализована поддержка формирования отчетов как в текстовом, так и в html-формате.

- **Sender**

Компонент отвечает за отправление писем либо напрямую в различные почтовые системы, либо по протоколам SMTP/LMTP. В зависимости от используемых почтовых систем и протоколов, функции компонента Sender выполняют разные модули (*drweb-Sender, drweb-cgp-Sender*
и т.д.). Компонент
Sender
может получать запросы на отправление писем от компонентов
drweb-maild, drweb-notifier
и
drweb-monitor
.

- **drweb-agent**

Обеспечивает возможность работы системы обработки почты как в автономном режиме, так и в режиме интеграции с Центром управления Dr.Web . Все компоненты системы (кроме drweb-monitor) получают свои конфигурационные данные через модуль drweb-agent, поэтому он должен запускаться перед другими компонентами. Так же, модуль drweb-agent отвечает за проверку лицензии и сбор статистической информации о работе компонентов системы: имена найденных блокируемых объектов, общий объем проверенной информации и т.д.

- **drweb-monitor**

Вспомогательный компонент, запускающий и останавливающий модули системы в заданном порядке, а также контролирующий их работу. В случае сбоя в работе какого-либо модуля системы, drweb-monitor осуществляет его перезапуск, а также, (если это задано настройками) уведомление об этом администратора системы.

Плагины

На текущий момент в **Dr.Web для почтовых серверов Unix** реализованы следующие плагины:

- **Drweb**

Drweb — плагин антивирусной проверки почты «движком» Dr.Web. Проверку осуществляет модуль Drwebd, необходимый для работы данного плагина. Этот модуль проверяет сообщения в уже «разобранном» виде, поэтому поддержка mime-разбора в «движке» или модуле Drwebd не требуется. Плагин обладает высокой производительностью сканирования файлов и приложений при максимальном качестве проверки, минимальном времени отклика и малых затратах системных ресурсов.

Стабильность работы

Модульная структура системы в целом, а также специальный модуль, ответственный за работоспособность, обеспечивают бесперебойное функционирование плагина. Вывести его из строя практически невозможно.

Высокая скорость отклика

Технология многопоточной проверки обеспечивает высокую скорость отклика системы. Проверка сообщений в каждом случае производится «на лету», параллельно с обработкой ранее принятых файлов. Это позволяет конечным пользователям получать корреспонденцию практически мгновенно после ее попадания на сервер.

Карантин

Обнаруженные инфицированные и подозрительные файлы могут перемещаться в карантин. Благодаря этому возможна дополнительная обработка этих файлов, в том числе извлечение необходимой информации, лечение или удаление.

Удобство управления

Конфигурационные файлы позволяют гибко настроить параметры работы плагина в удобном для пользователя режиме. Любые действия плагина отражаются в журналах системы, что позволяет анализировать ее поведение и выявлять узкие места. Удобная система оповещения администратора позволяет максимально быстро предпринимать необходимые действия.

Открытость

Благодаря открытой архитектуре системы MailD пользователь может самостоятельно реализовать дополнительный функционал, использующий возможности плагина, с помощью открытого SDK и подробной документации по работе с ним.

- **Headersfilter**

Headersfilter фильтрует почтовые сообщений по заголовкам. Плагин может проверять не только сами сообщения, но и вложения к ним. С помощью данного плагина пользователь может самостоятельно добавлять правила обработки почтовой корреспонденции. При задании правил фильтрации можно использовать регулярные выражения. Гибкие настройки плагина позволяют реализовывать любое количество правил. Плагин практически не создает нагрузки на систему и отличается безупречным быстродействием.

Удобство использования

Возможность использования регулярных выражений позволяет настроить систему как на пропуск, так и на фильтрацию поступающих почтовых сообщений. В связи с тем, что количество правил неограниченно, система может быть настроена так, как это нужно пользователю. Благодаря тому, что модуль может отрабатывать до остальных модулей системы, пользователь может получать корреспонденцию, получение которой было бы невозможным в ином случае.

Удобство управления

Используя регулярные выражения, пользователь может настроить параметры фильтрации полностью под свои потребности. Удобная система оповещения администратора безопасности позволяет максимально быстро предпринимать необходимые действия.

Открытость

Благодаря открытой архитектуре системы MailD пользователь может самостоятельно реализовать дополнительный функционал, использующий возможности плагина, с помощью открытого SDK и подробной документации по работе с ним.

Стабильность работы

Модульная структура системы в целом, а также специальный модуль, ответственный за работоспособность, обеспечивают бесперебойное функционирование плагина. Вывести его из строя практически невозможно.

Высокая скорость отклика

Технология многопоточной проверки обеспечивает высокую скорость отклика системы. Проверка сообщений в каждом случае производится «на лету», параллельно с обработкой ранее принятых файлов. Это позволяет конечным пользователям получать корреспонденцию практически мгновенно после ее попадания на сервер.

- **Modifier**

Плагин **modifier** предназначен для модификации почтовых сообщений в соответствии с правилами их обработки. Его использование позволяет обрабатывать всю входящую и исходящую почту в соответствии с корпоративными стандартами. В частности, применение плагина совместно с функцией архивации почтовых сообщений дает возможность организовать систему контроля за утечками конфиденциальной информации. При этом анализ отфильтрованной корреспонденции возможен при помощи утилиты управления карантином.

Удобство управления

Гибкая система настроек позволяет обеспечить практически ничем не ограниченные возможности по модификации сообщений. Системный администратор может создавать неограниченное количество правил, а значит – с помощью данного плагина возможно реализовать практически любые положения политики информационной безопасности по отношению к почтовой переписке. Используя регулярные выражения, пользователь может настроить параметры фильтрации полностью под свои потребности. Удобная система оповещения администратора безопасности позволяет максимально быстро предпринимать необходимые действия.

Открытость

Благодаря открытой архитектуре системы MailD пользователь может самостоятельно реализовать дополнительный функционал, использующий возможности плагина, с помощью открытого SDK и подробной документации по работе с ним.

Стабильность работы

Модульная структура системы в целом, а также специальный модуль, ответственный за работоспособность, обеспечивают бесперебойное функционирование плагина. Вывести его из строя практически невозможно.

Высокая скорость отклика

Технология многопоточной проверки обеспечивает высокую скорость отклика системы. Проверка сообщений в каждом случае производится «на лету», параллельно с обработкой ранее принятых файлов. Это позволяет конечным пользователям получать корреспонденцию практически мгновенно после ее попадания на сервер.

- **Vaderetro**

Плагин **vaderetro** осуществляет антиспам-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.

Зачастую продукты для сканирования почтовых сообщений не могут полностью продемонстрировать свой потенциал, поскольку этого не позволяют возможности почтового сервера. Возникает проблема, с которой сталкиваются практически все администраторы локальных сетей: систему защиты от вирусов, спама и нежелательной корреспонденции не удается сделать максимально эффективной. Dr.Web SMTP proxy успешно решает эту проблему.

Dr.Web для почтовых серверов Unix с модулем Dr.Web SMTP proxy может быть установлен как в демилитаризованной зоне (DMZ), так и внутри почтовой системы. Благодаря тому, что сервер проверки почтовых сообщений может быть вынесен в DMZ, а почтовый сервер – изолирован от Интернета, даже в случае взлома сервера злоумышленник не получит доступа к важной для компании информации. Обеспечивается полная проверка почтовой корреспонденции по протоколам SMTP/LMTP.

Преимущества

- Значительное улучшение качества фильтрации за счет отсутствия ограничений со стороны почтового сервера.
- Снижение нагрузки на внутренние почтовые серверы, серверы контентной фильтрации, почтовые и интернет-шлюзы, а также рабочие станции.
- Повышение стабильности проверки почты и безопасности сети в целом.

- **Защита от атак спамеров**

Администратор может ограничивать параметры SMTP-сессии, тем самым исключая вероятность спамерской атаки.

- **Защита от замаскированного спама**

Благодаря функции проверки подлинности IP-адреса компания защищена от спама, скрытого под недостоверным IP отправителя.

- **Защита от атак хакеров**

Продукт позволяет эффективно противостоять как пассивным атакам (типа PLAIN, LOGIN и т.д.), так и активным атакам без перебора по словарю.

- **Защита от спам-ловушек**

Dr.Web SMTP proxy позволяет проводить проверку получателя на спам-ловушку.

- **Защита от некорректно сформированных писем**

Продукт блокирует письма с пустыми полями отправителя, но в то же время корректно обрабатывает неверно составленные письма от почтовых клиентов.

- **Экономия интернет-трафика**

Использование Dr.Web SMTP proxy позволяет ограничить размер отправляемых по электронной почте вложений.

- **Ограничение Open Relays серверов**

Если нужно организовать такой сервер, с помощью Dr.Web SMTP proxy администратор может ограничить список доменов, на которые разрешена пересылка писем.

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.

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 почтовых серверов Unix 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 почтовых серверов Unix может выступать SMTP proxy. 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 proxy
- Антивирус + Центр управления + SMTP proxy
- Антивирус + Антиспам
- Антивирус + Антиспам + Центр управления
- Антивирус + Антиспам + SMTP proxy
- Антивирус + Антиспам + Центр управления + SMTP proxy

Также Dr.Web для почтовых серверов Unix доступен в составе экономичных Комплектов Dr.Web для малого и среднего бизнеса.