

Программно-аппаратные комплексы Dr.Web Office Shield

Высокопроизводительный и отказоустойчивый шлюз доступа в Интернет, позволяющий организовать централизованную антивирусную защиту рабочих станций и файловых серверов Windows, почтового и интернет-трафика. Использование Dr.Web Office Shield позволяет выполнить положения Федерального закона № 152-ФЗ «О персональных данных» в области антивирусной защиты персональных данных и контроля доступа в рекордно короткие сроки.

Повышайте эффективность труда персонала, сокращайте простои и снижайте стоимость владения антивирусом на 30%.



Dr.Web Office Shield это:

- Шлюз сети Интернет, позволяющий организовать безопасный доступ в Интернет для всех сотрудников компании;
- Антивирусная и антиспам-защита почтового трафика;
- Централизованная защита для рабочих станций и файловых серверов Windows.

Установленные сервисы:

- Корпоративный межсетевой экран;

- VPN-сервер;
- DHCP&DNS-сервер;
- Точка доступа Wi-Fi.

В отличие от традиционной модели, когда все необходимое программное обеспечение устанавливается на ранее закупленные серверы, Dr.Web Office Shield позволяет сократить время развертывания защиты сети до минимума — за счет отсутствия необходимости предварительной установки серверного программного обеспечения, его настройки и тестирования. Устройства просты в установке и обслуживании, с их управлением справится специалист любой квалификации. Устройства поставляются уже настроенными на оптимальную защиту — вам не придется подбирать параметры безопасности для вашей сети.

Программно-аппаратные комплексы Dr.Web Office Shield эффективно действуют с момента подключения и даже, при необходимости, позволяют создать сеть с нуля. Благодаря компактным корпусам они не требуют организации специальных серверных помещений. Бесшумные и отказоустойчивые, устройства обладают низким энергопотреблением и тепловыделением, нечувствительны к перепадам температур и влажности, могут быть установлены даже там, где обычный компьютер разместить невозможно. В процессе эксплуатации устройств можно увеличивать количество защищаемых объектов и лицензируемых компонентов.

Простота администрирования и минимальные затраты на обслуживание

Для управления Dr.Web Office Shield не требуется специальной подготовки, достаточно базовых компьютерных знаний. За счет интуитивно понятного интерфейса процесс администрирования устройства прост и может осуществляться с помощью любого интернет-браузера. Дополнительно предусмотрено администрирование из обычной консоли, устанавливаемой на рабочую станцию администратора или через SSH терминал, что позволяет провести тонкую настройку устройства. Высокая стабильность работы, предварительно настроенная конфигурация, функции автоматической диагностики и профилактики сводят к минимуму необходимость контроля администратора за работой Dr.Web Office Shield.

Максимально быстрое развертывание

Установка и ввод в эксплуатацию Dr.Web Office Shield состоят всего из нескольких интуитивно понятных и простых шагов. В большинстве случаев необходимо только сконфигурировать его под конкретные параметры локальной сети и устройство будет выполнять все возложенные на него задачи. Это стало возможно за счет использования оптимизированного программного обеспечения и удобной системы управления и настройки, применения предустановленного сценария антивирусной безопасности.

Контроль работоспособности

Наличие встроенных механизмов контроля работоспособности системы защиты позволяет автоматически восстанавливать работоспособность устройства в случае возникновения каких-либо проблем.

Снижение количества внеплановых остановок

Система оповещения администратора о проблемах, возникающих в антивирусной сети защищаемого предприятия, позволяет максимально оперативно реагировать на вирусные угрозы и активно им противодействовать.

Снижение потерь рабочего времени, простоев оборудования и персонала за счет уменьшения количества вирусных инцидентов в корпоративной сети

Согласно статистике, в незащищенной сети простои составляют в среднем 2 часа в месяц на одного пользователя. Чем выше служебное положение такого пользователя, тем выше стоимость его простоя.

Вирусы и спам являются основными угрозами информационной безопасности для организаций любого типа и размера. Анализ состояния корпоративной сети, работы по

предотвращению вирусных атак и действия по преодолению последствий вирусных инцидентов – задачи, которыми приходится заниматься IT-персоналу каждый день. Снижение простоев, вызванных действиями вредоносных объектов – одна из важнейших задач системных администраторов, от успеха решения которой зависят эффективность функционирования бизнес-процессов целого предприятия и его имидж надежного партнера. Dr.Web Office Shield является мощным инструментом снижения простоев, вызванных действиями вирусов и вредоносных объектов.

Высокая устойчивость к внешним атакам

Операционная система и основные программные модули антивирусного шлюза Dr.Web Office Shield недоступны для несанкционированной модификации как за счет реализации эффективной политики доступа, так и за счет использования предустановленного файрвола. Использование репозитория для проведения обновлений позволяет оперативно устранять выявленные уязвимости в используемом программном обеспечении и поддерживать высокий уровень защищенности Dr.Web Office Shield.

Оптимизация расходов на интернет-трафик и контроль за деятельностью сотрудников в сети Интернет

В отдельные периоды рабочего дня (например, обеденный перерыв) сотрудники компании занимают до 80% пропускной способности канала на задачи, не связанные с работой. Использование Интернета в личных целях транслируется в потери 30 – 40% производительности труда.

Всего один час в день использования Интернета в личных целях каждым сотрудником компании составляет 12,5% от всех расходов компании на заработную плату.

Dr.Web Office Shield — эффективное средство фильтрации контента, которое позволяет контролировать расход рабочего времени и ресурсов предприятия сотрудниками. Устройство позволяет предотвращать несанкционированный расход трафика, пресекать попытки посещения нежелательных страниц – например, интернет-магазинов, дает возможность прописывать политики доступа к веб-ресурсам.

Dr.Web Office Shield позволяет анализировать расход сетевого трафика по каждому компьютеру организации, что дает возможность оперативно корректировать политику безопасности, принятую на предприятии.

Повышение производительности труда путем снижения количества отвлекающих факторов

Во времена перепроизводства информации человеческое внимание — ценный и почти невозобновляемый ресурс. Обилие и даже переизбыток информации, ее большая доступность в связи с появлением Интернета, поглощают внимание людей. Чистка почтового ящика от спама, закрытие всплывающих окон и рекламных баннеров — все это рассеивает внимание, снижает уровень концентрации, негативно влияет на эмоциональное и психическое состояние человека. Информационные потоки, которые необходимо ежедневно обрабатывать персоналу, нарастают день ото дня. В противоположность этому производительность сотрудников — величина склонная к уменьшению в условиях перегрузки побочными действиями. В итоге, для предприятий стоимость поддержания необходимой производительности труда сотрудника оказывается дороже стоимости вычислительных ресурсов.

Сотруднику, чье внимание отвлечено от решения текущей бизнес-задачи, необходимо до 15 минут, чтобы заново сконцентрировать внимание.

Dr.Web Office Shield позволяет минимизировать потери рабочего времени. Используемая система антиспама позволяет максимально эффективно бороться со спамом и нежелательными сообщениями. В противовес обучаемым антиспам-системам, использование которых со временем достигает высокого уровня точности фильтрации, но требует ежедневной работы системного администратора, интеллектуальная система фильтрации антиспама Dr.Web позволяет использовать его прямо «из коробки» — в режиме «установил и забыл». При этом эффективность отсева спама достигает 97 — 99%.

Высокопродуктивная фильтрация

Разработчики антиспама ориентировались на создание решения для корпоративных серверов, поэтому именно высокая скорость фильтрации сообщений была одной из самых приоритетных задач при его разработке.

Разные технологии детектирования для разного вида нежелательных сообщений

В Антиспаме Dr.Web для каждого вида нежелательных писем — спама, фишинг-, фарминг-, скамминг-, bounce-сообщений – предусмотрены разные технологии фильтрации, что обеспечивает высокую вероятность распознавания. Так для некириллического спама эта цифра достигает 99%. При вынесении вердикта — спам/не спам — изучается совокупность очень большого числа признаков сообщения.

Регулярные обновления

Обновления к антиспаму Dr.Web выпускаются ежедневно и автоматически загружаются пользователям с помощью утилиты автоматического обновления Dr.Web. Уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил позволяют производить обновления не чаще одного раза в сутки и экономить трафик на скачивании громоздких и частых обновлений.

Являясь эффективным средством борьбы с многочисленными отвлекающими факторами, Dr.Web Office Shield помогает конвертировать внимание сотрудников в доходную статью бюджета предприятия.

Защита репутации компании

«Изобретательность» рядовых сотрудников компании зачастую является причиной того, что компьютеры компании сами становятся источником спама, что не только вредит престижу компании среди ее партнеров, но и приводит к отключению ее от сети Интернет, что в свою очередь может полностью парализовать ее работу. Dr.Web Office Shield позволяет не допустить такой ситуации.

Безопасный доступ к сети интернет

Dr.Web Office Shield представляет из себя полноценный сервер доступа в сети Интернет. Dr.Web Office Shield имеет функции как антивирусной защиты трафика, так и его анализа, что позволяет не только защитить пользователей от проникновения вирусов, но и обеспечить снижение затрат компании.

Комплексная централизованная защита всей сети от вирусов и спама

Использование возможностей Dr.Web Office Shield позволяет надежно защитить от проникновения вирусов и спама все компьютеры локальной сети.

Исключительная надежность

Dr.Web Office Shield создан на аппаратной платформе, предназначенной для использования во встроенных системах высокой степени надежности. Использование пассивного охлаждения позволяет избежать проблем, связанных с выходом вентилятора из строя, расширить список мест установки устройства и значительно сократить затраты на обслуживание системы за счет отказа от ряда обязательных процедур профилактики работы. Отсутствие вентиляторов сводит к минимуму возможность выхода Dr.Web Office Shield из строя в процессе непрерывной длительной эксплуатации.

Устойчивость к неблагоприятной среде

Dr.Web Office Shield обладает низким энергопотреблением и тепловыделением, неприхотлив к перепадам температур и влажности. Испытания показали, что стабильная работа процессора с полной загрузкой обеспечивается даже при температуре

окружающей среды 60°C.

Автоматическое восстановление и легкая переносимость

Используя встроенные инструменты резервного копирования можно создать копию работающего антивирусного сервера, в том числе и по расписанию. Администратор может легко распространить созданную конфигурацию на другие устройства за счет возможности сохранения всех настроек системы в единый архивный файл.

Отсутствие необходимости унифицировать компьютерный парк предприятия

Широчайший спектр поддерживаемых операционных систем, а также уникальная система обновлений компонентов и вирусных баз Dr.Web Office Shield не требуют от предприятия единообразия платформ защищаемых рабочих станций. Dr.Web Office Shield может использоваться на предприятиях, эксплуатирующих устаревшие ОС Windows.

Компактность

Традиционно высоконадежные программно-аппаратные комплексы выполняются в форм-факторе, требующем размещения их в специально оборудованных помещениях, имеющих системы кондиционирования и бесперебойного питания. Необходимость иметь такие помещения повышает затраты предприятия на информационные технологии, в том числе и за счет нерационального использования арендуемых помещений. Традиционная надежность и неприхотливость решений компании Dr.Web позволила создать решение, выполненное в компактном корпусе, который может быть расположен в самых различных местах — даже там, где обычный компьютер разместить невозможно.

Компактность и нетребовательность к квалификации обслуживающего персонала позволяют использовать Dr.Web Office Shield даже домашним пользователям (например, для организации домашних сетей)!

Варианты использования

Модульность решения и гибкость системы лицензирования позволяет использовать Dr.Web Office Shield в самых различных конфигурациях локальных сетей предприятий и организаций, реализуя их внутреннюю политику безопасности. В частности Dr.Web Office Shield может быть использован в качестве:

- сервера демилитаризованной зоны - максимально изолированного от внутренней сети устройства, отвечающего за антивирусную и антиспам-защиту предприятия;
- прокси-сервера (шлюза доступа пользователей внутренней интранет-сети к ресурсам сети Интернет), предназначенного для обеспечения защиты почтового и интернет-трафика от вирусов, разного рода вредоносных объектов и спама. Использование Dr.Web Office Shield в качестве шлюза значительно снижает затраты компаний на организацию безопасного доступа пользователей корпоративной интранет-сети к ресурсам сети Интернет и позволяет существенно экономить интернет-трафик;
- внутреннего сервера локальной сети, обеспечивающего централизованную защиту рабочих станций и файловых серверов Windows.

В состав Dr.Web Office Shield входят:

- Центр управления Dr.Web Enterprise Security Suite;
- Dr.Web Desktop Security Suite. Комплексная защита ;
- Dr.Web Mail Security Suite. Антивирус + Антиспам + SMTP proxy;
- Dr.Web Gateway Security Suite. Антивирус
- Корпоративный межсетевой экран;
- VPN сервер;
- DHCP&DNS сервер;
- Точка доступа Wi-Fi.

Важной особенностью Dr.Web Office Shield является то, что он может быть установлен как в

Галерея

