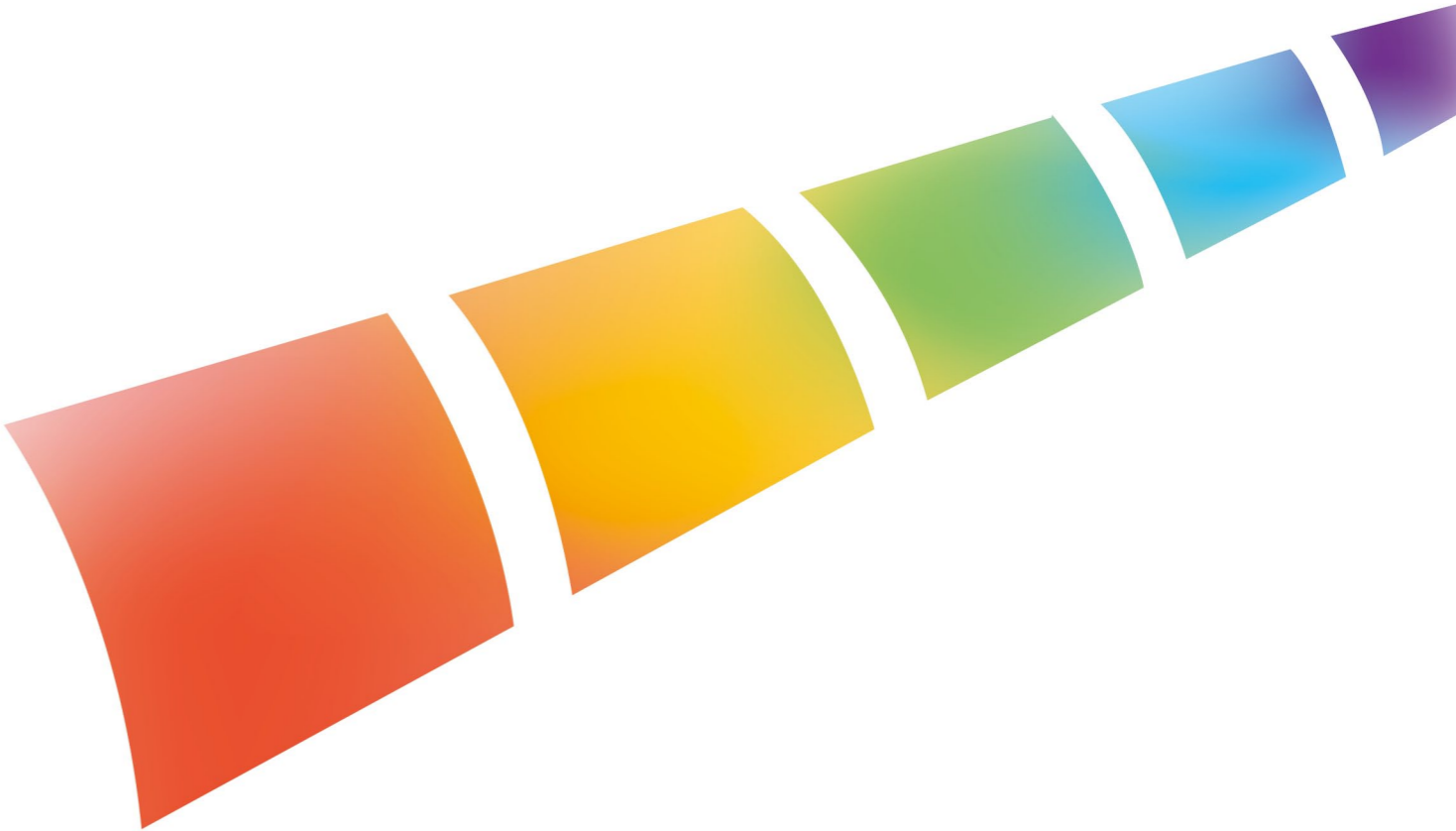




У вас есть что защищать?

У нас есть  **Dr.WEB®**
с 1992



Содержание

2	О компании
3	Лицензии и сертификаты
4	Технологии
7	Dr.Web Enterprise Security Suite – продукты для бизнеса
9	Лицензирование Dr.Web Enterprise Security Suite
10	Центр управления Dr.Web
12	Dr.Web Desktop Security Suite
14	Dr.Web для Windows
16	Антивирус Dr.Web для Mac OS X
17	Антивирус Dr.Web для Linux
17	Консольные сканеры
18	Dr.Web Server Security Suite
19	Dr.Web для серверов Windows
20	Dr.Web для серверов Novell NetWare
21	Dr.Web для Mac OS X Server
22	Dr.Web для серверов UNIX
23	Dr.Web для Novell Storage Services
24	Dr.Web Mail Security Suite
25	Dr.Web для почтовых серверов и шлюзов UNIX
27	Dr.Web для IBM Lotus Domino
28	Dr.Web для MS Exchange
29	Dr.Web для почтовых серверов Kerio
30	Dr.Web Gateway Security Suite
32	Dr.Web для интернет-шлюзов UNIX
33	Dr.Web для интернет-шлюзов Kerio
34	Dr.Web для Microsoft ISA Server и Forefront TMG
35	Dr.Web для MIMESweeper
35	Dr.Web для Qbik WinGate
36	Dr.Web Mobile Security Suite
38	Комплекты Dr.Web
40	Утилиты Dr.Web
42	Программно-аппаратные комплексы Dr.Web

О компании «Доктор Веб»

Компания «Доктор Веб» – известный российский разработчик средств информационной безопасности.

Антивирусные продукты Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ. Создание компании «Доктор Веб» в декабре 2003 года послужило началом стремительного роста продаж продуктов Dr.Web как в России, так и в других странах.

Сегодня «Доктор Веб» – это успешная, быстро растущая компания, которая играет одну из ведущих ролей на рынке средств информационной безопасности. Она располагает антивирусным ядром собственной разработки, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегическая задача компании, на которую нацелены усилия всех сотрудников, – создание средств антивирусной защиты, отвечающих всем современным требованиям. Не менее важна разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз. Линейка антивирусных продуктов компании «Доктор Веб» охватывает широчайший спектр операционных систем и совместимых приложений.

В распространении своих разработок компания опирается на партнерскую сеть, отказавшись от прямых продаж конечным пользователям.

Среди потребителей продуктов Dr.Web – домашние пользователи разных стран мира и крупные российские предприятия, небольшие организации и системообразующие корпорации, которым коллектив «Доктор Веб» благодарен за поддержку и многолетнюю преданность продукту. Государственные сертификаты и награды свидетельствуют о высоком доверии к антивирусу Dr.Web, созданному талантливыми российскими программистами.

Лицензии и сертификаты



В отличие от большинства конкурирующих решений программные продукты Dr.Web имеют сертификаты соответствия ФСТЭК, ФСБ и Министерства обороны РФ. Это позволяет использовать их в организациях с повышенными требованиями к уровню безопасности.

Dr.Web сертифицирован ФСТЭК на соответствие:

- ТУ и НДВ 4 на применение в составе подсистемы антивирусной защиты в информационных системах персональных данных (ИСПДн) класса К1;
- требованиям (по уровню контроля не ниже 4) руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» и требованиям технических условий.

Dr.Web полностью соответствует требованиям закона «О персональных данных», предъявляемым к антивирусным продуктам в части защиты от несанкционированного доступа и централизованной защиты каналов передачи данных, и может применяться в сетях, соответствующих максимально возможному уровню защищенности.

Компания «Доктор Веб» имеет следующие лицензии, сертификаты и свидетельства:

- лицензии Федеральной службы по техническому и экспортному контролю РФ (ФСТЭК) на проведение работ, связанных с созданием средств защиты информации, а также на деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- лицензия Министерства обороны Российской Федерации на деятельность в области создания средств защиты информации;
- лицензии ФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну;
- лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на разработку и (или) производство средств защиты конфиденциальной информации;
- сертификаты соответствия ФСБ РФ;
- сертификаты соответствия ФСТЭК РФ.

Все лицензии и сертификаты «Доктор Веб»:

http://company.drweb.com/licenses_and_certificates

Упаковка продуктов, сертифицированных ФСТЭК

Специальный медиапакет «Dr.Web Сертифицированный»

Комплектация: медиапакет; диск с сертифицированным дистрибутивом; формуляр; голографическая наклейка ФСТЭК.

Технологии Dr.Web

Антивирусы Dr.Web – семейство компьютерных программ, созданных талантливыми российскими программистами под руководством Игоря Данилова.

«Доктор Веб» – один из немногих антивирусных вендоров в мире, владеющих собственной уникальной технологией детектирования и лечения вредоносных программ. Компания имеет собственную службу вирусного мониторинга и аналитическую лабораторию. Благодаря этому специалисты могут быстро реагировать на новые вирусные угрозы и способны оказать помощь клиентам в решении проблем любой сложности в считанные часы.

Важной особенностью Dr.Web является его модульная архитектура. Все продукты и решения включают в себя единое антивирусное ядро, а также используют единую систему обновлений вирусных баз и глобальную систему технической поддержки. Технологии Dr.Web позволяют организовать надежную информационную защиту как в рамках крупных корпоративных сетей, так и на домашнем компьютере или в домашнем офисе.

Помимо вирусов и вредоносных программ Dr.Web способен также обнаруживать и удалять с компьютера различные нежелательные программы (рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы, программы взлома – spyware/riskware), спам и нежелательные электронные письма (фишинг-, фарминг-, скамминг и bounce-сообщения).

Технологии

Качественный антивирус должен уметь не только находить вирусы, но и лечить их. Ведь одно дело – удалить инфицированные файлы вместе с ценной информацией, и совсем другое – вернуть их в первоначальное «здоровое» состояние. Dr.Web относится к файлам пользователя бережно.

Лечит от вирусов

- Dr.Web успешно работает на уже инфицированном компьютере и неуязвим для вирусов в отличие от всех других аналогичных программ.
- У Dr.Web самый высокий в антивирусной индустрии процент эффективного лечения активного заражения.
- Перед установкой Dr.Web нет необходимости в предварительном лечении ПК: использование уникальных технологий обработки процессов в памяти и превосходные возможности по нейтрализации активного заражения позволяют устанавливать Dr.Web прямо на зараженную машину.
- Высокая вероятность успешного запуска сканирования на зараженном ПК – даже с внешнего носителя без установки в систему (например, с USB-stick).

Самозащита

Dr.Web обладает стойким иммунитетом к любым попыткам вредоносных программ вывести его из строя. Неуязвимость обеспечивает не имеющий аналогов на антивирусном рынке компонент самозащиты Dr.Web SelfPROtect.

- Dr.Web SelfPROtect реализован в виде драйвера и действует на самом низком системном уровне – его работу может прервать только перезагрузка системы. Таким образом, вредоносные программы не могут повлиять на самозащиту.
- Dr.Web SelfPROtect ограничивает доступ вредоносных объектов к сети, файлам и папкам, некоторым веткам реестра и сменным носителям на уровне системного драйвера, защищает от попыток антивирусных программ прекратить работу Dr.Web.
- Dr.Web SelfPROtect полностью самодостаточен и не модифицирует ядро Windows, в то время как некоторые конкурирующие продукты перехватывают прерывания, подменяют таблицы векторов, используют недокументированные функции и т. д., что может привести к серьезным проблемам в работе самой операционной системы, а также открывает новые пути для использования уязвимостей злоумышленниками.

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, запакрованных неизвестными Dr.Web способами.
- Уникальная технология несигнатурного поиска Origins Tracing™ позволяет Dr.Web с высокой долей вероятности распознавать вредоносные программы, еще не внесенные в его вирусную базу.
- Эвристический анализатор Dr.Web эффективно детектирует все распространенные типы угроз, определяя их класс по результатам проведенного разбора и характерным признакам.

Технологии спам-фильтрации

Технологии фильтрации Антиспама Dr.Web состоят из нескольких тысяч правил, которые условно можно разбить на несколько 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 содержание вложения к нему, если таковое имеется. Эвристический анализатор постоянно совершенствуется, к нему постоянно добавляются новые правила. Эвристический анализатор работает «на опережение» и позволяет распознавать еще неизвестные разновидности спама нового поколения до выпуска соответствующего обновления.
- **Фильтрация противодействия**
Фильтрация противодействия – одна из наиболее передовых и эффективных технологий антиспама Dr.Web. Состоит в распознавании уловок, используемых спамерами для обхода антиспам-фильтров.

■ Анализ на основе HTML-сигнатур

Сообщения, в состав которых входит HTML-код, сравниваются с образцами библиотеки HTML-сигнатур антиспама. Такое сравнение в сочетании с имеющимися данными о размерах изображений, обычно применяемых спамерами, защищает пользователей от спам-сообщений с HTML-кодом, в которые часто включаются онлайн-изображения.

■ Технология детектирования спамерских приемов по конвертам сообщений

Детектирование подделок в «штемпелях» SMTP-серверов и в других элементах, содержащихся в заголовках почтовых сообщений, является новейшим направлением развития методов борьбы со спамом. Адресу отправителя электронного сообщения нельзя доверять, так как может быть указан фальшивый обратный адрес. Поддельные письма – это не только спам, это могут быть мистификации или средства давления на персонал, например, анонимки и даже угрозы. Специальные технологии антиспама Dr.Web позволяют определять поддельные адреса и не принимать такие сообщения. Это позволяет экономить трафик и ограждать сотрудников от получения поддельных писем, которые могут подтолкнуть их к непредсказуемым действиям.

■ Семантический анализ

В ходе этого анализа производится сравнение слов и выражений сообщения со словами и идиомами, типичными для спама. Сравнение производится по специальному словарю, причем анализу подвергаются как видимые, так и скрытые для человеческого глаза специальными техническими уловками слова, выражения и символы.

■ Анти-скамминг-технология

Скамминг-сообщения (а также фарминг-сообщения – один из видов скамминга) – пожалуй, самая опасная разновидность спам-сообщений, к числу которых относятся т. н. «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

Так называемые bounce-сообщения возникают как реакция на вирусы, или как проявление вирусной активности – например, в результате действия почтового червя, рассылающего письма, или в виде сообщений о доставке письма – и не менее нежелательны, чем спам. Специальный модуль антиспама Dr.Web определяет такие сообщения как нежелательные.

Преимущества Антиспама Dr.Web

- Проверка поступающей и исходящей почты производится в режиме реального времени.
- Работа антиспама не зависит от используемой почтовой программы и не увеличивает время приема почты.
- Антиспам не требует настроек и начинает автоматически действовать с приемом первого сообщения.
- Разные технологии фильтрации обеспечивают высокую вероятность распознавания спама, фишинг-, фарминг-, скамминг- и bounce-сообщений при близком к нулю проценте ложных срабатываний.
- Отфильтрованные письма не удаляются, а перемещаются в специальную папку вашей почтовой программы, где их можно проверить в удобное для вас время на наличие ложных срабатываний.
- Модуль спам-анализатора абсолютно автономен; для его работы не требуется связи с внешним сервером или доступа к какой-либо базе данных, что позволяет существенно экономить трафик.
- Обновления к антиспаму Dr.Web выпускаются ежедневно. Уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил позволяют производить обновления не чаще одного раза в сутки и экономить трафик.

Особая организация вирусной базы Dr.Web

Вирусная база Dr.Web – самая маленькая по сравнению с базами других антивирусных программ. Достигнуто это благодаря собственной технологии создания вирусной базы на основе очень гибкого языка, специально разработанного для описания баз. Малый размер вирусной базы обеспечивает экономию трафика, позволяет занимать гораздо меньше места на диске после установки и в оперативной памяти, чем базы других производителей. Небольшой размер вирусной базы позволяет взаимодействовать компонентам программы Dr.Web в высокоскоростном режиме, не оказывая чрезмерной нагрузки на процессор.

Что самое главное в антивирусе? Обеспечивать защиту от вирусов. Обеспечивается защита, среди прочего, внесением в вирусную базу записей (сигнатур), позволяющих детектировать вирусы. А вот количество записей в вирусной базе абсолютно ничего не говорит о том, сколько реально вирусов ловит та или иная антивирусная программа. Чтобы понять, почему число записей в вирусной базе Dr.Web меньше числа записей в вирусных базах некоторых других производителей, надо знать, что не все вирусы уникальны. Существуют целые семейства родственных (подобных) вирусов, есть вирусы, сконструированные вирусными конструкторами. Разработчиками некоторых других антивирусов каждый такой вирус-близнец наделяется отдельной записью в вирусной базе, что утяжеляет ее. Другой принцип применен в вирусной базе Dr.Web, где всего одна запись позволяет обезвреживать десятки или сотни, а иногда даже тысячи подобных друг другу вирусов.

Преимущества вирусной базы Dr.Web

- Рекордно малое число записей.
- Малый размер обновлений.
- Всего одна запись позволяет определять десятки, сотни и даже тысячи подобных вирусов.

Принципиальное отличие вирусной базы Dr.Web от вирусных баз ряда других программ состоит в том, что при меньшем числе записей она позволяет детектировать такое же (и даже большее) число вирусов и вредоносных программ.

Что дают пользователю малый размер базы Dr.Web и меньшее число записей в ней?

- Экономия места на диске.
- Экономия оперативной памяти.
- Экономия трафика при скачивании базы.
- Высокая скорость установки базы и ее обработки при анализе вирусов.
- Возможность определять вирусы, которые еще только будут созданы в будущем путем модификации уже известных.

Глобальная система обновлений Dr.Web (Dr.Web GUS)

- Служба вирусного мониторинга Dr.Web производит сбор образцов вирусов по всему миру.
- «Горячие» обновления выпускаются немедленно после анализа новой вирусной угрозы и подготовки обновления.
- Перед выпуском обновления тестируются на огромном количестве «чистых» файлов.
- Обновления поступают к пользователям с нескольких серверов, находящихся в разных точках земного шара, что минимизирует время получения обновлений.
- Процесс обновления вирусных баз и программных модулей полностью автоматизирован.
- Обновления можно скачивать в виде заархивированных файлов.

Dr.Web Enterprise Security Suite

Продукты для бизнеса

Dr.Web Enterprise Security Suite. Продукты для бизнеса

Dr.Web Enterprise Security Suite – это комплекс продуктов Dr.Web, включающий элементы защиты всех узлов корпоративной сети и единый центр управления для большинства из них.

Продукты объединены в 5 групп по типу защищаемых объектов.

Коммерческие продукты Dr.Web	Программные продукты Dr.Web
Dr.Web Desktop Security Suite Защита рабочих станций, клиентов терминальных серверов, клиентов виртуальных серверов и клиентов встроенных систем	Dr.Web для Windows
	Dr.Web для Linux
	Dr.Web для Mac OS X
	Dr.Web для MS DOS
	Dr.Web для OS/2
Dr.Web Server Security Suite Защита файловых серверов и серверов приложений (в том числе виртуальных и терминальных)	Dr.Web для серверов Windows
	Dr.Web для серверов UNIX
	Dr.Web для Novell Storage Services
	Dr.Web для серверов Novell NetWare
	Dr.Web для Mac OS X Server
Dr.Web Mail Security Suite Защита почты	Dr.Web для почтовых серверов UNIX
	Dr.Web для MS Exchange
	Dr.Web для IBM Lotus Domino для Windows
	Dr.Web для IBM Lotus Domino для Linux
	Dr.Web для почтовых серверов Kerio для Windows
	Dr.Web для почтовых серверов Kerio для Linux
Dr.Web Gateway Security Suite Защита шлюзов	Dr.Web для интернет-шлюзов UNIX
	Dr.Web для интернет-шлюзов Kerio
	Dr.Web для Microsoft ISA Server и Forefront TMG
	Dr.Web для MIMESweeper
	Dr.Web для Qbik WinGate
	Dr.Web для почтовых серверов Kerio для Mac
Dr.Web Mobile Security Suite Защита мобильных устройств	Dr.Web для Android
	Dr.Web для Symbian OS
	Dr.Web для Windows Mobile

Лицензирование Dr.Web Enterprise Security Suite

Лицензирование продуктов для каждого объекта производится отдельно. Для защиты каждого объекта нужно выбрать базовую лицензию, и, если это необходимо, дополнительные компоненты.

Продукт	Поддерживаемые ОС и платформы	Базовая лицензия	Дополнительные компоненты
Dr.Web Desktop Security Suite Защита рабочих станций, клиентов терминальных и виртуальных серверов, клиентов встроенных систем	Windows 7/Vista/XP/2000	Комплексная защита*	■ Центр управления ■ Криптограф
	Mac OS X Linux	Антивирус**	■ Центр управления
	MS DOS OS/2		
Dr.Web Server Security Suite Защита файловых серверов и серверов приложений (в том числе терминальных и виртуальных серверов)	Windows Novell NetWare Mac OS X Server UNIX (Samba) UNIX (Novell Storage Services)	Антивирус	■ Центр управления
Dr.Web Mail Security Suite Защита почты	UNIX MS Exchange Lotus (Windows/Linux) Kerio (Windows/Linux)	Антивирус	■ Центр управления ■ Антиспам (кроме Kerio) ■ SMTP proxy
Dr.Web Gateway Security Suite Защита шлюзов	Интернет-шлюзы Kerio Интернет-шлюзы UNIX	Антивирус	■ Центр управления ■ Антиспам
	Microsoft ISA Server и Forefront TMG Qbik WinGate MIMESweeper		
Dr.Web Mobile Security Suite Защита мобильных устройств	Windows Mobile Android Symbian OS	Антивирус	■ Центр управления ■ Антиспам ■ Антиспам
Dr.Web Mobile Security Suite Защита мобильных устройств	Android	Комплексная защита***	■ Центр управления
	Symbian OS	Антивирус	
	Windows Mobile		

Универсальность

В соответствии с выбранным заказчиком решением создается единый ключевой файл Dr.Web для защиты всех интересных объектов. В состав ключа входят программные продукты Dr.Web для защиты того или иного объекта для всех ОС и платформ, поддерживаемых Dr.Web.

Полезные ссылки

Описание: http://products.drweb.com/enterprise_security_suite

* В лицензию *Комплексная защита* для рабочих станций входят следующие компоненты: антивирус, антиспам, веб-антивирус, офисный контроль, брандмауэр (соответствует продукту для домашних пользователей Dr.Web Security Space).

** В лицензию *Антивирус* входят антивирус, антишпион, антируткит, брандмауэр.

*** В лицензию *Комплексная защита* для мобильных устройств входят следующие компоненты: антивирус, антиспам, антивор, родительский контроль.

Центр управления Dr.Web Enterprise Security Suite

Централизованное
управление защитой всех узлов
корпоративной сети

Ключевые функции

- Централизованное управление всеми компонентами защиты, отслеживание состояния всех защищенных узлов, настройка автоматической реакции на вирусные инциденты.

Преимущества

- Низкозатратное управление системой защиты корпоративной сети из любой точки мира с одного рабочего места (через Веб-администратор), где бы оно ни находилось, даже вне корпоративной сети.
- Минимальная совокупная стоимость по сравнению с конкурирующими программами благодаря возможности развертывания сети под Windows- и UNIX-серверами, простоте установки и надежности защиты.
- Система защиты может быть развернута практически в любой корпоративной сети, вне зависимости от ее размера и особенностей – общего количества сотрудников и филиалов, топологии, наличия или отсутствия сервера Active Directory.
- Возможность развертывания агентов на рабочих станциях удобным для администратора способом – через политики Active Directory, стартовые скрипты, механизмы удаленной установки. Установка возможна, даже если узел сети является закрытым и недоступным для антивирусного сервера.
- Возможность реализации индивидуальных для конкретного предприятия и отдельных групп сотрудников политик безопасности.
- Автоматизация работы за счет интеграции с системой Windows NAP.
- Исключительная масштабируемость для сетей любого размера и сложности. Масштабирование обеспечивается за счет возможности использования иерархии взаимодействующих антивирусных серверов Центра управления и отдельного SQL-сервера для хранения данных, а также наличия комплексной структуры взаимодействия между ними и защищаемыми узлами сети.
- Поддержка нескольких сетевых протоколов для обмена данными между защищаемыми компьютерами и антивирусным сервером: TCP/IP (включая IPv6), IPX/SPX и NetBIOS, что позволяет использовать его в самых различных сетях.
- Безопасная передача данных между компонентами системы за счет возможности шифрования.
- Минимальный сетевой трафик. Компрессию данных между клиентом и сервером обеспечивает специально разработанный протокол обмена информацией в сетях, построенных на основе протоколов TCP/IP, IPX/SPX или NetBIOS.
- Прозрачность работы – журнал аудита действий администраторов позволяет отслеживать все шаги по установке и настройке системы. Все ее компоненты могут вести файлы отчетов с настраиваемым уровнем детализации.
- Удобная система оповещения администратора о проблемах, возникающих в антивирусной сети.

- Возможность назначения отдельных администраторов для различных групп, что позволяет использовать Центр управления как в компаниях с повышенными требованиями к безопасности, так и в многофилиальных организациях.
- Возможности настройки политик безопасности для любых типов пользователей, включая «мобильных», и для любых станций – даже отсутствующих в данный момент в сети – позволяют обеспечить актуальность защиты в любой момент времени.
- Гарантия невозможности самостоятельного изменения пользователями настроек защиты.
- Возможность защиты сетей, не имеющих доступа в Интернет.
- Возможность использования большинства существующих баз данных, как внутренних, так и внешних. При этом в качестве последних могут выступать Oracle, PostgreSQL, Microsoft SQL Server или Microsoft SQL Server Compact Edition, любая СУБД с поддержкой SQL-92 через ODBC.
- Возможность самостоятельного написания обработчиков событий на любом скриптовом языке, что дает прямой доступ к внутренним интерфейсам Центра управления.
- Возможность отката обновления – даже если процесс обновления вызвал ошибку, узел сети не останется без защиты.
- Открытость – с помощью этого комплекса системный администратор может устанавливать и синхронизировать дополнительные продукты сторонних производителей, что также снижает затраты на построение систем информационной безопасности.
- Наглядность системы контроля состояния защиты, непревзойденный по эффективности и удобству поиск станций сети.
- Возможности выбора списка обновляемых компонентов продукта и контроля перехода на новые версии позволяют администраторам устанавливать только необходимые и проверенные в их сети обновления.

Лицензирование

Центр управления лицензируется отдельно – как в составе группы продуктов Dr.Web Enterprise Security Suite, так и в качестве опции при покупке лицензии для отдельного продукта Dr.Web. Центр управления предоставляет возможность управления агентами для любых типов защищаемых объектов – рабочих станций, серверов, интернет-шлюзов и мобильных устройств. Центр управления лицензируется бесплатно.

Полезные ссылки

Описание:

http://products.drweb.com/enterprise_security_suite/control_center

Dr.Web Desktop Security Suite

Защита рабочих станций, клиентов терминальных и виртуальных серверов, клиентов встроенных систем

- Dr.Web для Windows
- Dr.Web для Linux
- Dr.Web для Mac OS X
- Консольные сканеры Dr.Web для Windows, MS DOS, OS/2

Лицензирование Dr.Web Desktop Security Suite

Виды лицензий

- По числу защищаемых рабочих станций, клиентов, подключающихся к терминальному или виртуальному серверу, или клиентов встроенных систем.

Программные продукты Dr.Web Desktop Security Suite можно приобрести отдельно или в составе Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются Центр управления Dr.Web Enterprise Security Suite (кроме консольных сканеров Dr.Web) и криптограф (только для Dr.Web для Windows).

При покупке этого продукта предоставляется право бесплатного использования Dr.Web Mobile Security Suite.

Варианты лицензий

	Windows 7/Vista/XP/2000 SP4 + Rollup 1	Windows 7/Vista/XP/2000 SP4 + Rollup 1	Linux	Mac OS X	MS DOS, OS/2
Базовая лицензия	Комплексная защита	Антивирус	Антивирус	Антивирус	Антивирус
Компоненты защиты базовой лицензии	<ul style="list-style-type: none"> ■ Антивирус ■ Антишпион ■ Антируткит ■ Антиспам ■ Веб-антивирус ■ Офисный контроль ■ Брандмауэр 	<ul style="list-style-type: none"> ■ Антивирус ■ Антишпион ■ Антируткит ■ Брандмауэр 	<ul style="list-style-type: none"> ■ Антивирус ■ Антишпион 	<ul style="list-style-type: none"> ■ Антивирус ■ Антишпион 	<ul style="list-style-type: none"> ■ Антивирус ■ Антишпион
Дополнительные компоненты					
Центр управления	+	+	+	+	-

Также продукты Dr.Web Desktop Security Suite доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Поддерживаемые ОС

Dr.Web для Windows	Dr.Web для Linux	Dr.Web для Mac OS X	Консольные сканеры Dr.Web
Windows 7/Vista/XP/2000 SP4 + Rollup 1 (32- и 64-битные системы)	Дистрибутивы с ядром Linux версии 2.6.x (32- и 64-битные системы)	Mac OS X 10.4 и выше (32- и 64-битные системы)	Windows, MS DOS, OS/2

Dr.Web для Windows

Защита рабочих станций, клиентов встроенных систем, клиентов терминальных и виртуальных серверов

Преимущества

- **Наличие сертификатов**
Dr.Web для Windows имеет сертификаты соответствия ФСТЭК и ФСБ. Это означает, что продукт можно использовать в организациях, требующих повышенного уровня безопасности. Dr.Web для Windows полностью соответствует требованиям закона о защите персональных данных, предъявляемым к антивирусным продуктам. Он может применяться в сетях, соответствующих максимально возможному уровню защищенности.
- **Гибкое лицензирование**
Dr.Web для Windows 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.
- **Централизованное управление**
Если необходимо обеспечить централизованное управление защитой рабочих станций, требуется лицензирование Центра управления Dr.Web Enterprise Security Suite. Центр управления одинаково надежно работает в сетях любого размера и сложности – от простых, состоящих из нескольких компьютеров, до распределенных интранет-сетей, насчитывающих десятки тысяч узлов.
- **Полная защита от существующих угроз**
Dr.Web для Windows обеспечивает надежную защиту от большинства существующих угроз. Непревзойденное качество лечения и высокий уровень самозащиты не дают шанса вирусам и другим вредоносным объектам проникнуть в защищаемую сеть. Наличие встроенного брандмауэра и функции Офисного контроля (лицензия «Комплексная защита») не только преграждает путь вирусам через уязвимости операционных систем и программ, но и обеспечивает надежный контроль над работой установленных приложений.
- **Увеличение производительности труда сотрудников**
Внедрение компонентов Dr.Web для Windows дает мгновенный положительный эффект. Снижение потока спама (лицензия «Комплексная защита») практически до нуля позволяет сотрудникам компании работать более эффективно – теперь важные сообщения не затеряются среди нежелательной корреспонденции. Заражение компьютеров сети исключено – а значит, не будет простоев в работе организации, которые раньше могли возникать во время восстановления потерянной из-за вирусов информации.

- **Сохранение репутации компании**
Внедрение Dr.Web для Windows не дает злоумышленникам возможности превратить локальную сеть в источник вирусов и спама, которые могут попасть к клиентам компании. Использование продукта – это надежная гарантия репутации любой организации как делового партнера.

Компоненты защиты

Обнаружение всех видов угроз (сканер Dr.Web)

- Быстрая, но при этом максимально тщательная проверка оперативной памяти, загрузочных секторов, жестких дисков и сменных носителей.
- Нейтрализация вирусов, троянских программ и других видов вредоносных объектов.
- Обширные базы для детектирования шпионского, потенциально опасного и рекламного ПО, хакерских утилит и программ-шуток.

Защита в режиме реального времени (файловый монитор SpiDer Guard®)

- Постоянный мониторинг здоровья компьютера – перехват «на лету» обращений к файлам на жестких дисках, дискетах, CD/DVD/Blu-ray-дисках, флеш- и смарт-картах.
- Высокая устойчивость файлового монитора к попыткам вредоносных программ помешать его работе.

Противодействие руткитам (антируткит Dr.Web Shield™)

- Надежная защита системы от вирусов, использующих rootkit-технологии и умеющих скрывать свое пребывание в инфицированной системе.
- Нейтрализация сложных руткитов (Shadow-based (Conficker), MaosBoot, Rustock.C, Sector).

Чистая почта без вирусов (почтовый монитор SpiDer Mail®)

- Антивирусная проверка почты «на лету» по протоколам SMTP/POP3/NNTP/IMAP4 не влияет на работу используемой почтовой программы и не задерживает прием писем.
- Индивидуальные правила обработки для каждого типа вредоносных программ – вирусов, потенциально опасного и рекламного ПО, хакерских утилит, программ платного дозвона, программ-шуток.
- Анализ состава и времени отправки писем позволяет выявить признаки вирусной активности и избежать массовых рассылок сообщений почтовыми червями.

...без спама и нежелательных сообщений (Антиспам Dr.Web)

- Проверка входящей и исходящей почты производится в режиме реального времени.
- Работа антиспама не зависит от используемой почтовой программы и не задерживает прием почты.
- Антиспам не требует настроек и начинает автоматически действовать с приемом первого сообщения.
- Разные технологии фильтрации обеспечивают высокую вероятность распознавания спама, фишинг-, фарминг-, скамминг- и bounce-сообщений.
- Защита от попадания в ботнеты – провайдер не отключит вам доступ к Интернету за рассылку спама.
- Отфильтрованные письма не удаляются, а перемещаются в специальную папку почтовой программы, где их всегда можно проверить на предмет ложных срабатываний.
- Модуль спам-анализатора абсолютно автономен; для его работы не требуется связи с внешним сервером или доступа к какой-либо базе данных, что позволяет существенно экономить трафик.

Щит от интернет-угроз (веб-антивирус SpiDer Gate™)

- Модуль SpiDer Gate™ в режиме реального времени прозрачно сканирует входящий и исходящий HTTP-трафик, перехватывает все HTTP-соединения, производит фильтрацию данных, автоматически блокирует зараженные страницы в любых веб-браузерах, проверяет файлы в архивах, защищает от фишинговых и других опасных интернет-ресурсов.
- Работа SpiDer Gate не зависит от используемого браузера.
- Фильтрация практически не влияет на производительность ПК, скорость интернет-соединения и объем передаваемых данных.
- В режиме «по умолчанию» не требуется никакой настройки: SpiDer Gate начинает сканирование сразу же после установки в системе.
- Контроль за интернет-серфингом (Офисный контроль Dr.Web)
- Запрет доступа сотрудников к нежелательным с точки зрения руководства веб-сайтам.
- Блокировка сайтов по 10 тематическим группам (оружие, наркотики, игры, порнография и др.).
- Запрет использования переносных хранилищ информации (флеш-дисков, USB-устройств), сетевых устройств, а также отдельных файлов и каталогов – дополнительная возможность обезопасить важную информацию от удаления или похищения злоумышленниками.

Защита от сетевых атак (брандмауэр Dr.Web)

- Защита от несанкционированного доступа извне, предотвращение утечек важных данных по сети, блокировка подозрительных соединений на уровне пакетов и приложений.
- Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам и регистрировать информацию о попытках доступа в журнале приложений.
- Фильтрация на уровне пакетов позволяет контролировать доступ к сети Интернет вне зависимости от программ, инициирующих подключение. Журнал пакетного фильтра хранит информацию о пакетах, переданных через сетевые интерфейсы.

Системные требования

Поддерживаемые ОС

- Windows 7/Vista/XP/2000 SP4 + Rollup 1 (32- и 64-битные системы).

Свободное пространство на жестком диске

Не менее 250 МБ свободного дискового пространства для установки всех компонентов Dr.Web, из них:

- до 70 МБ занимает установочный файл;
- до 90 МБ занимают временные файлы, которые будут автоматически удалены после завершения установки.

Полезные ссылки

Описание: <http://products.drweb.com/win/workstations>

Антивирус Dr.Web для Mac OS X

Базовая защита от вирусов и другого вредоносного ПО, написанного для инфицирования не только Mac OS X, но и других операционных систем

Преимущества

- Удобный центр управления.
- Высокая скорость сканирования.
- Возможность создания собственных профилей сканирования.
- Надежная защита в режиме реального времени.
- Минимальная нагрузка на защищаемую систему.
- Малый расход трафика при обновлениях.
- Разнообразные настройки.
- Простота управления.
- Стильный и удобный интерфейс.

Ключевые функции

- Проверка объектов автозапуска, сменных носителей информации, сетевых и логических дисков, почтовых форматов, файлов и каталогов, включая упакованные и находящиеся в архивах.
- Быстрое, полное и выборочное сканирование.
- Антивирусная проверка вручную, автоматически или по заранее составленному расписанию.
- Защита настроек монитора SpiDer Guard® паролем от несанкционированного изменения.
- Применение действий для зараженных, подозрительных объектов и объектов другого типа, включая лечение, перемещение в карантин и удаление, в том числе в случае, если выбранное ранее действие оказалось невозможным.
- Исключение из проверки путей и файлов по запросу пользователя.
- Обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками.
- Регистрация времени события, объекта проверки и типа воздействия на него.
- Загрузка обновлений автоматически (по расписанию) или по требованию.
- Автоматическое оповещение (в том числе с помощью звуковых уведомлений) о вирусных событиях.
- Изоляция зараженных файлов в карантине с возможностью задания времени хранения объектов в карантине и его максимального размера.
- Лечение, восстановление или удаление перемещенных в карантин объектов.
- Ведение подробного отчета о работе.
- Доступность модулей в виде утилит командной строки, с возможностью их встраивания в исполняемые для обслуживания системы Apple Scripts.

Системные требования

- Mac OS X 10.4 или выше (32- и 64-битные системы).
- Процессор Intel.
- 128 МБ оперативной памяти.
- 120 МБ свободного дискового пространства.
- Доступ к сети Интернет: для регистрации и получения обновлений.

Полезные ссылки

Описание: <http://products.drweb.com/mac>

Антивирус Dr.Web для Linux

Базовая защита от вирусов

Ключевые функции

- Детектирование и нейтрализация вирусов и других вредоносных объектов на жестких дисках и сменных носителях.
- Определение вирусов в архивах любой степени вложенности и в упакованных объектах.
- Проверка файлов, сжатых упаковщиками, в том числе неизвестными, с помощью технологии FLY-CODE™.
- Защита от неизвестных угроз при помощи технологии несигнатурного поиска Origins Tracing™ и интеллектуального эвристического анализатора Dr.Web.
- Быстрая, полная, выборочная или пользовательская проверка.
- Постоянный мониторинг здоровья компьютера – перехват «на лету» обращений к файлам на дисках, дискетах, CD/DVD/Blu-ray-дисках, флеш- и смарт-картах.
- Защита собственных компонентов от попыток вредоносных программ препятствовать работе антивируса.
- Изоляция зараженных объектов в карантине с возможностью их восстановления; функция ограничения размера карантина.
- Сбор полной статистики о работе антивируса.
- Автоматические обновления по расписанию и по требованию.

Консольные сканеры Dr.Web

Антивирусная защита с расширенными возможностями ее автоматизации для опытных пользователей

Консольные сканеры Dr.Web без графического интерфейса используют общую вирусную базу и поисковый модуль Dr.Web и предназначены для работы в операционных системах MS DOS, OS/2 и Windows. Для управления антивирусной защитой необходимы навыки работы с командной строкой.

Преимущества

- Удобный центр управления.
- Возможность проверки «на лету».
- Настройка пользовательских проверок.
- Управляемый карантин.
- Автоматические обновления.
- Стильный интерфейс.

Системные требования

- Платформа: полная поддержка системы команд процессора архитектуры x86 в 32- и 64-битном режиме.
- Не менее 154 МБ свободного дискового пространства + 70 МБ на каждого пользователя.
- Операционная система: дистрибутивы GNU/Linux, имеющие версию ядра 2.6.x.
- Доступ к сети Интернет: для регистрации и получения обновлений.

Полезные ссылки

Описание: <http://products.drweb.com/linux>

Преимущества

- Минимальные системные требования – сканеры прекрасно работают даже на встроенных системах и способны надежно защитить маломощные компьютеры прежних поколений.
- Удобство проверки – администратор может выбрать «ручное» сканирование или проверку по расписанию.
- Лечение зараженных рабочих станций и серверов, в том числе недоступных по сети.
- Высокая вирусоустойчивость и возможность установки на зараженный компьютер.
- Автоматизация повседневных работ с использованием богатых возможностей командной строки.
- Гарантированное удаление вирусов, неизвестных Dr.Web или помещенных в архивы с неизвестными форматами.
- Запуск с любого внешнего носителя (компакт-диска или USB-накопителя).

Полезные ссылки

Описание: <http://products.drweb.com/console>

Dr.Web Server Security Suite

Защита файловых серверов и серверов приложений (в том числе виртуальных и терминальных серверов)

- Dr.Web для серверов Windows
- Dr.Web для серверов Novell NetWare
- Dr.Web для Mac OS X Server
- Dr.Web для серверов UNIX (Samba)
- Dr.Web для серверов UNIX (Novell Storage Services)

Программные продукты Dr.Web Server Security Suite можно приобрести отдельно или в составе Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируется Центр управления Dr.Web Enterprise Security Suite.

	Dr.Web для серверов Windows	Dr.Web для серверов Novell NetWare	Dr.Web для Mac OS X Server	Dr.Web для серверов UNIX	Dr.Web для Novell Storage Services
Базовая лицензия	Антивирус				
Дополнительные компоненты					
Центр управления	+	+	+	+	+

Также все продукты Dr.Web Server Security Suite доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Поддерживаемые ОС

Dr.Web для серверов Windows	Dr.Web для серверов Novell NetWare	Dr.Web для Mac OS X Server	Dr.Web для серверов UNIX	Dr.Web для Novell Storage Services
Windows NT/ 2000/ 2003/ 2008 (32- и 64-битные системы)	Novell NetWare версии 3.12-6.5 с установленными дополнениями из Minimum patch list	Mac OS X Server 10.4 и выше	Дистрибутивы с ядром Linux версии 2.6.x (32- и 64-битные системы)	Поддерживаемые ОС: SUSE Linux, Enterprise Server, 10 SP3

Dr.Web для серверов Windows

Антивирусная защита файловых и терминальных серверов под управлением Windows, включая серверы приложений

Преимущества

- Возможность использования в организациях, требующих повышенного уровня безопасности, – продукт полностью отвечает требованиям российского законодательства и обладает сертификатами соответствия ФСТЭК и ФСБ.
- Высокая производительность и стабильность работы.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.
- Бесперебойная работа антивируса в автоматическом режиме.
- Гибкое распределение нагрузки на файловую систему сервера благодаря уникальной технологии отложенной проверки файлов, открываемых «на чтение».
- Гибкая клиентоориентированная система настройки – выбор объектов проверки, действий с обнаруженными вирусами или подозрительными файлами.
- Простота установки и администрирования.
- Полноценная защита сразу после установки (с настройками по умолчанию).
- Прозрачность – подробные файлы отчета с необходимой администратору степенью детализации.

Ключевые функции

- Проверка томов сервера по заранее заданному расписанию или запросу администратора.
- Сканирования на «лету» – непосредственно при записи или открытии файлов на сервере с рабочих станций.
- Многопоточная проверка
- Автоматическое отключение от сервера станции – источника вирусной угрозы.
- Мгновенное оповещение администратора, других пользователей и групп о вирусных инцидентах – по электронной почте либо путем отправки уведомлений на мобильный телефон или пейджер.
- Изоляция инфицированных файлов в карантине
- Лечение, восстановление и/или удаление файлов из карантина.
- Ведение журнала действий антивируса.
- Автоматические обновления вирусных баз.

Системные требования

- Процессор: поддерживающий систему команд i686 и старше.
- Операционная система: Microsoft Windows Server 2000/2003/2008 (32- и 64-битные версии операционных систем).
- Оперативная память: 512 МБ и больше.

Полезные ссылки

Описание: <http://products.drweb.com/fileserver/win>

Dr.Web для серверов Novell NetWare

Антивирусная защита файловых хранилищ

Преимущества

- Широчайший спектр поддерживаемых версий Novell NetWare – от 3.12 до 6.5.
- Поддержка пространства имен NetWare.
- Высокая скорость сканирования огромных массивов данных при минимальной нагрузке на операционную систему.
- Простота установки.
- Гибкая клиентоориентированная система настройки параметров проверки и действий с обнаруженными вредоносными объектами.

Ключевые функции

- Проверка томов сервера по расписанию или запросу администратора.
- Проверка «на лету» всех файлов, проходящих через сервер.
- Многопоточная проверка.
- Возможность регулировки степени загрузки процессора, что позволяет задавать приоритетность процесса сканирования в системе.
- Автоматическое отключение от сервера станции – источника вирусной угрозы.
- Протоколирование проверки; управление детализацией протокола.
- Уведомления об обнаружении инфицированных объектов.
- Лечение, удаление или перемещение инфицированных объектов в карантин.
- Администрирование антивируса при помощи консоли сервера или удаленной консоли.
- Ведение статистики сканирования и журнала действий антивируса.
- Автоматические обновления вирусных баз.

Системные требования

- Novell NetWare версии 3.12-6.5 с установленными дополнениями из Minimum patch list.
- 25 МБ оперативной памяти + 25 МБ оперативной памяти на каждый дополнительный процесс сканирования.
- 20 МБ дискового пространства.

Полезные ссылки

Описание: <http://products.drweb.com/fileserver/novell>

Dr.Web для Mac OS X Server

Антивирусная защита рабочих станций под управлением серверных версий ОС Mac OS X

Преимущества

- Удобный центр управления.
- Высокая скорость сканирования.
- Возможность создания собственных профилей сканирования.
- Надежная защита в режиме реального времени.
- Минимальная нагрузка на защищаемую систему.
- Малый расход трафика при обновлениях.
- Разнообразные настройки.
- Простота управления.
- Стильный и удобный интерфейс.

Ключевые функции

- Проверка объектов автозапуска, сменных носителей информации, сетевых и логических дисков, почтовых форматов, файлов и каталогов, включая упакованные и находящиеся в архивах.
- Быстрое, полное и выборочное сканирование.
- Антивирусная проверка вручную, автоматически или по заранее составленному расписанию.
- Защита настроек монитора SplDer Guard® паролем от несанкционированного изменения.
- Применение действий для зараженных, подозрительных объектов и объектов другого типа, включая лечение, перемещение в карантин и удаление, в том числе в случае если выбранное ранее действие оказалось невозможным.
- Исключение из проверки путей и файлов по запросу пользователя.
- Обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками.
- Регистрация времени события, объекта проверки и типа воздействия на него.
- Загрузка обновлений автоматически (по расписанию) или по требованию.
- Автоматическое оповещение (в том числе с помощью звуковых уведомлений) о вирусных событиях.
- Изоляция зараженных файлов в карантине с возможностью задания времени хранения объектов в карантине и его максимального размера.
- Лечение, восстановление или удаление перемещенных в карантин объектов.
- Ведение подробного отчета о работе.
- Доступность модулей в виде утилит командной строки, с возможностью их встраивания в используемые для обслуживания системы Apple Scripts.

Системные требования

- Mac OS X Server 10.4 или выше.
- Процессор Intel.
- 128 МБ оперативной памяти.
- 120 МБ свободного дискового пространства.
- Доступ к сети Интернет: для регистрации и получения обновлений.

Полезные ссылки

Описание: <http://products.drweb.com/fileserver/mac>

Dr.Web для серверов UNIX

Антивирусная защита файловых хранилищ

Преимущества

- Высокая производительность и стабильность работы.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.
- Гибкая клиентоориентированная система настройки – выбор объектов проверки, действий с обнаруженными вирусами или подозрительными файлами.
- Отличная совместимость – не конфликтует с известными межсетевыми экранами и файловыми мониторами.
- Удобство администрирования, простота установки и настройки.

Ключевые функции

- Проверка томов сервера по заранее заданному расписанию или запросу администратора.
- Сканирование на «ленту» – непосредственно при записи или открытии файлов на сервере с рабочих станций.
- Многопоточная проверка.
- Автоматическое отключение от сервера станции – источника вирусной угрозы.
- Мгновенное оповещение администратора, других пользователей и групп о вирусных инцидентах – по электронной почте либо путем отправки уведомлений на мобильный телефон или пейджер.
- Изоляция инфицированных файлов в карантине.
- Лечение, восстановление и/или удаление файлов из карантина.
- Ведение журнала действий антивируса.
- Автоматические обновления вирусных баз.

Системные требования

- Dr.Web Daemon (drwebd) версии не ниже 5.0.
- Samba 3.0 и выше.

Поддерживаемые ОС

- Дистрибутивы Linux, имеющие версию ядра 2.4.x и выше.
- FreeBSD версии 6.x и выше для платформы Intel x86.
- Solaris версии 10 для платформы Intel x86.

Полезные ссылки

Описание:
<http://products.drweb.com/fileserver/unix>

Dr.Web для Novell Storage Services

Антивирусная защита файловых хранилищ

Преимущества

- Высокая производительность и стабильность работы.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web для Novell Storage Services идеально функционировать на серверах практически любой конфигурации.
- Гибкая система настройки – выбор объектов проверки, действий с обнаруженными вирусами или подозрительными файлами.
- Отличная совместимость – не конфликтует с известными межсетевыми экранами и файловыми мониторами.
- Удобство администрирования. Простота установки и настройки.

Ключевые функции

- Возможность лечения или удаления любых типов вредоносных объектов.
- Асинхронное сканирование – при записи или открытии файлов на сервере с рабочих станций.
- Многопоточная проверка.
- Централизованный сбор статистики, учитывающей все аспекты работы системы.
- Оповещение администратора о результатах проверки по электронной почте с помощью шаблонов, описанных в системе, что позволяет получать информацию в максимально удобном виде.
- Изоляция инфицированных и подозрительных файлов в карантине. Лечение, восстановление и/или удаление файлов из карантина. Ведение журнала действий антивируса. Защита собственных модулей от сбоев.
- Автоматические обновления вирусных баз.

Системные требования

- Novell Open Enterprise Server SP2 на базе операционной системы SUSE Linux Enterprise Server 10 SP3.
- Установленная служба Novell Storage Services (NSS).
- Файловая система NSS, смонтированная в определенную директорию системы.
- Не менее 300 МБ свободного места на диске для установки продукта.

Остальные системные требования совпадают с требованиями операционной системы SUSE Linux Enterprise Server 10 SP3.

Поддерживаемые ОС

- SUSE Linux Enterprise Server 10 SP3.

Полезные ссылки

Описание: <http://products.drweb.com/fileserver/nss>

Dr.Web Mail Security Suite

Защита почты

- Dr.Web для почтовых серверов и шлюзов UNIX
- Dr.Web для MS Exchange
- Dr.Web для IBM Lotus Domino (Windows, Linux)
- Dr.Web для почтовых серверов Kerio (Windows, Linux)

Лицензирование Dr.Web Mail Security Suite

Виды лицензий

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

Программные продукты Dr.Web для защиты почты можно приобрести отдельно или в составе Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются Центр управления Dr.Web Enterprise Security Suite, Антиспам и SMTP проху.

Совместное использование продуктов для защиты почты и дополнительного компонента SMTP проху не только существенно повышает общую безопасность сети, но и снижает нагрузку на внутренние почтовые серверы и рабочие станции.

Варианты лицензий

	Dr.Web для MS Exchange	Dr.Web для IBM Lotus Domino	Dr.Web для почтовых серверов UNIX	Dr.Web для почтовых серверов Kerio
Базовая лицензия	Антивирус			
Дополнительные компоненты				
Антиспам	+	+	+	–
SMTP проху	+	+	+	+
Центр управления	+	+	+	+

Также продукты группы Dr.Web Desktop Security Suite (кроме Консольных сканеров) доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Поддерживаемые ОС

Продукт Dr.Web	Windows	Linux	FreeBSD	Solaris
			для платформы Intel x86	
Dr.Web для почтовых серверов UNIX		с версией ядра 2.4.x и выше	версии 6.x и выше	версии 10
Dr.Web для MS Exchange	Server 2000/2003/2008			
Dr.Web для IBM Lotus Domino	Server 2000/2003/2008/2008 R2 (32- и 64- битные версии)	Red Hat Enterprise Linux (RHEL) 4 и 5 версии, Novell SuSE Linux Enterprise Server (SLES) 9 и 10 версии (только 32-битные)		
Dr.Web для почтовых серверов Kerio	Server 2000/2003/2008 XP/ Vista/ 7	Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 и 11.1; CentOS Linux 5.2 и 5.3; Debian 5.0; Ubuntu 8.04 LTS		

Dr.Web для почтовых серверов и шлюзов UNIX

Антивирусная и антиспам-защита почтового трафика, проходящего через серверы под управлением UNIX (Linux/FreeBSD/Solaris(x86))

Преимущества

- Соответствие требованиям российского законодательства.
- Возможность гибкой настройки под потребности пользователей.
- Нетребовательность к квалификации администратора.
- Высокая скорость отклика.
- Дополнительные преимущества антиспама Dr.Web.
- Защита конфиденциальной информации.
- Удобство администрирования.
- Открытость.
- Возможность подключения неограниченного количества плагинов.

Ключевые функции

- Фильтрация почтовых сообщений на вирусы и спам.
- Разбор почтовых сообщений и анализ всех их компонентов.
- Корректная обработка большинства известных типов архивов, в том числе многотомных и самораспаковывающихся (SFX).
- Белые и черные списки.
- Настраиваемые уведомления.
- Ведение статистики, учитывающей все аспекты работы системы.
- Защита работы собственных модулей от сбоев.

Соответствие требованиям российского законодательства

Dr.Web для почтовых серверов UNIX обладает сертификатами соответствия ФСТЭК и ФСБ. Это позволяет использовать продукт в организациях, требующих повышенного уровня безопасности, в том числе в составе подсистемы антивирусной защиты информационных систем 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».

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.

Дополнительные преимущества антиспама Dr.Web

- Не требует обучения и начинает эффективно работать с момента установки – в отличие от антиспамов, построенных на использовании алгоритма Байеса (Panda, Kaspersky).
- 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 невозможной 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.

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 карантинном как через веб-интерфейс, так и через специальную утилиту, а также возможность архивации всех проходящих сообщений.

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. Реализованные плагины:

- Dr.Web – плагин антивирусной проверки почты средствами антивирусного движка Dr.Web.
- vaderetro – плагин, фильтрующий почту на спам через собственную библиотеку Vade Retro.
- headersfilter – плагин, фильтрующий сообщения по заголовкам.

Dr.Web SMTP proxy

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.

Ключевые возможности

- Защита от атак спамеров за счет возможности ограничения параметров SMTP-сессии.
- Защита от замаскированного спама благодаря функции проверки подлинности IP-адреса.
- Защита от атак хакеров – эффективное противостояние как пассивным атакам (типа PLAIN, LOGIN и т. д.), так и активным атакам без перебора по словарю.
- Защита от спам-ловушек.
- Защита от некорректно сформированных писем.
- Экономия интернет-трафика за счет ограничения размера вложений.
- Ограничение Open Relays серверов.

Поддерживаемые ОС

- Дистрибутивы Linux, имеющие версию ядра 2.4.x и выше.
- FreeBSD версии 6.x и выше для платформы Intel x86.
- Solaris версии 10 для платформы Intel x86.

Полезные ссылки

Описание: <http://products.drweb.com/mailserver/maid>

Dr.Web для IBM Lotus Domino

Антивирусная и антиспам-защита платформы IBM Lotus Domino под управлением Windows и Linux

Преимущества

- Минимальная совокупная стоимость.

Dr.Web для IBM Lotus Domino работает не только на отдельно стоящих серверах, но и на partitions-серверах и кластерах Lotus Domino. Копии антивирусов на разных разделах действуют в памяти компьютера автономно, используя общие базы и исполняемые файлы. В этом случае лицензировать необходимо только одну копию, что существенно снижает затраты на антивирусную защиту.

- 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.

- 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.

- 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 отправлять уведомления об обнаруженных вирусах отправителю, получателям и администраторам системы, сохранять заголовки полученных почтовых сообщений и вложения к ним, и т. д.

- Удобство администрирования.

Механизмы группирования и управление группами значительно упрощают администрирование антивирусной защиты.

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 сбоя.
- Автоматические обновления.

Поддерживаемые ОС

- Версия для Windows: Windows Server 2000/2003/2008/2008R2 (32- и 64-битные версии).
- Версия для Linux: Red Hat Enterprise Linux (RHEL) 4 и 5 версии, Novell SuSE Linux Enterprise Server (SLES) 9 и 10 версии (только 32-битные)

Полезные ссылки

Описание: <http://products.drweb.com/lotus>

Dr.Web для MS Exchange

Антивирусная и антиспам-проверка трафика, передаваемого через почтовые серверы MS Exchange 2000/2003/2007/2010

Преимущества

- Возможность использования в организациях, требующих повышенного уровня безопасности, – продукт полностью отвечает требованиям российского законодательства и обладает сертификатами соответствия ФСТЭК и ФСБ.
- Большие возможности по установке и тонкой настройке в зависимости от потребностей компании.
- Высокая скорость сканирования при минимальной нагрузке на операционную систему, что позволяет Dr.Web идеально функционировать на серверах практически любой конфигурации.
- Наличие поддержки концепции серверных ролей и транспортных агентов для MS Exchange Server 2007/2010 – проверка писем на предмет наличия вирусов и спама может выполняться как на транспортном уровне, так и на уровне поддержки антивирусного интерфейса VSAPI. Это позволяет обеспечить оптимальный уровень защиты организации.
- Встроенный антиспам, не требующий обучения (действует с момента установки), который существенно снижает нагрузку на сервер и увеличивает производительность труда сотрудников компании.
- Возможность фильтрации по черным и белым спискам, что позволяет как исключать из проверки определенные адреса, так и увеличивать ее эффективность.
- Новая возможность для гибкого конфигурирования параметров защиты приложения через браузер в удобном для пользователя режиме при помощи веб-консоли администратора.
- Возможность фильтрации по типам файлов, что позволяет компании уменьшить объем трафика.
- Наличие механизма группирования, что позволяет задавать различные параметры для разных групп сотрудников, а следовательно – существенно сокращает введение системы антивирусной защиты в строй и упрощает сопровождение продукта.
- Высокая производительность и стабильность работы благодаря функции многопоточной проверки.
- Уникальные технологии обнаружения неизвестных (новейших) упаковщиков и вредоносных объектов.
- Полностью автоматизированный запуск приложения (при старте системы).
- Удобная система обновлений при помощи штатного планировщика Windows.
- Исчерпывающая документация на русском языке.

Ключевые функции

- Антивирусная и антиспам-проверка почтовых сообщений, в том числе вложенных файлов, «на лету».
- Антивирусный мониторинг сообщений в почтовых ящиках пользователей, а также файлов в папках общего доступа.
- Антивирусная проверка транзитного почтового потока, проходящего через сервер MS Exchange.
- Лечение инфицированных файлов.
- Группирование пользователей при помощи ActiveDirectory.
- Сканирование с применением заданных параметров: выбор максимального размера и типов проверяемых объектов, действий (в том числе и для файлов, не поддающихся проверке), а также способов обработки инфицированных объектов.
- Детектирование вредоносных объектов в многократно заархивированных файлах.
- Применение различных действий в зависимости от вида спама, включая перемещение в карантин и добавление префикса к теме письма.
- В случае необходимости – добавление произвольных текстов к отсылаемым письмам.
- Изоляция инфицированных и подозрительных файлов в карантине.
- Выбор протокола рассылки уведомлений – MAPI (внутри организации Exchange), SMTP или HTTP (как внутри организации, так и в ее DMZ-зоне).
- Изменение параметров учетной записи сервиса программы и администрирование приложения из-под пользовательской (неадминистративной) учетной записи.
- Уведомление администратора или других пользователей о вирусных инцидентах.
- Ведение статистики работы комплекса.
- Автоматические обновления.

Системные требования

Свободное дисковое пространство

- 20 МБ для установки, 50 МБ для журнала событий, и еще 512 МБ может понадобиться для архива журнала событий.

Поддерживаемые ОС

- При использовании MS Exchange Server 2000/2003: Microsoft Windows 2000 Server или Advanced Server с установленным SP4; Microsoft Windows Server 2003 (версия Standard, Enterprise или Datacenter) с установленным SP1 или выше.
- При использовании MS Exchange Server 2007/2010: Microsoft Windows Server 2003 R2x64 с установленным SP2; Microsoft Windows Server 2008 x64.

Полезные ссылки

Описание: <http://products.drweb.com/exchange>

Dr.Web для почтовых серверов Kerio

Антивирусная проверка вложений всех почтовых сообщений, передаваемых по протоколам SMTP/POP3

Преимущества

- Прекрасная совместимость с почтовыми серверами Kerio, подтвержденная тестированиями Kerio Technologies.
- Возможность работы в режиме централизованной защиты при помощи Центра управления Dr.Web Enterprise Security Suite.
- Dr.Web – единственный на сегодняшний день российский антивирусный плагин для почтовых серверов Kerio, что особенно важно при поставке продукта государственным предприятиям.
- Локализованная поддержка пользователей, в России – на русском языке.
- Минимальное время доставки сообщений и повышенная надежность продукта за счет использования технологии многопоточной проверки.
- Щадящие системные требования и отсутствие нагрузки на локальную сеть.
- Гибкая клиентоориентированная система настройки: выбор объектов проверки и действий с обнаруженными вирусами или подозрительными файлами.
- Возможность выбора действий для файлов, не поддающихся проверке.
- Удобное управление из консоли администрирования почтового сервера Kerio.

Ключевые функции

- Проверка файловых вложений всех входящих и исходящих электронных сообщений.

Поддерживаемые ОС

- Версия для Windows: Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32- и 64-битные версии).
- Версия для Linux: Red Hat 9.0; Red Hat Enterprise Linux 4/5; Fedora Core 7 / 8; SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 и 11.1; CentOS Linux 5.2 и 5.3; Debian 5.0; Ubuntu 8.04 LTS.

Полезные ссылки

Описание: <http://products.drweb.com/mailserver/kerio>

Dr.Web Gateway Security Suite

Защита шлюзов

- Dr.Web для интернет-шлюзов UNIX
- Dr.Web для интернет-шлюзов Kerio
- Dr.Web для Microsoft ISA Server и Forefront TMG
- Dr.Web для MIMESweeper
- Dr.Web для Qbik WinGate

Лицензирование Dr.Web Gateway Security Suite

Виды лицензий

- По числу защищаемых пользователей (оно неограниченно).
- Посерверная лицензия – для проверки неограниченного объема трафика на одном сервере, с числом защищаемых пользователей не более 3 000.

Программные продукты Dr.Web для защиты шлюзов можно приобрести отдельно или в составе группы Dr.Web Enterprise Security Suite. В последнем случае дополнительно лицензируются Центр управления Dr.Web Enterprise Security Suite (кроме Dr.Web для MIMESweeper и Dr.Web для Qbik WinGate) и Антиспам (кроме Dr. Web для интернет-шлюзов UNIX и Kerio).

Варианты лицензий

	Dr.Web для интернет-шлюзов UNIX	Dr.Web для интернет-шлюзов Kerio	Dr.Web для Microsoft ISA Server и Forefront TMG	Dr.Web для MIMESweeper	Dr.Web для Qbik WinGate
Базовая лицензия	Антивирус	Антивирус	Антивирус	Антивирус	Антивирус
Дополнительные компоненты					
Антиспам	–	–	+	+	+
Центр управления	+	+	–	–	–

Также продукты Dr.Web для защиты шлюзов доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

Поддерживаемые ОС

Продукт Dr.Web	Windows	Linux	FreeBSD	Solaris
		для платформы Intel x86		
Dr.Web для интернет-шлюзов UNIX		с версией ядра 2.4.x и выше	версии 6.x и выше	версии 10
Dr.Web для интернет-шлюзов Kerio	2000/XP/2003/2008/7			
Dr.Web для Microsoft ISA Server и Forefront TMG	При использовании Microsoft ISA Server: <ul style="list-style-type: none"> ■ Microsoft® Windows Server® 2003 x86 с Service Pack 1 (SP1); ■ Microsoft® Windows Server® 2003 R2 x86 При использовании Microsoft Forefront TMG: <ul style="list-style-type: none"> ■ Microsoft® Windows Server® 2008 SP2 ■ Microsoft® Windows Server® 2008 R2 			
Dr.Web для MIMESweeper	2000 Server SP4 или выше/ Server 2003 или выше			
Dr.Web для Qbik WinGate	Vista/Server 2008/Server 2003/XP/2000 (32- и 64-битные системы)			

Dr.Web для интернет-шлюзов UNIX

Антивирусная проверка HTTP- и FTP-трафика, проходящего через корпоративный интернет-шлюз – прокси-сервер

Преимущества

- Эффективная фильтрация трафика на уровне ICAP-сервера – практически без замедления скорости доставки контента.
- Высокая масштабируемость.
- Способность обрабатывать гигантские массивы информации в режиме реального времени.
- Значительное снижение затрат на использование сети Интернет.
- Отличная совместимость – интеграция с любым программным обеспечением, поддерживающим ICAP-протокол, со всеми известными межсетевыми экранами.
- Нетребовательность к системным ресурсам.
- Гибкость и удобство администрирования.

Ключевые функции

- Антивирусная проверка FTP- и HTTP-трафика.
- Централизованное управление через Веб-администратор Центра управления Dr.Web Enterprise Security Suite.
- Фильтрация доступа по MIME-типу и размеру файлов или по названию хоста.
- Регулирование доступа к веб-ресурсам.
- Оптимизация проверки трафика за счет использования технологии Preview.
- Работа как с протоколом IPv4, так и с протоколом следующего поколения IPv6.
- Проверка и применение различных действий в зависимости от типов проверяемых файлов.
- Изоляция зараженных объектов в карантине.
- Предоставление отчетности в удобном виде.
- Обработка нескольких запросов в ходе одного соединения.
- Защита от несанкционированного доступа.
- Мониторинг и автоматическое восстановление работы системы.
- Оповещение пользователя о попытках загрузки вредоносной страницы или об обнаружении вируса.

Поддерживаемые ОС

- Linux с версией ядра 2.4.x и выше.
- FreeBSD версии 6.x и выше (для платформы Intel x86).
- Solaris версии 10 (для платформы Intel x86).
- Любые прокси-серверы, полноценно поддерживающие протокол ICAP, в частности Squid не ниже 3.0, Shweby не ниже 1.0, SafeSquid не ниже 3.0.

Полезные ссылки

Описание: <http://products.drweb.com/gateway/unix>

Dr.Web для интернет-шлюзов Kerio

Антивирусная проверка трафика, передаваемого по протоколам HTTP, FTP, SMTP и POP3, а также посредством веб-сервиса Kerio Clientless SSL VPN

Преимущества

- Надежная защита доступа в Интернет как для частных пользователей, так и для компаний любого размера и рода деятельности.
- Возможность работы в режиме централизованной защиты при помощи Центра управления Dr.Web Enterprise Security Suite.
- Удобство администрирования – возможность получать сообщения обо всех вирусных инцидентах как через почтовые уведомления, так и через СМС.
- Минимальное время доставки сообщений за счет многопоточной проверки.

Ключевые функции

- Детектирование вредоносных объектов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, а также посредством веб-сервиса Kerio Clientless SSL VPN.
- Детектирование инфицированных вложений в электронных письмах до их обработки почтовым сервером.
- Формирование списка проверяемых протоколов обмена данными.
- Просмотр информации о работе программы через веб-консоль.
- Сканирование с возможностью настройки параметров: выбор максимального размера, типов проверяемых объектов, способов обработки инфицированных файлов.
- Применение действий к обнаруженным угрозам согласно настройкам Kerio.
- Включение /отключение детектирования вредоносных программ (по их типам).
- Регистрация ошибок и происходящих событий в журнале регистрации событий (Event Log) и текстовом журнале.
- Рассылка почтовых уведомлений о различных событиях выбранным пользователям.
- Автоматические обновления вирусных баз.

Системные требования

- Не менее 55 МБ свободного дискового пространства.
- Операционная система Microsoft Windows 2000 SP4 + Rollup 1/XP/Vista/7, Microsoft Windows Server 2003/2008 (32- и 64-битные версии).
- Межсетевой экран Kerio 6 или более поздняя версия.

Полезные ссылки

Описание: <http://products.drweb.com/gateway/kerio>

Dr.Web для Microsoft ISA Server и Forefront TMG

Антивирусная и антиспам-проверка трафика, передаваемого через серверы Microsoft ISA Server и Forefront TMG

Преимущества

- Проверка любых объектов за минимальное время за счет использования технологий динамического анализа потребностей иных серверных сервисов в ресурсах и мгновенное автоматическое переключение между задачами.
- Использование возможностей новейших платформ для ускорения скорости проверки.
- Возможность работы на серверах любой конфигурации – в том числе с малым количеством оперативной памяти.
- Защита как реальных, так и виртуальных серверов.
- Встроенный антиспам, не требующий обучения (действует с момента установки), обеспечивающий снижение нагрузки на сервер и увеличение производительности труда сотрудников компании.
- Блокировка доступа к различным интернет-ресурсам и возможность фильтрации по типам файлов, что позволяет компании исключить проникновение вирусов с заведомо вредоносных ресурсов и уменьшить объем трафика.
- Уникальные технологии обнаружения неизвестных (новейших) упаковщиков и вредоносных объектов.
- Большие возможности по установке и тонкой настройке в зависимости от потребностей компании.
- Исчерпывающая документация на русском языке.

Ключевые функции

- Антивирусная и антиспам-проверка всего проходящего трафика, в том числе вложенных файлов.
- Возможность проверки проходящих файлов «на лету» с возможностью обнаружения вредоносных объектов в многократно заархивированных файлах.
- Лечение инфицированных файлов.
- Применение различных действий в зависимости от вида спама.
- Добавление сопроводительного текста к почтовым сообщениям, которые содержали угрозы безопасности.
- Блокирование доступа к инфицированным данным для всех пользователей локальных сетей.
- Ограничение доступа пользователей к интернет-ресурсам с помощью Офисного контроля.
- Изоляция инфицированных и подозрительных файлов в карантине.
- Уведомление администратора о вирусных инцидентах.
- Ведение статистики работы комплекса.
- Автоматические обновления.

Системные требования

При использовании Microsoft ISA Server:

Процессор Pentium III 733 МГц и выше.

ОЗУ: 1 ГБ и больше.

Свободное дисковое пространство: 300 МБ для установки. Дополнительный необходимый размер свободного дискового пространства требуется для временного хранения данных на этапе антивирусной проверки.

ОС: Microsoft® Windows Server® 2003 x86 с Service Pack 1 (SP1), Microsoft® Windows Server® 2003 R2 x86.

Прокси-сервер: Microsoft® ISA Server 2004, Microsoft® ISA Server 2006.

При использовании Microsoft Forefront TMG:

Процессор Pentium III 1.86 ГГц и выше.

ОЗУ: 2 ГБ и больше.

Свободное дисковое пространство: 300 МБ для установки. Дополнительный необходимый размер свободного дискового пространства требуется для временного хранения данных на этапе антивирусной проверки.

ОС: Microsoft® Windows Server® 2008 SP2, Microsoft® Windows Server® 2008 R2.

Прокси-сервер: Microsoft® Forefront® TMG 2010.

Полезные ссылки

Описание: <http://www.drweb.com/products/gateway/isa>

Dr.Web для Qbik WinGate

Антивирусная и антиспам-проверка трафика, передаваемого по протоколам HTTP/POP3/FTP прокси-сервера и SMTP-сервера Qbik WinGate

Преимущества

- Dr.Web для Qbik WinGate – единственный на сегодняшний день полностью русифицированный плагин для Qbik WinGate.
- Только Dr.Web для Qbik WinGate имеет как документацию, так и техническую поддержку непосредственно от производителя.
- В отличие от конкурирующих аналогов, продукт компании «Доктор Веб» имеет возможность антиспам-фильтрации. Эффективный и компактный модуль антиспама не требует обучения, позволяет задавать различные действия для каждой из трех предусмотренных программой категорий спама, а также создавать черный и белый списки электронных адресов.

Dr.Web для MIMESweeper

Антивирусная и антиспам-защита почтового трафика, проходящего через серверы контентной фильтрации ClearSwift MIMESweeper

Преимущества

- 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).
- 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.
- 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 по-

- Наличие не имеющей аналогов дополнительной технологии обнаружения неизвестных вредоносных объектов (Origins Tracing™), в том числе в архивах с неизвестным форматом.

Ключевые функции

- Антивирусная и антиспам-проверка почтовых сообщений, передаваемых по протоколам SMTP и POP3, включая проверку вложенных файлов.
- Антивирусная проверка файлов и данных, передаваемых по протоколам HTTP и FTP.
- Лечение инфицированных файлов, передаваемых по протоколу HTTP.
- Журнал регистрации событий.
- Собственная панель управления и менеджер карантина.
- Автоматические обновления вирусных баз.

Полезные ссылки

Описание: <http://products.drweb.com/gateway/qbik>

лучателю без изменений. Вредоносные письма, которые плагин Dr.Web не может нейтрализовать, помечаются и по умолчанию перемещаются в карантин.

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 черных и белых списков.
- Ведение статистики работы комплекса.
- Автоматические обновления.

Системные требования

- Место на жестком диске не менее 35 МБ свободного дискового пространства.
- ОС Windows Server 2000 с пакетом обновления 4 (SP4) или выше Server 2003 или более поздняя версия.
- Почтовый контентный фильтр ClearSwift MIMESweeper™ for SMTP 5.2 или более поздняя версия.

Полезные ссылки

Описание: <http://products.drweb.com/mimesweeper>

Dr.Web Mobile Security Suite

Защита мобильных устройств

- Dr.Web для Android
- Dr.Web для Symbian OS
- Dr.Web для Windows Mobile

Лицензирование Dr.Web Mobile Security Suite

Dr.Web для защиты мобильных устройств лицензируется по числу защищаемых мобильных устройств.

Варианты лицензий

Dr.Web для Android	Dr.Web для Symbian OS	Dr.Web для Windows Mobile
■ Комплексная защита + Центр управления	■ Антивирус + Антиспам	
	■ Антивирус + Антиспам + Центр управления	

Продукты Dr.Web для мобильных устройств доступны в составе экономичных комплектов Dr.Web для малого и среднего бизнеса.

	Dr.Web для Android	Dr.Web для Symbian OS	Dr.Web для Windows Mobile
Компоненты защиты	Антивирус + Антиспам + Антивор + Род.контроль	Антивирус + Антиспам	
Централизованное управление в составе Dr.Web Enterprise Security Suite	+	–	+
Поддерживаемые ОС	Android OS: 1.5/1.6/2.0/2.1/2.2/3.0/ 3.1/3.2	Symbian Series60	Windows Mobile 2003/2003 SE/5.0/6.0/6.1/6.5
Ключевые функции			
Проверка «на лету»	+	+	+
Проверка файлов, поступающих через GPRS/Infrared/Bluetooth/Wi-Fi/USB-соединения или во время синхронизации с ПК	+	+	+
Два типа проверки: полная и выборочная	+	+	+
Возможность включения/выключения постоянной проверки карты памяти	+	–	+
Сканирование всей файловой системы или отдельных файлов и папок по требованию	+	+	+
Проверка файлов в архивах ZIP, SIS, CAB, RAR	+	+	+
Черные и белые списки входящих телефонных звонков и СМС-сообщений	+	+	+
Удаление инфицированных файлов	+	+	+
Перемещение подозрительных файлов в карантин	+	+	+
Восстановление файлов из карантина	+	+	+
Обновления через Интернет:	+	+	+
■ по протоколу HTTP с использованием встроенного модуля GPRS;			
■ через Infrared/Bluetooth/Wi-Fi/USB-соединение;			
■ путем синхронизации ПК, имеющего доступ к сети Интернет, через соединение ActiveSync.			
Детальные отчеты о сканировании системы	+	+	+
Удаленное управление мобильным устройством в случае его утери или кражи – с помощью «Антивора»	+		

Специальное предложение

Бесплатная лицензия на Dr.Web Mobile Security Suite предоставляется зарегистрированным пользователям:

- всех коробочных продуктов Dr.Web;
- Dr.Web Security Space;
- Антивируса Dr.Web для Windows;
- Dr.Web Enterprise Security Suite при условии покупки лицензии для защиты рабочих станций.

Полезные ссылки

Описание: <http://products.drweb.com/mobile>

Комплекты Dr.Web

В состав комплектов
включены продукты Dr.Web для
защиты всех типов объектов

Комплект Dr.Web «Универсальный»

Доступная комплексная защита enterprise-класса для предприятий малого и среднего масштаба

Небольшие компании зачастую не имеют возможности выделить значительные средства на комплексную информационную защиту. Именно на них рассчитан комплект Dr.Web «Универсальный» – экономичное предложение для организаций с числом ПК от 5 до 100.

ВАЖНО! На комплект не распространяются никакие скидки, в том числе на продление. Чтобы продолжить пользоваться комплектом, необходимо приобрести новую лицензию за полную стоимость. Предоставляется скидка на продление при переходе с комплекта на отдельные продукты Dr.Web.

	Dr.Web Desktop Security Suite	Dr.Web Server Security Suite	Dr.Web Mail Security Suite	Dr.Web Gateway Security Suite	Dr.Web Mobile Security Suite
Защищаемые объекты	Рабочие станции	Серверы	Пользователи почты	Пользователи шлюзов	Мобильные устройства
Лицензия	Комплексная защита	Антивирус	Антивирус + Антиспам	Антивирус	Антивирус + Антиспам
Комплектация	От 5 до 50	1	Равняется количеству станций	Равняется количеству станций (от 25)	Равняется количеству станций

Полезные ссылки

Комплекты Dr.Web: <http://products.drweb.com/bundles/choose>

Утилиты Dr.Web

Лечащие утилиты Dr.Web предназначены для диагностики и экстренного лечения в случае необходимости. Они не обеспечивают постоянной защиты компьютера.

Dr.Web CureNet!

Централизованное лечение локальных сетей любого масштаба, в том числе с установленным антивирусом другого производителя

Потенциальные пользователи	Малые, средние, крупные и очень крупные предприятия, в локальных сетях которых установлен антивирус другого производителя.	
Решаемые задачи	<ul style="list-style-type: none"> Удаленное централизованное лечение рабочих станций и серверов Windows Проверка качества антивирусной защиты другого производителя. 	
Особенности утилиты	<ul style="list-style-type: none"> Не требует деинсталляции антивируса другого производителя перед проверкой и лечением. Не требует наличия сервера или установки дополнительного ПО. Может использоваться в сетях, полностью изолированных от Интернета. Мастер Dr.Web CureNet! можно запустить с любого внешнего носителя, в том числе с USB. 	
Описание продукта	http://products.drweb.com/curenet	
Поддерживаемые ОС	MS Windows 7/2008/Vista/2003/XP Professional/2000 (32- и 64-битные системы).	
Что такое «Мой Dr.Web CureNet!»?	Это личный кабинет, в котором в течение всего срока действия лицензии хранится индивидуальная ссылка для скачивания обновленного дистрибутива. Также через личный кабинет можно связаться со службой техподдержки, отправить подозрительный файл на анализ, воспользоваться другими сервисами.	
Лицензирование	Утилита лицензируется по количеству станций, на 10 или 30 дней использования. Также предусмотрены особые сервисные лицензии на 30 и 365 дней. Они дают право оказывать услуги по лечению корпоративных сетей с помощью Dr.Web CureNet! сторонним организациям.	
Демоверсия	Без функции лечения.	
Системные требования	Мастер	<ul style="list-style-type: none"> Любой ПК под управлением Windows Не менее 164 МБ свободного места на жестком диске, из них до 78 МБ занимает установочный файл. Доступ в Интернет для обновления вирусных баз и компонентов Dr.Web CureNet!. Локальная сеть TCP/IP.
	Сканер	<ul style="list-style-type: none"> Не менее 42 МБ свободного места на жестком диске проверяемого компьютера. ПК под управлением ОС MS Windows 7/2008/Vista/2003/XP Professional/2000 (32- и 64-битные системы).

Dr.Web CureIt!

Экстренное лечение ПК и серверов под управлением Windows, в том числе с установленным антивирусом другого производителя

Потенциальные пользователи	Малые, средние, крупные и очень крупные предприятия, на компьютерах которых установлен антивирус другого производителя.	
Решаемые задачи	<ul style="list-style-type: none"> Экстренное лечение рабочих станций и серверов Windows. Проверка качества антивирусной защиты другого производителя. 	
Особенности утилиты	<ul style="list-style-type: none"> Не требует установки, не конфликтует ни с одним антивирусом, а значит, на время сканирования не требуется отключать установленный антивирус другого производителя. Повышенная самозащита и усиленный режим для эффективного противодействия блокировщикам Windows. Обновления один или несколько раз в час. Утилиту можно запустить с любого внешнего носителя, в том числе с USB. 	
Описание продукта	http://free.drweb.com/cureit	
Поддерживаемые ОС	MS Windows 2000/XP/2003/Vista/2008/7 (32- и 64-битные системы).	
Лицензирование	Утилита лицензируется по количеству станций, на 10 или 30 дней использования. Также предусмотрены особые сервисные лицензии на 30 и 365 дней. Они дают право оказывать услуги по лечению ПК и серверов с помощью Dr.Web CureIt! сторонним организациям.	
Особенности лицензирования	Утилита бесплатна для лечения собственного домашнего ПК.	
Демоверсия	Отсутствует.	
Системные требования	<ul style="list-style-type: none"> ПК под управлением ОС MS Windows 7/2008/Vista/2003/XP Professional/2000 (32- и 64-битные системы). Не менее 100 МБ свободного места на жестком диске. 	

Программно-аппаратные комплексы Dr.Web Office Shield

Высокопроизводительные и отказоустойчивые серверы для комплексной централизованной защиты рабочих станций и файловых серверов Windows, а также почтового и интернет-трафика

Преимущества

- Экономичная защита корпоративной сети решением enterprise-класса.
- Возможность использования решения в условиях отсутствия высококвалифицированных специалистов («поставил и забыл»).
- Снижение потерь рабочего времени, простоев оборудования и персонала благодаря уменьшению количества вирусных инцидентов и высокой устойчивости устройства к внешним атакам.
- Существенное сокращение расходов на интернет-трафик и возможность контроля над деятельностью сотрудников в сети Интернет.
- Экономия рабочего времени системного администратора за счет простоты управления.

Dr.Web Office Shield можно использовать 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 Интернета), предназначенного для обеспечения защиты почтового и интернет-трафика от вирусов, различных вредоносных объектов и спама. Использование Dr.Web Office Shield в качестве шлюза значительно снижает затраты компаний на безопасность доступа к Сети и позволяет существенно экономить интернет-трафик;
- внутреннего сервера локальной сети, обеспечивающего централизованную защиту рабочих станций и файловых серверов Windows.

Dr.Web Office Shield можно установить в действующую сеть или использовать в качестве основы для создания новой сети – это важная особенность программно-аппаратного комплекса. Наличие сервисов DHCP и DNS позволит провести эту работу с минимальными усилиями.

В состав Dr.Web Office Shield входят:

- Dr.Web Desktop Security Suite – централизованная защита рабочих станций и файловых серверов Windows;
- Dr.Web для интернет-шлюзов UNIX – защита доступа пользователей внутренней интранет-сети к ресурсам Интернета;
- Dr.Web для почтовых шлюзов UNIX – антивирусная и антиспам-защита почтового трафика;
- корпоративный межсетевой экран;
- VPN-сервер;
- DHCP&DNS-сервер;
- точка доступа Wi-Fi.

Виды поставки

 NEO	Защищаемые объекты <ul style="list-style-type: none">■ почтовый трафик■ интернет-трафик Рекомендуемое кол-во пользователей: от 10 до 150
 TWISTER	Защищаемые объекты <ul style="list-style-type: none">■ рабочие станции Windows■ файловые серверы Windows■ почтовый трафик■ интернет-трафик Рекомендуемое кол-во пользователей: от 10 до 50
	Защищаемые объекты <ul style="list-style-type: none">■ рабочие станции Windows■ файловые серверы Windows■ почтовый трафик■ интернет-трафик Рекомендуемое кол-во пользователей: от 50 до 250
	Защищаемые объекты <ul style="list-style-type: none">■ почтовый трафик■ интернет-трафик Рекомендуемое кол-во пользователей: от 50 до 250

Лицензирование

- Безлимитная лицензия.
- Лицензия по количеству защищаемых объектов: рабочих станций, пользователей почты и шлюзов.

Применяются все действующие на момент покупки скидки, предусмотренные для продуктов Dr.Web (кроме случая с безлимитной лицензией).

Dr.Web LiveDemo

Сервис удаленного онлайн-тестирования Dr.Web LiveDemo позволяет еще до приобретения программно-аппаратного комплекса испытать выбранную конфигурацию в виртуальной локальной сети на сервере компании «Доктор Веб».

Полезные ссылки

Описание: http://solutions.drweb.com/office_shield

Россия

ООО «Доктор Веб»

125124, Москва, 3-я улица Ямского поля, вл. 2, корп.12 А

Телефон: +7 (495) 789-45-87 (многоканальный)

Факс: +7 (495) 789-45-97

Бесплатный телефон технической поддержки:
8-800-333-7932

www.drweb.com | www.av-desk.com | www.freedrweb.com |
mobi.drweb.com

Германия

Doctor Web Deutschland GmbH

Rodenbacher Chaussee 6, D-63457 Hanau

Телефон: +49 (6039) 939-5414

Факс: +49 (6039) 939-5415

www.drweb-av.de

Казахстан

ТОО «Доктор Веб – Центральная Азия»

050009, Алматы, ул. Шевченко / уг. ул. Радостовца,
1656/72г, офис 910

Телефон: +7 (727) 323-62-30, 323-62-31, 323-62-32

www.drweb.kz

Украина

ООО «Центр технической поддержки «Доктор Веб»

01001, Киев, ул. Костельная, 4, офис 3

Телефон/факс: +38 (044) 238-24-35, 279-77-70

www.drweb.ua

Франция

Doctor Web France

333 b Avenue de Colmar, 67100 STRASBOURG

Телефон: +33 (0) 3-90-40-40-20

Факс: +33 (0) 3-90-40-40-21

www.drweb.fr

Япония

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku,
Kawasaki-shi, Kanagawa-ken
210-0005, Japan

Телефон: +81 (0) 44-201-7711

www.drweb.co.jp

