Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite – это комплекс продуктов Dr.Web, включающий элементы защиты всех узло

- рабочих станций, клиентов терминальных серверов и клиентов встроенных систем на платформах Windows, Linux и Mac OS X;
- файловых серверов и серверов приложений (включая терминальные серверы) Windows и Novell NetWare;
- почтовых серверов Unix, Microsoft Exchange, IBM Lotus, Kerio;
- мобильных устройств на основе Windows Mobile.

Минимальная стоимость

Dr.Web Enterprise Security Suite включает все необходимые компоненты защиты отдельных узлов сети и единый центр управления.

Возможность установки комплекса на серверах Unix и наличие встроенной базы данных отличают этот продукт от многих аналогов. Эти особенности позволяют минимизировать совокупную стоимость внедрения – вместе с Dr.Web Enterprise Security Suite компании не придется приобретать дорогостоящее оборудование.

Гибкое лицензирование

В отличие от многих конкурирующих решений, **Dr.Web Enterprise Security Suite** имеет максимально гибкую и мультивариантную систему лицензирования (см. вкладку «Лицензирование»). 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.

Установка в день приобретения

Покупатели **Dr.Web Enterprise Security Suite** могут установить приобретенные продукты уже в день платежа, а иногда и ранее. Наличие сервиса мгновенной выписки лицензионных ключевых файлов сокращает время их получения до нескольких минут, в то время как на получение «ключей» от других производителей могут уходить дни и даже недели.

Наличие сертификатов

В отличие от большинства конкурирующих решений, продукты в составе Dr.Web Enterprise Security Suite имеют сертификаты соответствия ФСТЭК России и ФСБ . Это означает, что комплекс можно использовать в организациях, требующих повышенного уровня безопасности.

Dr.Web Enterprise Security Suite полностью соответствует требованиям закона о защите персональных данных, предъявляемым к антивирусным продуктам. Он может применяться в сетях, соответствующих максимально возможному уровню защищенности.

Опыт крупных проектов

Среди клиентов компании «Доктор Веб» – крупные компании с мировым именем, российские и международные банки, государственные организации, в том числе многофилиальные, сети которых насчитывают десятки тысяч компьютеров. Продуктам и решениям Dr.Web доверяют высшие органы государственной власти России, компании топливно-энергетического сектора, предприятия с мультиаффилиатной структурой.

Полная защита от существующих угроз

Использование **Dr.Web Enterprise Security Suite** 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 в системе защиты рабочих станций встроенного брандмауэра и функции Офисного контроля не только преграждает путь вирусам через уязвимости операционных систем и программ, но и обеспечивает надежный контроль за работой установленных приложений.

Увеличение производительности труда сотрудников

Внедрение компонентов **Dr.Web Enterprise Security Suite** дает мгновенный положительный эффект. Снижение потока спама 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 и простоев в работе организации, которые раньше могли возникать во время восстановления потерянной из-за вирусов информации.

Сохранение репутации компании

Внедрение **Dr.Web Enterprise Security Suite** не дает злоумышленникам возможности превратить локальную сеть в источник вирусов и спама, которые могут попасть к клиентам компании. Использование комплекса – это надежная гарантия репутации любой организации как делового партнера.

Снижение непрофильных затрат

Использование **Dr.Web Enterprise Security Suite** в локальной сети не только освобождает системных администраторов от работы по устранению последствий вирусных эпидемий, но и позволяет:

- уменьшить вынужденные простои сотрудников и предприятия в целом – нет необходимости в устранении последствий вирусных инцидентов;
- уменьшить затраты на приобретение новых серверов и рабочих станций – теперь сотрудникам не будет поступать поток вирусов и спама.

Уникальные особенности Dr.Web Enterprise Security Suite

- Возможность централизованной защиты всех узлов сети – рабочих станций, почтовых, файловых серверов и серверов приложений, включая терминальные, интернет-шлюзов и мобильных устройств;
- комплексная защита рабочих станций от большинства существующих угроз благодаря наличию встроенных антивируса, антиспама, брандмауэра и офисного контроля;
- минимальная совокупная стоимость по сравнению с конкурирующими программами благодаря возможности развертывания серверов как под Windows, так и под Unix, простоте установки и надежности защиты;
- возможность установки агентской части на уже зараженную машину и высокая доля вероятности излечения;
- минимальное использование ресурсов компьютеров и серверов благодаря компактности антивирусного ядра и использованию в нем новейших технологий;
- высокая эффективность обнаружения угроз, включая еще не известные вирусы;
- возможность управления всей инфраструктурой защиты сети с одного рабочего места (через Веб-администратора), где бы оно ни находилось;
- возможность реализации необходимых для конкретного предприятия и отдельных групп сотрудников политик безопасности;
- возможность назначения отдельных администраторов для различных групп, что позволяет использовать Dr.Web Enterprise Security Suite 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;
- возможность назначения отдельных администраторов для различных групп, что позволяет использовать Dr.Web Enterprise Security Suite как в компаниях с повышенными требованиями к безопасности, так и в многофилиальных организациях;
- возможность защиты сетей, не имеющих доступа в Интернет;
- возможность использования большинства существующих баз данных. При этом в качестве внешних 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, что дает прямой доступ к внутренним интерфейсам Центра управления;

- одновременная поддержка нескольких сетевых протоколов (TCP/IP (включая IPv6), IPX/SPX, NetBIOS), что позволяет развернуть антивирусную сеть, не меняя исторически сложившейся сетевой инфраструктуры;
- открытость Dr.Web Enterprise Security Suite – 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.

Онлайн-тестирование Dr.Web Enterprise Security Suite

Dr.Web LiveDemo – это не имеющий аналогов у конкурентов сервис удаленного онлайн-тестирования некоторых программных продуктов Dr.Web, в том числе Dr.Web Enterprise Security Suite.

Он позволяет системным администраторам еще до приобретения **Dr.Web Enterprise Security Suite**
протестировать выбранную конфигурацию комплекса в виртуальной локальной сети на сервере компании «Доктор Веб. Чтобы получить доступ к сервису Dr.Web LiveDemo необходимо лишь заполнить анкету, описав интересующую конфигурацию
Dr.Web Enterprise Security Suite
.

В настоящий момент онлайн-тестирование возможно только для рабочих станций и серверов Windows, а также почтовых серверов Unix.

Бесплатные бонусы пользователям Dr.Web Enterprise Security Suite

-

Защита мобильных устройств. При покупке лицензии для защиты рабочих станций предоставляется право бесплатного использования продуктов Dr.Web для защиты мобильных устройств под управлением Windows Mobile/Symbian OS. Количество лицензий для защиты мобильных устройств равняется количеству лицензируемых рабочих станций.

-

Диагностика и лечение корпоративных сетей. При покупке лицензии для защиты рабочих станций предоставляется право бесплатного использования лицензии на сетевую лечащую утилиту Dr.Web CureNet! для диагностики и лечения такого же количества ПК, которое указано в Вашей лицензии на Dr.Web Enterprise Security Suite, в течение всего срока действия лицензии. Для получения индивидуального дистрибутива Dr.Web CureNet! необходимо использовать
серийный номер к Dr.Web Enterprise Security Suite
.

-

Диагностика и лечение отдельно стоящих станций. При покупке лицензии для защиты рабочих станций предоставляется право бесплатного использования лицензии на лечащую утилиту Dr.Web CureIt! для диагностики и лечения такого же количества ПК, которое указано в Вашей лицензии на Dr.Web Enterprise Security Suite, в течение всего срока действия лицензии. Для получения индивидуального дистрибутива Dr.Web CureIt! необходимо использовать серийный номер к Dr.Web Enterprise Security Suite
.

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. Так, например, базовыми лицензиями для рабочих станций

являются **Антивирус** и **Комплексная защита**.

Продукт	Поддерживаемые ОС и платформы	Базовая лицензия	Дополнительные компон
Dr.Web® Desktop Security Suite			
Защита рабочих станций, клиентов терминальных серверов, клиентов виртуальных серверов и к			
	Windows 7/Vista/XP/2000 SP 4 + Rollup 1 Windows 7/Vista/XP/2000 SP 4 + Rollup 1 Антивирус	Комплексная защита	Центр управления
	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, виртуальных и терминальных

Windows	Антивирус	Центр управления
Novell NetWare		
Mac OS X Server		
Unix (Samba)		
Novell Storage Services		

Dr.Web® Mail Security Suite

Защита почты

Unix	Антивирус

Антиспам

SMTP proxy

Центр управления

MS Exchange	
Lotus (Windows/Linux)	
Kerio (Windows/Linux)	SMTP proxy

Центр управления

Dr.Web® Gateway Security Suite

Защита шлюзов

Интернет-шлюзы Kerio Интернет-шлюзы Unix Qbik WinGate MIMEsweeper	Антивирус Антиспам	Центр управления

Dr.Web® Mobile Security Suite

Защита мобильных устройств

Windows Mobile Android Symbian OS	Антивирус Антиспам	Центр управления

* — Dr.Web для Kerio (под Mac) в разработке.

Универсальность

В соответствии с выбранным заказчиком решением создается единый ключевой файл Dr.Web для защиты всех интересующих объектов. В состав ключа входят программные продукты Dr.Web для защиты того или иного объекта для всех ОС и платформ продукта, поддерживаемых Dr.Web. Если в течение действия лицензии необходимо совершить переход, например, с Unix на Windows, не надо менять ключ – достаточно просто скачать нужный дистрибутив с сайта www.drweb.com – это бесплатно.

Также смотрите Комплекты Dr.Web .

Центр Управления Dr.Web Enterprise Security Suite

Центр Управления Dr.Web Enterprise Security Suite обеспечивает централизованное управление защитой всех узлов корпоративной сети:

- рабочих станций, клиентов терминальных серверов и клиентов встроенных систем на платформах Windows, Linux и Mac OS X;рабочих станций, клиентов терминальных серверов и клиентов встроенных систем на платформах Windows, Linux и Mac OS X;
- файловых серверов и серверов приложений (включая терминальные серверы) Windows и Novell NetWare;
- почтовых серверов Unix, Microsoft Exchange, IBM Lotus, Kerio;
- мобильных устройств на основе Windows Mobile.

Центр Управления **Dr.Web Enterprise Security Suite** позволяет управлять системой защиты корпоративной сети из любой точки мира. Для его работы достаточно компьютера с любой операционной системой и выходом в Интернет. При этом для управления защитой не требуется доустанавливать какое-либо программное обеспечение. Единственным требованием является наличие браузера.

Интуитивно понятный интерфейс позволяет развернуть всю антивирусную сеть за рекордно короткие сроки. При этом 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. Развертывание с легкостью можно провести из любой точки мира, причем для этого от администратора не потребуется никаких специальных навыков.

Центр Управления позволяет администратору, работающему внутри сети или на удаленном компьютере, централизованно управлять всеми компонентами защиты, отслеживать состояние всех защищенных узлов, получать уведомления о вирусных

инцидентах и настраивать автоматическую реакцию на них. Для этого достаточно лишь наличия связи между рабочим местом администратора и антивирусным сервером.

Низкозатратное администрирование

Возможность «взгляда сверху» на антивирусную сеть предприятия с одного рабочего места (через Веб-администратор), где бы оно ни находилось, и минимальная трудоемкость обслуживания сети, во многом связанная с простотой администрирования, сокращают время обслуживания системы до минимума.

Наличие удобного Веб-администратора, возможность автоматизации работы за счет интеграции с системой Windows NAP и возможность написания собственных обработчиков событий на любом скриптовом языке значительно снижают нагрузку на системных администраторов, освобождая от повседневной «антивирусной» рутины.

Исключительная масштабируемость

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. 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.

Объединение антивирусных серверов Центра Управления в иерархическую систему позволяет создать единую антивирусную сеть, состоящую из взаимосвязанных рабочих станций, что обеспечивает сбор консолидированной информации о всей сети на одном сервере. Реализация иерархии серверов делает комплекс незаменимым для компаний, имеющих многофилиальную структуру, изолированную от сети Интернет.

Широкий спектр поддерживаемых сетевых протоколов

Центр Управления одновременно поддерживает несколько 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. При этом безопасность передачи данных между компонентами системы обеспечивается за счет возможности шифрования. Поэтому администрировать антивирусную сеть можно из любой точки мира через Интернет.

Экономия трафика локальной сети

По сравнению с аналогичными решениями других производителей Центр Управления гарантирует 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

Работа антивирусной сети, основанной на Dr.Web, совершенно прозрачна. Журнал аудита действий администраторов позволяет отслеживать все шаги по установке и настройке системы. Все ее компоненты могут вести файлы отчётов с настраиваемым уровнем детализации. В итоге любые действия над файлами отображаются в статистике. Предусмотрена система оповещения администратора о проблемах, возникающих в антивирусной сети. Ее сообщения могут отображаться в Веб-администраторе или приходить по электронной почте.

Особенностями системы являются:

- возможность редактирования текстов сообщений, предупреждающих об угрозах;
- наличие средств оповещения администратора о проблемах, возникающих в антивирусной сети;
- возможность уведомлений о вирусной атаке, результатах сканирования и удалениях – по электронной почте или через Веб-администратор;
- наличие специальной иконки предупреждения об угрозе;
- возможность удобного просмотра отчетов непосредственно через

Веб-администратор, экспорт статистики в форматах CSV, HTML, XML;
- возможность выбора степени детализации отчетов;
- возможность получения информации о:
- вирусной активности с возможностью группирования обнаруженных вирусов по типам;
- наличии уязвимых клиентов;
- ошибках при сканировании;
- компонентах, запущенных на защищаемой рабочей станции;
- необычном поведении защищаемых станций.

Уникальные особенности Центра Управления Dr.Web Enterprise Security Suite

- Возможность централизованной защиты всех узлов сети – рабочих станций, клиентов встроенных систем, почтовых, файловых серверов и серверов приложений, включая терминальные;
- минимальная совокупная стоимость по сравнению с конкурирующими программами благодаря возможности развертывания сети под Windows- и Unix-серверами, простоте установки и надежности защиты;
- возможность установки как на 32-, так и на 64-битные версии операционных систем;
- возможность установки агентской части на уже зараженную машину и высокая доля вероятности излечения;
- минимальное использование ресурсов компьютеров и серверов благодаря компактности антивирусного ядра и использованию в нем новейших технологий;
- возможность управления всей инфраструктурой защиты сети с одного рабочего места (через Веб-администратор), где бы оно ни находилось, даже вне корпоративной сети;
- возможность реализации индивидуальных для конкретного предприятия и отдельных групп сотрудников политик безопасности;
- 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;
- защита от самостоятельного изменения настроек пользователями;
- возможность защиты сетей, не имеющих доступа в Интернет;
- возможность развертывания агентов на рабочих станций удобным для администратора способом – через политики Active Directory, стартовые скрипты,

механизмы удаленной установки. Установка возможна, даже если узел сети является закрытым и недоступным через Веб-администратор Центра управления;

- 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, что дает прямой доступ к внутренним интерфейсам Центра управления;
- одновременная поддержка нескольких сетевых протоколов (TCP/IP (включая IPv6), IPX/SPX, NetBIOS), что позволяет развернуть антивирусную сеть, не меняя исторически сложившейся сетевой инфраструктуры;
- 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.

Веб-администратор Dr.Web

Не требуя инсталляции дополнительного программного обеспечения, этот компонент Центра Управления Dr.Web позволяет администратору системы контролировать работу всех сервисов с любого компьютера и оперативно реагировать на возникающие проблемы.

Веб-администратор представляет собой доступное всегда и везде, даже извне защищаемой сети, визуальное средство удаленного управления защитой сотен и даже тысяч географически удаленных рабочих станций, серверов, интернет-шлюзов и мобильных устройств через единый графический интерфейс. Использование Веб-администратора возможно на любом компьютере под управлением любой ОС. Интуитивно понятный интерфейс обеспечивает контроль всей иерархии защищаемой сети.

- **Низкозатратное администрирование.** Веб-администратор Dr.Web позволяет с

легкостью управлять изменяющейся средой антивирусной сети. Его использование повышает производительность работы системных администраторов, позволяет автоматизировать рабочие процессы и производить повседневную работу за считанные минуты: изменять ключевые параметры защиты объектов и запускать задания на выполнение.

- **Немедленная реакция на угрозы.** Средства планирования регулярных сканирований и обновлений, предоставляемые через Веб-администратор, предельно упрощают задачи администратора антивирусной сети. Разнообразные статистические средства сбора и анализа информации позволяют контролировать состояние защищаемых объектов и сети в целом, реагировать на обнаруженные инциденты буквально в течение нескольких секунд, определять источники инфекции и максимально быстро адаптировать политику безопасности предприятия к изменяющимся условиям.

- **Полный контроль за состоянием сети.** Веб-администратор Dr.Web позволяет настроить любой из компонентов антивирусной сети — например, задать расписание для антивирусного сервера или какой-либо группы агентов — не покидая рабочего места. Возможности Веб-администратора контроля состояния антивирусной сети совместно с функцией блокировки агента в определенный период позволяют исключить возникновение эпидемий. Возможности Веб-администратора по контролю за состоянием антивирусной системы защиты компании совместно с функцией блокировки доступа к сети на время сканирования.
- **Сбор статистики «в один клик».** Возможность сбора и анализа антивирусной статистики позволяет создавать отчеты за определённый период с требуемой детализацией и экспортировать их во внешний файл.

- **Средства мгновенного оповещения.** Интерфейс отправки сообщений позволяет администратору системы отсылать уведомления отдельным пользователям или группам пользователей. В случае если ПК пользователя подключен к антивирусной сети, сообщение будет доставлено мгновенно, в противном случае сообщение будет доставлено сразу после подключения. Данная возможность может быть использована, например, для:
  - рассылки сообщений об эпидемиях и о порядке действий в случае заражения вредоносными программами;
  - рассылки технических сообщений;
  - поздравлений с праздниками.

Антивирусный сервер

Антивирусный сервер Центра Управления **Dr.Web Enterprise Security Suite** обеспечивает централизованное управление защитой сети, включая развертывание, обновление вирусных баз и программных модулей компонентов, мониторинг состояния сети, извещения о вирусных событиях, сбор статистики. Детальный перечень возможностей централизованного управления для отдельных продуктов описан на вкладках «Центр Управления» соответствующих продуктов.

- **Развертывание.** Антивирусный сервер Центра Управления **Dr.Web Enterprise Security Suite** может быть установлен на один из компьютеров локальной сети. Сервер хранит дистрибутивы антивирусных пакетов для различных ОС (для рабочих станций), обновления вирусных баз и программных модулей пакетов, пользовательские ключевые файлы, настройки защищаемых объектов и отсылает их по запросам агентов на соответствующие компьютеры. Платформонезависимая архитектура серверной части ПО Центра управления **Dr.Web Enterprise Security Suite** позволяет использовать его как на Windows-, так и на Unix-серверах, чего не обеспечивает ни одно другое аналогичное решение. Для связи антивирусного сервера с антивирусными агентами могут использоваться практически все существующие на данный момент протоколы – TCP/IP (как IPv4, так и IPv6), IPX/SPX, NetBIOS, что позволяет развернуть систему защиты, не меняя исторически сложившейся инфраструктуры сети.

- **Обновление.** Обновление вирусных баз и компонентов агентов целиком ложится на антивирусный сервер, что приводит к значительной экономии интернет-трафика и отсутствию необходимости настраивать этот процесс вручную. Обновление компонентов защиты может производиться как с самого антивирусного сервера, так и напрямую с серверов обновления компании «Доктор Веб», что является критически важным для компьютеров и ноутбуков, не имеющих постоянной связи с сервером.
- **Сбор статистики.** Антивирусный сервер в своей базе данных содержит настройки каждого агента, расположенного в антивирусной сети, статистику по сканированиям, проводимым каждым компонентом антивируса на каждом компьютере, входящем в антивирусную сеть, и другую полезную информацию. При этом может использоваться как внутренняя база данных, реализованная в антивирусном сервере, так и внешняя.

Антивирусные агенты

Антивирусные агенты устанавливаются на защищаемые компьютеры, серверы и

мобильные устройства, в том числе при необходимости и на антивирусный сервер. Агенты отсылают данные о вирусных событиях и другую необходимую информацию антивирусному серверу.

С помощью агентов **Dr.Web Enterprise Security Suite** может управлять защитой следующих объектов:

Защищаемые объекты	Поддерживаемые ОС и платформы
Рабочие станции	
Клиенты терминальных серверов	
Клиенты встроенных систем	
	Windows
	Mac OS X
	Linux
Файловые серверы и серверы приложений	
	Windows
	Novell NetWare
	Mac OS X Server

Пользователи почты и SMTP-шлюзов

Unix

MS Exchange

Lotus (Windows/Linux)

Kerio (Windows/Linux)

Пользователи интернет-шлюзов Kerio
Мобильные устройства Windows Mobile

Системные требования

Для установки Центра Управления **Dr.Web Enterprise Security Suite** требуется:

- локальная сеть, основанная на протоколе IP (включая IPv6), IPX, или NetBIOS (в этой сети должны находиться все защищаемые компьютеры и антивирусный сервер). На всех компьютерах, на которых предполагается установка, для совместной работы антивирусных компонентов должны быть открыты:
- порт 2193 по протоколам TCP и UDP, а также 23 по протоколу NetBIOS - для связи антивирусных компонентов с сервером;
- сокет 2371 по протоколам IPX/SPX - для связи антивирусных компонентов с сервером;
- порты 2193 и 2372 по протоколу UDP – для работы сканера сети;
- 139 и 445 по протоколам TCP и UDP – для работы сетевого инсталлятора;
- 9080 по протоколу HTTP – для работы Веб-администратора;
- 9081 по протоколу HTTPS – для работы Веб-администратора.

- для работы антивирусного сервера – компьютер с процессором не ниже Pentium

III-667, оперативная память не менее 512 Мб (1 Гб при использовании встроенной БД), свободное место на жестком диске до 12 Гб (до 8 Гб для встроенной базы данных (каталог установки), до 4 Гб в системном временном каталоге (для рабочих файлов)). Операционная система Windows 2000/XP/2003/Vista/2008/7, Linux (glibc2.3 и выше), FreeBSD (6.4 и выше), Solaris (платформы Intel и Sparc);

- для автоматического получения содержимого централизованного каталога установки и обновлений с сервера обновлений необходим доступ к серверам Всемирной Системы Обновлений Dr.Web;
- между Веб-администратором и сервером должна быть установлена связь по протоколу TCP/IP;
- для работы Веб-администратора необходим любой интернет-браузер;

ВАЖНО! Для установки антивирусного сервера для Windows в состав системного ПО компьютера должен входить MS Installer 2.0. Данная программа включается в состав Windows, начиная с 2000 (при наличии SP3). При использовании более ранних версий Windows необходимо предварительно загрузить и установить MS Installer 2.0.

ВАЖНО! На защищаемых рабочих станциях сети не должны быть установлены другие антивирусные программы (в том числе другие версии ПО Dr.Web).

Системные требования к другим продуктам, управление которыми осуществляется с помощью Центра Управления Dr.Web Enterprise Security Suite, находятся на страницах описаний соответствующих программных продуктов.