

Dr.Web Enterprise Suite

**Централизованно-управляемая комплексная защита
рабочих станций, файловых серверов
корпоративных сетей **любого масштаба****

Сергей Салакин
Руководитель направления
ssalakin@polikom.ru

История проекта

- **Начало разработки:** 2002
- **Задача:** разработка антивирусной защиты для рабочих станций и серверов с возможностью централизованного управления для Всероссийской сети ГАС «Выборы»
- **Сдача проекта:** начало 2003
- **Коммерческий выпуск Dr.Web Enterprise Suite:** август 2005



Защити созданное

Dr.Web Enterprise Suite

Ключевые функции

Защити созданное

- **Централизованное управление** защитой рабочих станций Windows, файловых серверов Windows, почтовых серверов Unix
- **Централизованное управление** антивирусной сетью и получение информации о ней как с рабочих мест в корпоративной сети, так и удаленно через Интернет
- Удаленная **централизованная установка** (для компьютеров, работающих под управлением Windows 2000/XP/Vista/W7)
- Настройка групповых политик
- **Централизованная настройка** антивирусного ПО, постановка/отмена задач рабочим станциям
- **Централизованный мониторинг** состояния антивирусной защиты сети, сбор и изучение информации о вирусных событиях на всех защищаемых объектах
- Система оповещения администратором групп пользователей, или отдельных пользователей

Исключительные возможности Dr.Web Enterprise Suite

- **Кросс-платформенность** серверного ПО (Windows/Unix)
- **Работа в сетях:** TCP/IP(включая IPv6), IPX/SPX, NetBIOS
- **Безопасность передачи данных** - опция шифрования
- **Минимальный сетевой трафик** за счет механизмов сжатия
- Возможность **группирования** нескольких серверов Dr.Web Enterprise Suite с комплексной структурой взаимодействия между ними
- Возможность **установки консоли** администратора на любой ПК под управлением любой ОС
- Возможность **распределения нагрузки** между серверами

Развертывание

Защити созданное

Поддержка сетей различного типа	
Кросс-платформенность серверного программного обеспечения – возможность установки сервера как на ОС Microsoft Windows, так и ОС UNIX	✓
Возможность выбора типа базы данных сервера защиты	✓
Возможность построения иерархической системы серверов защиты	✓
Работа в сетях TCP/IP(включая IPv6), IPX/SPX, NetBIOS	✓
Наличие специальной политики для мобильных пользователей, в том числе возможность обновления через Интернет	✓
Возможность шифрования данных при обмене между различными компонентами системы	✓
Возможность автоматического распределения рабочих станций по нескольким серверам с уменьшением нагрузки на каждый из них, выбор сервера обновлений	✓
Размер защищаемой сети	Без ограничений

Компоненты Dr.Web Enterprise Suite

- Антивирусный сервер
- Консоль управления
- Веб-интерфейс администратора
- Антивирусные агенты

Антивирусный сервер

Главная функция – централизованное администрирование информационной защиты сети предприятия включая:

- развертывание
- обновление вирусных баз и программных модулей компонентов
- мониторинг состояния сети
- извещения о вирусных событиях
- сбор статистики

Антивирусный сервер Dr.Web Enterprise Suite – уникальные особенности

- Платформо-независимая архитектура серверной части ПО Dr.Web Enterprise Suite позволяет использовать его как на Windows, так и на UNIX-серверах - **это не позволяет делать ни одна другая аналогичная программа.**
- Обновление антивирусных агентов, в том числе вирусных баз, целиком ложится на антивирусный сервер, что приводит к **значительной экономии интернет-трафика** и отсутствию необходимости настраивать обновления вручную.



Защити созданное

Антивирусный сервер Dr.Web Enterprise Suite

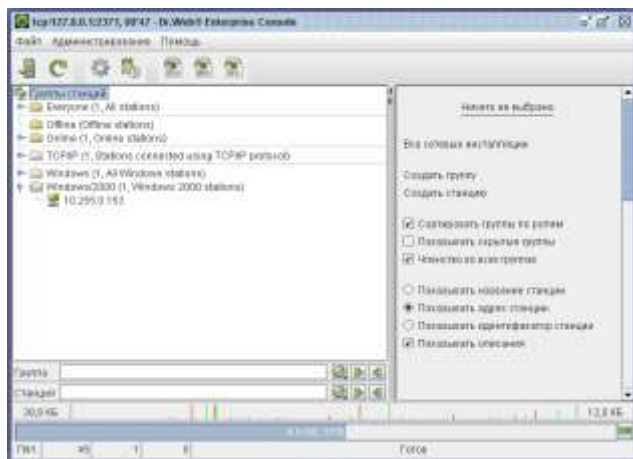
- Хранит дистрибутивы антивирусных пакетов для различных ОС, обновления вирусных баз и программных модулей пакетов, пользовательские ключи, настройки защищаемых компьютеров
- Содержит в своей базе данных настройки каждого агента, расположенного в антивирусной сети, статистику по сканированиям, проводимым каждым компонентом антивируса на каждом компьютере, входящем в антивирусную сеть и другую полезную информацию

Dr.Web Enterprise Suite

Удобство администрирования

Защити созданное

Консоль Dr.Web Enterprise Suite •



- Платформо-независимое приложение
- Может быть установлена на компьютере с любой ОС, поддерживающей виртуальную машину Java
- Связь между консолью и сервером обеспечивается по протоколу TCP/IP или IPv6
- Доступна всегда и везде, даже извне защищаемой сети
- Наглядный контроль за состоянием защиты станций, в том числе за счет группировки станций с различным состоянием защиты
- Шифрование данных обеспечивает безопасное администрирование через Интернет из любой точки мира

Настройка расписаний

Администратор имеет возможность устанавливать:

- расписания сканирований
- уровни глубины сканирований
- списки исключений из проверки
- последовательность действий в случае обнаружения вируса

Веб-интерфейс администратора



- Не требует наличия дистрибутива java-консоли и инсталляции
- Работает со всеми популярными браузерами.
- Позволяет контролировать работу всех сервисов с любого компьютера даже не находясь физически в офисе
- **Интерфейс отправки сообщений** дает возможность отправлять информационные сообщения отдельным пользователям или группам пользователей.
- **Журнал аудита** действий администраторов дает возможность отслеживать все действия по установке и настройке системы.

Статистика и отчетность

- Версии антивирусных пакетов/ перечень компонентов, запущенных на защищаемых ПК
- Время и даты установки и обновлений ПО антивирусной рабочей станции с указанием версии ПО
- Время и даты входа в систему и данные о временных отключениях от антивирусного сервера
- Время и даты обновлений вирусных баз с указанием их версий
- Версия ОС, установленная на защищаемом ПК, тип процессора, расположение системных каталогов ОС и т.п.
- Конфигурация и режимы работы антивирусных пакетов
- Информация о вирусных событиях
- Возможность создания отчетов в заданное время/отправка их на e-mail
- Формирование графиков активности вирусов, статистики по найденным типам вредоносных объектов, произведенных над ними действий

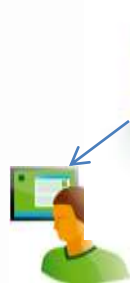
Dr.Web Enterprise Suite

Распределение обновлений

Защити созданное

Главный сервер
Dr.Web ES

Подчиненный сервер
Dr.Web ES



Сервер BCO Dr.Web

Подчиненный
сервер
Dr.Web ES

Экономия трафика!!!

Dr.Web для Windows 6.0

Борьба с неизвестными угрозами

Защити созданное

Передовые технологии Dr.Web позволяют программе работать на «опережение», блокируя даже еще неизвестные угрозы

- **FLY-CODE** – не имеющая аналогов технология универсальной распаковки. Позволяет распаковывать неизвестные Dr.Web упаковщики.
- **Origins Tracing** - Уникальная технология несигнатурного поиска – высокая вероятность распознавания вирусов, еще не известных вирусной базе Dr.Web.
- **Эвристический анализатор Dr.Web** надежно ловит все распространенные типы угроз, определяя их класс по результатам проведенного разбора и характерным признакам.

Dr.Web для Windows 6.0

Модуль самозащиты Dr.Web SelfPROtect

- **Ограничивает доступ** вредоносных объектов: к сети, файлам и папкам, веткам реестра, сменным носителям, защищает от попыток антивирусных программ прекратить функционирование Dr.Web
- Реализован в виде драйвера и действует на самом низком системном уровне
- Выгрузка и остановка его работы невозможны до перезагрузки системы
- Постоянный мониторинг работающей системы обеспечивает защиту файлов и каталогов системы защиты Dr.Web от несанкционированного или ненамеренного удаления, модификации пользователем и вредоносным ПО
- **Является полностью самодостаточным** (в отличие от некоторых конкурирующих продуктов, модифицирующих ядро Windows, которые перехватывают прерывания, подменяют таблицы векторов, используют недокументированные функции и т.д., что может привести к серьезным проблемам в работе самой операционной системы, а также создает новые пути для использования уязвимостей)
- **Защита от отключения** вредоносными программами - через «капчу»



Защиты созданное

Dr.Web для Windows 6.0

Функциональные возможности

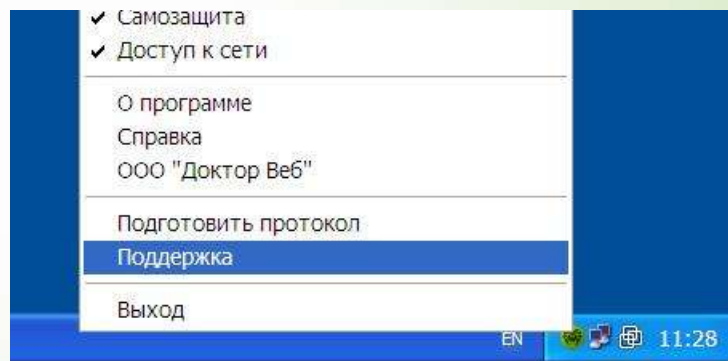
Защити созданное

Комплексная защита	Антивирус
Антивирус	Антивирус
Веб-антивирус	Антируткит
Антируткит	Антишпион
Антишпион	
Антиспам	
Офисный контроль	
Широчайший набор функций!	Классика отрасли!

Оперативная техподдержка



Сбор информации о ПК
«одной кнопкой» и
упаковка файла отчета



Защити созданное

Лицензирование Dr.Web Enterprise Suite

- **Минимальная лицензия:** от 5 станций
- **Максимальная лицензия:** не ограничена
- **Сроки лицензий:** 1, 2 или 3 года
- **Виды лицензий:** антивирус, комплексная защита

Варианты лицензий

- Dr.Web Enterprise Suite –защита рабочих станций
- Dr.Web Enterprise Suite + Dr.Web для файловых серверов Windows
- Dr.Web Enterprise Suite + Dr.Web для почтовых серверов Unix (на базе MailD)

Специальные предложения при покупке Dr.Web Enterprise Suite



1. Dr.Web Enterprise Suite + файловый сервер	2. Dr.Web Enterprise Suite + защита почты
От 15 ПК и выше – файловый сервер по цене 1 000 рублей	Защита ПК со скидкой 50%

Комплекты Dr.Web для малого и среднего бизнеса


Комплект	Защищаемые объекты
Dr.Web «Малый бизнес»	5 ПК/1 сервер/5 адресов почты + Dr.Web для Windows Mobile в подарок
Dr.Web «Универсальный»	5-100 ПК + сервер / почта / пользователи шлюза
Комплекты для школ	5,10, 25 ПК + 1 сервер

Защити созданное

Преимущества Dr.Web

 Доктор Веб, Россия

Продукт	Тест	Дата	Награда	
DrWeb Security Space 6.0	Самозащита	2010, Сентябрь	Платина	»»»
Dr.Web Anti-Virus 5.00	Лечение активного заражения	2010, февраль	Золото	»»»
Dr.Web Security Space 5.0	Самозащита	2009, Январь	Платина	»»»
Dr.Web Anti-Virus 4.44	Лечение компьютера	2008, Октябрь	Платина	»»»
Dr.Web Anti-Virus 4.44 Beta	Лечение компьютера	2007, Сентябрь	Золото	»»»

 www.anti-malware.ru/tests_history#drweb

Защити созданное

Вопросы?

Благодарим за внимание!

www.polikom.ru