Dr.WEB®
с 1992 года

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks*

* Уничтожает активные угрозы и новые атаки

Dr.Web KATANA

Kills **A**ctive **T**hreats **A**nd **N**ew **A**ttacks

Несигнатурный антивирус нового поколения для усиления защиты ПК «в связке» с вашим традиционным антивирусом

Для любого предприятия критичны нарушения бизнес-процессов, несанкционированный доступ к устройствам, эксплуатация уязвимостей, подбор паролей, фишинг и другие противоправные действия, производимые в том числе в ходе вирусозависимых компьютерных инцидентов (ВКИ) с помощью вредоносного ПО (ВПО).

К сожалению, сегодня в силу целого комплекса причин полагаться на антивирусную защиту только одного вендора нельзя.

Технологически сложные и особо опасные вирусы вирусописатели проверяют на обнаружение вирусными базами всех антивирусов перед тем как выпустить такой вирус в «живую природу».

Поэтому если полагаться на проверку только вирусными базами антивирусов — какими бы качественными они ни были — злоумышленники всегда будут иметь временную фору: вредоносный код уже может быть известен антивирусному вендору, но еще не получен антивирусом на устройстве пользователя.

Угроза заражения новейшим НЕИЗВЕСТНЫМ вирусом есть ВСЕГДА.

Одним из методов снижения вероятности инфицирования является использование **нескольких антивирусных решений**. Так, требование **ФСТЭК России** гласит:

«4) в информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей».

Когда нужны два антивируса?

- Когда основной антивирус пропускает угрозы.
- Когда основной антивирус нельзя часто обновлять.
- Когда ПК долго находится вне зоны доступа к Интернету.
- Когда ПК находится в изолированной сети, обновления в которую доставляются редко.

Несигнатурный антивирус нужен всегда: вы не можете знать, пропустил ли уже ваш антивирус вредоносную программу или нет.

Предлагаем в целях усиления защиты локальной сети, а также отдельных компьютеров от новейших и наиболее опасных вредоносных угроз — в том числе троянцев-шифровальщиков — использовать в дополнение к традиционному сигнатурному антивирусу (не Dr.Web) несигнатурный антивирус **Dr.Web KATANA**.

На сегодняшний день ни один антивирус не знает 100% вредоносных программ в момент проникновения. К сожалению, наиболее опасные вредоносные программы, такие как шифровальщики, могут обходить традиционные методы антивирусной защиты.

Даже если используемый антивирус является многократным победителем различных тестов, нужно помнить, что на момент тестирования все тестовые вредоносные программы были уже известны аналитикам и организаторам тестирований. А значит, награда в тестировании ничего не говорит о способности этого антивируса отражать неизвестные в момент атаки активные угрозы.

Почему многие компании, защищенные продуктами — призерами тестирований, пострадали от WannaCry? Их антивирусы не имели сигнатуры нового троянца, а поведенческие анализаторы не справились с защитой.

А вот клиенты Dr.Web не пострадали от WannaCry.

Дополнительная защита от новейших современных угроз, которые могут быть не известны вашему сигнатурному антивирусу, может быть реализована на основе технологий Dr.Web KATANA за счет анализа поведения программ — поиска в запущенных процессах признаков вредоносного поведения. Продукт защищает от угроз, не обнаруживаемых традиционными методами детектирования (сигнатурами).

Все троянцы делают это

Действуют по схожим алгоритмам,	**Совершают одну и ту же ошибку:**
используют одни и те же критические места в операционных системах для проникновения, имеют одинаковые наборы вредоносных функций.	начинают действовать первыми (нападают на систему).

Начала проявления активности троянца достаточно для Dr.Web KATANA, чтобы увидеть и обезвредить его.

Несигнатурный антивирус Dr.Web KATANA решает те же задачи, что и традиционный антивирус:

- распознаёт вредоносные процессы,
- отражает атаки вредоносных программ,
- пресекает попытки проникновения в систему, — но делает это... тоньше.

Dr.Web KATANA определит вредоносную активность, как только троянец попытается действовать.

- Многие троянцы действуют по схожим алгоритмам, используют одни и те же критические места в операционных системах для проникновения, имеют одинаковые наборы вредоносных функций.
- Все троянцы совершают одну и ту же ошибку: начинают действовать первыми (нападают на систему).
- Проявления активности троянца достаточно для Dr.Web KATANA, чтобы увидеть врага и нанести ему смертельный удар.

- Dr.Web KATANA «на лету» анализирует поведение угроз и немедленно пресекает вредоносные сценарии и процессы, которые не успел распознать (= ПРОПУСТИЛ) ваш антивирус.

И не нужно никаких сигнатур, что делает Dr.Web KATANA необыкновенно легким оружием.

Традиционные поведенческие анализаторы полагаются на жестко прописанные в базе знаний правила поведения известных нелегитимных программ.

Эти правила знают и злоумышленники!

Наличие уязвимостей и возможность внедрения эксплойтов позволяет им обойти такую защиту.

Dr.Web KATANA действует «на лету»	**На анализ уходят доли секунды**	**Обращения к «тяжелым» вирусным базам не требуется**

Что контролирует Dr.Web KATANA

- Процессы легитимных приложений.
- Критические участки системы и системные службы — загрузочные области диска, ключи реестра, в том числе отвечающие за драйверы виртуальных устройств.
- Правила запуска программ.
- Отключение безопасного режима Windows.
- Возможности добавления в логику работы операционной системы новых задач, нужных злоумышленникам.
- Загрузки новых или неизвестных пользователю драйверов.
- Коммуникации между компонентами шпионского ПО и его управляющим сервером.
- Процессы штатного создания резервных копий файлов.
- Все популярные интернет-браузеры (Internet Explorer, Mozilla Firefox, Яндекс.Браузер, Google Chrome, Vivaldi Browser).
- Приложения MS Office (Word/Excel/InfoPath/Lync/Access/Outlook/Visio/WordPad), Windows Media Player.
- Системные приложения.
- Приложения, использующие java- (Java 1.8/6/7), flash- и pdf-технологии (Acrobat Reader).

Функциональные возможности Dr.Web KATANA

- Защищает критически важные участки системы от модификаций вредоносными программами.
- Выявляет и прекращает вредоносные, подозрительные или ненадежные сценарии и процессы.
- Распознаёт нежелательные изменения файлов, отслеживая работу всех процессов в системе в поисках действий, характерных для поведения вредоносных программ (например, действий троянцев-вымогателей), не позволяя вредоносным объектам внедриться в процессы других программ.
- Обнаруживает и нейтрализует новейшие угрозы: троянцев-вымогателей (шифровальщиков), инжекторы, удаленно управляемые вредоносные объекты (распространяемые для организации ботнетов и шпионажа), а также вирусные упаковщики.

- Защищает от эксплойтов — вредоносных объектов, пытающихся для проникновения в систему использовать уязвимости, в том числе еще не известные никому, кроме вирусописателей (так называемые уязвимости «нулевого дня»).
- Контролирует работу не только наиболее популярных браузеров, но и любых плагинов к ним; защищает от блокировщиков браузеров.
- Блокирует возможность изменения вредоносными программами загрузочных областей диска с целью невозможности запуска (например, троянцев) на компьютере.
- Предотвращает отключение безопасного режима Windows, блокируя изменения реестра.
- Не позволяет вредоносным программам добавлять в логику работы операционной системы исполнение новых задач, нужных злоумышленникам. Блокирует ряд параметров в реестре Windows, что не дает, например, изменить вирусам нормальное отображение Рабочего стола или скрыть присутствие троянца в системе при помощи руткита.
- Не позволяет вредоносному ПО изменить правила запуска программ.
- Пресекает загрузки новых или неизвестных драйверов без ведома пользователя.
- Блокирует автозапуск вредоносных программ, а также определенных приложений, например анти-антивирусов, не давая им зарегистрироваться в реестре для последующего запуска.
- Блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможной установку нового виртуального устройства.
- Блокирует коммуникации между компонентами шпионского ПО и управляющим ими сервером.
- Не позволяет вредоносному ПО нарушить нормальную работу системных служб, например вмешаться в штатное создание резервных копий файлов.

Алгоритм работы Dr.Web KATANA

- При обнаружении попытки использования уязвимости Dr.Web принудительно завершает процесс атакуемой программы. Никакие действия антивируса над файлами приложения, включая перемещение в карантин, не производятся.
- В качестве информации к сведению пользователь видит уведомление о пресечении попытки вредоносного действия, реагировать на которое не требуется.
- В журнале событий Dr.Web создается запись о пресечении атаки.
- Облачная база знаний системы получает немедленное уведомление об инциденте. Если необходимо, специалисты «Доктор Веб» мгновенно отреагируют на него — например, улучшением алгоритма контроля.

Как помогает защите Облако Dr.Web

В Облаке Dr.Web содержатся:

- данные об алгоритмах программ с вредоносными намерениями;
- информация о заведомо «чистых» файлах;
- информация о скомпрометированных цифровых подписях известных разработчиков ПО;
- информация о цифровых подписях рекламного / потенциально опасного ПО;
- алгоритмы защиты приложений.

Облачная система получает информацию о работе Dr.Web KATANA на защищаемом ПК, в том числе об обнаруженных новейших угрозах, что позволяет оперативно реагировать на выявленные в работе системы недочеты и обновлять правила, хранящиеся на компьютере локально.

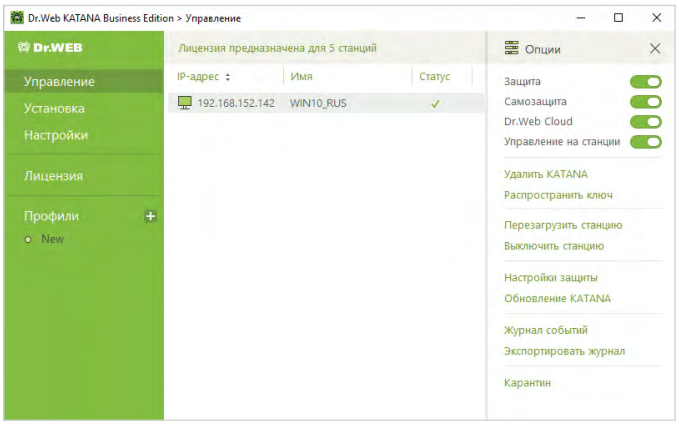
Никакой передачи пользовательских файлов из защищаемой системы на серверы «Доктор Веб» не происходит!

Максимальное упреждение	Исключительная стойкость	Возможность автономной работы
▪ Dr.Web KATANA обеспечивает безопасность практически с момента запуска операционной системы. ▪ Начинает защищать еще до завершения загрузки традиционного сигнатурного антивируса — вашего другого антивируса.	▪ В составе Dr.Web KATANA имеется не имеющий аналогов на рынке модуль самозащиты Dr.Web SelfPROtect. ▪ Если троянец «убьет» процесс другого антивируса, далее ему нужно будет вывести из строя Dr.Web KATANA, но на его пути встанет модуль самозащиты. ▪ Благодаря самозащите Dr.Web KATANA выстоит, а вредоносный процесс будет остановлен.	▪ Троянцы не умеют самостоятельно распространяться. ▪ Сотрудники сами переносят их на флешках и других устройствах. ▪ Там, где установка «тяжелого» сигнатурного антивируса невозможна, спасет несигнатурный антивирус Dr.Web KATANA, обладающий минимальными системными требованиями и возможностью работы без доступа к Интернету.

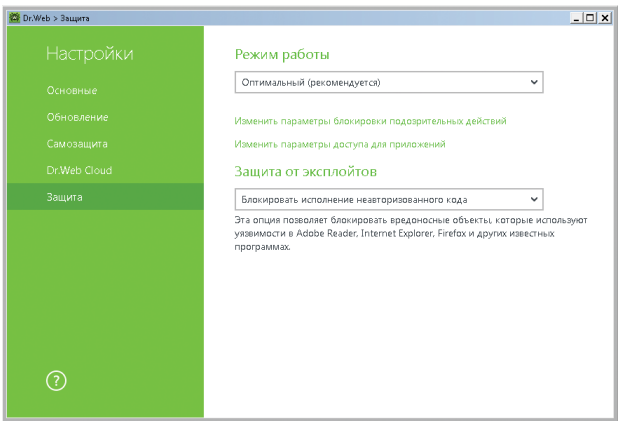
Управление

▪ Централизованная установка на защищаемые станции сети, настройка и мониторинг вирусных событий, а также состояния Dr.Web KATANA на защищаемых станциях.	▪ Предустановленные сценарии защиты (оптимальный, средний, параноидальный) — продукт работает прямо «из коробки».	▪ Возможность создавать гибкие правила для доверенных приложений и не допустить возникновения конфликтов ПО при работе Dr.Web KATANA.	▪ Возможность настройки параметров контроля защиты для конкретного приложения, обеспечение для него доступа только к определенным ресурсам.

Центр управления



Агент



Совместимость

В ходе разработки Dr.Web KATANA была подтверждена совместимость с продуктами Trend Micro, Symantec, Kaspersky, McAfee, ESET и др.

Новинка! Dr.Web vxCube

Облачный интеллектуальный интерактивный анализатор подозрительных объектов для специалистов по информационной безопасности и киберкриминалистов

Dr.Web vxCube:

- Удаленно анализирует объект в среде, соответствующей именно вашей ситуации.
- Позволяет наблюдать за процессом анализа.
- Воспроизводит любое действие подозрительного объекта для его исследования.
- Предоставляет полный отчет о проведенном анализе.

При обнаружении угрозы будет изготовлена **специальная сборка утилиты Dr.Web CureIt!** с целью лечения вашей системы – раньше, чем с проблемой смогут справиться установленные у вас средства защиты. Dr.Web CureIt! способен работать без установки даже при наличии другого антивируса.

Подробнее о Dr.Web vxCube

Экспертиза вирусозависимых компьютерных инцидентов (ВКИ)

Экспертиза включает:

- Предварительную оценку инцидента, объема экспертизы и мер, необходимых для устранения последствий произошедшего.
- Экспертные исследования компьютерных и других артефактов (накопителей на жестких магнитных дисках, текстовых, звуковых, фото-, видеоматериалов), предположительно имеющих отношение к ВКИ.
- Не имеет аналогов! Психологическую экспертизу личностей (персонала) с целью выявления фактов причастности к совершению / пособничеству / укрывательству / поощрению противоправных действий в отношении заказчика (комплексное определение рисков), а также фактов бездействия или халатного отношения к служебным обязанностям.
- Рекомендации по вопросам построения антивирусной системы защиты с целью недопущения ВКИ или сокращения их количества в будущем.

Подробнее об экспертизе «Доктор Веб»

Заявки на экспертизу принимаются по адресу:

https://support.drweb.ru/expertise

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.
Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Его использование позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  - информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  - отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97

www.антивирус.рф | www.drweb.ru