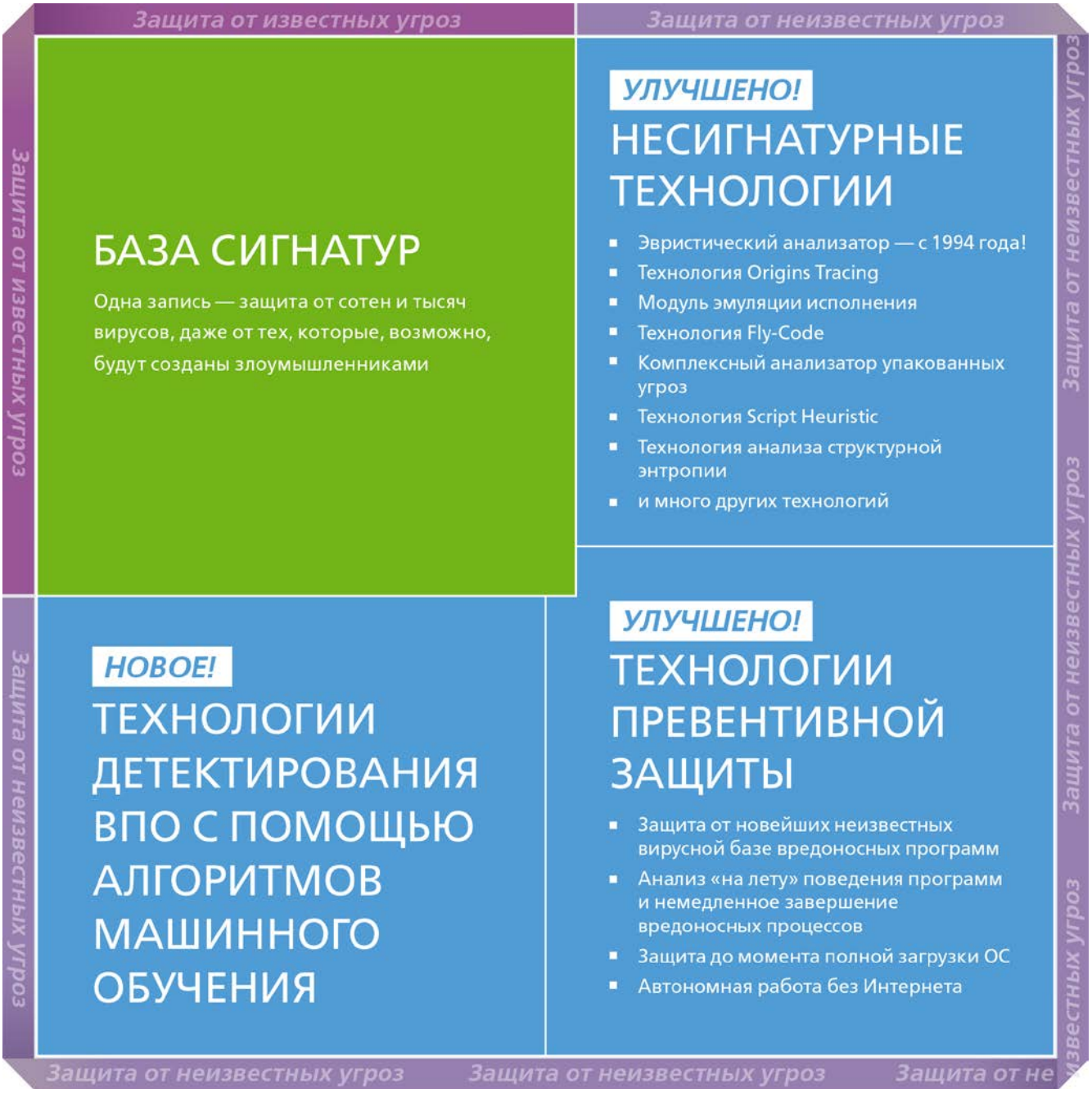
Dr.WEB®
с 1992 года

Технологии Dr.Web

- БОЛЕЕ 25 ЛЕТ ОПЫТА ИЗУЧЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ
- УМЕНИЕ ПРЕДВИДЕТЬ ПУТИ ЭВОЛЮЦИИ ВРЕДОНОСНЫХ ПРОГРАММ
- ПОСТОЯННОЕ РАЗВИТИЕ БАЗОВЫХ АНТИВИРУСНЫХ ТЕХНОЛОГИЙ, ЗАРЕКОМЕНДОВАВШИХ СЕБЯ КАК ЭФФЕКТИВНЫЕ
- РАЗРАБОТКА НОВЫХ ПРОГРЕССИВНЫХ АНТИВИРУСНЫХ ТЕХНОЛОГИЙ

Квадрат безопасности Dr.Web



Сочетание в Dr.Web традиционной сигнатурной вирусной базы, несигнатурных технологий и технологий превентивной защиты позволяет держать оборону против любых вредоносных угроз —

WannaCry не прошел!

Технологии превентивной защиты Dr.Web

Для защиты от новых неизвестных вредоносных программ

Сегодня вирусописательство — это хорошо налаженный **криминальный бизнес**. Новые вредоносные программы, большинство из которых троянцы, появляются ежедневно сотнями тысяч.

Задача антивируса — не допускать заражения.

Считается, что антивирус обязан обнаруживать все вредоносные программы в момент их проникновения.

Однако:

30% вредоносного ПО обнаруживает сигнатурами современный антивирус	**70%** вредоносного ПО — не известно антивирусу в момент проникновения

Технологически сложные и особо опасные троянцы, особенно созданные для извлечения коммерческой выгоды, вирусописатели проверяют на обнаружение по всем антивирусам, перед тем как выпустить свое творение в «живую природу», чтобы вирус существовал незамеченным антивирусами как можно дольше. Поэтому всегда существует временная дельта между выпуском троянца злоумышленниками, попаданием его образца на анализ в вирусную лабораторию и изготовлением противоядия.

УГРОЗА ЗАРАЖЕНИЯ НОВЕЙШИМ НЕИЗВЕСТНЫМ ВИРУСОМ ЕСТЬ ВСЕГДА.

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, чтобы увидеть и обезвредить его.

Это возможно благодаря разнообразным технологиям **Превентивной защиты Dr.Web**, действующим на опережение и не допускающим проникновения новейших, наиболее опасных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами, — объектов, которые еще не поступили на анализ в антивирусную лабораторию, а значит, не известны вирусной базе Dr.Web на момент проникновения в систему. По схожести поведения подозрительной программы с известными моделями подобного поведения Dr.Web умеет распознавать и блокировать такие программы.

В отличие от традиционных поведенческих анализаторов, полагающихся на жестко прописанные в базе знания, а значит, известные злоумышленникам правила поведения легитимных программ, интеллектуальная система превентивной защиты Dr.Web анализирует «на лету» поведение каждой запущенной программы и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности и нейтрализует угрозу. Технологии **Превентивной защиты Dr.Web** могут действовать автономно, даже без доступа к Интернету.

Несигнатурные технологии Dr.Web

Для защиты от неизвестных вредоносных программ, подобных уже известным

В продуктах Dr.Web для обнаружения и обезвреживания неизвестного вредоносного ПО, схожего с уже известными образцами, применяется множество эффективных несигнатурных технологий, сочетание которых позволяет обнаруживать даже неизвестные вирусной базе угрозы до получения сигнатуры.

WannaCry был остановлен эвристическим анализатором Dr.Web, который разрабатывается с 1994 года.

Эвристический анализатор	Технология Origins Tracing	Модуль эмуляции исполнения
Обнаружение неизвестных вредоносных программ на основании знаний (эвристики) об определенных особенностях (признаках) вирусов — как характерных именно для вирусного кода, так и, наоборот, крайне редко встречающихся в вирусах. ! Эвристики обнаруживают только новые модификации ранее попавших на анализ вредоносных программ, с известным антивирусу поведением.	Распознавание вирусов, еще не добавленных в вирусную базу Dr.Web, путем сканирования исполняемого файла, который рассматривается как некий образец, построенный характерным образом, и сравнения полученного образца с базой известных вредоносных программ	Обнаружение полиморфных и сложношифрованных вирусов, когда непосредственное применение поиска по контрольным суммам невозможно либо крайне затруднено (из-за невозможности построения надежных сигнатур), путем имитации исполнения анализируемого кода эмулятором — программной моделью процессора (и отчасти компьютера и ОС).

Технология Fly-Code	Комплексный анализатор упакованных угроз	Технология Script Heuristic
Качественная проверка упакованных исполняемых объектов. Распаковка любых (даже нестандартных) упаковщиков методом виртуализации исполнения файла. Обнаружение вирусов, упакованных даже неизвестными антивирусному ПО Dr.Web упаковщиками.	Значительное повышение уровня детектирования якобы «новых угроз» — известных вирусной базе Dr.Web, но скрытых под новыми упаковщиками. Исключает необходимость добавления в вирусную базу все новых и новых записей об угрозах.	Предотвращение исполнения любых вредоносных скриптов в браузере и PDF-документах без нарушения функциональности легитимных скриптов. Защита от заражения неизвестными вирусами через веб-браузер. Работа независимо от состояния вирусной базы Dr.Web совместно с любыми веб-браузерами.

Технология анализа структурной энтропии	И много других технологий
Обнаружение неизвестных угроз по особенностям расположения участков кода в защищенных криптоупаковщиками проверяемых объектах.	

Вирусная база Dr.Web

Для защиты от известных угроз

Защита от вирусов обеспечивается, среди прочего, внесением в вирусную базу записей (сигнатур), позволяющих детектировать вирусы. Если бы и сегодня антивирус умел распознавать новые вирусы только на основании записей в вирусных базах, такие базы не смог бы уместить в своей памяти ни один компьютер, проверка занимала бы много времени, а быстродействие ПК было бы серьезно замедлено.

Не все вирусы уникальны. Существуют целые семейства родственных (подобных) вирусов, есть вирусы, сконструированные вирусными конструкторами — специальными программами для создания вирусов. Все они очень похожи друг на друга, очень часто — как две капли воды. Разработчиками некоторых других антивирусов каждый такой вирус-близнец наделяется отдельной записью в вирусной базе, что утяжеляет ее.

Вирусная база Dr.Web не имеет аналогов в отрасли

Всего одна запись в вирусной базе позволяет Dr.Web определять сотни и даже тысячи вредоносных файлов — включая те, которые, возможно, будут созданы злоумышленниками.	«Доктор Веб» проводит регулярную очистку баз от дублирующих записей без потери качества детектирования. Антивирус не должен тормозить!	Уникальной особенностью вирусных баз Dr.Web является алгоритм поиска сигнатур в вирусных базах, базах правил брандмауэра и поведенческого анализатора, не увеличивающий время поиска при увеличении количества записей.	Интеллектуальная система добавления родственных вирусов позволяет в автоматическом режиме включать описания новых вредоносных файлов в вирусные базы, что сокращает время реакции на атаки злоумышленников.

Сохранение компактности вирусной базы Dr.Web позволяет не увеличивать системные требования и обеспечивает малый размер обновлений — при традиционном неизменно высоком качестве детектирования и лечения.

Новое!

Технологии детектирования на основе алгоритмов машинного обучения

Для обнаружения вредоносных сценариев JavaScript

! До миллиона потенциально вредоносных образцов поступает в сутки в антивирусную лабораторию «Доктор Веб».

Не всё пришедшее — вредоносные программы. Но все они должны быть обработаны нашими специалистами. Огромный поток вредоносных программ, поступающих на анализ в «Доктор Веб», позволяет разбить данные на характерные участки и выделить среди них вредоносные.

Начиная с версии 11.5 в решениях Dr.Web используются правила, создаваемые на основе алгоритмов **машинного обучения — технологии SpIDer ML Anti-Script.**

- Благодаря новой технологии Dr.Web SpIDer Guard может определять еще больше новейших неизвестных вредоносных программ в файлах скриптовых языков, не дожидаясь обновлений традиционных вирусных баз.
- Правила детектирования, создаваемые системой машинного обучения на основе знаний о том, какой код является вредоносным, позволяют Dr.Web SpIDer Guard «предсказать» поведение программы до запуска ее вредоносного содержимого и нейтрализовать ее.
- Сложнейшие математические алгоритмы системы машинного обучения позволяют автоматически вырабатывать новые правила детектирования вредоносных программ — без участия вирусных аналитиков и практически мгновенно.
- В Dr.Web используется множество технологий, позволяющих защищать от новейших вредоносных программ без участия вирусных баз. Новые технологии на основе машинного обучения подняли планку качества детектирования таких программ еще выше!
- Благодаря в том числе и этой новой технологии вирусная база Dr.Web сохраняет минимальный объем, а качество детектирования только улучшается при рекордно низком количестве ложных срабатываний.

Dr.Web лечит от вирусов

Антивирус обязан не допускать заражения.

А если оно произошло — антивирус должен лечить от уже проникших активных вредоносных программ.

Именно поэтому наиболее важным показателем качества антивирусной программы является не ее способность находить вирусы, а способность лечить их; не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и уметь возвращать их в первоначальное «здоровое» состояние.

Ни один антивирус не может обнаружить все вредоносные программы в момент начала атаки.

Однако только антивирус способен вылечить систему от уже проникших и активных вредоносных программ.

Возможность установки и работы на уже инфицированном компьютере и исключительная вирусоустойчивость выделяют Dr.Web среди всех других антивирусов.

Самозащита Dr.Web

Для защиты антивируса от уже проникших вредоносных программ

Стойкий иммунитет к любым попыткам вредоносных программ вывести Dr.Web из строя обеспечивает не имеющий аналогов в антивирусной отрасли компонент самозащиты Dr.Web SelfPROtect.

Предназначение	Преимущество
Защита от действий нелегитимного ПО (вредоносных программ, хакерских утилит) и действий злоумышленников, прослушек и других видов слежения.	Высочайшая вирусостойкость и невозможность вывода Dr.Web из строя в результате действия вредоносных программ.

Особенности

- Dr.Web SelfPROtect реализован в виде драйвера и действует на самом низком системном уровне. Выгрузка и остановка его работы невозможны до перезагрузки системы.
- 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 анти-антивирусных программ прекратить функционирование Dr.Web.
- В отличие от некоторых конкурирующих продуктов, модифицирующих ядро Windows (перехватывающих прерывания, подменяющих таблицы векторов, использующих недокументированные функции и т. д.), что может привести к серьезным проблемам в работе самой операционной системы, а также создает новые пути для использования уязвимостей, модуль защиты Dr.Web SelfPROtect является полностью самодостаточным.
- Возможность автоматического восстановления собственных модулей.

Функции

- Криптостойкая идентификация доверенных процессов на базе цифровых сертификатов.
- Верификация сертификатов в ядре ОС без использования Windows API, которое может быть скомпрометировано.
- Защита доверенных процессов от завершения и компрометации, в том числе в некоторых случаях при доступе из ядра ОС.
- Защита GUI доверенных процессов от эмуляции действий вредоносного ПО и злоумышленников.
- Защита заданных файлов/каталогов от удаления, модификации. Эффективно против деструктивных действий вредоносного ПО и злоумышленников.
- Запрет на полный доступ к файлам или каталогам для защиты важных файлов / документов / баз данных от утечек, кражи и т. п. Полный доступ получают только доверенные процессы.
- Защита файлов от кражи и модификации при попытках чтения через карту секторов диска.

- Защита заданных параметров и ключей реестра. Эффективно против деструктивных действий вредоносного ПО и злоумышленников.
- Запрет на полный доступ к параметрам и ключам реестра для защиты важных данных / параметров / ключей лицензирования и другой чувствительной информации от кражи и компрометации.
- Защита именованного канала (named pipe) от попыток подключения недоверенными процессами. Позволит реализовать безопасное межпроцессорное взаимодействие между доверенными процессами, не опасаясь прослушки и компрометации данных.
- Защита доверенных процессов от инжектов, в том числе от всех популярных и модных техник типа APC, CreateRemoteThread, SetThreadContext, UnmapSection, WriteProcessMemory, AppInit_Dlls, Process Hollowing, Double Agent, Process Doppelganging и т. п.
- Отслеживание создания и удаления новых исполняемых модулей в системе.
- Контроль попыток модификации/компрометации заданных файлов/каталогов на дисках.
- Контроль смены времени в системе.

Подробнее о технологиях Dr.Web

Технологии лечения	**Технологии превентивной защиты**	**Несигнатурные технологии**	**Технологии самозащиты**	**Вирусная база**

Все технологии Dr.Web

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

антивирус.рф | www.drweb.ru