Dr.WEB
с 1992 года

# «Песочница» Dr.Web vxCube

## Интеллектуальный интерактивный анализатор подозрительных объектов для ваших корпоративных клиентов

Для использования в Республике Беларусь и Республике Казахстан


www.drweb.ru

Dr.WEB
с 1992 года

# Кому будет полезен Dr.Web vxCube

Dr.Web vxCube предназначен для коммерческих и государственных организаций, которым необходимо повысить уровень защиты от потенциальных кибератак и выявить уже идущие, — в том числе при имеющейся информационной защите

**С Dr.Web vxCube могут работать:**

- специалисты по информационной безопасности
- киберкриминалисты

# Почему [иногда] Dr.Web vxCube незаменим

Установленный антивирус может выявить вредоносный объект — но не всегда.
Если в сети наблюдаются аномалии, а какие-либо файлы вызывают подозрение (пусть пока и не обоснованное) — подтвердить или опровергнуть их поможет Dr.Web vxCube.
Также анализатор позволяет проверить на вредоносность ПО перед его установкой.

# Как действует Dr.Web vxCube

Проверяет
подозрительные объекты
в изолированной среде

Анализирует действия
подозрительного
объекта

Выявляет обращения
к сетевым ресурсам,
известным Dr.Web как
источники распространения
вредоносного ПО

По результатам
предоставляет отчет
о поведении вредоносной
программы и карту ее
сетевой активности

В случае выявления
вредоносной активности
формирует специальную
утилиту на базе
Dr.Web CureIt!
для нейтрализации
обнаруженной угрозы

# Преимущества Dr.Web vxCube

- Dr.Web vxCube работает незаметно для изучаемого объекта — он обходит более **370** методов обнаружения виртуальной среды.
  На сегодняшний день у вредоносных файлов нет шансов замаскироваться и уйти от наблюдения
- Dr.Web vxCube позволяет сформировать подробный отчёт, а значит — детально анализировать действия ВПО и эффективно планировать меры борьбы с ним
- По результатам работы возможно проведение расследования инцидента силами специалистов «Доктор Веб»

# 2 вида использования Dr.Web vxCube: облачный и программно-аппаратный

## ОБЛАЧНАЯ

версия подразумевает отправку файлов для анализа на серверах «Доктор Веб» и создание лечащей утилиты Dr.Web CureIt! в случае обнаружения угроз

## ПРОГРАММНО-АППАРАТНАЯ

версия On-premise позволяет анализировать подозрительные файлы в пределах собственной сети клиента, без их отправки на внешние сервисы

# Dr.Web vxCube в деталях

| Какие файлы проверяются | Как происходит анализ |
| --- | --- |
| ▪ Исполняемые файлы JAVA<br>▪ Исполняемые файлы Windows<br>▪ Пакеты Android<br>▪ Файлы Acrobat Reader<br>▪ Скрипт-файлы<br>▪ Документы и служебные файлы Microsoft Office/OpenOffice | ▪ На виртуальной машине тщательно отслеживается поведение файла<br>▪ Используя список правил, анализатор распределяет его действия по категориям<br>▪ Все действия записываются и доступны для последующего анализа<br>▪ В результате даётся оценка вредоносности файла по шкале от 0 до 100, а также отчёт с техническими подробностями |

Dr.Web vxCube обеспечивает расширенный набор взаимодействий с сервисом благодаря наличию API.
Имеется раздел для работы с YARA-правилами, которые позволяют проверять файлы по заданным параметрам, автоматически выставлять теги для отдельных типов угроз и указывать степень вредоносности анализируемого файла.

# Что содержит отчёт Dr.Web vxCube

- Описание действий вредоносного ПО и его модулей
- Оценку изученного файла: вредоносный, потенциально опасный или нейтральный
- Данные об обращении к сетевым ресурсам, известным Dr.Web как вредоносные и потенциально опасные
- Информацию о влиянии обнаруженного вредоносного ПО на зараженную систему
- Индикаторы в форматах STIX и MAEC для поиска признаков проанализированной угрозы в защищаемом периметре

# Как лицензируется Dr.Web vxCube

- В «облачной» версии Dr.Web vxCube лицензируется по числу файлов, которые можно проверить с помощью анализатора
- Лицензия на версию On-premise позволяет проверить неограниченное количество файлов в течение срока действия лицензии
- «Облачная» версия доступна также в деморежиме, в котором клиент может загрузить и проверить 10 файлов в течение 10 дней