КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как выжить в году 2019? Пройдемся по ошибкам

Dr.WEB®
с 1992 года

Вячеслав Медведев
ООО «Доктор Веб»

ТЕЛЕФОН: +7 495 789-45-87

EMAIL: v.medvedev@drweb.com

13 июня 2019
Калининград

Dr.WEB®
с 1992 года

Вопрос:

Защищает ли резервное копирование от шифровальщиков?

Dr.WEB®
с 1992 года

Вопрос:

Защищает ли антивирус от вредоносных программ?

Dr.WEB®
с 1992 года

Рекламная вставка

Как спикер я давно уже заметил, что если я начинаю говорить, что антивирус может пропускать, то у пользователей возникает мнение, что пропускает конкретный антивирус. Психология…

Dr.WEB®
с 1992 года

Антивирус это не только антивирусные базы

#CODEIB

Защита от известных угроз

Защита от неизвестных угроз

БАЗА СИГНАТУР

Одна запись — защита от сотен и тысяч вирусов, даже от тех, которые, возможно, будут созданы злоумышленниками

УЛУЧШЕНО!

НЕСИГНАТУРНЫЕ ТЕХНОЛОГИИ

- Эвристический анализатор — с 1994 года!
- Технология Origins Tracing
- Модуль эмуляции исполнения
- Технология Fly-Code
- Комплексный анализатор упакованных угроз
- Технология Script Heuristic
- Технология анализа структурной энтропии
- и много других технологий

НОВОЕ!

ТЕХНОЛОГИИ ДЕТЕКТИРОВАНИЯ ВПО С ПОМОЩЬЮ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

УЛУЧШЕНО!

ТЕХНОЛОГИИ ПРЕВЕНТИВНОЙ ЗАЩИТЫ

- Защита от новейших неизвестных вирусной базе вредоносных программ
- Анализ «на лету» поведения программ и немедленное завершение вредоносных процессов
- Защита до момента полной загрузки ОС
- Автономная работа без Интернета

Защита от известных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от неизвестных угроз

Защита от не

Dr.WEB®
с 1992 года

В лабораторию Dr.Web приходит на анализ
до 12 миллионов (в день!) программ. Огромный поток данных позволяет разбить поступающие данные на характерные участки и выделить среди них вредоносные.
Технологии машинного обучения на основе полученных данных позволяют автоматически вырабатывать новые правила — без участия аналитиков и практически мгновенно.

Big Data, да

Dr.WEB®
с 1992 года

Несигнатурные методы детектирования неизвестных угроз Dr.Web Enterprise Security Suite

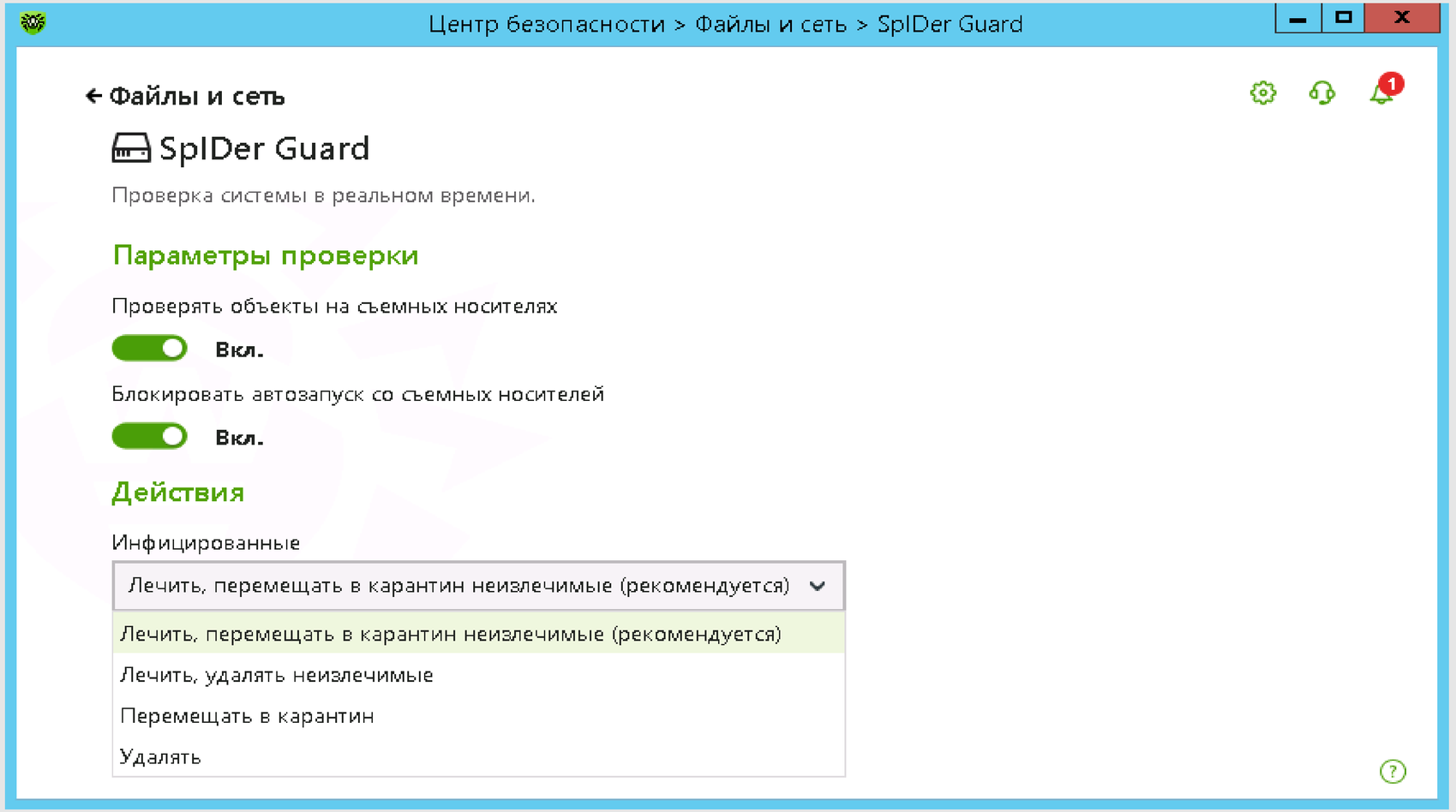
- ✓ Возможность обнаружения угроз без постоянного обращения к вирусным базам – что положительно сказывается как на быстродействии, так и качестве обнаружения новейших угроз
- ✓ Обнаружение угроз до фактического исполнения их кода
- ✓ Обнаружение популярных в данных момент действий злоумышленников - использование вредоносных майнеров, загрузчиков вредоносного ПО - как активных, так и предназначенных к запуску во всех областях системы

Dr.WEB®
с 1992 года

Но вернемся к майнерам, точнее их необнаружению.

Dr.WEB®
с 1992 года

Антивирусное ядро определяет любые виды майнеров

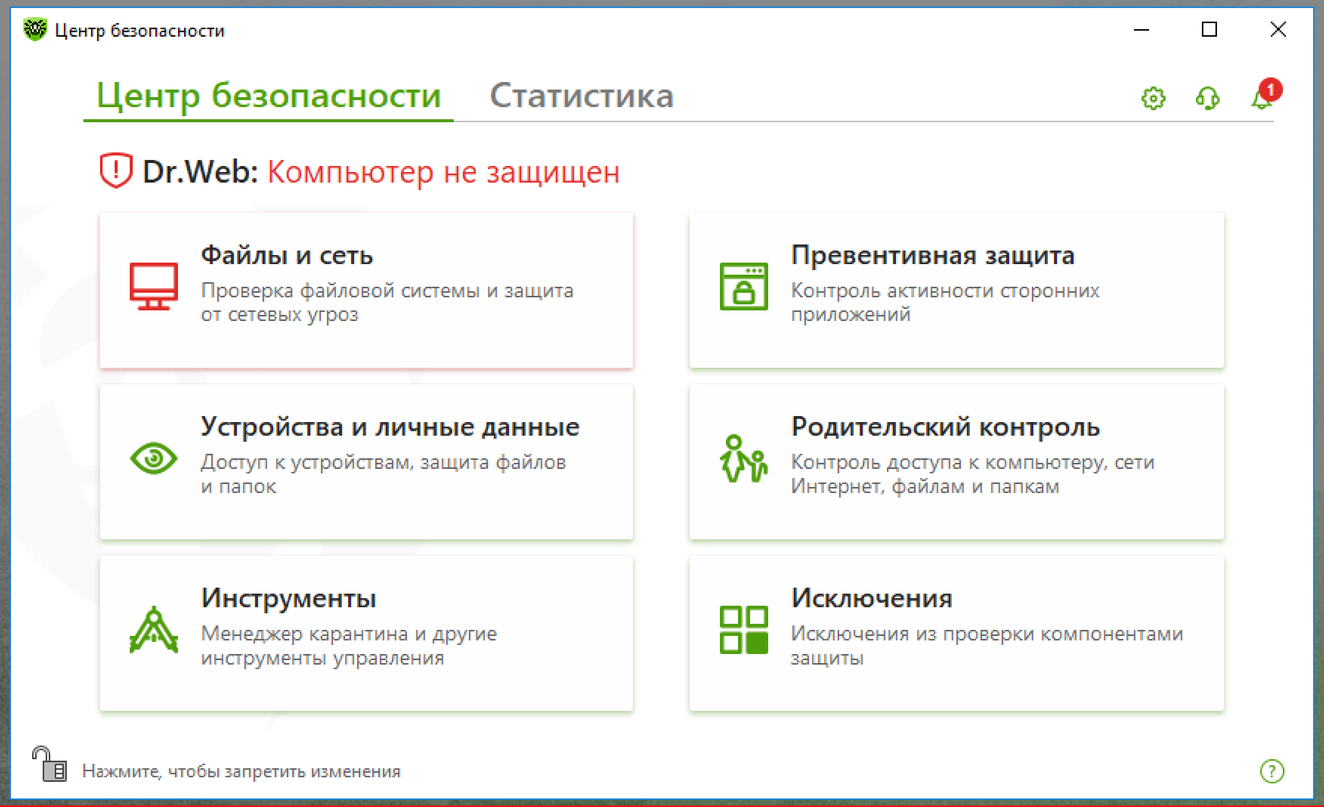


Dr.WEB®
с 1992 года

Антивирус должен быть настроен!

Dr.WEB®
с 1992 года

ЛИШНИХ МОДУЛЕЙ В АНТИВИРУСЕ – НЕТ!



Опасно – и иногда для жизни!

#CODEIB

Dr.WEB®
с 1992 года

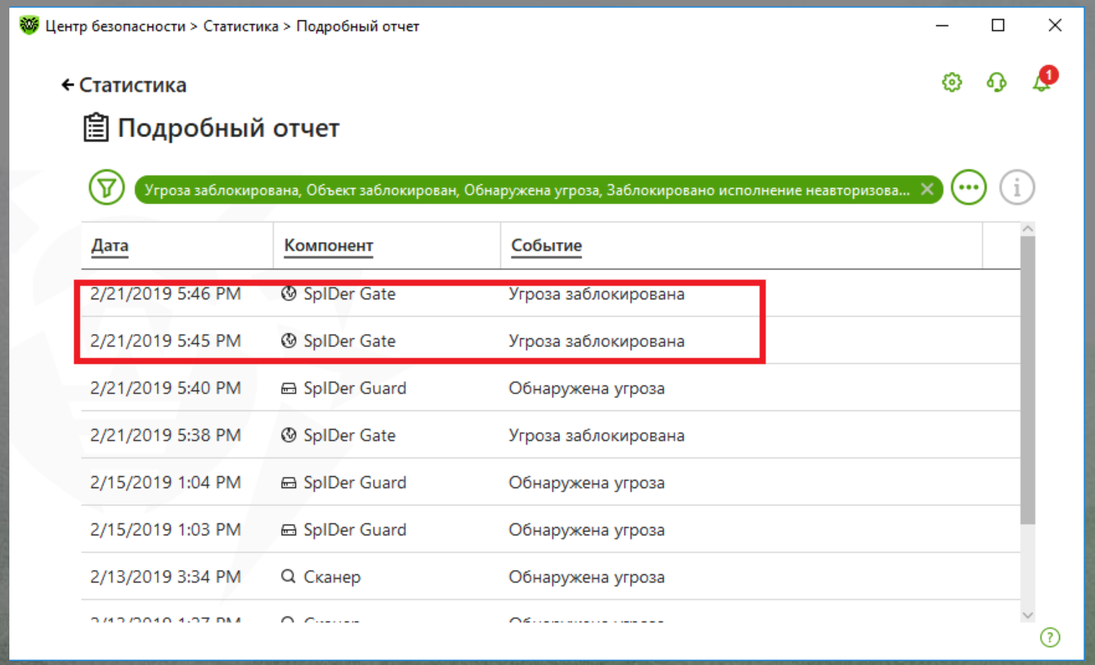
1. Использование компонента Dr.Web Антиспам позволяет блокировать получение неизвестных вредоносных файлов по признакам распространения мошеннических писем

2. Превентивная защита (Dr.Web Process Heuristic) определяет до 99 процентов шифровальщиков, еще неизвестных антивирусному ядру

3. Проверка трафика (Dr.Web SpIDerGate) защищает от коммуникаций с сайтами, используемыми злоумышленниками

Dr.WEB®
с 1992 года

ТОЛЬКО ОДИН «НЕ ЛИШНИЙ» МОДУЛЬ



Компонент Dr.Web SpIDerGate доступен в составе Dr.Web Security Space, тарифном пакете Dr.Web Премиум услуги «Антивирус Dr.Web» и в лицензии Dr.Web Desktop Security Suite, Комплексная защита)

#CODEIB

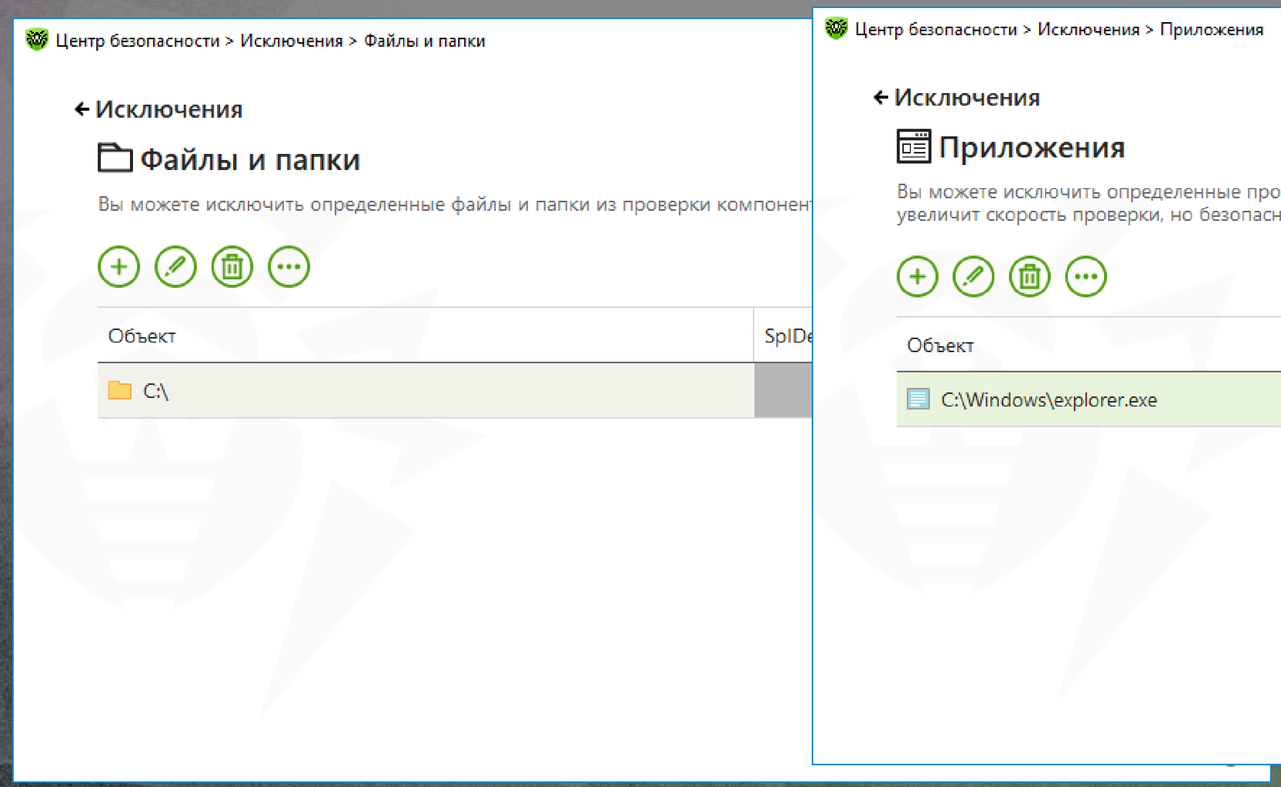
Dr.WEB®
с 1992 года

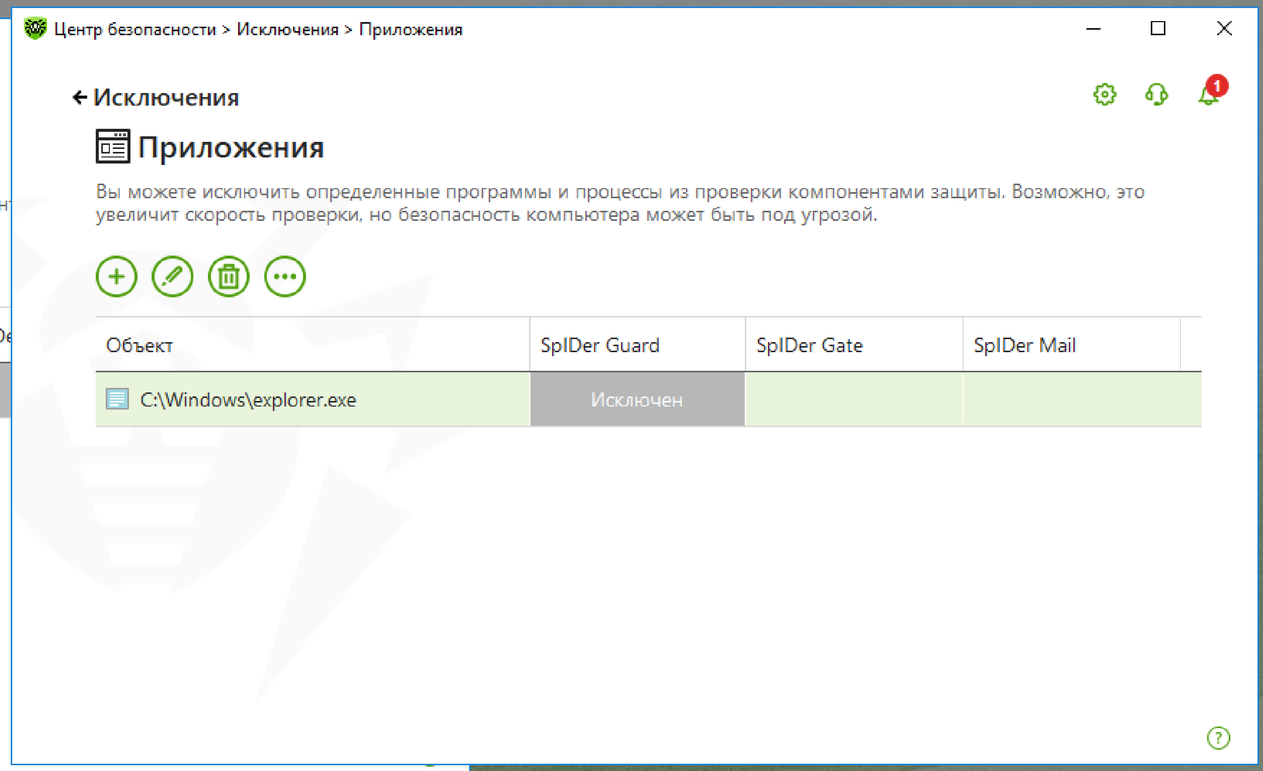
ОБЛАЧНАЯ ЗАЩИТА DR.WEB CLOUD ОБЕСПЕЧИВАЕТ ВОЗМОЖНОСТЬ МГНОВЕННОЙ РЕАКЦИИ НА НОВЕЙШИЕ УГРОЗЫ – ДО МОМЕНТА ПОЛУЧЕНИЯ ОБНОВЛЕНИЯ

#CODEIB

Dr.WEB®
с 1992 года

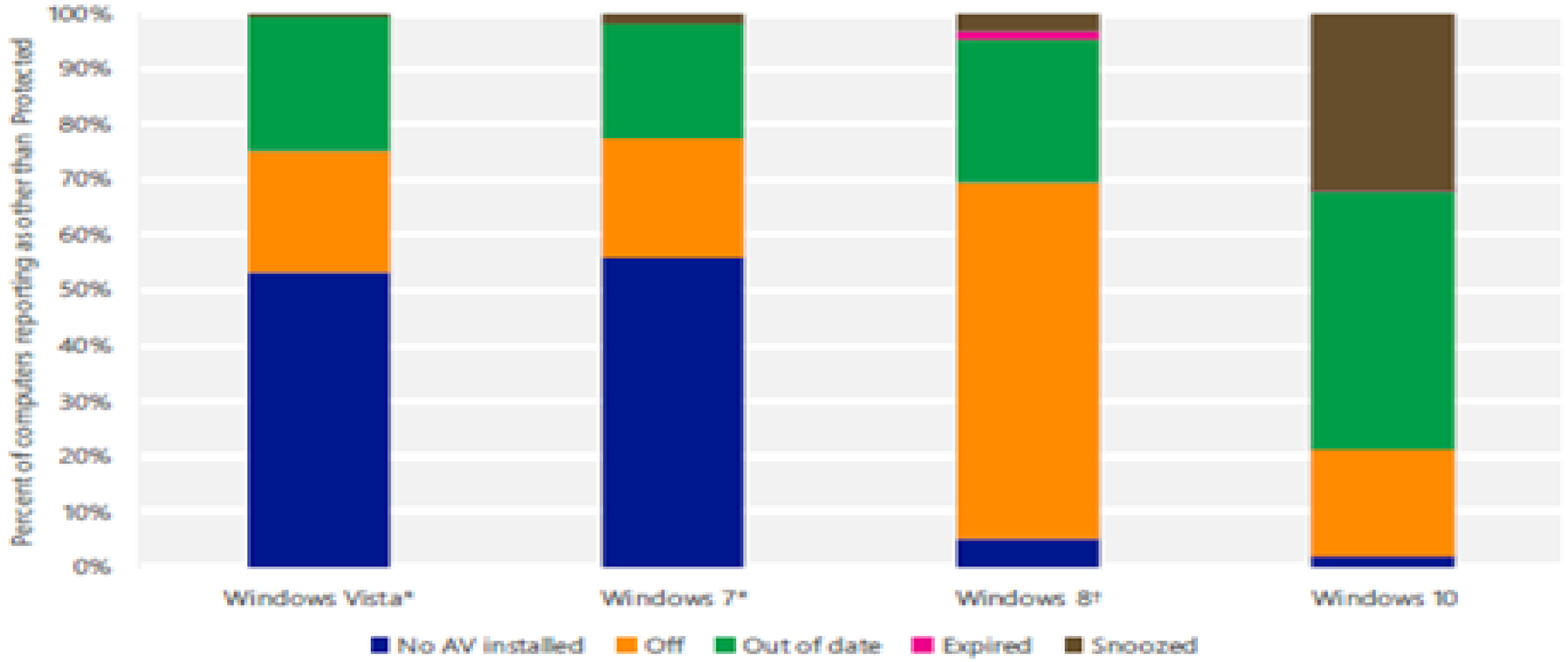
НЕ ИСКЛЮЧАЙТЕ ИЗ ПРОВЕРКИ БОЛЬШЕ ФАЙЛОВ И ПРОЦЕССОВ, ЧЕМ ЭТО НУЖНО!





#CODEIB

Всего одна статистика

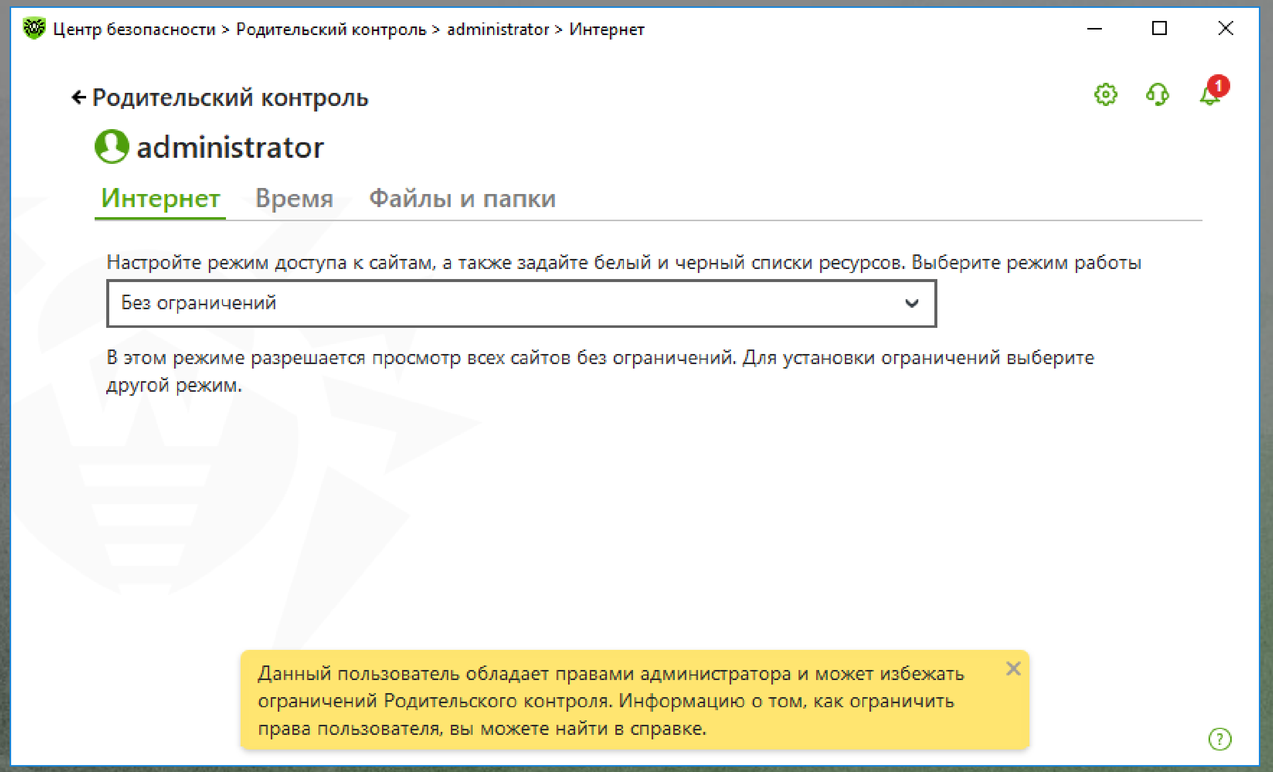


Желтый цвет — установленный и выключенный антивирус, зеленый — установленный, но не обновляемый.

Microsoft Security Intelligence Report Volume 22

Dr.WEB®
с 1992 года

ОГРАНИЧЬТЕ ДОСТУП ПОЛЬЗОВАТЕЛЕЙ К СЕТЕВЫМ И ЛОКАЛЬНЫМ РЕСУРСАМ

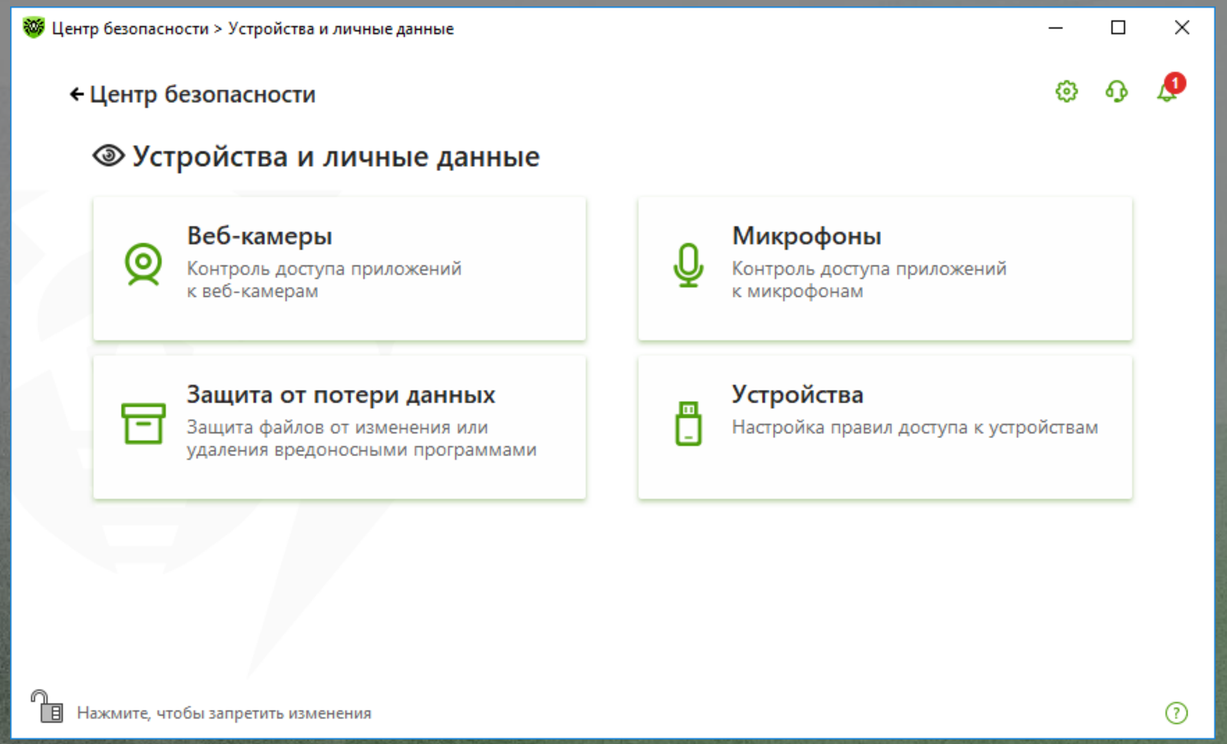


Компонент «Родительский контроль» доступен в составе Dr.Web Security Space, тарифном пакете Dr.Web Премиум услуги «Антивирус Dr.Web» и в лицензии Dr.Web Desktop Security Suite, Комплексная защита)

#CODEIB

Dr.WEB®
с 1992 года

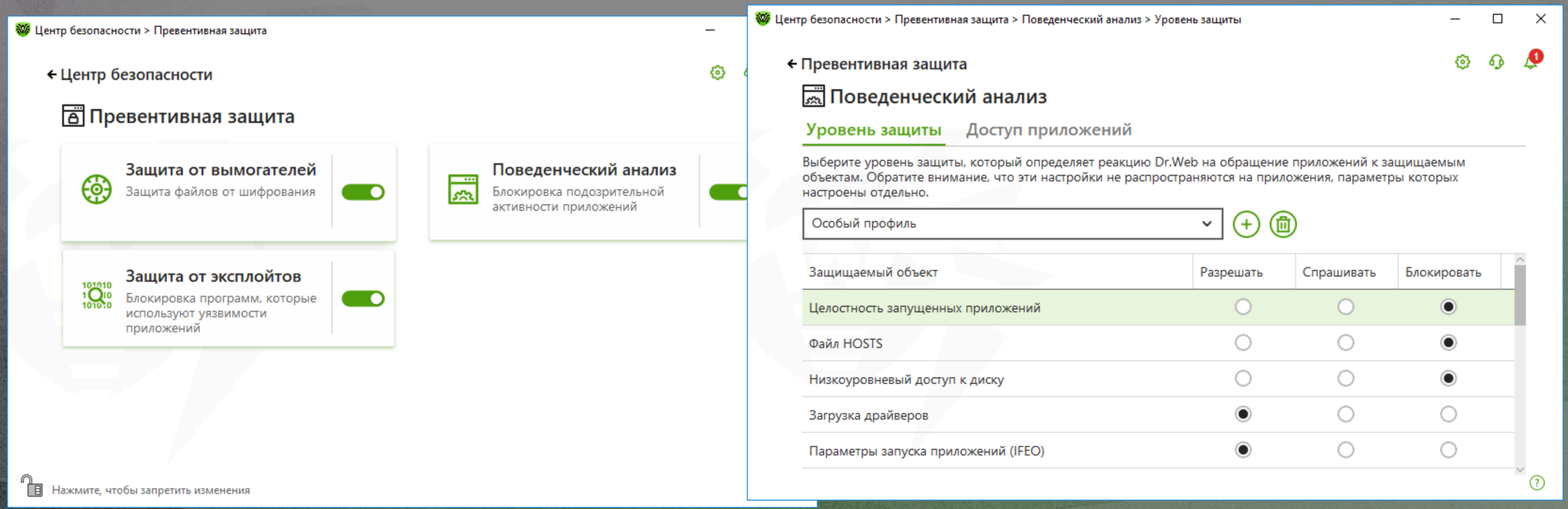
ОГРАНИЧЬТЕ ДОСТУП ПОЛЬЗОВАТЕЛЕЙ К СМЕННЫМ НОСИТЕЛЯМ



#CODEIB

Dr.WEB®
с 1992 года

НАСТРОЙТЕ ОГРАНИЧЕНИЯ ПРОАКТИВНОЙ ЗАЩИТЫ DR.WEB PROCESS HEURISTIC И БРАНДМАУЭРА. НАСТРОЙКИ ПРОАКТИВНОЙ ЗАЩИТЫ НЕ ДОЛЖНЫ ПОЗВОЛЯТЬ ВНЕДРЕНИЕ ЭКСПЛОЙТОВ В РАБОТАЮЩИЕ ПРИЛОЖЕНИЯ



#CODEIB

Если нужно защититься от угроз

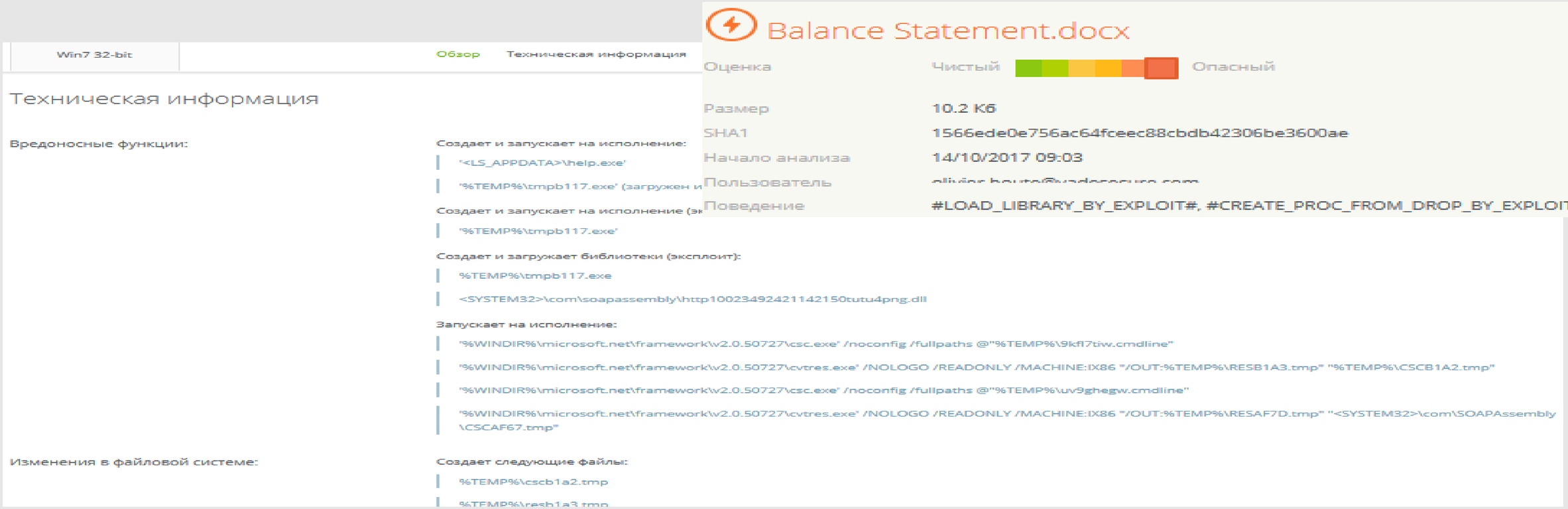
1. Антивирус должен стоять везде
2. Антивирус должен вовремя продлеваться
3. Антивирус должен быть актуален
4. Антивирус должен быть настроен
5. Пользователь должен быть ограничен в правах
6. Бекап и еще раз бекап

Dr.WEB®
с 1992 года

Достаточно ли одного антивируса?

Dr.WEB®
с 1992 года

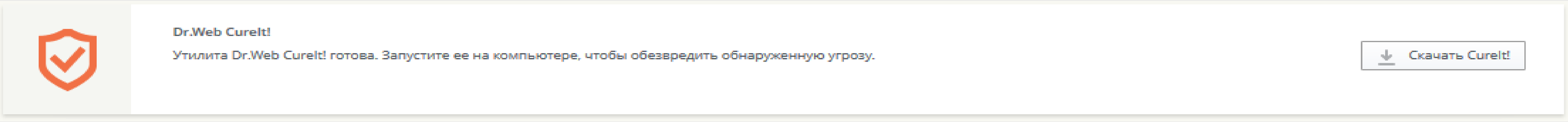
Дополнительно к основной системе защите должен использоваться сервис экстренной проверки



Dr.Web vxCube

Dr.WEB®
с 1992 года

Отправив подозрительный файл на анализ, вы получаете не только полный отчет об интересах злоумышленника, но и специальную сборку лечащей утилиты Dr.Web CureIt!



Dr.WEB®
с 1992 года

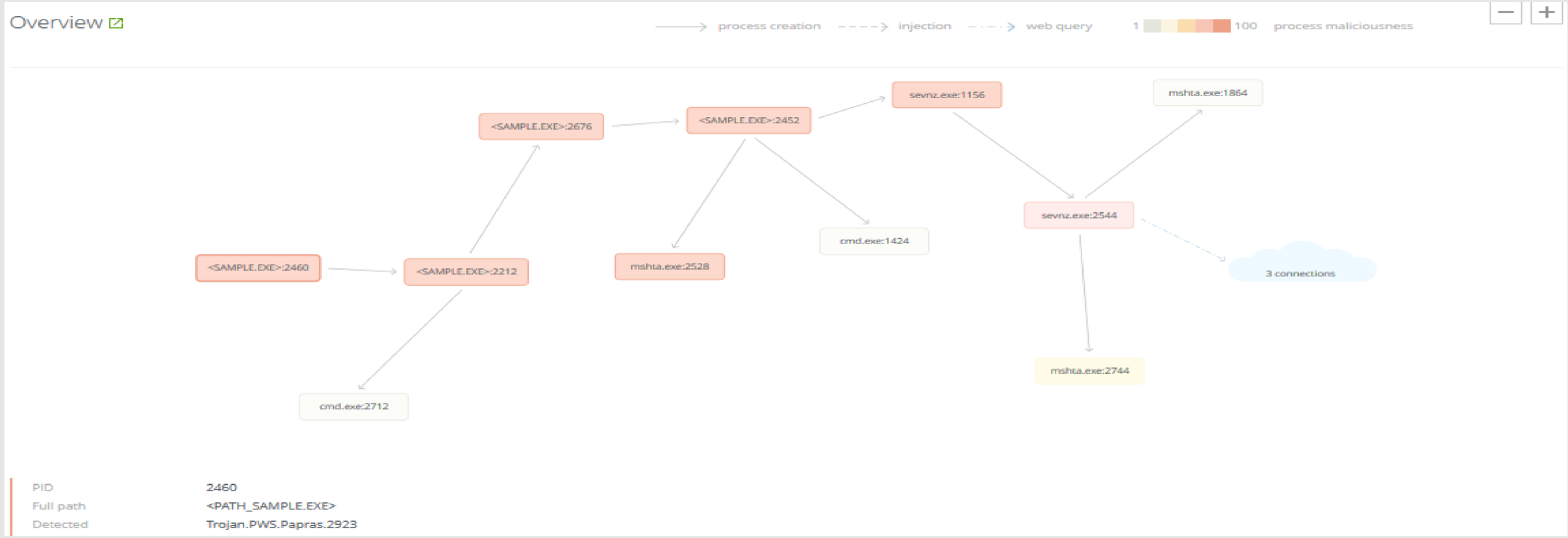
Для анализа также доступна техническая информация, ресурсы, к которым обращается анализируемый файл, список создаваемых им файлов, изменяемых ключей реестра и многое другое

Отчет можно просмотреть в личном кабинете или скачать в виде архива.

Так же в личном кабинете можно ознакомиться с результатами предыдущих проверок

Dr.WEB®
с 1992 года

Примеры выявленных связей



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Благодарим за внимание!

Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –
возникла проблема – набери DRWEB!

8-800-33-DRWEB

Убедитесь, что на ваших компьютерах нет вирусов

Dr.WEB®
с 1992 года

#CODEIB