Defendset

Описание программного продукта

версия 1.0.1.7

Оглавление

Общие сведения

Программа Defendset предназначена для защиты компьютера от вредоносных программ, выполнения несанкционированных операций над файлами и защиты данных.

Минимальные системные требования

- Процессор Intel Pentium 1 ГГц и выше (или совместимый аналог)
- 1024 МБ свободной оперативной памяти
- 40 МБ свободного места на жестком диске
- Подключение к Интернет (для активации и обновления)
- Операционная система Windows 7/8/8.1/10, Windows Server 2008/2012/2016

Функционал

Программа осуществляет предотвращение операций над файлами, копирование файлов при их изменении и регистрацию операций в журнале событий. Работа программы регламентируется правилами – совокупностью установленных параметров, санкционирующих взаимодействие процессов с заданными наборами файлов.

Параметры правила обуславливаются выбором типа защиты:

1. **Контроль операций**: файловые операции – создание, изменение, удаление, открытие (запуск); предотвращение операций (если выбран – операция блокируется).
2. **Сохранение версий** (версионирование): путь сохранения, интервал, количество копий, максимальный размер обрабатываемых файлов.

Общие параметры правила:

1. Пути (локации) – адреса наблюдаемых каталогов папок на жестком диске.
2. Маски – шаблоны поиска файлов.
3. Процессы-исключения – системные или доверенные приложения, не обрабатываемые правилом.

Под событием подразумевается ситуация, удовлетворяющей параметрам одного из правил – операция над файлом, находящимся в наблюдаемой локации и соответствующему заданной маске.

Операции

Создание

Создание нового файла.

- Создание нового файла в наблюдаемой локации.
- Копирование нового файла в наблюдаемую локацию.
- Перемещение файла в наблюдаемую локацию.
- Сохранение из приложения нового файла в наблюдаемую локацию.
- Восстановление файла из корзины в наблюдаемую локацию.

Изменение

Изменение существующего файла.

- Изменение имени файла в наблюдаемой локации.
- Копирование или перемещение файла поверх существующего файла в наблюдаемой локации.
- Запись в файл в наблюдаемой локации.

Удаление

Удаление существующего файла.

- Удаление в корзину файла из наблюдаемой локации.
- Непосредственное удаление файла из наблюдаемой локации.
- Перемещение файла из наблюдаемой локации.

Открытие

Открытие, запуск существующего файла.

- Чтение файла из наблюдаемой локации.
- Копирование файла из наблюдаемой локации.
- Перемещение файла из наблюдаемой локации.
- Запуск исполняемого файла из наблюдаемой локации.
- Открытие файла из наблюдаемой локации с ассоциированным приложением.

Исключения

Для более гибкой настройки в правиле предусмотрены исключения для следующих параметров:

Папки

Папки, исключаемые из наблюдаемого каталога (локации).

Маски

Шаблоны поиска файлов, не обрабатываемых правилом.

Процессы

Приложения, не обрабатываемые правилом (могут задаваться именем файла или маской).

Системные процессы

Исполняемые файлы из каталога операционной системы, а также исполняемые файлов запущенных от имени пользователей \NT AUTHORITY\SYSTEM и \NT AUTHORITY\LOCAL SERVICE

В целях безопасности из системных процессов исключаются:

- Исполняемые файлы из корневого каталога операционной системы Windows.
- Исполняемые файлы из каталога Windows\SysWOW64 в 64-битных системах.
- Файлы dllhost.exe, wscript.exe, cscript.exe, cmd.exe, powershell.exe.

Версионирование

Версионирование – сохранение копии файла после его модификации. Версионирование актуально, когда по каким-либо причинам невозможно обеспечить блокировку изменения файла, но при этом возникает потребность в восстановления его содержимого.

В зависимости от настроек, механизм позволяет восстановить содержимое файла, хранящееся в нем ранее от нескольких секунд, до нескольких месяцев.

Через две секунды после возникновения события «изменение» программа в соответствии с настройками предпримет попытку сохранить новую копию файла в специальную папку, предназначенную для хранения версий. В конец имени файла версии добавляется девятисимвольный временной штамп, позволяющий различать версии и ранжировать их по дате сохранения.

Чтобы избежать накопления идентичных версий, перед сохранением версии файла производится проверка хеш-кодов текущей и последней хранимой версии, если код совпадает, то сохранение версии не выполняется. К сожалению, не все приложения предоставляют уникальный хеш,

например, Microsoft Excel сохраняя один и тот же файл, вносит корректировки в его содержимое, поэтому одинаковые по содержанию файлы имеют разный хеш и будут сохраняются как разные версии файла.

Параметры настройки

Параметры настройки доступны в карточке правила, при выборе типа защиты «Сохранение версий»

Путь сохранения версий - папка, предназначенная для хранения версий файлов.

Интервал сохранения версии - временной промежуток после последнего удачного сохранения, в течение которого новая версия файла не сохраняется. Например, если значением интервал выбрано 30 мин., то следующая версия файла будет сохранена только по прошествии 30 минут.

Максимальное число версий – количество хранимых файлов версий. При сохранении новой версии, превышающей максимально допустимое число, будет удалена самая ранняя версия файла.

Обрабатывать файлы не более – наибольший размер файла для сохранения версий.

Следует помнить, что регулярное копирование больших файлов увеличивает нагрузку на дисковую подсистему, поэтому целесообразно ограничивать размер сохраняемых файлов.

Запись журнала и уведомление о событии оформляется специальным значком – часами. В случае возникновения ошибки цвет обводки часов красный. Текст ошибки отображается красным цветом.

Журнал событий

Обеспечивает регистрацию возникших событий. Содержит следующие реквизиты:

- **Дата** – дата и время возникновения события.
- **Операция** – операция, производимая над файлом.
- **Признак предотвращения** – показатель блокировки операции.
- **Имя файла** – имя файла события.
- **Имя пользователя** – имя пользователя операционной системы, под учетной записью которого возникло событие.
- **Процесс** – приложение операционной системы, выполняющее операцию.
- **Владелец процесса** – приложение операционной системы, запустившее процесс.

Лицензионная политика

Работа приложения обеспечивается лицензией. Без активной лицензии программа функционирует в ограниченном режиме, не предусматривающим предотвращение операций сохранения версий, все остальные возможности сохраняются в полном объеме.

Программа распространяется по принципу «попробуй перед тем, как купить». Для обеспечения пробного периода при установке пользователь получает пробную лицензию на 30 дней. Период действия пробной лицензии исчисляется с момента установки ПО. Во избежание злоупотреблений номер лицензии сопоставляется с идентификатором CPU рабочей станции, по которому при повторной установке восстанавливается первоначальная лицензия. Данный функционал не позволяет многократно переустанавливать программу, каждый раз получая новую 30-дневную тестовую лицензию.

Для использования программы в полнофункциональном режиме после пробного периода, необходимо активировать лицензию соответствующего типа.

Типы лицензий:

1. Домашняя – для личного использования в ОС Windows 7/8/8.1/10.
2. Корпоративная – для использования на предприятии в ОС Windows 7/8/8.1/10.
3. Серверная – для использования на сервере в ОС Windows Server 2008/2012/2016.

Количество компьютеров, на которых активируется лицензия, определяется количеством активаций, указанном при её приобретении. Период действия лицензии исчисляется с первой активации лицензии на любом из устройств.

Лицензия привязывается к аппаратной части компьютера, на котором функционирует программа. Для переноса лицензии на другой компьютер, либо при замене ключевых комплектующих компьютера, необходимо сначала выполнить деактивацию лицензию. При замене одной из ключевых компонент (кроме CPU), реактивация лицензии не требуется.

Учет лицензий ведется на сервере программы, поэтому для осуществления операций с кодом активации лицензии необходимо подключение к сети Интернет.

Программные модули

В приложении используются следующие обособленные программные модули:

Наименование	Назначение
Консоль настроек	Осуществление настроек для работы программы, просмотр журнала событий, обновление, работу с лицензиями.
Агент уведомлений	Вывод информационного окна о событиях, оперативное включение и выключение защиты, открытие консоли настроек, отображение текущего состояния защиты в системном лотке.
Сервис защиты	Предотвращение и регистрация событий согласно установленных настроек.