Outpost 7
Основы проактивной защиты

Технические заметки Agnitum

По мере роста количества и изощренности кибер-угроз прогрессивные антивирусные решения наращивают новые уровни защиты компьютера. Сегодня для эффективной защиты компьютера необходимо сочетать два подхода: реактивные методы (например, антивирус, спам-фильтры и веб-контент) и проактивные средства (брандмауэр и HIPS).

«Технические заметки Agnitum» рассказывают о проактивных средствах защиты, которые встроены в новом поколении программного обеспечения Outpost для безопасности персональных компьютеров.

Содержание

Содержание 1
Необходимость проактивной защиты 2
Виды проактивной защиты 3
Измерение эффективности 3
Показатели проактивной защиты 3
Outpost 7: продвинутая проактивная защита 4
Защита от утечек (Anti-leak, усовершенствовано в версии 7.0) 5
Защита системы (усовершенствовано в версии 7.0) 7
Защита приложений (новинка версии 7.0) 8
Защита файлов и папок (новинка версии 7.0) 9
Самозащита (усовершенствовано в версии 7.0) 9
Дополнительные возможности мониторинга (новинка версии 7.0) 10
Заключение 10

Необходимость проактивной защиты

Во-первых, ответим на вопрос: «Что такое проактивная защита и зачем она нужна?»

Однозначный ответ дать трудно, поэтому в целях данной статьи предлагаем определить проактивную защиту как набор профилактических мер, которые ограничивают сферу действий подозрительных или неизвестных приложений, предотвращая таким образом негативное воздействие на систему и укрепляя традиционные (реактивные) методы.

Проактивные инструменты защиты дополняют существующие реактивные инструменты путем определения правомерности тех или иных действий приложений и предотвращения их опасной деятельности. Например, вместо того, чтобы:

- проверять каждый файл или веб-страницу на наличие сомнительных элементов
- или проверять источник всех входящих сообщений электронной почты,

проактивная защита устанавливает определенные границы для действий, которые имеют право совершать незнакомые объекты в системе.

Реактивные инструменты защиты, такие, как классические антивирусы, работают на основе анализа отдельных файлов и сверки их с базой данных последних «сигнатур» известных вредоносных программ. Если соответствующий образец («образ файла») содержится в базе, антивирус сообщает, что файл действительно опасный, и он будет заблокирован или удален. И наоборот, если в базе нет образца, который соответствует инфицированному файлу, антивирус его не обнаружит. **Здесь вступает в игру проактивная защита** – она позволяет ограничить деятельность неизвестных объектов таким образом, что они не смогут нанести вред системе даже в тех случаях, когда мощный антивирус не смог сдержать распространение инфекции.

Десятки тысяч новых вредоносных программ появляются в Интернете каждый день, и на практике инструменты проактивной защиты оказываются необходимым дополнением для борьбы с неизвестными угрозами, которые могут привести к краже личных данных и другим потерям.

Виды проактивной защиты

Сегодня возможности проактивной защиты продуктов безопасности ассоциируются с модулями HIPS (системы предотвращения вторжений). Более консервативный и даже старомодный подход используют такие компании, как ESET, которая сводит проактивную защиту исключительно к возможностями эвристического обнаружения.

Являясь основой проактивной защиты, модуль HIPS управляет взаимодействием приложений друг с другом и с операционной системой. Модуль также позволяет пользователям определить политику доступа и создавать новые правила для новых приложений и процессов.

Превентивная концепция Outpost, впервые представленная в 2003 году, уже через несколько лет использовалась в программном обеспечении других производителей. HIPS и дополнительные проактивные компоненты расширили возможности Outpost по обеспечению безопасности ПК и усилили контроль над средой приложений, обеспечивая новый уровень защиты и возможностей конфигурации.

Измерение эффективности

Общепризнанных способов измерить эффективность проактивной защиты не существует, однако, в последние годы была проделана большая работа по стандартизации методов оценки. Сайт Matousec.com предлагает множество полезных инструментов тестирования для оценки отдельных компонентов проактивной защиты. С 2007 года Outpost занимает лидирующее положение в результатах сравнительных тестирований Matousec, и это не удивительно – Outpost всегда был направлен на защиту от неизвестных угроз.

Показатели проактивной защиты

В приведенной ниже таблице приведены результаты продуктов Agnitum в тестированиях Matousec.com за последние 3 года.

	Март 2008	**Июль 2008**	**Ноябрь 2008**	**Февраль 2009**	**Июнь 2009**	**Июль 2010**
Outpost Firewall Pro	91%	99%	89%	то же*	93%**	то же*
Outpost Security Suite	то же*	то же*	то же*	93%	92%	97%

*Отдельно не тестировалось

** Рейтинг присужден Outpost Firewall Free

Конечно же, в реальной жизни, лучшим мерилом эффективности превентивной защиты является отсутствие инфекции и целостность хранимых данных!

Outpost 7.0: продвинутая проактивная защита

Первым продуктом линейки Outpost, который предложил пользователям проактивную защиту, стал Outpost Firewall Pro версии 2.0, выпущенный в 2003 году. В то время он был одним из немногих продуктов на рынке, которые имели встроенные механизмы проактивной защиты. Конечно, многое с тех пор изменилось, но и сегодня Outpost опережает конкурентов по данному показателю, предлагает пользователям превосходный арсенал превентивных средств.

Рассмотрим спектр проактивной защиты Outpost подробнее:

Защита от утечек	•Компонент "Проактивной защиты". Контролирует поведение и реагирует на подозрительные действия активных приложений
Защита системы	•Компонент "Проактивной защиты". Обеспечивает автоматическую защиту целостности системы и приложений и возможность ее настройки.
Защита приложений	•Автоматически защищает критически важные данные (идентификаторы, пароли, журналы программ и т.д.) популярных интернет-приложений
Защита файлов и папок	•Предотвращает доступ к файлам и папкам, которые пользователи Outpost хотят защитить от стороннего вторжения
Внутренняя защита	•Обеспечивает непрерывную защиту Outpost, предотвращая несанкционированную деактивацию программы.
Монитор «Доступ к файлам и реестру»	•Обеспечивает расширенные возможности мониторинга событий и взаимодействия приложений в системе.

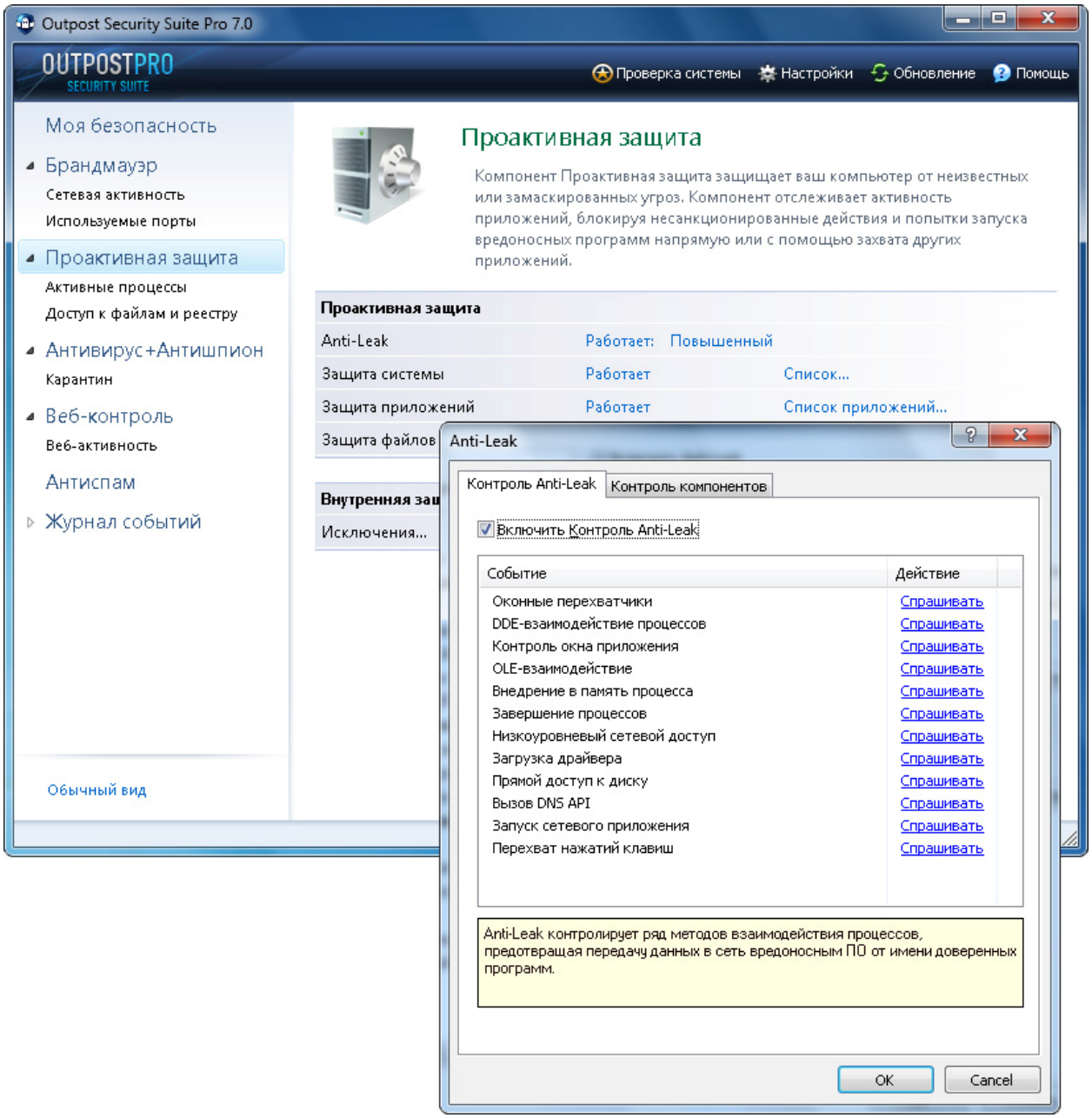
Защита от утечек (Anti-leak, усовершенствовано в версии 7.0)

В центре модуля "Проактивная защита" – функциональность, защищающая от утечки данных. Этот проверенный временем механизм, многие годы приносящий брандмауэру Agnitum наивысшие оценки в тестированиях на предотвращение утечки данных и сравнительных испытаниях на предмет защиты от атак, охраняет систему пользователя от изощренных способов вторжения и активности вредоносного ПО. Outpost Pro Anti-Leak контролирует множество аспектов сетевой активности, таких, как:

- целостность приложений (исполнимые файлы и общие компоненты)
- целостность памяти
- целостность Интернет-обозревателей
- произвольная установка системных и сетевых драйверов
- активность файловой системы
- доступ к устройствам

Анализируя все виды активности, Outpost Pro обеспечивает невозможность выполнения неправомочных сетевых операций. Этот модуль предотвращает активацию вредоносного кода, принадлежащего подозрительным или неизвестным видам вредоносного ПО. Способ действия модуля прост: как только обнаруживается новый вид активности, пользователь получает уведомление-запрос на разрешение или запрет такой активности.

Для помощи пользователю в принятии данного решения используются заранее настроенные правила доступа, а также система ImpoveNet, с помощью которой возможно решить каждый конкретный случай автоматически, основываясь на опыте других пользователей.



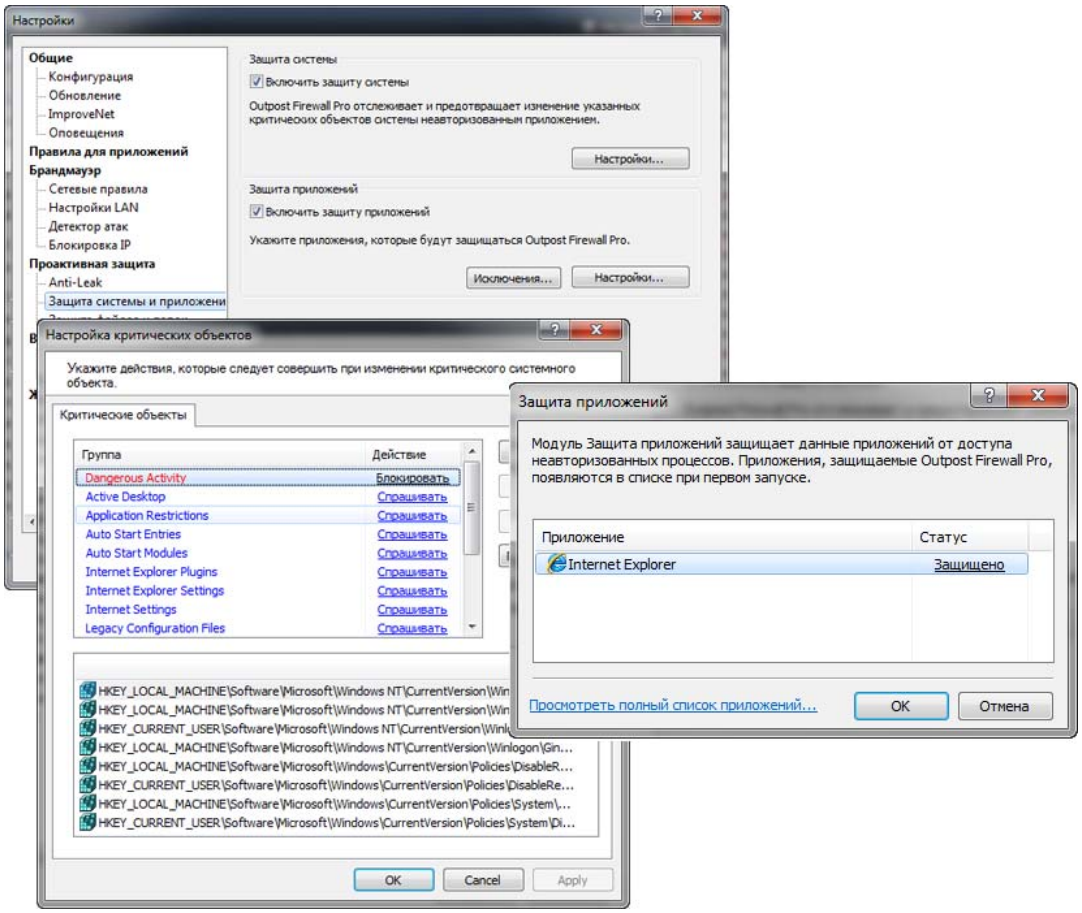
Проактивная защита контролирует многочисленные события и операции на ПК и блокирует несанкционированную активность.

Защита системы (усовершенствовано в версии 7.0)

Обновленный модуль "Защита системы" предоставляет пользователю расширенные возможности контроля над системной активностью и событиями. С его помощью вы можете заблокировать от неавторизованного доступа и модификации определенные объекты, такие как:

- настройки реестра;
- настройки сети;
- отдельные файлы;
- программы из автозапуска.

Хотя этот функционал в большей степени нацелен на опытных пользователей, он предоставляет гибкие возможности конфигурирования в целях защиты системы. Менее искушенные пользователи Outpost 7 оценят предустановленные параметры "Защиты системы", которые позволяют работать с модулем без дополнительной настройки.



"Защита системы" контролирует целый спектр системных событий.

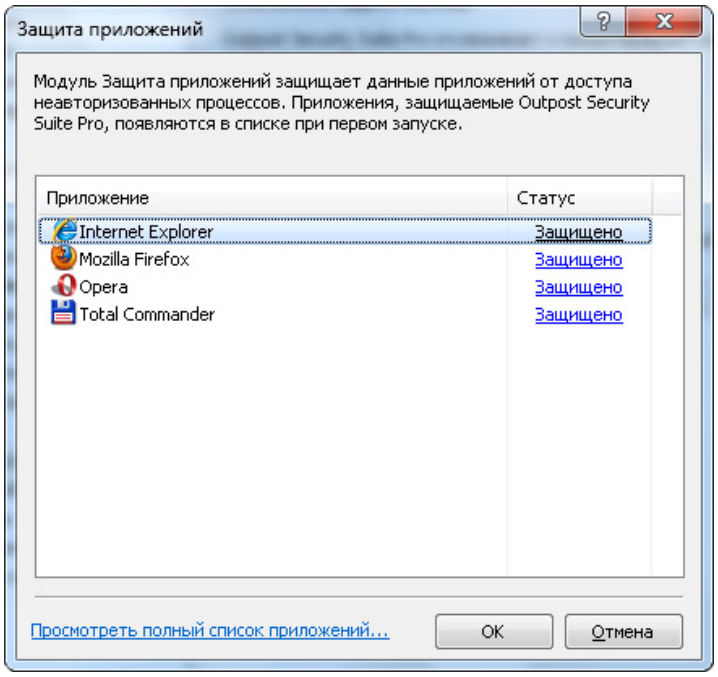
Защита приложений (новинка версии 7.0)

Эта новая функциональность автоматически защищает внутреннюю структуру уязвимых Интернет-приложений таким образом, чтобы предотвратить кражу или злонамеренное изменение приватных данных вредоносным ПО.

Модуль защищает такие ключевые объекты, как:

- регистрационные пароли и автоматически запомненные данные, сохраняемые Интернет-обозревателями;
- адресные книги почтовых клиентов;
- историю чатов Интернет-пейджеров;
- содержимое электронных кошельков;
- множество других подверженных риску и потенциально уязвимых приложений, список которых регулярно обновляется.

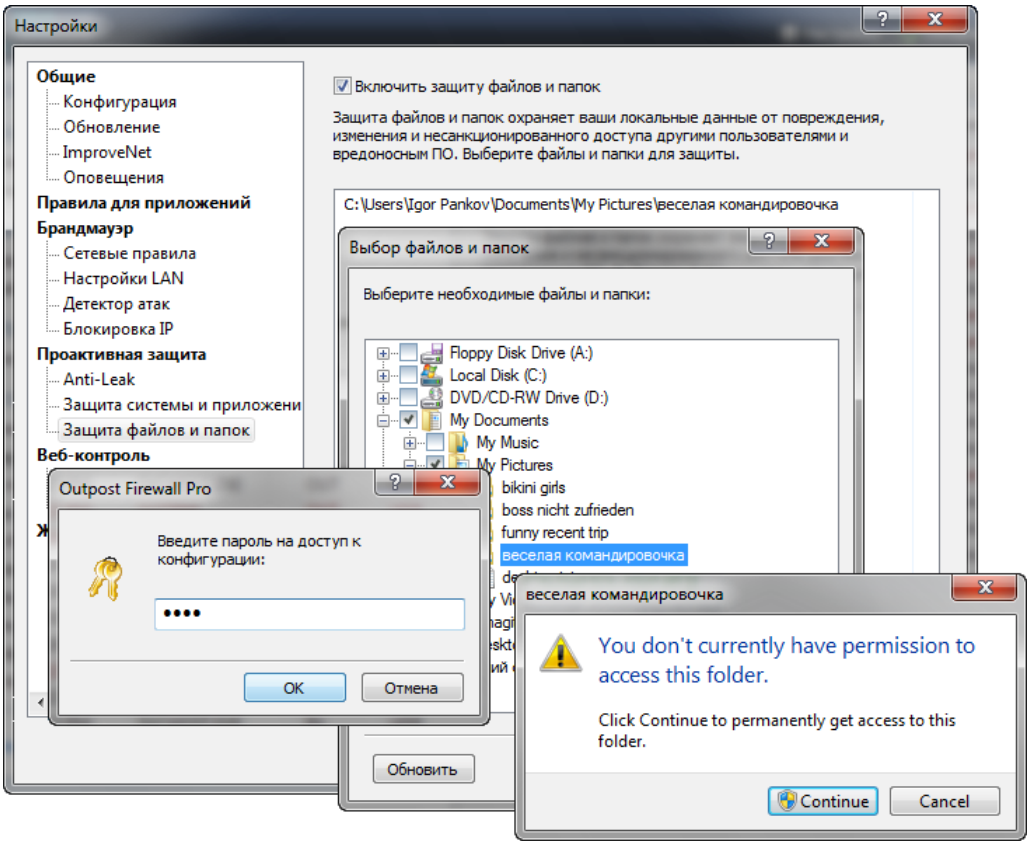
Защищая эти и другие уязвимые компоненты приложений, Outpost 7 предотвращает непреднамеренное разглашение частных данных и кражу финансовой информации и обеспечивает приватность просмотра веб-страниц. В любой момент, когда вы запускаете связанное с Интернетом приложение, данные, генерируемые этим приложением, автоматически защищаются, и вы можете быть уверены, что не станете жертвой веб-угроз.



"Защита приложений" автоматически защищает наиболее известные Интернет-приложения от вторжений и саботажа.

Защита файлов и папок (новинка версии 7.0)

Новая функциональность защиты папок направлена на блокировку доступа к заранее выбранным папкам и файлам на вашем компьютере. Таким образом, вы не только ограждаете свою частную жизнь от возможного вмешательства других пользователей общего компьютера, но и имеете возможность закрыть содержание той или иной папки от вездесущего вредоносного ПО. Если вы храните конфиденциальную информацию на ПК, задумайтесь о том, чтобы скрыть ее от кого-либо или чего-либо, например, от неопределяемых вирусов и троянцев, которые могут в противном случае получить доступ к вашим секретам.



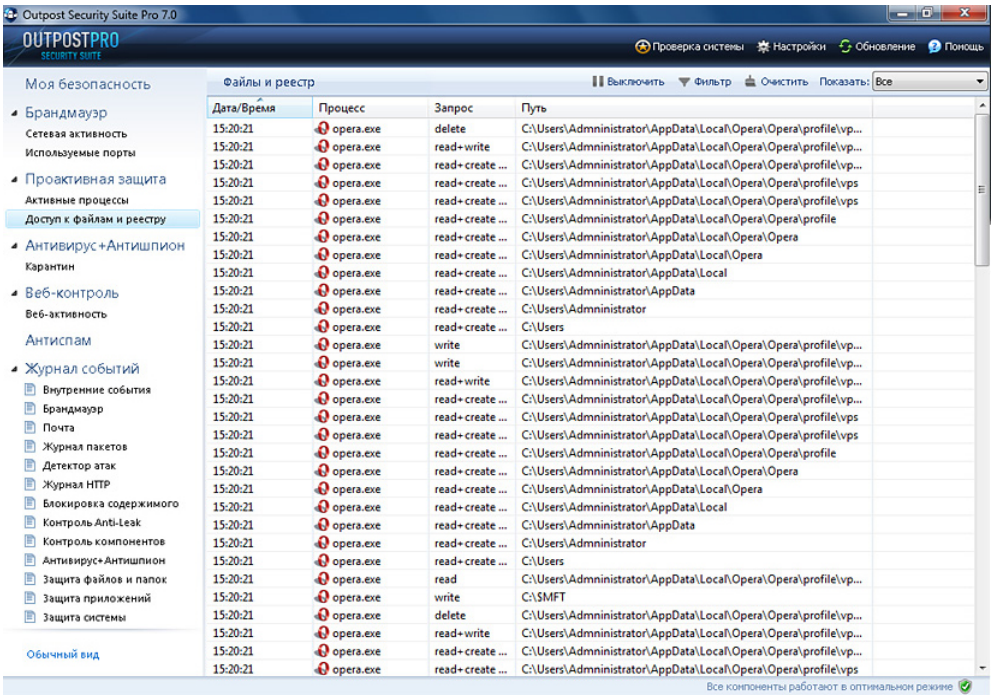
"Защита файлов и папок" защищает определенные локации о нелегального или несанкционированного доступа.

Самозащита (усовершенствовано в версии 7.0)

Роль модуля самозащиты в рамках проактивной защиты трудно переоценить. При этом принцип ее работы очень прост: модуль "Самозащита" контролирует функционирование Outpost, не позволяя кому-либо и чему-либо, кроме авторизованного пользователя, отключить активную защиту продукта. Имея своей целью обеспечение бесперебойной работы Outpost, модуль "Самозащита" получил заслуженное признание и высшие баллы в тестах на деактивацию защиты, проводимых лабораторией Matousec.

Дополнительные возможности мониторинга (новинка версии 7.0)

Для детального анализа системной активности на ПК вы можете воспользоваться введенным в версии 7.0 инструментом "Монитор файловой и реестровой активности", который предоставляет данные о состоянии реестра и историю операций с файлами в режиме реального времени для любого избранного процесса. Выберите любое запущенное приложение и опцию “Просмотреть активность” для данного объекта – вы увидите подробный список связанных с процессом событий по мере их возникновения. Этот инструмент делает мониторинг и анализ системы более удобным для системных администраторов и опытных пользователей.



"Монитор файловой и реестровой активности" позволяет отслеживать активность любого процесса в реальном времени, включая системные модификации и взаимодействие с другими программами.

Заключение

Проактивная защита в продуктах Интернет-безопасности становится скорее насущной необходимостью, чем приятным дополнением, так как она противостоит угрозам, с которыми традиционные средства защиты не справляются. Outpost как одно из лидирующих решений в области превентивной защиты предлагает расширенный современный функционал для обеспечения безопасности ПК в виду угрозы изощренного и трудно определяемого вредоносного ПО.

Загрузите Outpost Security Suite или Firewall Pro сегодня, обезопасив свои цифровые данные, и убедитесь в эффективности превентивной защиты продуктов Agnitum!