



# Outpost Pro 7.5

## Технология SmartDecision –

Ваш советчик в вопросах безопасности

### Содержание

Введение .....	2
О продуктах Outpost Pro .....	2
О технологии SmartDecision.....	3
Для чего нужна SmartDecision .....	3
Многоуровневая система оценки рисков .....	4
Критерии классификации файлов.....	4
Как работает SmartDecision .....	4
Окна диалогов с подсказками.....	5
Отправка подозрительных файлов .....	6
Интеграция с Outpost 7.5 .....	7
Ограничения .....	7
Дальнейшее развитие технологии SmartDecision .....	7

## Введение

### *О продуктах Outpost Pro*

Outpost Pro – это линейка продуктов по безопасности, предлагаемая компанией Agnitum для круговой защиты ПК и отличающаяся минимальным воздействием на системные ресурсы. Outpost Pro включает антивирус Outpost Antivirus Pro и брандмауэр Outpost Firewall Pro, а также комплексный продукт по безопасности Outpost Security Suite Pro.

Многоуровневую защиту флагманского продукта Outpost Security Suite Pro обеспечивают следующие компоненты:

1. **Антивирус + Антишпион** для борьбы с вирусами, червями, троянами, шпионским и рекламным ПО, руткитами;
2. **Брандмауэр** для защиты сетевых соединений;
3. **Проактивная защита** для предотвращения новых и ранее неизвестных угроз;
4. **Веб-контроль** для безопасного нахождения в Интернете;
5. **Антиспам** для защиты почтового ящика от нежелательной почты.

С 2006 года в продуктах Outpost внедрена уникальная "облачная" система ImproveNet, благодаря которой осуществляется сбор и распространение часто используемых (проверенных компанией Agnitum) конфигураций продуктов Outpost среди пользователей.



## ***О технологии SmartDecision***

Технология SmartDecision впервые представлена в продуктовой линейке Outpost Pro 7.5 – Performance Edition в 2011 году. SmartDecision осуществляет бессигнатурный статический анализ файлов и процессов перед запуском в соответствии с заданным набором критериев. Технология SmartDecision призвана помочь пользователям в вопросах безопасности и выполняет роль личного советчика, предлагая вниманию пользователя визуальные подсказки-рекомендации, выделенные цветами светофора – красным, желтым или зеленым.

Также SmartDecision позволяет отправлять подозрительные файлы на проверку в лабораторию компании Agnitum непосредственно из интерфейса приложения.

## ***Для чего нужна SmartDecision***

Технология SmartDecision реализована в продуктах Outpost, чтобы усилить проактивную составляющую защиты, а также в доступной форме пояснить пользователю действия продуктов.

Антивирусное ядро, входящее в состав Outpost Pro, сканирует каждое запускаемое приложение и проверяет его на наличие в системе ImproveNet. В "облачной" базе ImproveNet хранится информация о доверенных приложениях, ранее отправленная участниками сообщества Outpost и проверенная вирусной лабораторией Agnitum. В случае, когда антивирус не детектирует приложение как "Недоверенное", а ImproveNet – как "Доверенное", привлекается технология SmartDecision для анализа файла "на лету". В соответствии с результатами анализа вниманию пользователю предлагается подсказка-рекомендация о возможных дальнейших действиях – разрешить или заблокировать активность приложения.

Для многих пользователей вопрос о том, как поступить с неизвестным файлом, является непростым. Технология SmartDecision призвана помочь в принятии решений по безопасности, выступая в качестве Вашего личного советчика. Визуальные оповещения красного, желтого или зеленого цвета позволят Вам быстро среагировать на угрозу и предотвратить заражение ПК.

## Многоуровневая система оценки рисков

В технологии SmartDecision применяется многоуровневая система оценки рисков с заданным набором критериев для проверки надежности файлов. Предлагаем Вашему вниманию список критериев, созданный вирусными аналитиками компании Agnitum на основе многолетнего опыта с целью противодействия потенциальным угрозам.

### *Критерии классификации файлов*

- Стандартные (тип и размер файла, цифровая подпись и т.д.);
- Системно-зависимые (дата создания, файловые атрибуты и т.д.);
- Локационно-зависимые (имя файла и каталога, присутствует ли файл в разделе автозапуска, присутствует ли файл в соответствующем разделе деинсталляции и т.д.);
- Структурно-зависимые (соответствие между расширением файла и его структурой, используется ли для сжатия файла так называемый ехе-пакер, размер таблицы импорта файла, проверка заголовка запускаемого файла и т.д.);
- Критерии, определяемые взаимодействием с системными компонентами (анализ используемых API-функций операционной системы Windows).

Эти и многие другие атрибуты вносят вклад в усиление защитных свойств продуктов Outpost против новых и ранее неизвестных угроз.

### *Как работаем SmartDecision*

Технология SmartDecision оценивает рейтинг любого запускаемого файла. Каждый параметр из вышеприведенного списка обладает заданным "весом", и сумма "весов" всех критериев определяет общий рейтинг файла.

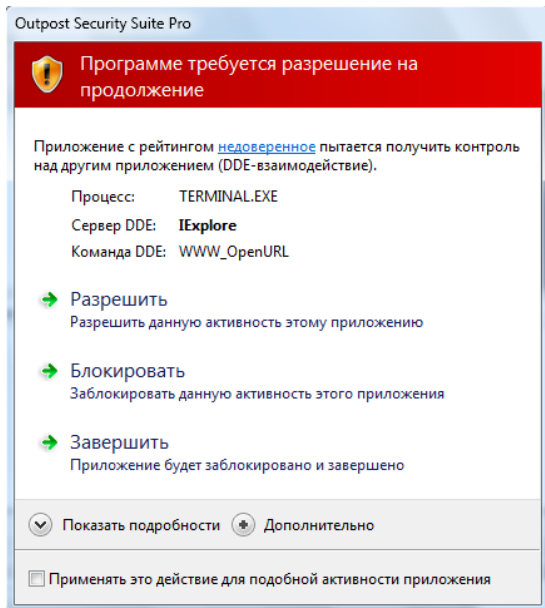
Возможные типы рейтинга (в порядке возрастания риска):

1. Доверенное (уведомление зеленого цвета);
2. Хорошее (уведомление зеленого цвета);
3. Умеренно-подозрительное (уведомление желтого цвета);
4. Подозрительное (уведомление желтого цвета);
5. Недоверенное (уведомление красного цвета).

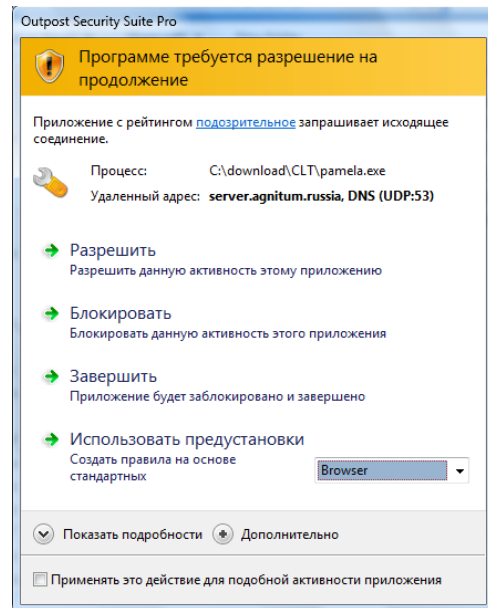
В соответствии с рейтингом приложения пользователю предлагается подсказка по дальнейшим действиям красного, желтого или зеленого цвета.

## Окна диалогов с подсказками

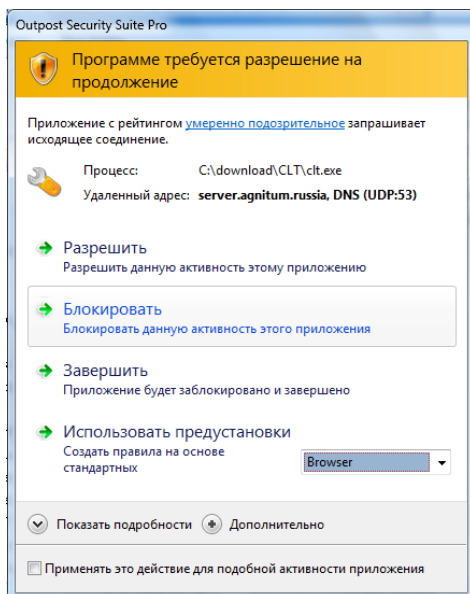
SmartDecision определяет уровень благонадежности каждого приложения и отображает информацию в соответствующем диалоге с подсказками. Значения отдельных критериев, например, название процесса, дата создания, атрибуты и размер, также отображаются в окне диалога. Красное оповещение соответствует файлам с рейтингом "недоверенное", желтое – "подозрительное" или "умеренно-подозрительное", зеленое – "хорошее" или "доверенное".



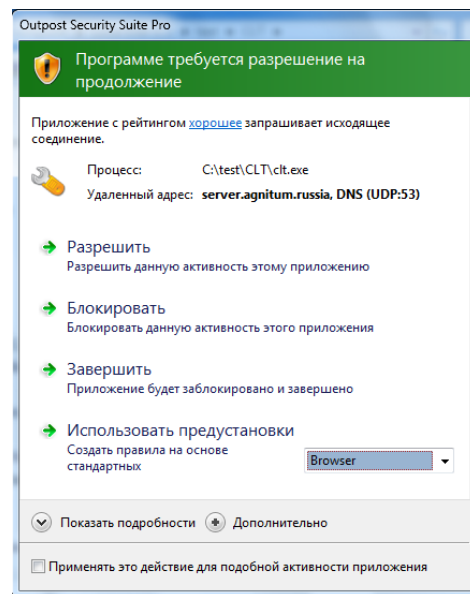
Красное уведомление – рейтинг "недоверенное".



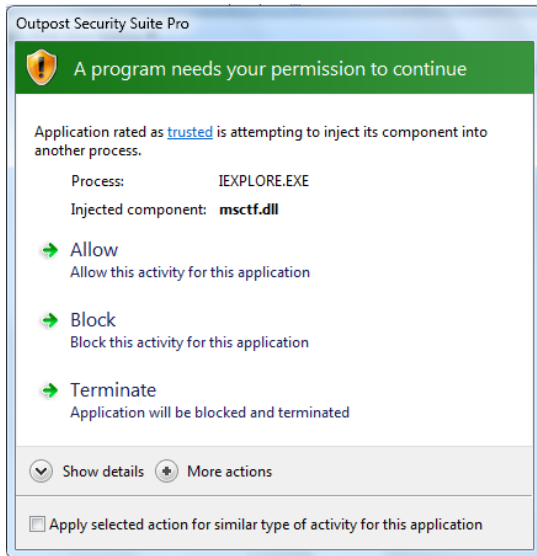
Желтое уведомление – рейтинг "подозрительное".



Желтое уведомление – рейтинг "умеренно-подозрительное".



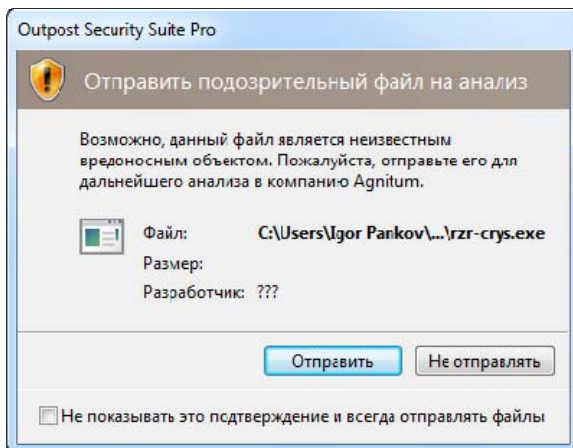
Зеленое уведомление – рейтинг "хорошее".



*Зеленое уведомление – приложение с рейтингом "доверенное".*

## Отправка подозрительных файлов

Функциональность Outpost 7.5 включает возможность отправки подозрительных файлов на проверку напрямую из интерфейса продуктов. С помощью этой опции любой пользователь может внести вклад в расширение защитных свойств Outpost, отправив информацию о новых сетевых приложениях и вредоносных программах инженерам компании Agnitum.



*Отправка подозрительных файлов в лабораторию Agnitum*

## Интеграция с Outpost 7.5

Технология SmartDecision тесно интегрирована с модулями проактивной защиты и брандмауэра:

- **Запуск приложений** – для анализа приложений перед запуском;
- **Оповещения режима обучения** – в помощь при создании правил проактивной защиты и брандмауэра;
- **Режим автообучения** – для быстрой реакции на новые файлы или процессы (разрешить/блокировать) без вовлечения пользователя.

## Ограничения

Оповещения, предлагаемые технологией SmartDecision, носят рекомендательный характер и призваны помочь пользователям в принятии решений по вопросам безопасности.

Реализация SmartDecision не исключает ложных срабатываний, которые возможны в следующих случаях:

- 1) анализируемый код приложения не удовлетворяет некоторым стандартам, например, для случаев, когда используются шифровальщики и пакеры;
- 2) код приложения изменен сторонним продуктом (например, крякером или неизвестным дополнением), что привело к нарушению цифровой подписи.

## Дальнейшее развитие технологии SmartDecision

На сегодняшний день технология SmartDecision представляет собой огромный шаг в развитии проактивной защиты, который призван упростить взаимодействие пользователя и продукта в вопросах безопасности.

Компания Agnitum постоянно расширяет набор критериев классификации файлов, чтобы обеспечить надежную защиту Вашему ПК. В рамках улучшений технологии SmartDecision запланирована реализация поведенческого анализатора. Станьте подписчиком сайта <http://www.agnitum.ru/news/rss.php> и блога компании Agnitum на <http://www.internet-security.ru/> и следите за нашими новостями!