



Outpost Pro 7.5

SmartDecision Technology – Your Personal Virus Adviser

Contents

Introduction	2
What is Outpost Pro?	2
What is SmartDecision?	3
Why SmartDecision?	3
Multi-level risk evaluation.....	4
Criteria for file classification.....	4
How does SmartDecision work?	4
Prompt dialogs	5
Suspicious file submission	6
Integration with Outpost 7.5.....	7
Disclaimer	7
Future SmartDecision development	7

Introduction

What is Outpost Pro?

Outpost Pro is Agnitum's line of Internet security products designed for all-round PC protection with minimal system impact. The product line includes the standalone [Outpost Antivirus Pro](#) and [Outpost Firewall Pro](#), as well as the all-in-one [Outpost Security Suite Pro](#).

The flagship Outpost Security Suite Pro's multi-layered protection is provided by the following key components:

1. **Combined anti-virus and anti-spyware** detection to keep viruses, worms, Trojans, spyware, rootkits, and adware out of your PC.
2. **Two-way firewall** to secure PC connections.
3. **Proactive protection** to prevent new and unknown threats.
4. **Web control** for fast, safe web surfing.
5. **Anti-spam** to keep your inbox clean of unsolicited emails.

Since 2006, Outpost products have also included Agnitum's unique cloud-based ImproveNet that uses data from the Outpost user community to help provide comprehensive PC protection.



What is SmartDecision?

Introduced in Outpost Pro 7.5 in 2011, SmartDecision performs non-signature static analysis for files and processes before launch by checking executable files for credibility against a certain number of criteria for file classification. Aimed at helping users to make the best security decisions, SmartDecision acts as a personal Virus Adviser by providing visual, intuitive recommendations along with a corresponding alert color – red, yellow or green. In addition, SmartDecision includes the automatic submission of suspicious files directly from the product to Agnitum's Virus Lab for analysis.

Why SmartDecision?

SmartDecision technology has been implemented in order to enhance the proactive protection aspect of the products and clearly explain what the products are doing.

Outpost Pro scans each executed application using its antivirus engine and checks whether an application is already covered in ImproveNet. ImproveNet is the cloud-based system of known legitimate applications submitted by the Outpost user community and verified by Agnitum engineers. If the antivirus engine does not recognize this application as “Bad” and ImproveNet does not recognize it as “Good”, SmartDecision steps in to conduct an on-the-fly analysis of the file. According to the results of the analysis, the user will receive advice on how to proceed – allow or block this application’s actions.

Without SmartDecision it can be a challenge for users to decide what to do about an unknown file, no matter whether you’re a home user or an IT professional. SmartDecision technology is designed to be your Personal Virus Adviser, ready to help whenever uncertainty arises. Visual recommendations in red, yellow or green colors are easy to understand, so you can quickly and easily react to keep your PC safe.

Multi-level risk evaluation

SmartDecision technology uses a comprehensive risk-evaluation system with a set of criteria to define whether a file is good or potentially dangerous. To give you a general idea of how SmartDecision performs, here are some of the criteria created by Agnitum's virus analysts over the years which have proved to be effective in confronting potential threats.

Criteria for file classification

- Standard (file type, file size, digital signature evaluation, etc)
- System-specific (date of creation, file attributes, etc)
- Location-specific (folder and file name, whether a file is present in the autorun section, whether a file is present in the corresponding uninstall section, etc)
- Structure-specific (matching between file extension and its structure, whether a file is compressed with a so-called "exe packer", file import size, header of the executable file validation, section name evaluation, etc)
- Interaction-specific (analysis of used Windows API functions, etc)

These and many more attributes contribute to make Outpost detection of new and unknown threats robust and powerful.

How does SmartDecision work?

SmartDecision analyzes an executable file and calculates its overall 'safety score'. Each parameter from the above list has its own weight and the overall score is defined as the sum of the weights of all the criteria.

The following scores are possible (in order of increasing risk):

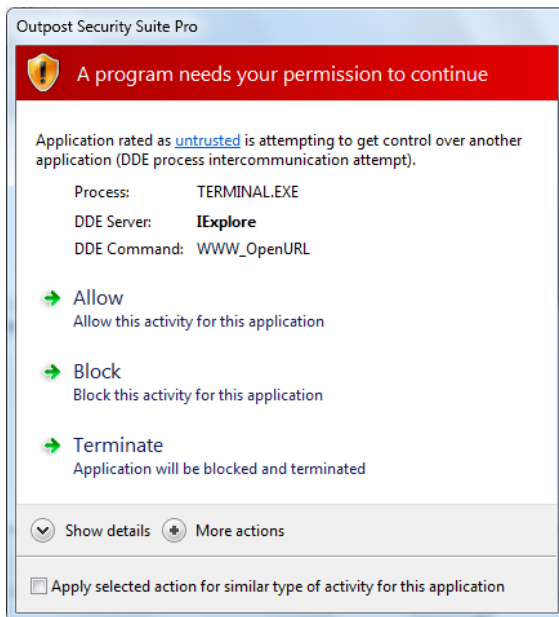
1. Trusted (green)
2. Good (green)
3. Moderate (yellow)
4. Suspicious (yellow)
5. Untrusted (red)

According to the overall rating, the user is notified by a visual recommendation with the matching color – green, yellow or red – and can choose how to proceed.

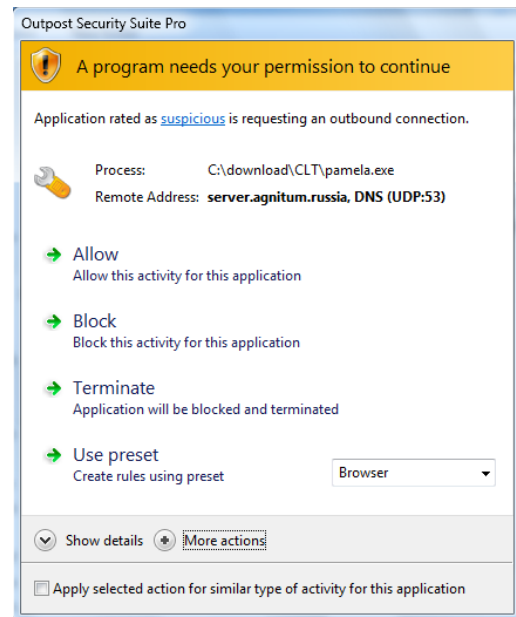
Prompt dialogs

SmartDecision detects the level of safety for each requesting application and displays the corresponding information in the prompt dialog. Some of the evaluation criteria, including process name, folder, date of creation, attributes and size, are also displayed.

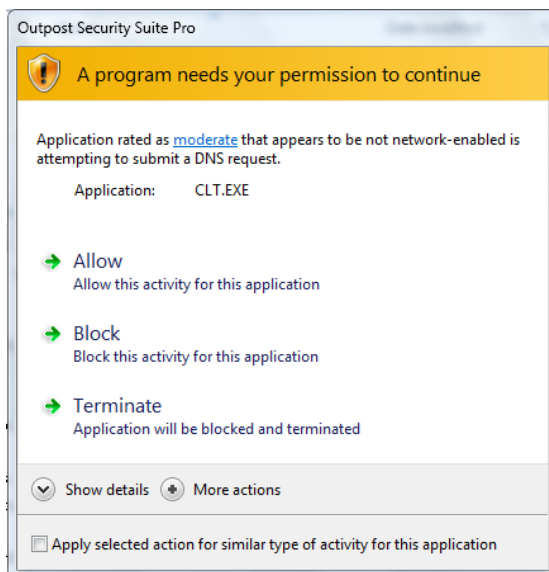
Red dialogues indicate files rated as untrusted, yellow as suspicious or moderate, and green as good or trusted.



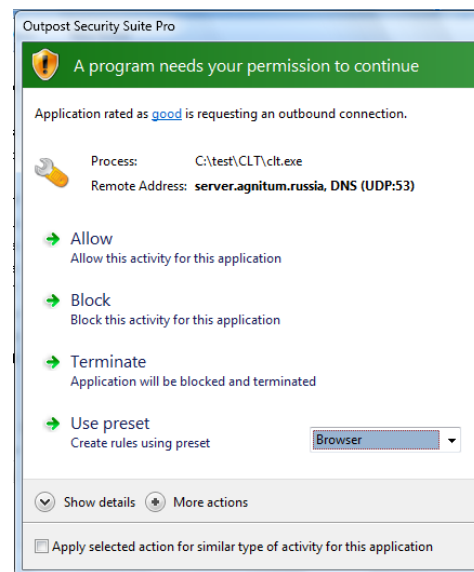
SmartDecision alert. Red – files rated as untrusted.



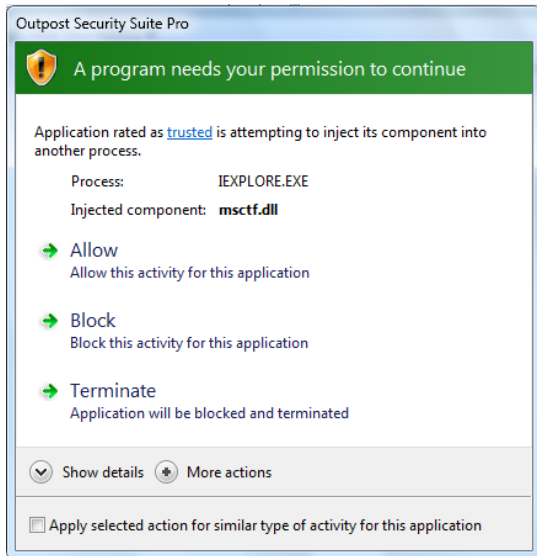
SmartDecision alert. Yellow – files rated as suspicious.



SmartDecision alert. Yellow – files rated as moderate risk.



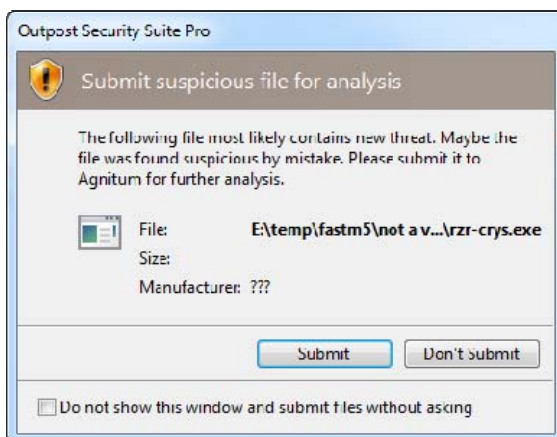
SmartDecision alert. Green – files rated as safe.



SmartDecision alert. Green – files rated as trusted.

Suspicious file submission

Outpost 7.5 now enables you to automatically submit suspicious files for analysis directly from the action request window. We encourage all users to help us expand our protection capabilities and let other Outpost users benefit from enhanced PC security as well by participating in this community process.



Pop-up dialog to send a file to Agnitum's analysts

Integration with Outpost 7.5

SmartDecision technology is closely integrated with the Outpost firewall and proactive protection modules:

- **Application launch** – to analyze applications before they are executed.
- **Rules Wizard alerts** – to help in creating Proactive Protection and Firewall rules.
- **Auto-Learn mode** – to effectively block or allow new files/processes without requiring a user decision.

Disclaimer

SmartDecision notifications are recommendations only, designed to assist users with decision-making, based on static criteria analysis, and should not be relied upon alone for critical decision-making.

SmartDecision implementation does not completely exclude false positives that may occur when, for example:

- 1) analyzed software code does not meet some standards, including using of encryptors and packers;
- 2) software code is changed by third-party software (like “cracks” or unofficial add-ons), e.g. software has corrupted digital signature.

Future SmartDecision development

SmartDecision technology is today a great step forward in proactive protection, simplifying user interaction by making the security decision-making process more simple and transparent.

We are continually expanding the criteria for file classification to ensure robust PC protection; the next enhancement is expected to include a dynamic behavioral analyzer. Follow our blog at <http://agnitumblog.blogspot.com/> to learn more about this exciting development as it happens!