



Anti-Malware Technology in Outpost Security Suite Pro

Saves you time by scanning faster!

Abstract

This document details the new technologies in Outpost Security Suite Pro that help to effectively combat malicious programs without slowing down system performance.

Introduction

Outpost Security Suite Pro incorporates a dedicated anti-malware module that, unlike traditional anti-virus or anti-spyware, protects against multiple threat types: viruses, spyware, botnet-generating Trojans, rootkits, and more. The module is optimized to deliver faster scanning without disrupting normal activity.

Two engines, one comprehensive scanner

The anti-malware module in Outpost Security Suite Pro extends the anti-spyware and anti-Trojan technology in Outpost Firewall Pro through the inclusion of a dedicated antivirus engine. The combined anti-malware scanner delivers two discrete malware-fighting mechanisms updated by two independent expert research teams working together to deliver seamless protection against today's blended threats.

Licensed from Virus Buster of Hungary, the antivirus engine has won many awards and is certified by West Coast Labs, ICSA Labs and Virus Bulletin (click [here](#) to learn more).

When the anti-malware scanner checks for malicious programs, it uses both engines simultaneously to locate and remove threats. The malware definition updates are consolidated and delivered daily to ensure continuous up-to-date protection.

Scan performance gains

Most security products offer protection against viruses and other malicious programs by scanning for the presence of viral code. Essentially, this involves zeroing in on each object on the drive being scanned and comparing it against a set of known malware fingerprints extracted from past threats.

Comparing a file against a large database of malware definitions takes time and system resources. If the computer being scanned also contains a large number of files, as many of today's huge hard drives do, the task of checking the entire computer can be extremely time-consuming.

For most users, however, relatively few of the files on their hard drive are changing on a daily basis. So the typical daily scan is going over a lot of unnecessary old ground. Outpost Security Suite Pro calls upon the new SmartScan technology to take a more intelligent approach by scanning only those objects that have changed in some way since the last scan, resulting in much faster scans and far less system resource usage.

How SmartScan works

SmartScan can substantially reduce the amount of time needed to scan a system that has been scanned at least once before by Outpost's anti-malware module. This optimization is attained through the use of cache files that store information about the status of the last scan performed on each object. If the object has not changed since the last scan, it is excluded from subsequent scans. The memory-resident scanner also makes use of SmartScan technology: if a new application is loaded into memory, it is checked only if it has not previously been validated or has changed since the last execution. This not only increases real-time scanning speeds, making the system more responsive, but also speeds up boot times.

Technical implementation

During the initial scan, Outpost Security Suite Pro creates two auxiliary index files in each folder - OP_CACHE.ATR and OP_CACHE.IDX. These files are hidden from directory listings to make them as resistant as possible to tampering. These files are also protected by Outpost's Self-Protection function that ensures Outpost components cannot be accessed, modified or disabled by unauthorized programs.

In order to keep track of past scan results, Outpost updates the internal registry of those index files with data such as which files in a folder have been checked before and when, the date of the last modification of files, and other maintenance information. The scanner retrieves information from these files on the status of past anti-malware scans of all elements belonging to any given folder.

Any previously-checked object will remain excluded from further scans as long as its contents don't change or your malware signatures have not been updated. Otherwise, the cache files will be reset and the object will lose its privileged "clean" status, triggering a mandatory check on the next scan.

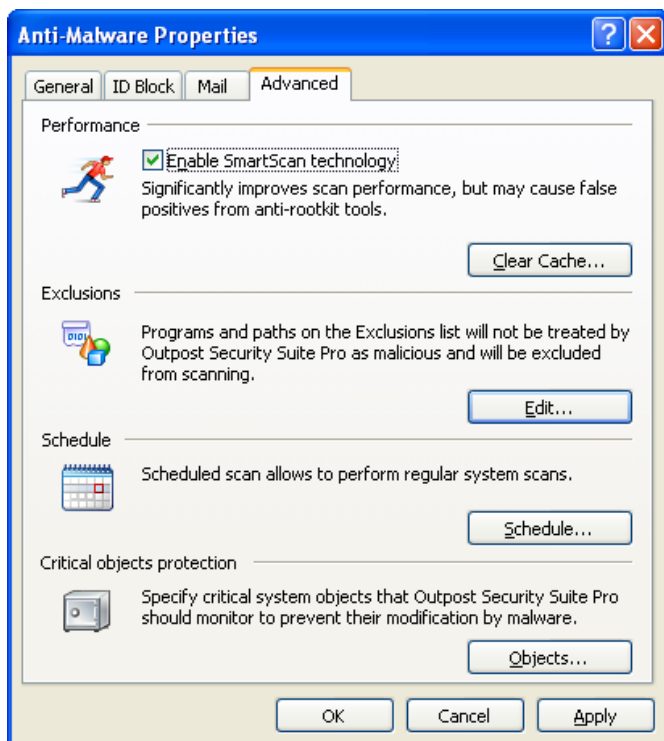
Unlike other popular anti-malware products using superficially-similar caching technologies, SmartScan supports all types of PC file systems, not just NTFS.

The performance benefits of SmartScan technology are summarized in chart form at the end of this document in Appendix 1.

Using SmartScan

You can activate the use of SmartScan in the Configuration Wizard after the installation of Outpost Security Suite Pro. Alternatively, SmartScan properties can be accessed at any time by following these steps: 1) Click Options on the Outpost interface and go to Plug-Ins Setup. 2) Select the Anti-Malware Plug-in. 3) Click on the Advanced tab. 4) Check the box labeled Enable SmartScan technology as shown below.

You can purge the cache files at any time by clicking the Clear Cache button. These files are automatically removed after Outpost is uninstalled.



A note on anti-rootkit tools: Cache files have read-only attributes and may not be visible with the use of conventional file managers such as Windows Explorer. Some anti-rootkit software may report cache files as suspicious because the methods of hiding contents to prevent malware abuse may be seen as characteristic of rootkits. Unfortunately, because anti-rootkits work in different ways, it's not possible for us to 'flag' the Outpost cache files as harmless, but you can rest assured that they are indeed quite safe.

Resident scanner optimization

If a malware-infected file is opened, the risk of the infection activating and spreading is huge. Fortunately, this risk does not arise if the file is simply copied, renamed or its properties viewed; the payload will only be activated if the file is executed.

Outpost Security Suite Pro offers users a choice as to how they prefer the anti-malware component to check program activity in real time: on access or on execution. The latter will clearly result in faster performance.

- **Check files on execution.** This prevents malicious programs from launching and scans files only if they are opened. Other file access commands such as copying or viewing a file's properties or displaying folder contents are not impacted by this selection.
- **Check files on access.** This mode will trigger a malware scan if any type of file access is attempted.

Benefits

This approach delivers tailored protection for everyone. Some people only feel safe if they check every window and door in their house every day - for those users, on-access file checking makes sense for maximum peace of mind. Others are happy to just check when there's real potential for risk, and for those users, checking files on execution is the better choice.

Technical implementation

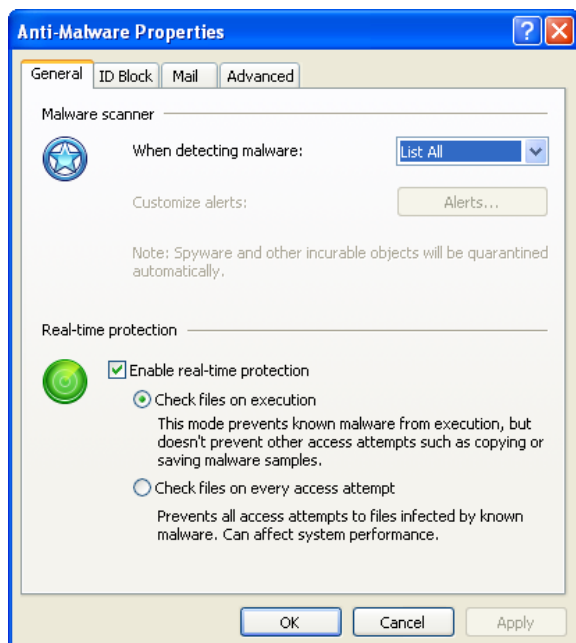
In on-execution mode, Outpost Security Suite Pro intercepts loading of modules responsible for code execution. This code is thoroughly checked by the anti-malware plug-in before it is permitted to establish control. This mode checks both executable program files and document files (like Word or Excel) that have the potential to contain macro commands and other 'hidden executable' code. It does not, however, check files for viruses during copy or save operations.

In on-access mode, all attempts to access the file are intercepted. This ensures that access to files that are not normally designed to contain program code but that may have been exploited by a vulnerability are also monitored and secured.

Selecting the appropriate mode

To select the appropriate mode:

1) Select the Anti-Malware Plug-in from the Outpost Options menu. 2) Click on the General tab. 3) Check the box labeled Enable Real-time Protection and then click the appropriate radio button for the desired mode of operation, as shown below.



Summary

Outpost Security Suite Pro's new combination of anti-malware module with SmartScan technology is constantly on guard against all possible risks. It scans quickly and accurately, reduces the load on system resources, activates only when necessary, and is very easy to use. For further information and to download a trial copy, go to <http://www.agnitum.com/products/security-suite/index.php>.

Appendix 1: Performance Chart

