

# Why Anti-Spyware from Agnitum?

## The rising threat of spyware

Spyware is a growing problem that has affected many personal computer users. In its study, the National Cyber Security Alliance estimates that 9 out of 10 PCs connected to the Internet are infected with spyware.

Although detailed definitions of spyware remain somewhat blurred, it is generally agreed that the spyware 'label' covers any software that:

- installs itself surreptitiously, without the user's knowledge or consent
- makes modifications to existing software or the internal configuration of the operating system
- may display unsolicited ads
- can allow sensitive user information to be extracted from the computer

Spyware evades conventional security tools such as anti-virus and basic firewalls, and its removal requires specialized technology not provided by these more general tools. Spyware is designed to operate covertly in the background and, for most people, the presence of spyware is felt only after it has done its damage.

## Separate protection is no longer enough

Today, many security vendors offer standalone anti-spyware programs that can detect and clean spyware from an already-infected computer. Because these solutions employ what is called a reactive approach — that is, dealing with the problem only after it has become a problem — these products can hardly be considered the ultimate in protection against spyware. For an anti-spyware program to be truly effective, both proactive (preventative blocking) and reactive (removal upon detection) mechanisms need be in place.

Additionally, because most standalone anti-spyware products are definition-based, their users are ill-prepared to deal with zero-day threats and lesser known malware for which signatures have not yet been prepared — even assuming those users are regularly updating their software — not always a safe assumption to make.

## Outpost Firewall Pro 3.0 combines anti-spyware and firewall technology

Agnitum's Outpost Firewall Pro 3.0 provides an integrated security solution by combining firewall and spyware protection technology, thus safeguarding the computer against current and future spyware threats. Combining both types of threat protection enables Outpost to deliver the ultimate solution to the spyware problem.

So why is an integrated solution preferable to two independent products?

- **Coordination of all defense mechanisms around one engine.** This approach improves internal functioning of program modules, eliminates the threat-response gap, resolves compatibility issues and contributes to more effective future operation.
- **Management, control and updates deployable from a single console.** This approach improves effectiveness and usability of the program, saves time and eliminates the need to perform separate updates.
- **Decreased burden on computer resources.** Memory consumption, hard disk performance and processing power are streamlined when fewer tasks are run.

Outpost's proactive protection means that even before spyware attempts to contact a target PC, it is stopped in its tracks by the firewall without the need for specific threat identification. And any malware already present on the system is detected and eliminated by the reactive, signature-based technology.

## Spyware attack scenarios and how Outpost protects users

Outpost Firewall Pro provides multi-layered protection against spyware, trojans, worms and other destructive programs. Here are just a few examples of what can happen and how Outpost's approach protects users:

## Stages of Spyware Invasion

### Stage 1: Spyware approaches the target system, establishes contact, and attempts to install itself

#### How it happens

By taking advantage of inadequate security settings in the browser

Concealed in an email attachment.

'Drive-by' downloads from spyware-transmitting websites.

Bundled with benign software (e.g. shareware, P2P clients).

By exploiting system vulnerabilities.

#### How Outpost protects you



Outpost's Active Content plug-in reinforces security in the browser by closing possible access channels by which spyware might get into the computer.



Outpost's Attachment Quarantine plug-in lets users quarantine attachments by file type, thus preventing anyone from accidentally opening files that may be infected with spyware.



Outpost's Spyware Scanner lets users check any downloaded item and remove any spyware immediately.



Outpost's Real-time Monitor keeps a constant watch on computer activity and removes spyware immediately upon detection.



Outpost's Firewall Engine lets users create custom rules specifying how system-level functions are handled and what internal permissions the vulnerable components may have. Helps mitigate the problem before a patch is available from the manufacturer.

### Stage 2: Spyware infects the computer and is entrenched deep in the system

#### What happens

Spyware activates on a computer

Benign parts of installed applications are replaced with malicious code (application hijacking), causing spyware to run instead of the intended 'legal' program.

Browser and Windows settings are modified by embedded spyware.

#### How Outpost protects you



Outpost's Real-time Spyware Monitor registers active spyware in memory and immediately stops the process. After the process is disabled, it removes all traces of the malware code.



Outpost's Component Control, Hidden and Open Process Control functions allow users to choose whether to allow one application to share data with another and start processes on its behalf, thus closing a loophole frequently used by spyware to transmit user data.



Outpost tracks modifications made to programs and displays an alert window where users can decide whether to allow a particular modification to take place.

### Stage 3: Spyware succeeds in gaining control and attempts to complete its unauthorized mission

#### What happens

Spyware sends out sensitive user data

Spyware displays unsolicited ads, opens multiple pop-up windows, displays inappropriate or unexpected web content

#### How Outpost protects you



Application filtering in the firewall prevents data transmission. The spyware is identified and removed by the anti-spyware module, which also implements an ID block to prevent any previously-defined data from leaving the user's computer.



Outpost's Ads plug-in blocks ads based on size, broadcaster, animation type, etc, and the pop-up blocker prevents redundant windows from being opened. The Content plug-in enables word-based as well as URL-based content blocking.



It's clear, then, that Outpost Firewall Pro 3.0 with Anti-Spyware protects users against spyware at all stages of the infection process, effectively safeguarding private information and keeping PCs running smoothly.

To learn more about Outpost Firewall PRO, please visit <http://www.agnitum.com/products/outpost>.