



## What's new in Outpost Firewall PRO 4.0 — The Ultimate in Proactive Protection

The new Outpost Firewall Pro 4.0 from Agnitum is the ultimate solution for the protection of vulnerable electronic information. With this release, a new standard in software security is set: Outpost gives users the highest possible level of proactive protection against Internet-borne spyware, keyloggers, Trojans and other unauthorized attempts to access the data on your PC - even PCs running 64-bit Windows.

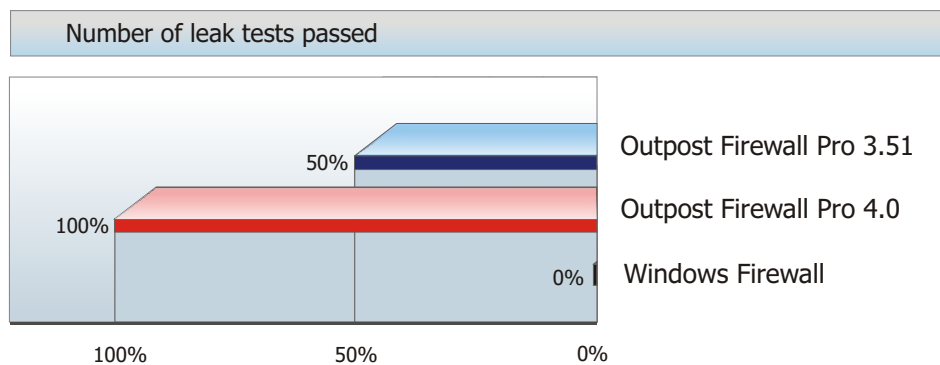
Let's take a closer look at what's new.



### Information leak prevention technology that really works

Leak tests measure a firewall's effectiveness in preventing the leak of personal information through outbound filters. Outpost Firewall Pro 4.0 is able to block all known existing techniques to steal confidential data from a user's PC via unauthorized channels such as spyware. For more details, see [www.agnitum.com/r/outpost/leaktests/](http://www.agnitum.com/r/outpost/leaktests/).

In addition to previously implemented leak prevention functions, additional protection for confidential information in Outpost 4.0 includes:



- **Customizable prevention of any application's attempts to gain control over another application.** Users can customize the list of applications trusted to make outbound data transfers to prevent stealthy access attempts by malicious applications masquerading as legitimate applications.
- **Suppression of attempts to launch a browser using command-line parameters.** Many applications can be configured to launch browser windows when a user clicks a URL (Outlook, Microsoft Office, ICQ and many more). In order to avoid unwanted browser launches by malicious programs, users can customize the list of programs that are allowed to open browser windows.
- **Customizable control over application memory.** Users can customize the list of trusted applications and avoid malicious programs using the memory space of a trusted application to execute.
- **Active Desktop control.** Active Desktop components can contain malicious code that is able to transfer confidential data on behalf of Windows Explorer. Outpost prevents such code from installing or executing.
- **Prevention of attempts to control other applications' windows.** Malicious programs can emulate user keystrokes in other program windows and make unauthorized data transfers between those windows. Outpost now detects such attempts, checks for legitimacy and blocks any unauthorized attempts to transfer data.
- **Prevention of attempts to modify critical registry entries.** The registry contains the configuration settings for all programs. Users can customize the list of applications that are allowed to make changes to the registry.
- **Double DNS resolution control.** Advanced hacking techniques allow intruders to steal data through DNS requests, which are now successfully blocked.
- **Low-level network access control.** Malicious code, once installed on a user's system, may attempt to mimic normal system activity and thus initiate outbound connections. Outpost detects such attempts, alerts the user and displays a prompt for next action.



## Anti-spyware control that's second to none

Agnitum's engineers have significantly increased the level of protection against spyware. Here's how Outpost Firewall Pro 4.0 now even more effectively monitors, detects and removes known and unknown spyware:

- **Improved system performance.** A new method of comparing programs with the spyware database has been implemented, which significantly increases scan speed.
- **Additional protection through "scan before execute" option.** All applications without exception are scanned before they are permitted to execute. To do this, Outpost simulates execution of the program in a closed 'sandbox' and tests it for legitimacy before permitting or blocking its actual execution. System performance is unaffected.
- **New spyware signature analyzer.** Even more accurate spyware detection algorithms increase users' protection against known and unknown malware.



## Self-protection

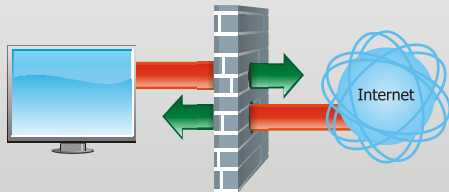
Outpost Firewall Pro now includes a self-protection mode that acts as a defense shield around the program to prevent the firewall from being deactivated by viruses, Trojans or spyware. Even attempts to shut down the firewall by simulating keystrokes are detected and stopped. Outpost continuously monitors its own files on the hard drives as well as registry entries, memory status and running services and blocks any attempted changes by malicious applications. This self-protection mode can be turned off and on by the user, enabling the installation of new plug-ins and other configuration adjustments by more advanced users.



## An improved ImproveNet

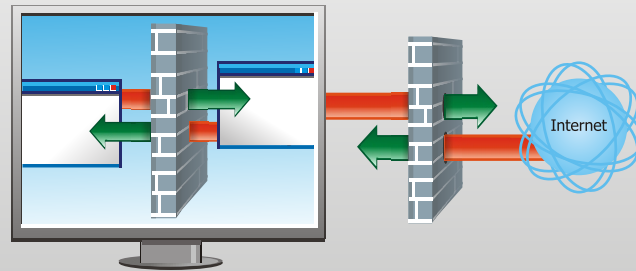
ImproveNet was introduced in an earlier version of Outpost Firewall Pro as a means of saving users' time and providing additional security by collecting, approving and redistributing commonly used rule sets among Outpost users.

In Outpost 4.0, ImproveNet gathers information at the local PC level about how programs interact. These new local rules are automatically updated for ImproveNet subscribers and used to differentiate between safe and unsafe activities. This approach provides a new level of security over local processes.



3.51

ImproveNet 3.51  
As shown at the picture, rules that users receive with ImproveNet subscription, affect inbound and outbound traffic and connections. This works in Outpost Firewall Pro v3.51



4.0

ImproveNet 4.0  
As shown at the picture, users receive a new generation protection level. In addition to previous features, applications interactions between each other are under control by security rules that are distributed to ImproveNet subscribers.



## Improved usability

**Entertainment mode.** When you're playing intense games or watching a movie online, you don't want to be interrupted by requests from your firewall to make a decision about allowing or rejecting a particular connection. So Outpost Firewall Pro 4.0 offers an "Entertainment Mode" that suppresses firewall pop-up messages when specific programs (the list is customizable) are running. Switching to entertainment mode does not affect the security level of the firewall while users are focused on the task at hand.

**For Advanced Users: Adaptive Firewall Rules.** Outpost Firewall Pro 4.0 includes macro definitions for applications that allow users to manually define security rules for individual applications and Windows-based services. For example, users can now choose to limit DNS requests to the list of DNS services built into the network adaptor. If DNS is trying to reach an unlisted DNS server, the user will be prompted to allow or block this action.

## In conclusion

With the release of Outpost Firewall Pro 4.0, PC users around the world can experience the full benefits of Ultimate Proactive Protection and high usability in a personal firewall that doesn't cost the earth. Now available for 64-bit operating systems.

Visit [www.agnitum.com](http://www.agnitum.com) to download a 30-day trial, upgrade your current version or purchase a full copy of Outpost Firewall Pro 4.0 from September 27, 2006.