

Why should I choose Outpost Firewall over Windows built-in Firewall ?

Given the amount of Internet crime nowadays, it is no surprise that Microsoft decided to provide Windows users with a built-in firewall.

The Microsoft firewall, Internet Connection Firewall (ICF), is designed to run on every PC equipped with Windows XP Security Pack 2, unless a user prefers to activate a different firewall.

The good idea of all Windows users being protected by default firewall turned out to be tricky: when the same software protects everyone, hackers do not need to invent too many ways to intrude. Imagine all the houses in your neighborhood being equipped with the same door locks: it is enough to break one of them to figure out how to open the others. Therefore all security software vendors, including Agnitum, strongly recommend that Windows users use a different firewall, rather than Microsoft.

Why would you choose Outpost over Microsoft Firewall? Check out the comparison table of how these two products cope with most wide spread Internet dangers.

Trojans and Worms

Some Trojan horses can be injected as a module of a legitimate application (for example, your browser) and thus gain the privileges to go online. Worms propagate over a network, reproducing as they go.



Windows Firewall (SP2)

Microsoft Firewall does not guard any outbound connections, and thus cannot block Trojans. It also cannot block a worm spreading from your e-mail.



Outpost Firewall PRO 2.5

Component Control guards all network activity performed by attachment components on your PC and bans all illegal connections, thus making Trojans powerless.

Hidden Process control goes even further and prohibits trusted applications from running unknown programs that might appear dangerous for your system.

Denial-of-Service Attacks

A hacker figures out a responding port on your PC and sends a huge amount of data to it. The port is just unable to accept all of the data, the system resources exhaust, and the system crashes and cannot operate any more.



Windows Firewall (SP2)

Microsoft Windows Firewall can thoroughly scan the incoming traffic, but does not have an utility for detecting and alerting Denial-of-Service attacks on your computer. Besides Windows Firewall can not block intruder by IP and close him all access to your PC. That means your system can be attacked, and you will not even know about it.



Outpost Firewall PRO 2.5

Outpost Firewall detects all known types of hacker attacks, including Denial-of-Service, and blocks them promptly. By default Outpost puts your system into stealth mode.

Attack Detection Plug-in guards all the data entering your computer and bans dangerous packets. Outpost alerts you on all blocked attacks and saves this data in the Log Viewer.

Protocol settings allow filtering of all the packets that go through your ports and sort out malicious code. You can choose the security level yourself, and Outpost will alert you each time an attack was blocked.

Privacy Leak

Spyware programs gather information about you and your interests (such as your surfing habits, what other software you have on your PC, etc.) without your knowledge or consent.



Windows Firewall (Sp2)

Windows Firewall does not filter outgoing traffic, and your personal data may be leaking.



Outpost Firewall PRO 2.5

Not only does Outpost protect you from hijacking, it also keeps your private info from leaking.

Active Content Plug-in conceals your surfing history and blocks cookies.

Component Control won't let malicious programs go online and send your data to a remote host.

Since Outpost monitors all **network activity** and blocks illegal connections, no spyware can work on your PC either.

Undesirable Content

The Internet contains a lot of web sites that should better be concealed from your children's eyes or should not be available in your office.



Windows Firewall (SP2)

Microsoft Firewall can block separate domains, manually added to the 'black list', but cannot provide keyword-based filtering of information, and therefore 100% protection is not possible.



Outpost Firewall PRO 2.5

Content filtering plug-in blocks entire domains such as sex.com, or any web page containing specific words like "bomb", "home-made explosive", "sex", etc.

Once set, the filter is impossible to overcome without the password, making it ideal for parental or employee controls.

Ease of Use

A firewall should not only protect you, but also be easy to use on any system and for user of any level of computer literacy.



Windows Firewall (SP2)

Microsoft Firewall does not provide a special tool for analyzing and logging the network activity and is rather hard to configure for a novice user. It provides every user with quite raw standard preferences which are not very easy to change.



Outpost Firewall PRO 2.5

Outpost Firewall Pro provides you with a full out-of-box protection from the moment of installation.

Auto-Configuration of security settings are applied to all the software on your PC, and the firewall starts protecting right away.

Wizard Mode will help the novices to work with the program settings and **Application Rulesets**, that automatically guard the network activity of all the applications on your PC.

Visual Alert System signals you every time an attack was blocked or suspicious e-mail attachment re-named.

Conclusion: Outpost wins 5-0!

A built-in firewall is another step in the Windows security taken by Microsoft; however it is hardly enough to protect you, mostly because it is a very standard solution.

To protect yourself from hackers and other dangers, you need an arsenal of defense not available to intruders. Outpost is tough on hackers, but not on you: it guards all connections on your PC, but it is easy to use. 100% filtering of outbound and inbound traffic provided by Outpost and a high level of control over connections will protect your computer from all known dangers and attacks.