



DataSheet

Outpost Firewall Pro 2009

Your Essential Defense against Internet Threats

What Makes an Essential Defense?

New types of threats require new types of protection. Mass-distribution viruses and worms are giving way to profit-driven attacks designed to steal identities, money, and other valuable electronic commodities through spyware and botnets.

Given the complexity and diversity of today's threats, users need protection that controls the main propagation route – their Internet connection. Zero-day threats, one of the newest and most difficult to detect, are becoming more frequent, and an appropriate response must be in place for users to have adequate security when they go online. Even simple web browsing is these days fraught with danger from drive-by infections and inadvertent disclosure of personal information.

While there are plenty of all-in-one security solutions that purport to offer total protection, in reality they all depend on a firewall to deliver the first level of defense against the spread of malware and data theft. Today's sophisticated, hard-to-detect malicious programs cannot be stopped with anti-virus alone; proactive security tools are needed to monitor program behavior and alert users to suspicious, unauthorized or explicitly malicious activity before it can do damage. As web-borne attacks now constitute the majority of malware attacks, a solution that's specifically designed to counter online threats is essential.

Outpost Firewall Pro is just such a tool. It stops malware and hacker attacks before they can activate, by monitoring and controlling Internet access at all times. What's more, it does most of its work automatically, so users are not interrupted while they're working or playing on the web. Outpost Firewall Pro is award-winning protection that's lightweight, customizable, reliable, and easy to use; it's what every computer deserves, so keep reading to find out more about how Outpost provides the most robust security protection possible for users in today's world of cyberthreats.

Key Technologies

- **Two-way firewall** to guard network access
- **Intrusion Detection System (IDS) and Ethernet protection** for automated defense against vulnerability probes and internal breaches
- **Anti-spyware** to fend off basic malware attacks
- **Host protection** for proactively blocking unknown threats
- **Web & transaction security** to protect against web-borne risks
- **Self-protection** to maintain continuity of protection
- **Automated, updatable configurations** to simplify work



Key Benefits

- The award-winning firewall keeps hackers and malware away, so users can feel safe when they're online. Two-way access control means that unauthorized network activity is impossible, and special Ethernet protection shields local networks against man-in-the middle attacks and WiFi-borne intrusions. The IP Blocklist component will block connectivity to predefined Internet hosts, keeping your family members away from the sites that you consider inappropriate.
- Host protection monitors program behavior and interactions to proactively defend against unauthorized activity, stopping Trojans, rootkits and keyloggers in their tracks without the need to scan each suspicious object for known malware. Outpost's Host Protection achieved a 100% pass rate for all current leaktests, providing reliable protection against unknown and/or sophisticated hacker attacks.
- The integrated anti-spyware module provides comprehensive protection against all forms of spyware, automatically defending users from the risk of compromised personal information, unauthorized system modifications, and intrusive pop-ups, amongst other online annoyances.
- The versatile web control module safeguards users' browsing activities against the Internet's darker side by steering away from websites infected with drive-by downloads, preventing the inadvertent disclosure of personal information, limiting exposure to potentially unsafe web properties, and keeping identity private.
- Outpost's self-protection capability ensures that it cannot be deactivated by targeted attacks, ensuring uninterrupted protection.
- Thanks to advanced events logging mechanism and new process activity view that shows detailed information about all currently active programs, users get the ultimate in transparent, hands-on protection.

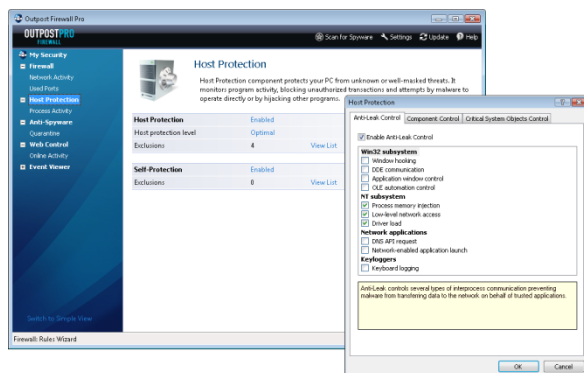
Outpost Firewall Pro has been designed to meet the needs of users who understand the need for robust, efficient security. While it provides great protection "out of the box" for users at all levels of experience, Outpost Firewall Pro also includes an extensive array of customizable settings and options for advanced users to tweak and personalize their protection. Less-experienced users also get great protection because Outpost lets them define and apply most settings automatically, eliminating potential configuration errors. The intuitive interface and accessible controls ensure ease of use for everyone.

Key Features

Proactive security

Preemptive threat protection

Outpost Firewall Pro provides the first line of defense against malicious software by proactively controlling how programs behave and interact on a PC and preventing security breaches. The host protection module proactively monitors for and blocks sophisticated hacking techniques used to compromise or steal data. By analyzing threats and displaying actionable alerts, it blocks zero-day attacks and other unauthorized activities, providing advanced protection against botnets, rootkits and inadvertent data disclosure. This latest version extends the range of monitored events and operations for even greater and more customizable protection. Outpost excels in all currently-known leaktests, with additional focus on keylogger-like activities.



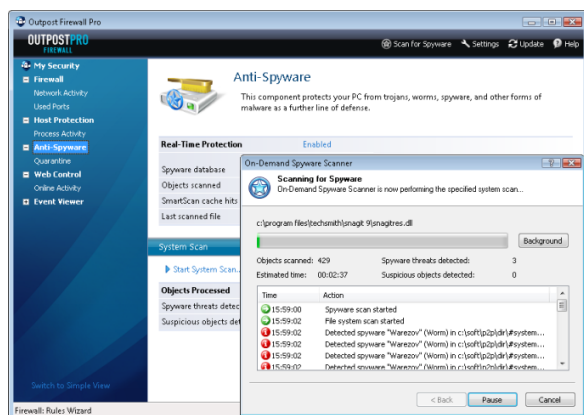
Self-protection

Today's malware frequently seeks to shut down security software to make its infection process easier. By incorporating solid tamper-proof protection for all its components, Outpost Firewall Pro makes it impossible for anyone except the authorized user of the program to disable or close active protection.

Anti-spyware

Essential spyware protection

Outpost's anti-spyware module safeguards PCs against the threat of spyware - from displaying annoying ads to hijacking the browser homepage to stealing user identity and confidential data. Spyware is blocked at every possible stage — installation, activation, transmission of information and re-installation. The on-demand scanner scours the system for traces of deactivated spyware and erases them completely. Even if active spyware protection is switched off during processor-intensive tasks like online games, new network connections are proactively verified in the background to be spyware-free before being allowed to proceed.



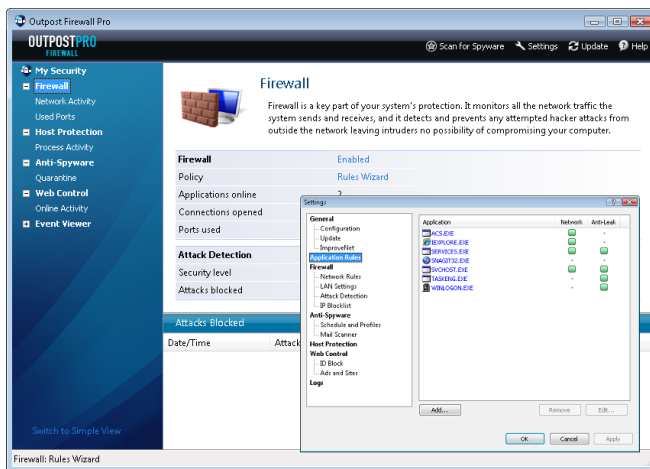
Network security & continuity

Connection security

The two-way firewall monitors the computer's inbound and outbound connections and prevents local and remote unauthorized network access. It conceals access ports, making the user's presence on the Internet invisible. The Ethernet Protection module guards network connections and prevents insider attacks by controlling the transmission of data over the network. This eliminates the potential risk for data such as chat windows or authenticated browser sessions to be delivered to the wrong destination or intercepted while in transit.

Application access control

The firewall controls which programs are allowed to access the Internet, proactively protecting the PC against both zero-day threats and malware attempts to "phone home".



Comprehensive coverage

Outpost Firewall Pro secures all types of connections (Ethernet, WiFi, DSL, cable, cellular, and dial-up), automatically applying the necessary security settings when the computer is connected to a new provider.

Intrusion protection

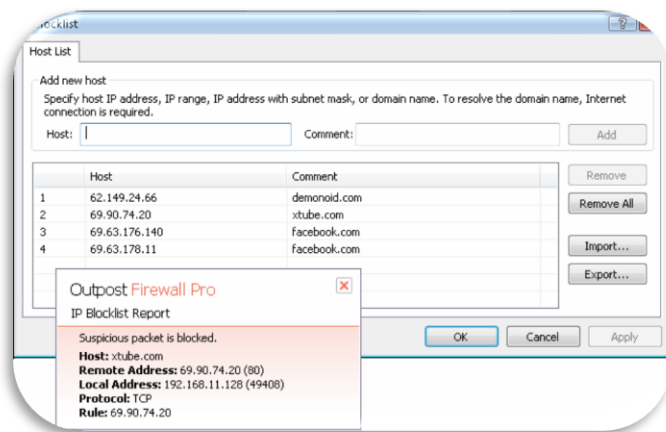
The Attack Detection module automatically blocks known types of hacker attacks from gaining access to the computer.

Privacy & web safety

IP Blocklist keeps surfing clean

Based on the BlockPost plug-in in earlier Outpost versions, the integrated IP Blocklist lets users restrict access to specified Internet domains. A valuable tool for both sensitive individuals and concerned parents, IP Blocklist will deny incoming/outgoing connectivity to ill-intent Internet zones, such as those distributing spyware or delivering obnoxious ads and graphics spam.

The blocked entries can either be manually defined or imported as an aggregated list from community-maintained sources.



Unsafe web site access restriction

Outpost can optionally alert and block access to potentially malicious or unwanted web sites based on a predefined list of URLs. This filtering ensures users don't become a victim of inadvertent drive-by malware infection or phishing attacks that are looking to steal passwords, login information and other sensitive data. The list of blocked sites is updated via the automatic updates and can be edited to reflect individual preferences.



Safe repository for personal data

Any confidential information – for example, bank account numbers and passwords – that users define using ID Block is blocked from leaving the confines of the PC through communication channels such as IM, web or email. ID Block protects against identity theft and phishing attacks that target personal, confidential information. Plus, it ensures that no-one else – including other members of the household - can accidentally or deliberately disclose this information on the web.

Ad-free, anonymous surfing

By managing cookies and external referral URLs, Outpost lets users maintain a high level of privacy when visiting shopping, entertainment or news sites while at the same time allowing trusted sites to collect only the information needed to personalize pages. Additionally, Outpost Firewall Pro lets users limit the elements displayed on web pages, providing cleaner and faster browsing. Users can also define the sites that are permitted (or not permitted) to display images, rotate advertising banners, execute external code such as ActiveX or Java scripts, or deliver pop-ups. The latest version of Outpost ensures compatibility with even the most complex and sophisticated websites, delivering smooth performance and heightened online safety.

Tracking & control

Network activity monitoring

Outpost's Network Activity Monitor shows every connection the user's PC makes with other computers on the Internet or local network, so users can see what's happening on their PC at all times and quickly close down any unauthorized connections. In the new 2009 version, connections can be grouped/ungrouped according to application, and you can quickly edit any existing rules right from the interface.

Password-protection, multiple configuration profiles

Users can set passwords to protect their configurations from accidental or deliberate modification, as well as create and use multiple configuration profiles to suit their current risk exposure. For advanced users, the ability to construct multiple restore points through the save/load configuration command is a big plus.

Better manageable events logs

Outpost's old Log Viewer showed the history of past events on a computer. The new version improves on the Log Viewer's clarity and manageability, adding support for per-category listings that can be sorted and filtered according to different user-specified criteria.

Compatibility

Driver certification and latest Windows platforms compatibility

Outpost has received WHQL (Windows Hardware Quality Labs) certification, meaning that its protection complies with Microsoft's stringent quality, compatibility and stability requirements.

Adaptive firewall rules

When traveling with a laptop, or changing ISP, users don't need to manually adjust their security for new connection settings - Outpost handles it automatically by designating connection-specific parameters such as DNS or gateway server addresses as environment variables.

Entertainment mode for uninterrupted gameplay and video viewing

While users play full-screen games or watch videos on their PC, Outpost's Entertainment Mode ensures the program won't interrupt with alerts if it detects new activity. New activity notifications are handled in the background without sacrificing current protection levels. Users can customize which applications will automatically trigger the switch to Entertainment Mode.

Convenience and ease of use

Auto-learning mode

When Outpost is first started, it runs in a special "learning mode" where all alert notifications are suppressed. During this time, the program is silently learning the user's typical program activity and firewall-monitored connections. After the learning period is over, the Firewall reverts to normal mode, and will prompt for a response only when new activity is seen, dramatically reducing the number of alerts requiring your involvement.

Automatic configuration

Rules for most programs that access the Internet are applied automatically, relieving users of the need to enter rules manually every time a new application accesses the Internet or interacts with another program. This means that for most of the time, users won't need to deal with questions relating to Internet access, minimizing interruptions and risk exposure due to insecure configurations. Outpost

includes a wide range of predefined access policies; these settings can be customized to meet individual requirements at any time.

ImproveNet delivers more ready-made configurations

ImproveNet is a voluntary system of program configuration aggregation and distribution. After being reviewed and approved by Agnitum engineers, rulesets submitted by Outpost users are distributed across the user base, providing all users with the most secure and up-to-date rules for a wide range of activities and applications.

Smartadvisor - instant, context-sensitive help

If ImproveNet doesn't have the answer, SmartAdvisor is always on hand to help users make the right decision when configuring access information for an application.

Hands-free updates

Whenever an update to Outpost Firewall Pro is released during the license period, the update module automatically retrieves the latest version from the Agnitum server and applies it as soon as it is authorized to do so.

Performance & optimization

Faster, more intelligent scans

SmartScan, the intelligent file sensing monitor, scans only the modified portions of the file system, avoiding repeat scans of files that have not changed since the last scan. The fast and intelligent anti-spyware engine has no impact on overall system performance and can operate in the background while you work. SmartScan has been further optimized to deliver up to ten times faster performance boost for some scan and datastream data checking operations.

Specifications

Supported platforms: 32- and 64-bit Windows (Vista, XP, Server 2003, 2008), Windows 2000 (SP3 and above).

Min. hardware requirements: 450 MHz CPU(x-86/x-64/multi-core), 256Mb RAM, 100MB free disk space.

© 2008 Agnitum Ltd. All rights reserved. Agnitum®, Outpost Firewall Pro™, Outpost Security Suite Pro™ and Outpost Antivirus Pro™ are trademarks or registered trademarks of Agnitum Ltd.