

What's New in Outpost Pro Version 7 (Personal Security Software Line-Up from Agnitum)

Continuing its tradition of innovation with perfection, Agnitum is proud to present its new generation of PC security products – Outpost version 7.0 (Outpost7 family: Antivirus, Firewall, and Internet Security Suite).

With the current seventh version of Outpost software which took us more than a year (we've been working on it since the release of Outpost 2009 New Year edition) to develop and crash-test, we put all our efforts to making your internet experience safe and secure while bringing you unparalleled speed and simplicity of use. Recognizing increased adoption of Windows 7 OS and consequent growth in processing power, Outpost7 capitalizes on new advancements to deliver more stable and efficient protection to your PC. Empowered by native filtering technologies opened to security developers, Outpost7 boasts better compatibility and interoperability with future Windows platforms and third-party applications.

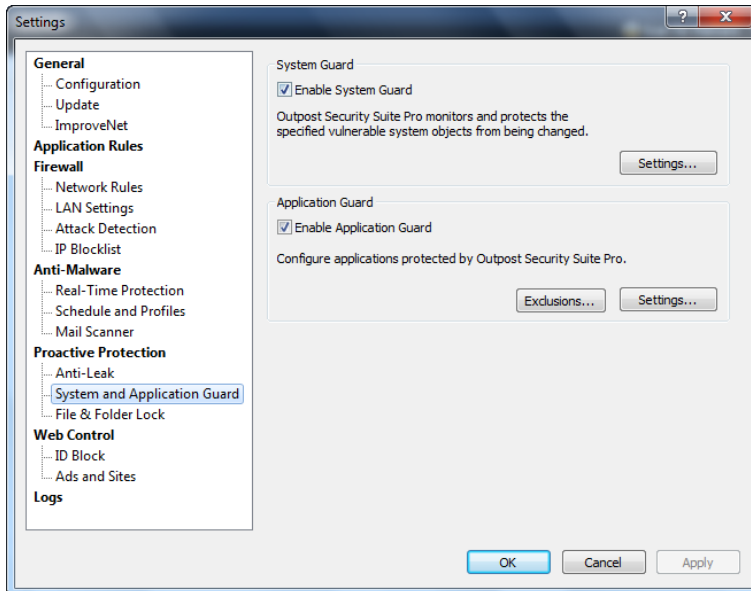
Inside the new Outpost7, you are going to find a host of new (and some reinstated) features and improvements designed to make your Internet surfing more fluid and secure. New defense mechanisms will beef up your protection against emerging types of malicious programs, while redesigned notification windows, and more clear-cut Antimalware action prompts will aid visibility and transparency of configuration and operation. Outpost emphasizes a “talking less, doing more” mindset, providing high standards of protection in conjunction with high usability levels by automating majority of operations and requiring minimal user participation.

Component	Status
Firewall policy	Rules Wizard
Self-protection	Enabled
System integrity protection level	Optimal
Real-time malware protection	Enabled
Malware database	3/4/2010 Update...
License	Trial, 30 days left Purchase...

Without further ado let's zoom in to the novelties and improvements in Outpost7 in regards to Security, Privacy, Tracking and Control, Performance, Compatibility and Usability aspects.

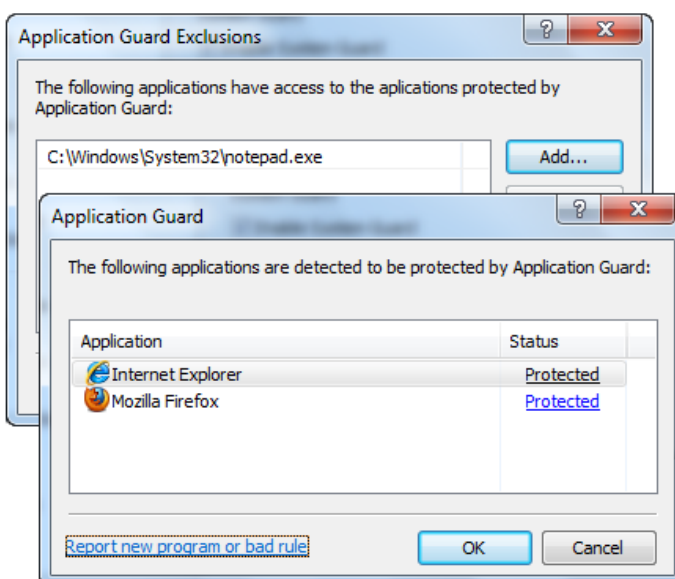
Security Improvements

Outpost7 adds a new security layer to its formidable defense arsenal – access control to application-specific data – by verifying whether an arbitrary program has permission to access internal files and configuration settings belonging to many well-known applications. This measure helps preserve integrity of installed applications and their components (known “critical objects”).



New! Application guard

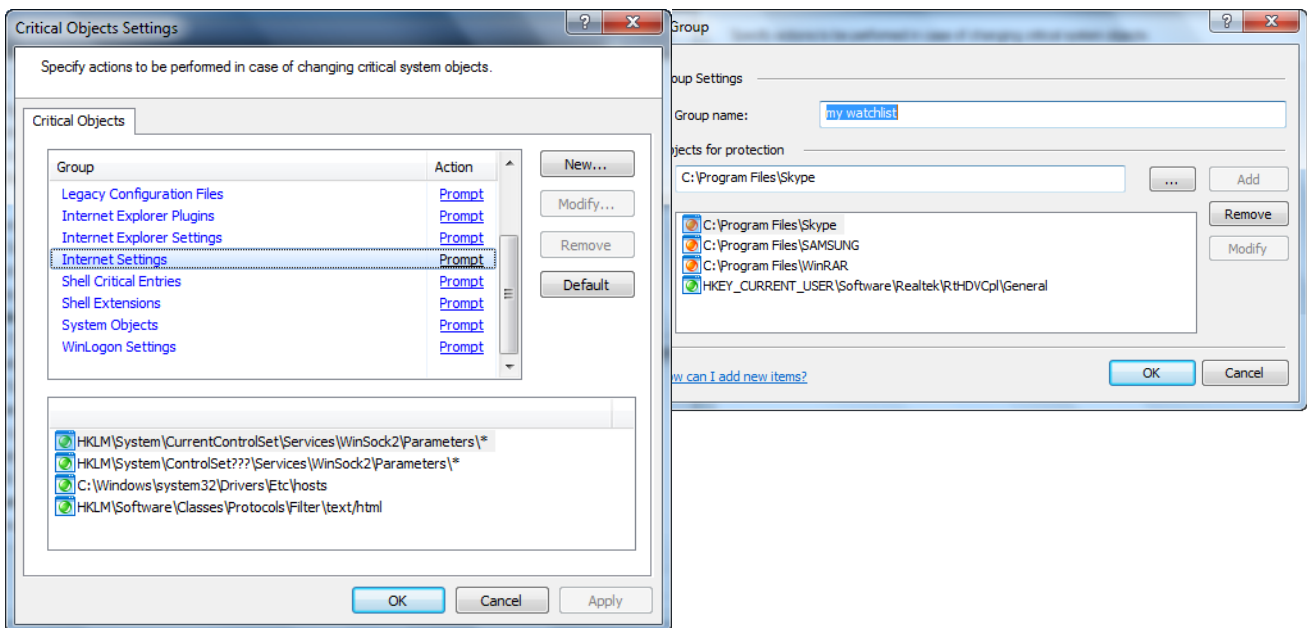
The new *Application Guard* feature, which comes as an upgrade to Outpost's *Proactive Protection* module, defends sensitive data stored by various Internet-enabled applications such as instant messengers, web browsers, e-mail clients and e-banking software from compromise. Items such as cached/saved login details and passwords, configuration files, electronic wallet contents, etc. are now shielded from being tampered or hijacked by unauthorized non-related applications, enabling to counter a common attack technique employed by modern malware-makers. Thus, only the Yahoo! messenger application would be able to retrieve personal Yahoo! messenger credentials, only Internet Explorer would be granted access to its cookie files and so forth.



Outpost7's Application Guard is equipped with predefined access policies with updatable list of protected software titles, and you can add access exclusions to enable a particular program to modify Critical Objects.

Improved! System guard

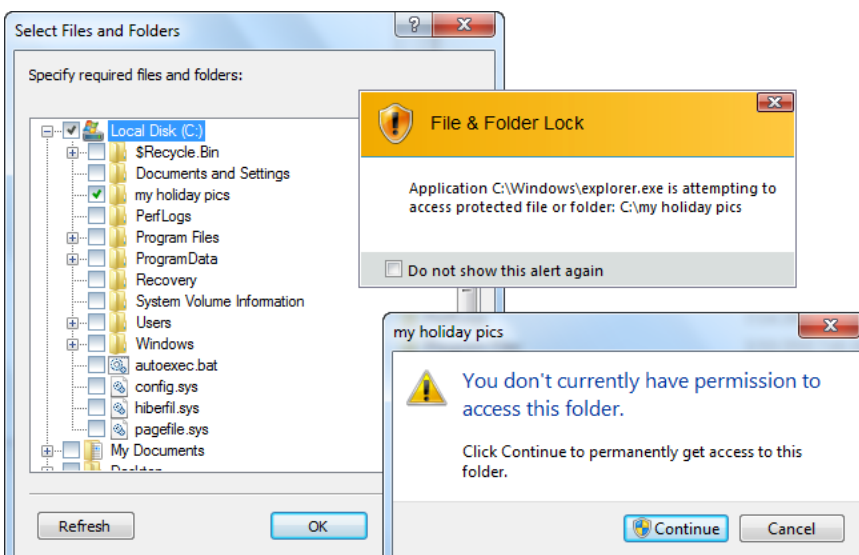
As an extension to Outpost's *Proactive Protection* module, the System Guard feature secures *critical system files and configurations* against misuse or compromise. The list of protected items could be extended by adding the program of your choosing to the protected system software list.



Privacy Improvements

New! File and folder lock

File & Folder Lock functionality enables protection of locally-stored assets from corruption, modification or illegal access by other users or malware. Primarily, this tool could be used as a restrictive measure to prevent unwanted viewing of private file and folder contents by unauthorized users (children, colleagues, etc.) on a shared computer. With just a few clicks within the "File and Folder Lock" section of the Proactive Protection settings panel in Outpost, you can simply select a folder or file you wish to protect and set limitations by defining access password. You can also create groups of protected objects (for example: financial info, adult content, secret documents, etc.) and add your personal contents to these groups in the future. Allow and Block choices are available and may apply to any object you'd like to secure.



Improved! Extended Anti-Leak capabilities

New types of data leak techniques have been incorporated into Outpost's Proactive Defense module to ensure up-to-date protection against new attacks employed in zero-day threats. The module's effectiveness has been proved by successfully thwarting new malware samples and passing existing leak tests.

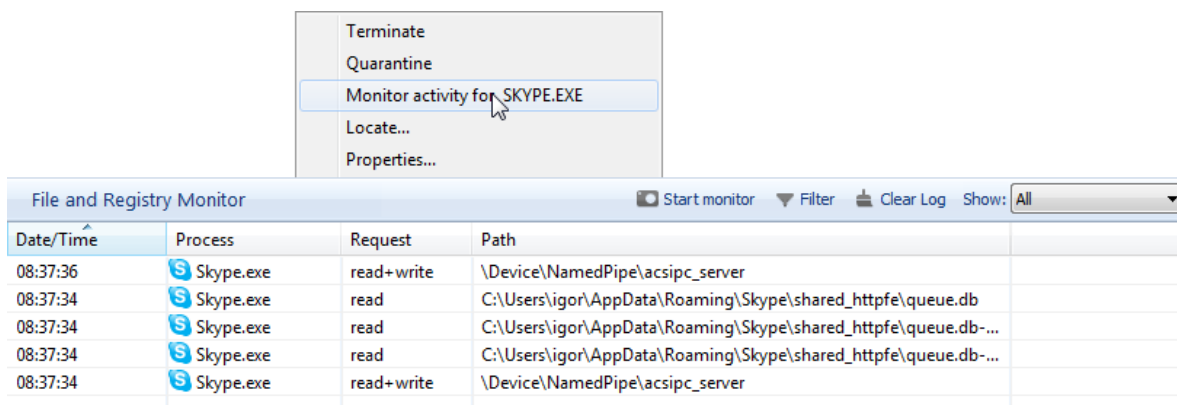
Improved! Intensified cumulative updates schedule

Security updates to Outpost's antivirus database definitions are now distributed twice on a workday, bringing protection maximally up-to-date. Additionally, whenever updates to the main antivirus engine (executable module) become available, they will be automatically applied without the need for user participation (providing, of course, for system reboot). This ensures latest protection is always in place without any hassles from the user's end.

Tracking and Control Improvements

New! Real-time File and Registry Activity monitoring

Ever wondered what is currently happening on your system and what changes have been made once you've launched an unknown program or an executable file? If the answer is "yes", as it is for many other advanced PC users, then this feature is made especially for you. File and Registry Activity provides an invaluable opportunity to look into system events at a closer range by monitoring activity of any given active process and tracking system changes in real time.



In a Process Activity view one may right-click on a process and choose to terminate, quarantine or – monitor activity for it – that's when the new feature jumps in. The Monitor provides nifty filtering options so that you can exclude or include running processes and concentrate on what's precisely of interest at the moment. The user can analyze every active process, its path and time as well as track registry modifications in order to take action with Outpost's ample functionality. Besides, using Start/Stop monitor buttons you may opt to take a snapshot of the monitor's records for deeper analysis.

Improved! Additional URL blocking options

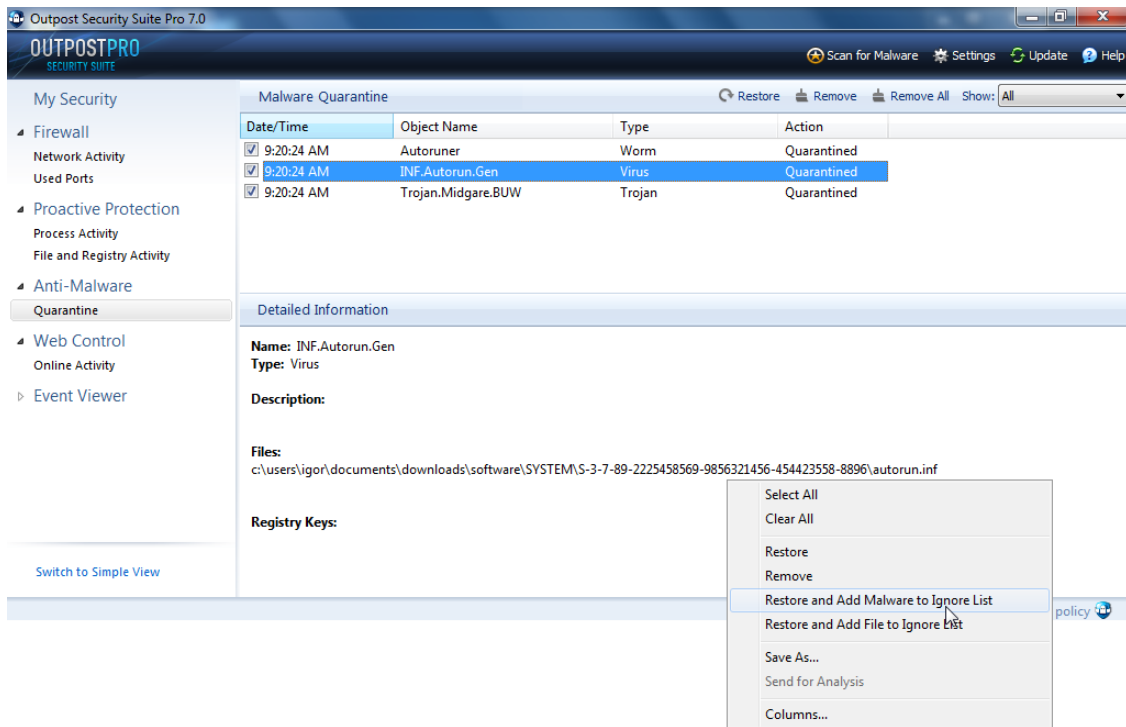
Outpost7 is back with all functionality lost along the development process in quest for practicality and simplicity. Version 4's feature that allows blocking access to specific sites with predefined keywords is back and extended in the "Web Control" module. Now you have three possibilities to prevent yourself or your family or fellow workers from winding up on an inappropriate web site:

- entering "black listed" words as in original concept
- using other "Web Control" feature which includes Agnitum's updatable stoplist of URLs
- uploading IP addresses lists into IP BlockList engine ("Firewall" module)

Using Outpost7 you may effectively limit your or your kids' exposure to offensive or adult contents ample on the Internet.

Improved! Anti-Malware Quarantine actionability

Actionable Quarantine facilitates decision-making regarding neutralized suspicious objects; quarantined files can be easily restored, removed or removed in bulk right from the new menu in a couple of clicks. Detected malware can also be filtered and sorted by certain criteria. For known "beasts" detailed information is available.



Performance Improvements

Outpost 2010 solutions deliver improved performance and use fewer system resources thanks to a number of measures:

Improved! More efficient data processing

As a result of implementing new filtering standards based on Windows Filtering Platform (WFP) from Microsoft, transmitted data is handled more efficiently, resulting in increased performance and heightened system responsiveness in cases of intensive Peer-to-Peer activity, broadband downloads and viewing of audio and video streams online, as well as multiplayer gaming.

Improved! Modernized updates

A new anti-malware update routine utilizing local servers and requiring decreased data volume provides for more efficient and expeditious security updates.

Compatibility advancements

Improved! Stability on new platforms

The introduction of new standards to the Outpost 7 lineup make it better compatible and stable running on the new Windows 7 platform, with fewer occurrences of slowdowns and interoperability issues. These changes make Outpost even better positioned to meet the future arrival of new Windows OS.

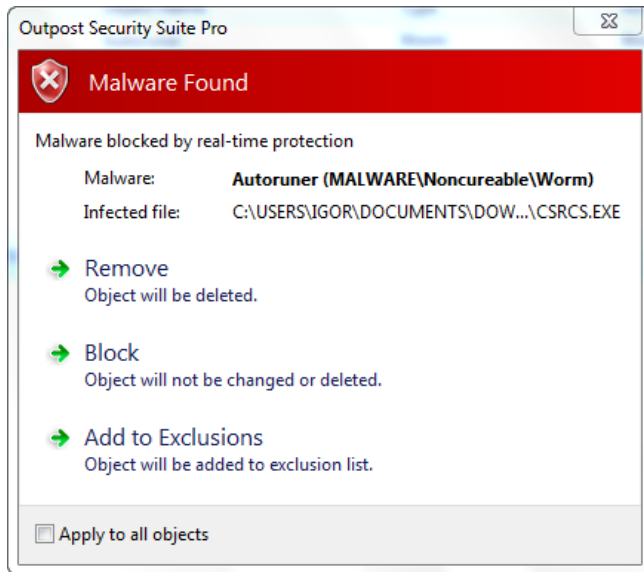
Improved! Better compatibility with Eastern text characters

ImproveNet advancements have enabled improved interoperability with applications and web-sites using Middle and Far East language character sets.

Usability Improvements

Improved! Anti-Malware that's easier to interact with

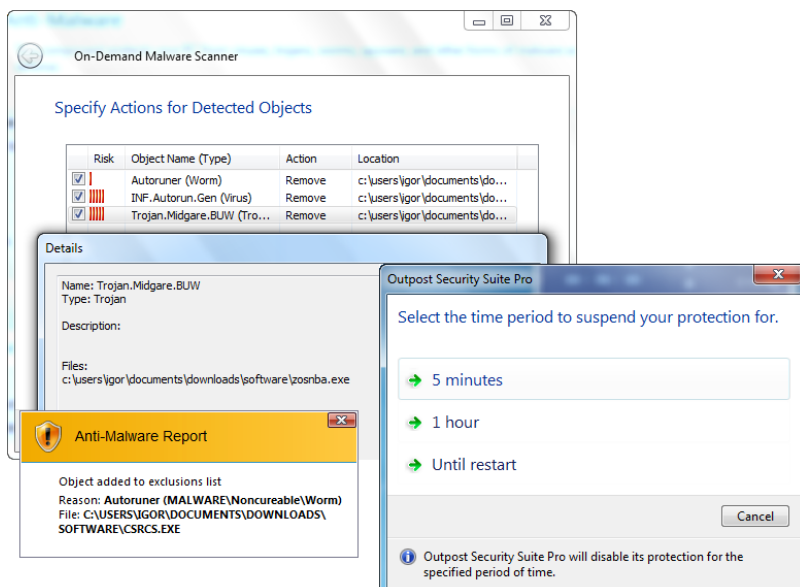
The antimalware module has become more transparent and easy to operate, with concrete information on threat type and source. Plus the warnings are designed in a user-friendly fashion to indicate relevancy of this or that event.



The option to automatically cure infected objects detected by the real-time monitor is now set as default action and applies to all suspicious/infected objects found. This measure caters to average users who rightfully prefer the program to perform an optimal operation rather than rely on their own decision.

Improved! User interface with a facelift

The interface changes were designed to reflect the modern Windows 7 look and provide better visibility of product notifications. Redesigned setting panels make program configuration more intuitive.



Improved! Quick-to-configure application activity rules

The local activity rules for Proactive Protection module relating to individual applications can now be configured right from the main menu.

Your next step

All these new features have been made to make it easier for you to protect your valuable assets. Some of them can be seen and qualified, while others are hidden inside the depths of technical aspects of program development and networking technologies. But there is one thing we recommend you to do to experience the changes firsthand – download the program and test-drive it. So why delay—do it straight away and witness the power of true, lightweight protection with heavy duty output!



<http://www.agnitum.com/products/>