Single Product Review

SoftSphere Technologies

DefenseWall HIPS

Language: English
May 2009
Revised last: 2009-05-20

www.av-comparatives.org

Table of Contents

About Softsphere Technologies

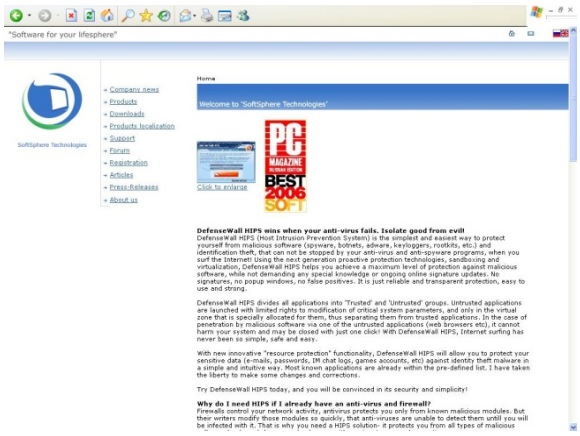
SoftSphere Technologies was established in the year 2002 and consists of a team of highly specialized and experienced programmers. The organization is primarily active in the field of information security and its mission is to develop reliable means of protection against existing and future threats, such as viruses, spyware or rootkits. In this context, SoftSphere Technologies gives due importance to ensuring that its products are easy to operate and the applications are compact and not an undue drain on resources.

The most important product of SoftSphere Technologies is "DefenseWall HIPS", which we would like to discuss in this review in more detail. According to information given by the manufacturer, DefenseWall HIPS (Host Intrusion Prevention System) is the simplest and most comfortable way of protecting oneself from harmful software, such as spyware, adware, keyloggers or rootkits.

Please visit our website www.av-comparatives.org for the latest results.

Website & Information

The SoftSphere Technologies website (www.softsphere.com) has been designed coherently and structured in a clear manner. The website is available in English and Russian. Overloaded charts and diagrams have been intentionally omitted, and emphasis given to text-based content so that the attention of the visitor is drawn to the most important aspects dealt with by the website.



The layout is reproduced correctly by all prevalent browsers and you can also navigate with the help of a Screen Reader. This means that the site is free from barriers and even persons whose physical abilities are restricted have access to the products and support.

The navigation menu is located on the left side of the screen beside the logo and provides an excellent overview with its 10 entries. The first three menu items (News, Products and Downloads) immediately offer to most visitors of the site what they need to download the product DefenseWall HIPS and to test it free of charge.

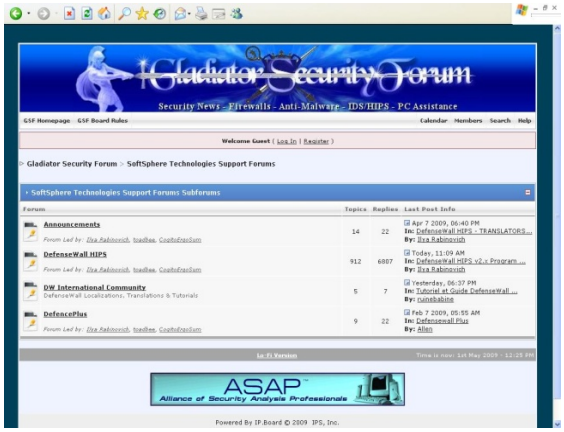
Softsphere Technologies is well aware of the fact that such a project nowadays is not only needed in English. Therefore, they provide also localized versions of the user interface in German, Polish, French, Swedish, Italian, Traditional and Simplified Chinese, Estonian and Brazilian Portuguese. With version 2.55 of DefenseWall, also Russian will be supported.

Besides the two menu entries Support and Forum, there also is the item Registration, where it is possible to acquire and register the full version of the product. Right at the end of the navigation menu, there are other items for various articles and press reports as well as a brief on SoftSphere Technologies.

At this point, we would like to briefly describe the area of Help & Support, which, in our opinion, is very important for both testers and users of the purchased version.

Help & Support

At SoftSphere Technologies, Support is subdivided in e-mail support and the Forum within the website (www.gladiator-antivirus.com). As for e-mail support, a distinction is made between registered and non-registered users. The former are assured a turnaround response time of three working days. There are no assurances made to unregistered users regarding the time taken to respond to their queries.



Softsphere does not have Hotline or Live Support. This makes rapid support impossible.

Downloading the Test Version

All the important functions of the website are easily accessible and we now proceed to obtain a test version of DefenseWall HIPS.

We click onto "Downloads". There we select the product "DefenseWall HIPS", which is needed for our test.

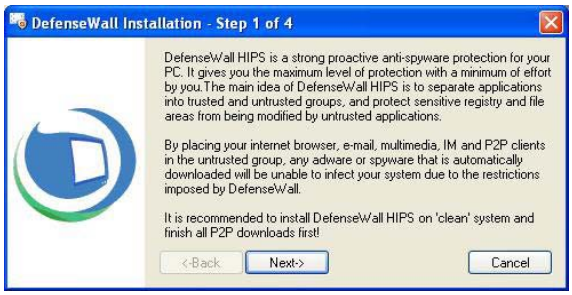
No other input or registration is required to download the 30-day test version, which is a plus feature when compared to competitors' products. Moreover, there is a link for downloading the other language variants of the user interface.

Our test system

In order to get the most comprehensive result, we consciously used a somewhat older business machine of IBM for this test. This was an IBM ThinkCentre 8171-CTO having an Intel Pentium 4 CPU at 3 GHz and 512 MB RAM. The operating system used was an English version of Windows XP Pro with Service Pack 3. Quite naturally, the system was re-configured entirely in order to exclude the possibility of any existing problems from introducing an element of bias in the test.

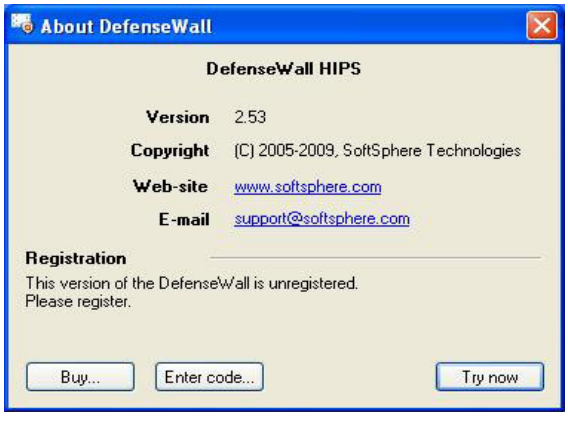
Installation

We saved the test version on our desktop and now proceed with the actual installation by double clicking on the setup file. The setup procedure consists of only 4 steps. The first step consists of a brief explanation about the manner in which DefenseWall HIPS works.



In the second step you have to accept the terms of the usual software license agreement. If you do not accept it, you cannot proceed with the setup. In the third and most important step, you must specify the destination for the installation, whereby the default in the "Program Files" folder would be the right choice for most users. In the fourth and final step, the system prompts for system restart, which may be deferred by ticking the checkbox. All in all, the initial installation barely takes 5 seconds (!) to complete.

After clicking on "Finish", the setup wizard terminates and the computer is restarted as desired. After the system restarts, DefenseWall HIPS displays a welcome window, which indicates the version of the package currently installed and prompts for purchasing, entering the license code or testing the product.



Clicking on "Buy ..." opens the corresponding website where the product is added to the shopping basket. The connection used is secure and you can choose one of various currencies for payment. However, we navigate

away from the shop at this point in order to continue with testing the product.

However, out of curiosity, we quickly click on the option "Enter code …", which opens up a dialog window to select a registration file (*.dwu). Since we do not have the corresponding file, we close the dialog and click on "Try now" instead. A new window pops up prompting for configuration of the Internet settings for automatic update of DefenseWall. We accept the option (you could defer this setup to the next week or ignore it permanently).

The subsequent dialog box prompts for settings pertaining to proxy connections or a direct Internet connection. Since everything has already been configured correctly for our purpose we can click on the "Check for Updates" option. The program then searches automatically for new versions and downloads them. After the update, you have to restart the computer.

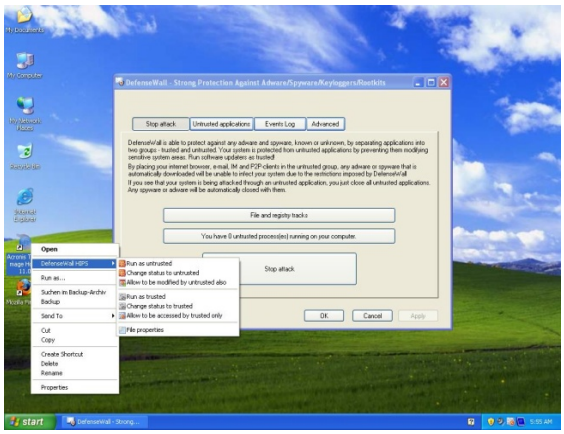
Even after this restart, DefenseWall welcomes us with the now familiar window. We click again on "Try now" to proceed.

On the whole, you can say that the installation executes with very few steps and is fast and reliable. Another good feature is that the program performs an update immediately after restarting, which is in the interest of the average user and his/her security.

First steps

After installing the program and updating it, we would like to turn our attention to the functions as such.

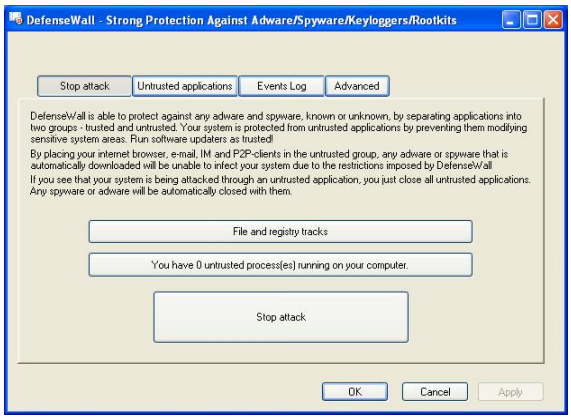
All important functions of DefenseWall can be accessed via the Tray Icon in the Task Bar (System Tray) or the context menus of the Windows File Explorer.



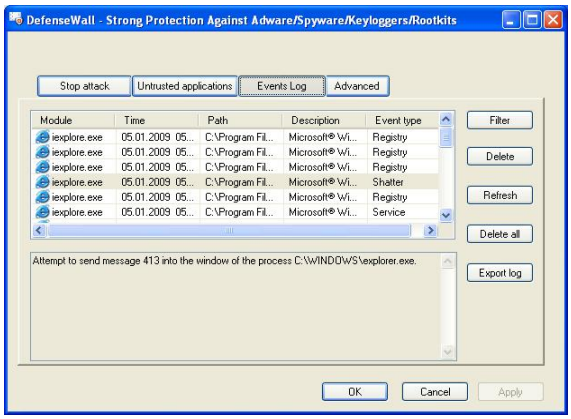
The corresponding Tray Menu will be opened by clicking on it with the right mouse key. This menu offers the following options: Main (for opening DefenseWall), Expert Mode (a special mode that makes DefenseWall not remember untrusted files status), Disable Protection (for allowing the user to temporarily disable DefenseWall), Go Banking/Shopping (for switching the computer over to a special browser mode enabling a secure transaction), Stop Attack (for closing all the suspicious and dubious processes at the same time), Events Log (for showing the log entries), Check for Updates, Help, Online Support (for opening the Support Forum), About and Exit.

At this point, we open the main window of DefenseWall using the "Main" menu option. There are four tabs here, which we would like to present in detail.

The first button "Stop Attack" shows us which untrusted processes are running and what registry entries or data changes are caused by this. Here individual changes can be admitted or cancelled deliberately. Like in the context menu, clicking on "Stop Attack" will close all the insecure ("untrusted") processes that are running at present so that you can be on the safe side if something strange seems to be happening.

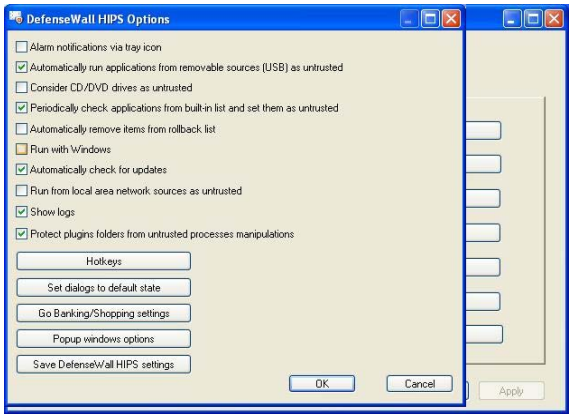


The second tab, "Untrusted Applications", displays a list of programs falling in this category. The list automatically includes programs that have already been started. Of course, you can manually rate programs as "un-trusted" or cancel this rating again manually. Using exceptions, you can configure DefenseWall as needed.



The button "Event Log" shows a separate log for each process graded as being insecure ("untrusted"). For making everything easier to grasp, the list can also be filtered, updated or emptied manually according to certain criteria. What is also of interest is the possibility to export log entries for purposes of later analysis. Thanks to this, one's knowledge can be extended continually in co-operation with the Forum Community in case of uncertainties.

For those, to whom the default settings of DefenseWall are not acceptable, or those who have other things in mind, can configure the settings as they like to explore various possibilities as they choose using the last tab, "Advanced". There are 7 other options available here: Options (various settings, such as those for Hotkeys, Banking/Shopping, pop-up windows etc.), File and Registry Excludes (you can exclude certain changes from protection), Secured Files (a list of trustworthy files), Download Areas (a list of folders to which you can download files), Check for Updates, Password Protection (you can assign a password for all settings in future) and Resource Protection (here, you can protect your passwords, game accounts and other sensitive data).

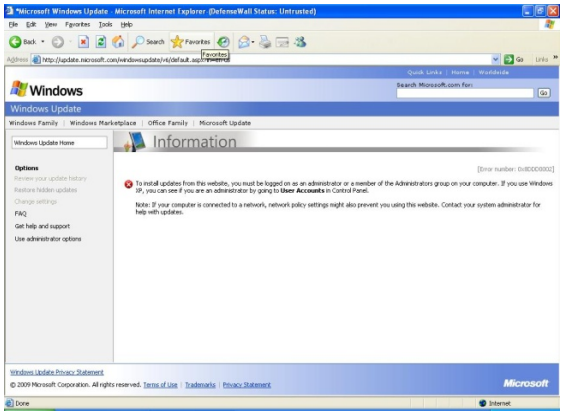


Since we would like to design and structure our test so that it comes as close to a realistic situation as possible, we retain all the settings recommended by DefenseWall, just as most other users probably would.

If you click on the icon of a program with the right mouse key, you will find a new entry with the name "DefenseWall HIPS >" in the context menu. This entry will open a new sub-menu. Here it is not only possible to grade the program as being "Trusted" or "Untrusted" or start it, but also to directly change this status. In addition, it enables the option "File Properties" to provide the current rating of the program set within DefenseWall.

First Steps: (Automatic) Windows Updates

Since we have configured our system only with Service Pack 3, there are still some updates from Microsoft that need to be installed by us. The automatic update notification appearing as a yellow icon in the tray indicates this in the usual manner. We click on "Download" in order to install these updates. The download runs in the background as usual but gets cancelled without displaying any message. We thus start Internet Explorer 6 (as an untrusted application) and click on Tools and then on Windows Update. Here again, we cannot get very far because the Windows Update website tells us we have no administrator privileges.



Here DefenseWall obviously is effective. Thus we make a double click on the Tray Icon of DefenseWall and there on the button "Untrusted Applications". In the list, we select Internet Explorer and click on "Run as Trusted" with the right mouse key. Then Internet Explorer will open a new window with the correct identifier. Now the Windows Updates will work normally as we expect. We start to update the system.

After almost 38 updates and two restarts, no further updates are displayed and we can proceed with the rest of the product test.

Installation tests

We have considered a list of 21 programs for the following test, which we would download via the internet in the "Untrusted Mode" and which we would try to install directly from the browser. If this does not work, we would try to install them manually via Windows Explorer and this too as "Trusted" in case it does not work otherwise. This list includes the following programs: OpenOffice 3.0.1, Gimp 2.6.6, WinRAR 3.8, Firefox 3.0.10, Thunderbird 2.0.0.21, Adobe Reader 9.1, Xnview 1.96, Quicktime 7.6, Realplayer 11.1, VLC Media Player 0.9.9, Java 6 Update 7, Shockwave 11.5, Silverlight 2, PGP Desktop 9.10, Truecrypt 6.1a, Google Toolbar, Yahoo! Messenger 9.0, Windows Live Messenger, ICQ 6.5, Skype and Trillian 3.1.12.0.

OpenOffice 3.0.1

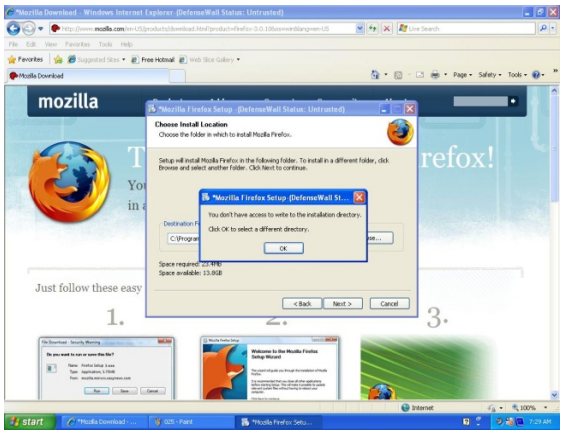
Click on the download link. There is a warning. The download starts. Installation is successful (Trusted). The program works.

Java 6 Update 7

This program has been installed along with OpenOffice 3.0.1. Installation is successful. The program works.

Firefox 3.0.10

Click on the download link. There is a warning. The download and installation fail (Untrusted). Manual installation is successful (Trusted). The program works.

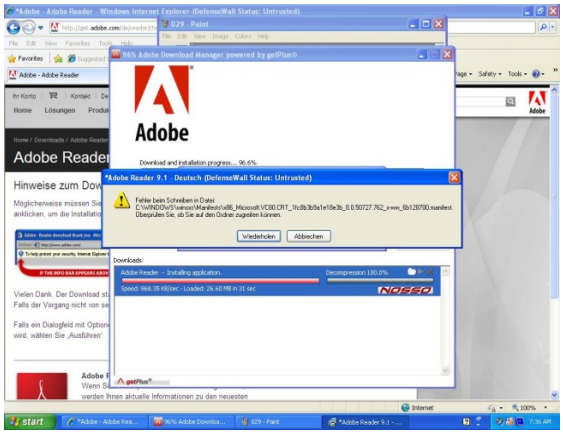


Thunderbird 2.0.0.21

Click on the download link. There is a warning. The download starts. Installation is successful (Untrusted). The program works.

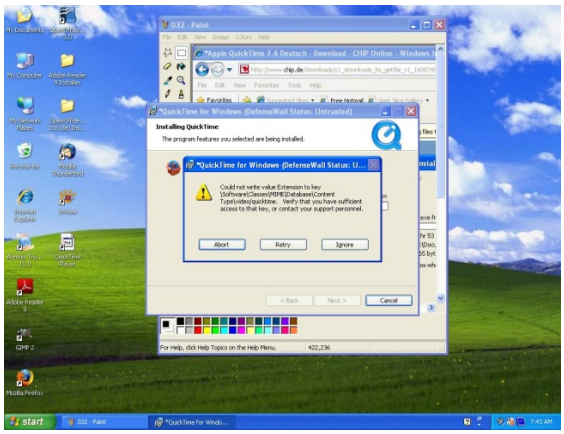
Adobe Reader 9.1

Click on the download link. There is a warning. The download starts. Installation fails (Untrusted). Manual installation is successful (Trusted). The program works.



Gimp 2.6.6

Click on the download link. There is a warning. The download starts. Installation is successful (Untrusted). The program works.



Realplayer 11.1

Click on the download link. There is a warning. The download is started. Installation fails (Untrusted). Manual installation is successful (Trusted). The program works.

Quicktime 7.6

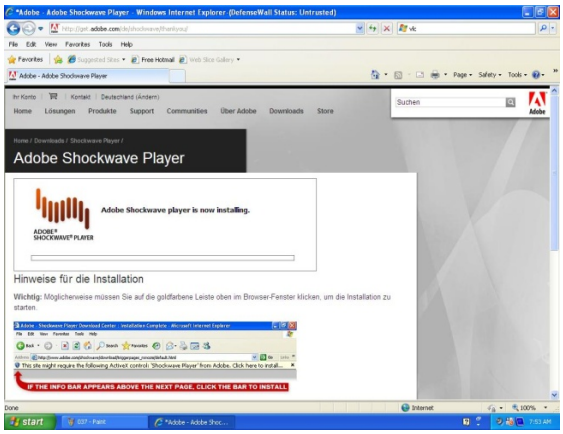
Click on the download link. There is a warning. The download starts. Installation fails (Untrusted). Manual installation is successful (Trusted). The program works.

VLC Media Player 0.9.9

Click on the download link. There is a warning. The download starts. Installation is successful (un-trusted). The program works.

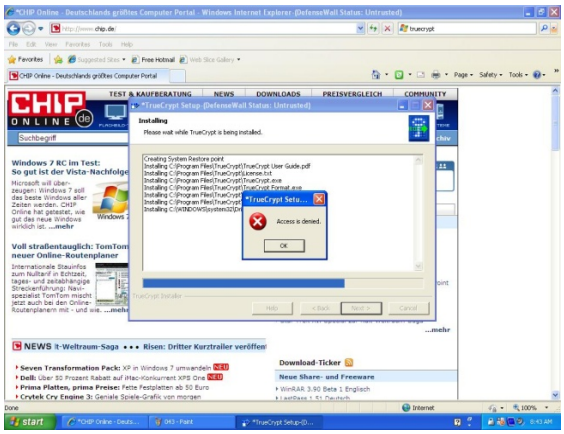
Shockwave 11.5

Click on the download link. There is a warning. The download starts. Installation is discontinued (Untrusted). Manual installation is successful (Trusted). The program works.



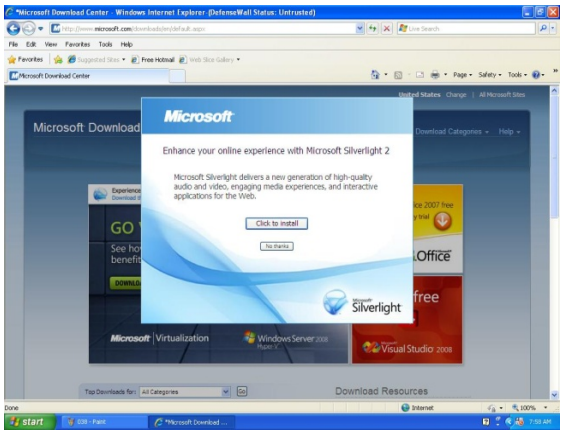
Truecrypt 6.1a

Click on the download link. There is a warning. The download starts. Installation fails (Untrusted). Manual installation is successful (Trusted). The program works.



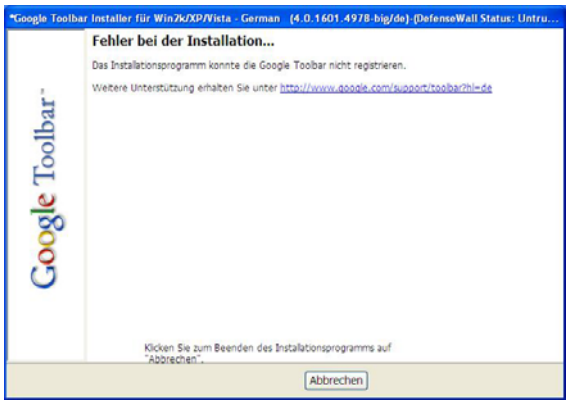
Silverlight 2

Click on the download link. There is a warning. The download starts. Installation fails (Untrusted). Manual installation fails (Trusted). The program cannot be installed.



Google Toolbar

Click on the download link. There is a warning. The download starts. Installation is discontinued (Untrusted). Manual installation fails (Trusted). The program cannot be installed.

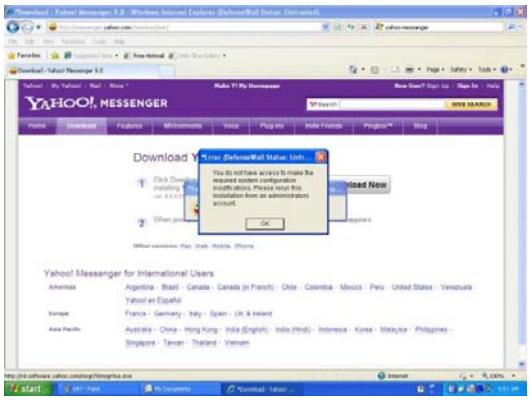


Xnview 1.96

Click on the download link. There is a warning. The download starts. Installation is successful (un-trusted). The program works.

Yahoo! Messenger 9.0

Click on the download link. There is a warning. The download starts. Installation fails (Untrusted). Manual installation is successful (Trusted). The program works.

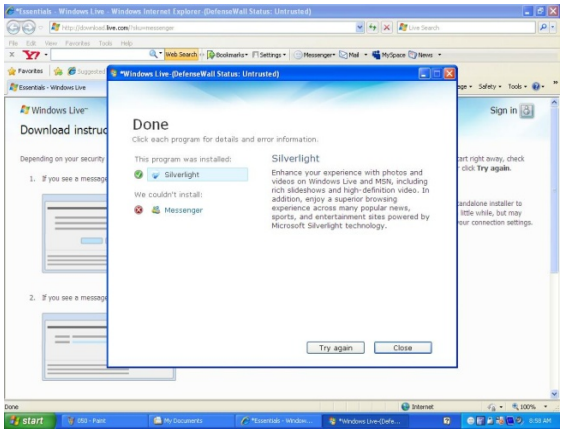


PGP Desktop 9.10

Click on the download link. There is a warning. The download starts. The setup starts directly from the Windows ZIP Container. Installation is successful (Trusted). The system restarts. The license is activated. The program works.

Windows Live Messenger

Click on the download link. There is a warning. The download starts. Installation fails (There is a continuous change from "Untrusted" to "Trusted" in the window). Silverlight is installed while Messenger is not. Installation fails (Trusted). The program cannot be installed.

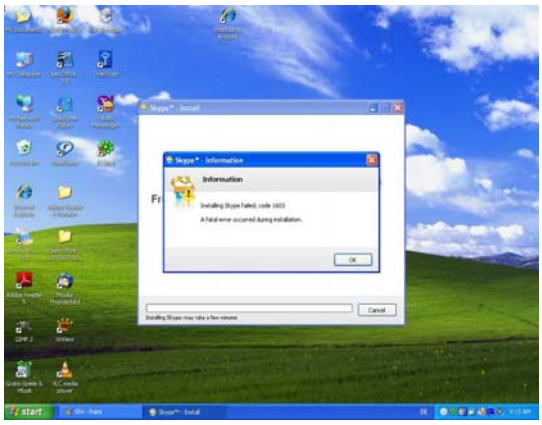


WinRAR 3.8

Click on the download link. There is a warning. The download starts. Installation is successful (Untrusted). The program works.

Skype

Click on the download link. There is a warning. The download starts. Installation is discontinued (Untrusted). Manual installation fails (Trusted). The program cannot be installed.



Trillian 3.1.12.0

Click on the download link. There is a warning. The download starts. Installation is successful (Untrusted). The program works.

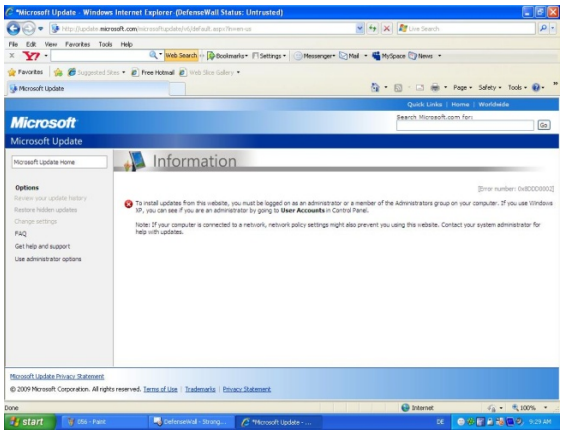
ICQ 6.5

Click on the download link. There is a warning. The download starts. Installation is successful (Untrusted). The program works.

Office 2003 Professional

Office 2003 was the only package that we installed from a CD because there were no alternatives. The setup was detected as being "Trusted" and could execute without problems. As in the case of Windows Update, the updates could only be imported as "Trusted". In our test environment, an error had crept into Internet Explorer or DefenseWall during the course of the installation. Updates were no longer possible starting from this point of time until DefenseWall was uninstalled. All attempts to repair the condition manually (fresh

registration of the dll files, repair scripts, etc.) failed and could not provide a solution.

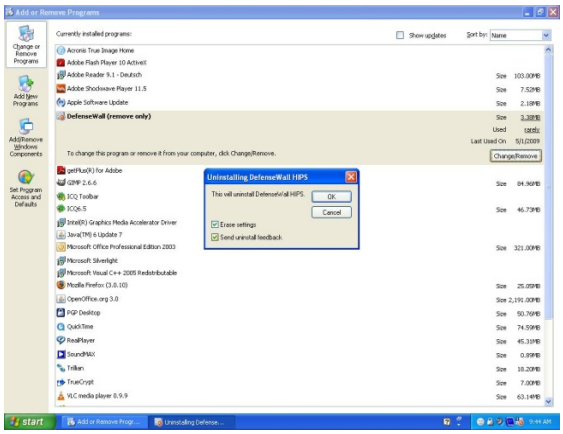


Most programs start as being untrusted. However, some trustworthy programs do not start as being untrusted (possibly because of Certificates).

Notes: Skype, Windows Live and Silverlight issues are fixed in the 2.55 version of DefenseWall.

Uninstallation

During the uninstallation procedure, we were particularly eager to see what happens to the programs that had been installed as being "untrusted". We thus start the Control Panel and un-install the program using the "Add or Remove Program" option. Uninstallation, too, was completed within a matter of seconds, and we were prompted to restart the computer.



After rebooting, all programs installed previously continued to work perfectly: OpenOffice 3.0.1, Gimp 2.6.6, WinRAR 3.8, Firefox 3.0.10, Thunderbird 2.0.0.21, Adobe Reader 9.1, Xnview 1.96, Quicktime 7.6, Realplayer 11.1, VLC Media Player 0.9.9, Java 6 Update 7, Shockwave 11.5, PGP Desktop 9.10, Truecrypt 6.1a, Yahoo! Messenger 9.0, Windows Live Messenger, ICQ 6.5 and Trillian 3.1.12.0.

Malware Test

We have tested the software on 100 current Malware Samples (Adware, Spyware, Viruses, Trojan Horses, Backdoors, etc.) that were not detected by other major Anti-Virus products at time of testing. All the samples were detected or executed as being untrusted or without compromising the system.

Even though a protection rate of 100% was achieved at this test, it should be clarified that in reality, there is no 100% protection with any product.

What should be emphasized is that the software should be regarded as being a supplement to an Anti-Virus product and not as a replacement.

DefenseWall's defense is at driver-level. In theory, it would be possible for malware to get loaded before DefenseWall's driver, but to do this it would have to fully penetrate its sandbox defense first.

DefenseWall HIPS does not block e.g. buffer overflows (so far), phishing attacks, Internet connections/browser hijacks.

Conclusion

DefenseWall HIPS, manufactured by SoftSphere Technologies, is a well-designed product, which really has the potential to protect users, who are not well-versed in computers, from all types of threats from the Internet, since it treats almost all processes running under e.g. in browsers as "untrusted". As long as you observe this setting, hardly anything can happen to you.

Minor issues we encountered during our review were reported by us to the developer, which promptly addressed and fixed them in the version 2.55 of DefenseWall.

Currently the program costs about $ 29.95 in the on-line shop and can also be delivered as a CD upon extra charge.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives e.V. (May 2009)