Anti-Virus Comparative

Summary Report 2011

Awards, winners, comments

Language: English
December 2011
Last Revision: 22nd December 2011

www.av-comparatives.org

Table of Contents

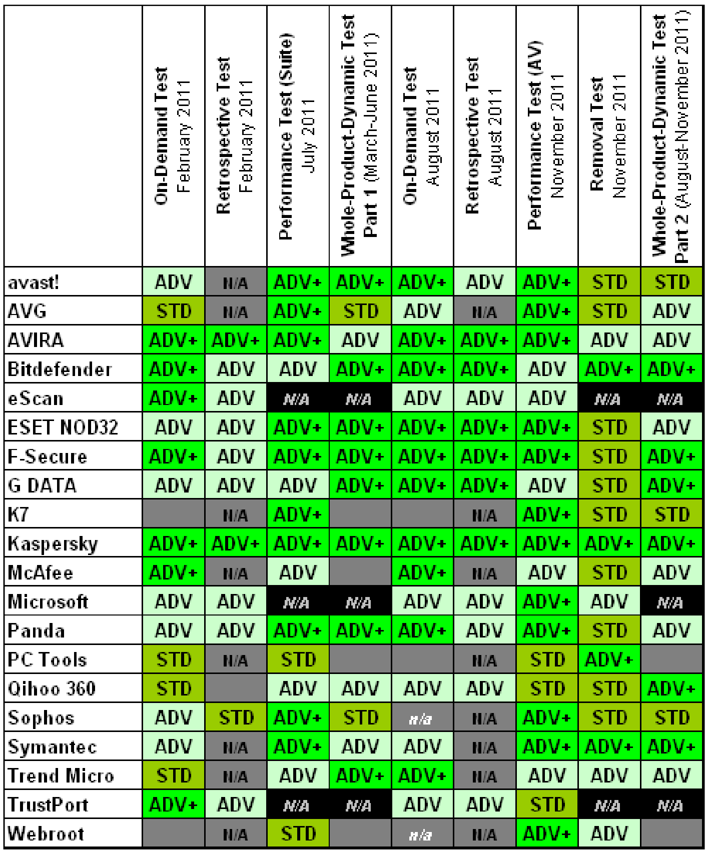
Introduction

At the end of every year, AV-Comparatives releases a summary report to comment on the various anti-virus products tested over the year, and to mention again the high-scoring products of the various tests. Please bear in mind that this report looks at all the comparative tests of 2011, i.e. not only the latest ones. Comments and conclusions are based on the results shown in the various comparative test reports of AV-Comparatives, as well as from observations made during the tests (http://www.av-comparatives.org/comparativesreviews).

Overview of levels reached during 2011

It is important that readers understand that the STANDARD level/award is already a good score, since it requires a program to reach a certain standard of quality. Additionally, all the products tested are security programs from reputable and reliable manufacturers.

Below is an overview of levels/awards reached by the various anti-virus products in AV-Comparatives' tests of 2011. Vendors, who did not want to see some features of the product evaluated, renounced being considered for the summary awards.



	On-Demand Test February 2011	**Retrospective Test** February 2011	**Performance Test (Suite)** July 2011	**Whole-Product-Dynamic Test** **Part 1** (March-June 2011)	**On-Demand Test** August 2011	**Retrospective Test** August 2011	**Performance Test (AV)** November 2011	**Removal Test** November 2011	**Whole-Product-Dynamic Test** **Part 2** (August-November 2011)
avast!	ADV	N/A	ADV+	ADV+	ADV+	ADV	ADV+	STD	STD
AVG	STD	N/A	ADV+	STD	ADV	N/A	ADV+	STD	ADV
AVIRA	ADV+	ADV+	ADV+	ADV	ADV+	ADV+	ADV+	ADV	ADV
Bitdefender	ADV+	ADV	ADV	ADV+	ADV+	ADV+	ADV	ADV+	ADV+
eScan	ADV+	ADV	*N/A*	*N/A*	ADV	ADV	ADV	*N/A*	*N/A*
ESET NOD32	ADV	ADV	ADV+	ADV+	ADV+	ADV+	ADV+	STD	ADV
F-Secure	ADV+	ADV	ADV+	ADV+	ADV+	ADV+	ADV+	STD	ADV+
G DATA	ADV	ADV	ADV	ADV+	ADV+	ADV+	ADV	STD	ADV+
K7		N/A	ADV+			N/A	ADV+	STD	STD
Kaspersky	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+	ADV+
McAfee	ADV+	N/A	ADV		ADV+	N/A	ADV	STD	ADV
Microsoft	ADV	ADV	*N/A*	*N/A*	ADV	ADV	ADV+	ADV	*N/A*
Panda	ADV	ADV	ADV+	ADV+	ADV+	ADV	ADV+	STD	ADV
PC Tools	STD	N/A	STD			N/A	STD	ADV+	
Qihoo 360	STD		ADV	ADV	ADV	ADV	STD	STD	ADV+
Sophos	ADV	STD	ADV+	STD	*n/a*	N/A	ADV+	STD	STD
Symantec	ADV	N/A	ADV+	ADV	ADV	N/A	ADV+	ADV+	ADV+
Trend Micro	STD	N/A	ADV	ADV+	ADV+	N/A	ADV	ADV	ADV
TrustPort	ADV+	ADV	*N/A*	*N/A*	ADV	ADV	STD	*N/A*	*N/A*
Webroot		N/A	STD		*n/a*	N/A	ADV+	ADV	

Key:

ADV+: ADVANCED+

ADV: ADVANCED

STD: STANDARD

Grey: TESTED

Grey+N/A: vendor refused to get evaluated

Black+N/A: vendor did not take part

Although STANDARD is already a good score, tests in which a STANDARD award (or lower) was reached indicates areas which need further improvement compared to other products. ADVANCED indicates areas which may need some improvement, but are already very competent.

Winners

If you plan to buy an anti-virus program, please visit the vendor's website and evaluate their software by downloading a trial version, as there are also many features and important considerations (e.g. compatibility, graphical user interface, ease of use, price, support etc.) that you should evaluate for yourself. As explained above, the perfect anti-virus program or the best one for all needs and for every user does not exist. Our winners' category is based on test results and does not evaluate or consider other factors that may be of importance for specific users' needs or preferences. Being recognized as "Product of the Year" does not mean that a program is the "best" in all cases and for everyone; it only means that its overall performance in our tests throughout the year was consistent and unbeaten. The Product of the Year award depends on the number of Advanced+ awards received in all our tests. As all products receiving an Advanced+ award are considered (statistically speaking) to be as good as each other, a product can receive the Product of the Year award without necessarily reaching the highest score in any individual test.

Overall winner of 2011 (Product of the Year):

To be rated "Product of the Year" by AV-Comparatives, an anti-virus program must have very high detection rates of malware (with internet access and latest signatures), good heuristic detection, produce very few false positives (FP), scan fast and reliably with a low system impact, protect the system against malware/websites with malicious software without relying significantly on user decisions/interactions, have good malware removal capabilities, cause no crashes or hangs, and have no annoying bugs.

Looking at the awards given in all of our tests in 2011, only one product received the Advanced+ award in every single test. The Product of the Year award goes to

Kaspersky

Top Rated Products 2011

This year, like last year, a number of products reached a very high standard in all our tests. Although we still only have one Product of the Year, we have decided to recognise all those products with excellent overall results by giving them the new AV-Comparatives Top Rated award.

We used the number of Advanced+ results in all tests as the basis for this award; products that got at least 5 Advanced+ awards received the Top Rated award, whereby good results in the detection/protection tests are essential. Good results in the performance tests cannot make up for weak results in the detection tests.

Top Rated products for 2011 are

AVIRA - Bitdefender - ESET - F-Secure - Kaspersky

On-Demand Malware Detection winners:

A high detection rate of malware – without causing too many false alarms - is still one of the most important, deterministic and reliable features of an anti-virus product (as e.g. it is not heavily dependent of vectors and other factors).

The following products received the ADVANCED+ award in both overall On-Demand Detection tests, in February and August 2011. The figure shown is the average of the two test results: ***F-Secure*** (98.2%), ***AVIRA*** (98.2%), ***Bitdefender*** (97.7%), ***Kaspersky*** (97.4%) and ***McAfee*** (96.8%).

AWARDS

AV
comparatives
ON-DEMAND MALWARE DETECTION 2011
GOLD

F-Secure

AV
comparatives
ON-DEMAND MALWARE DETECTION 2011
SILVER

AVIRA

AV
comparatives
ON-DEMAND MALWARE DETECTION 2011
BRONZE

Bitdefender

Proactive On-Demand Detection winners:

The retrospective tests show how good the static/offline heuristic detection of the various Anti-Virus products with highest settings is (how good they are at detecting new/unknown malware). A high heuristic detection rate must be achieved with a low rate of false alarms.

The following products received the ADVANCED+ award in both retrospective tests of 2011. The figures shown are the AVERAGE of the two test results, but the SUM of the false positives from both tests: ***AVIRA*** (~60.7%, 20 FPs) and ***Kaspersky*** (~57.6%, 13 FPs).

AWARDS

AV
comparatives
PROACTIVE
MALWARE
DETECTION
2011
GOLD

AVIRA

AV
comparatives
PROACTIVE
MALWARE
DETECTION
2011
SILVER

Kaspersky

False Positives winners:

False positives can cause as much trouble as a real infection. Due to this, it is important that anti-virus products undergo stringent quality assurance testing before release to the public, in order to avoid false positives. The products with the lowest rate of false positives during 2011 were ***McAfee*** (0), ***Microsoft*** (2) and ***F-Secure*** (9). These figures represent the SUM of the false positives from both FP Tests.

AWARDS

McAfee

Microsoft

F-Secure

On-Demand Scanning Speed winners:

It is recommended that users regularly perform a full scan of their entire systems, in order to check that all the files on their machines are still clean. The products with the highest on-demand throughput rate were ***Avast*** (~16.4 MB/sec), ***K7*** (~13.0 MB/sec) and ***Trend Micro*** (~12.9 MB/sec).

AWARDS

Avast

K7

Trend Micro

Overall Performance (Low-System-Impact) winners:

Anti-virus products must remain turned on under all circumstances, while users are performing their usual computing tasks. Some products may have a higher impact than others on system performance while performing some tasks. ***ESET***, ***Symantec***, ***K7*** and ***AVIRA*** demonstrated a lower impact on system performance than others.

AWARDS

AV
comparatives
BEST OVERALL SPEED 2011
GOLD

ESET, Symantec

AV
comparatives
BEST OVERALL SPEED 2011
SILVER

K7

AV
comparatives
BEST OVERALL SPEED 2011
BRONZE

AVIRA

Malware Removal winners:

A very useful ability for an anti-virus program is removal of malware which has already infected a system. In this year's test, ***Bitdefender***, ***PC Tools***, ***Kaspersky*** and ***Symantec*** received the Advanced+ award.

AWARDS

AV
comparatives
MALWARE
REMOVAL
2011
GOLD

Bitdefender

AV
comparatives
MALWARE
REMOVAL
2011
SILVER

PC Tools

AV
comparatives
MALWARE
REMOVAL
2011
BRONZE

Kaspersky, Symantec

Whole-Product Dynamic Protection winners:

Security products include various different features to protect systems against malware. Such protection features can be taken into account in whole-product dynamic protection tests, which are tests under real-world conditions. Products must provide a high level of protection without producing too many false alarms, and without requiring the user to make many decisions. ***Bitdefender***, ***F-Secure***, ***G DATA*** and ***Kaspersky*** all received the Advanced+ award in both tests of 2011.

AWARDS

AV
comparatives
DYNAMIC
PROTECTION
2011
GOLD

Bitdefender

AV
comparatives
DYNAMIC
PROTECTION
2011
SILVER

F-Secure

AV
comparatives
DYNAMIC
PROTECTION
2011
BRONZE

G DATA

AV-Comparatives Summary Report 2011

Review Section

Important note

The awards and certifications mentioned in this report are based purely on our test results. The program reviews are based on our own observations and opinions. We strongly recommend potential buyers of any of the programs in this report to evaluate the software themselves by using a trial version, and to consider other factors which we have not looked at here (such as e.g. compatibility, price and technical support), before deciding to use a particular product.

Individual reviews of programs tested by AV-Comparatives in 2011

Features and settings of each program described in the review

Please note that for the sake of convenience, we generally refer to the programs reviewed, as a group, as (Internet security) suites, although in at least some cases this is not strictly true. We feel that this small technical inaccuracy results in a more readable report.

Components

We list the major protection components included in the suite, such as antivirus (antimalware), antispam, firewall, parental control, backup, and shredder. We have noted these for the convenience of our readers only; we do not want to imply that any feature other than the antivirus component is essential for protection against malware, or that e.g. a suite/program that includes its own firewall is necessarily superior to one that relies on Windows Firewall.

Installation

In this section, we looked at the installation process to see if it was simple for non-expert users, and if it offered a custom option for advanced users. We considered whether the installation file was a full installation package, or a downloader that simply downloaded the files over the internet during the setup process. Please note that in the case of downloader files, the file size we have mentioned is only the downloader itself, and the total installation may be very much bigger. Where we are aware that both types of installer are available, we have reported this. We note that downloaders are useless without an Internet connection. Some setup files contain a complete package, but check online for a newer version, and download this if it exists. We consider this to be an ideal solution.

Almost all of the manufacturers in this review make a simple antivirus program without any extra components, which would then rely on e.g. Windows own firewall. It therefore seems reasonable to check whether it is possible to choose the components of the Internet security suite, so that advanced users could use an alternative firewall or antispam program if they chose to.

Some installers are multilingual and offer a choice of interface languages; in some cases, multiple languages can be installed, and the interface language changed after installation. We have noted the language options available as they would be of interest e.g. to multilingual families.

We report whether the suite asks about the network type, i.e. whether it is to be regarded as public or private, and thus whether file and printer sharing etc. should be allowed. We suggest that it is reasonable either to adopt the same network type set in Windows Network and Sharing Center, or to ask the user during the setup process.

It is standard for security programs to register with Windows Action Center (Security Center in older Windows versions) as antivirus, antispyware and firewall programs. We checked to see how each suite registers, and whether it disables Windows Firewall and/or Windows Defender. Microsoft clearly recommends disabling Windows Firewall if another software firewall is used on the same computer; hence we generally assume that a suite should switch off Windows Firewall if it is installing its own. In the case of Windows Defender, we take a neutral view. A good Internet security suite or antivirus program should provide excellent protection against adware and spyware by itself, rendering Windows Defender redundant; equally, most suites seem to co-exist peacefully with Windows Defender, so turning it off is not very important. We regard Action Center/Security Center as an important tool in assessing the security state of a computer, and so we consider it essential that a security program should accurately register the components installed and whether they are active or not.

An item that should not be forgotten is the Internet security suite's uninstaller. Whilst all fulfil the basic requirement of removing the program from the computer, others offer a selective removal of components (e.g. removal of the antispam element), whilst leaving other components intact. This can be helpful to advanced users and so we have noted whether this is possible. Another feature found in some uninstallers is a repair function, which will replace missing or corrupted files and settings. This is a very quick and convenient way of repairing a malfunctioning suite, so we have mentioned those programs that offer it.

Program interface

In describing the layout of each suite's main window, we have concentrated mostly on elements we feel are essential to maintaining good security, and how visible/accessible they are. Firstly, we consider a status display, showing whether important protection components such as real-time antivirus are up-to-date and working correctly, to be very important. In the event that something is amiss, we would expect the status display to show this clearly, and provide an easy means of correcting this (or at least attempting to correct it) automatically. A big and obvious "Fix All" button is an obvious means of doing this, although there are other possibilities. In addition to the status display, we look for an update button, to download the very latest malware definitions. In the case of programs that use only cloud-based definitions, such a feature is of course unnecessary. However, we would be pleased to see programs that use cloud-based signatures issuing a warning when they are unable to reach their respective servers. We hope to see such warnings being introduced in future versions.

Another important feature that should be easily accessible is a scan button. We look to see whether it is quick and easy to run both full and custom scans from the main window.

Other points we look for in the interface are easy access to subscription information, so that the user can renew the subscription in time and ensure continuous protection, and the help features.

Default configuration

In this section of the review, we have looked at the default configuration for each suite regarding firewall settings, and the message displayed/action taken when malware is discovered. We have especially considered the needs of non-expert users, who largely require the software to make sensible decisions for them, rather than ask questions they cannot understand.

Scanning and malware discovery

We have looked at how to configure a scheduled scan, and whether one is set by default. We also consider whether it is possible to do a boot-time scan, to remove malware before the Windows interface has loaded.

The next test checks how each suite reacts when malware is discovered, by scanning a few common malware and rogue antivirus files. We must stress that this is NOT a detection test, and we ignored any cases where the suite being tested did not detect or remove one of the samples. The aim is to see how each suite reacts to multiple malware items, and how it informs the user.

To test each suite, we copied the malware (in a password-protected zip file) to our test PC, and then deliberately disabled the real-time protection in order to unpack the malware files into a normal folder. We then right-clicked the folder and chose the scan option provided by the security suite manufacturer. We noted how the suite informed the user about the malware found, and whether it automatically took action or gave the user a choice. We then repeated the procedure but ran a custom scan on the folder from the program interface. Finally, we attempted to download the EICAR test file from www.eicar.org and again noted the result.

We feel that to be suitable for non-expert users, a suite should either take action automatically or present a very clear default option (quarantine being ideal in both cases). Where it takes action automatically, the program should make clear that it has done so, and that no further action needs to be taken.

Inbound firewall settings – if applicable

When creating the Windows image to be used on our test PC, we set the network type to Work, and enabled file and printer sharing in Windows Network and Sharing Center; we also set up a file share with a text document in, which could then be opened and edited from another computer on the same network.

During the setup process for each suite, if we were asked whether the PC's current network should be regarded as public or private, we always selected private, meaning that file sharing should continue to function after the suite had been installed. When each suite was up and running, we tested firstly whether we could ping the test PC from another computer on the LAN, and then whether it was possible to open, edit and save the text file in the file share.

In the case of the programs that did not contain their own firewall, but used Windows Firewall, this section was redundant.

Outbound firewall/application control

In order to test the outgoing firewall/application control settings of each suite, we developed a simple program which we describe as a firewall tester. This simply attempts to contact an FTP server over the Internet, and download a simple text file. This assesses whether the default settings of the suite block the program's operation, allow it without question, or query whether it should be allowed. We must again stress that this is NOT a detection test; the program is entirely harmless and should not be recognised as malicious. In fact, we would argue that if it is to be regarded as suitable for beginners, a suite should allow the firewall tester to complete its task without any form of restriction and without asking any questions. We are of the opinion that asking non-expert users whether to allow a particular program or process to access the Internet is totally counter-productive; the user will almost certainly not be able to make an informed decision, and will probably either allow all requests or block all requests, making the process either pointless or even actually destructive.

In the event that the firewall tester completed its task without query, we looked for firewall/application control settings which would ask if the program should be allowed; we consider this to be a valid option for advanced users. If the suite's default action is to ask about allowing the firewall tester, we checked to see if there is a setting which will switch this behaviour off.

We ran this test with all the programs we reviewed; however, in the case of programs that used Windows Firewall we did not feel it was necessary to mention the result in the report. When the firewall tester is run on a system using only Windows Firewall with default configuration, there is no interaction or interference from the firewall at all, and the test completes successfully without any interference or query.

Spam protection – if applicable

We checked to see if the suite's spam protection (if applicable) was switched on by default; we also tried to find out what action would be taken with spam mails, and which email clients were supported, although not all suites made these point clear in their settings.

We did not consider it important whether spam protection was on or off by default, provided the user was clear about the state, and did not assume protection was on when it wasn't.

Parental Control – if applicable

We looked to see if this feature could be considered active in any way by default, and how to configure it. As with the spam protection, we felt that if it needed to be configured before becoming active, then the program interface should make this clear to the user.

Safe Mode

In order to remove a malware infection from a PC, it can be valuable to start in Safe Mode. To test how each security program would function in Safe Mode, we copied our zip file of malware programs to the test PC, and then started in Safe Mode with Networking. We unzipped the malware files into a folder on the desktop. Next, we attempted to open the security suite's program window; enable real-time protection; run an update (hence Safe Mode with Networking); run a custom scan on the malware folder. We also attempted to run a scan on the malware from Windows Explorer's context menu – this was the only option available in cases where we could not open the program window.

We must stress that this is NOT a malware removal test; all the samples were inactive. We were only testing each program's ability to function in Safe Mode on an entirely clean and functional PC.

Help and documentation

The final area we looked at for each security program was the help functions. We looked for both local help (i.e. help files installed on the local PC) and online help, i.e. pages of the manufacturer's website and downloadable manuals. Conducting a full review of the entire help and documentation available for 20 programs would be a mammoth task, so to get a rough idea of the usefulness of the help functions, we searched for answers to two questions in both local and online help (where both existed). We attempted to find out how to set a scheduled scan, and how to exclude a folder from scans. We felt that these were questions many users might want answered, and so a reasonable help function should cover them. We tried slightly different search terms depending on whether we expected complete sentences to be understood ("How do I… ?") and whether previous searches had been successful. For example, if "scan exceptions" had not produced any relevant results, we tried "scan exclusions".

We consider a useable help function to be important in a security program, especially for non-expert users. It can also be very helpful to advanced users if the interface is complicated and particular features or settings are hard to find.

Verdict

To conclude, we gave our overall opinion of the suite, and its suitability for expert and non-expert users. We also list plus and minus points for each program.

avast! Internet Security 6.0

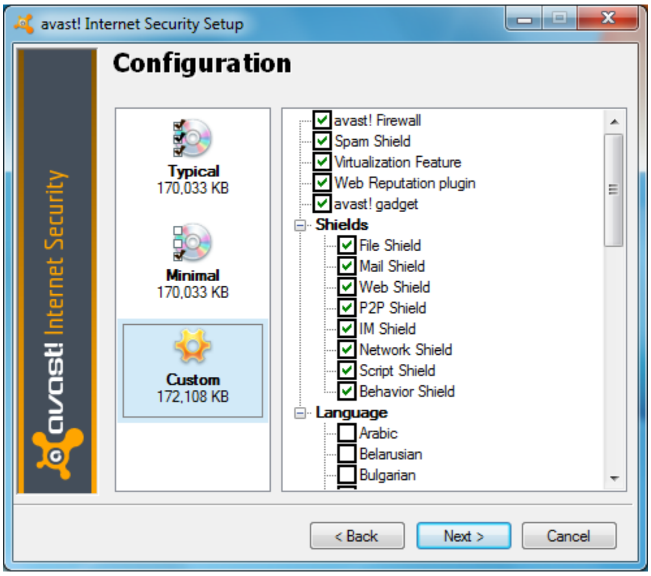
Components

- Antimalware
- Antispam
- Firewall

NB: An avast! boot CD is available (price €9.90). We have not considered this in the review, as it is not an integral part of the suite and is not included in the price.

Installation

We installed avast! Internet Security from a 79 MB .exe file. The setup wizard offers a choice of languages for the setup process, the opportunity to participate in the avast! Community (anonymous cloud-based sharing of malware information), and a custom installation (which we accepted). There then follows a choice of installation folder, product activation/trial mode selection, and a very detailed choice of both components and interface languages:



avast! Internet Security Setup

Configuration

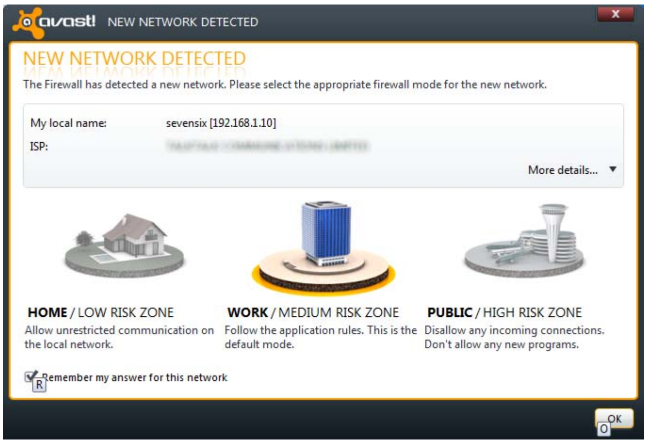
Typical
170,033 KB

Minimal
170,033 KB

Custom
172,108 KB

- ☑ avast! Firewall
- ☑ Spam Shield
- ☑ Virtualization Feature
- ☑ Web Reputation plugin
- ☑ avast! gadget
- Shields
  - ☑ File Shield
  - ☑ Mail Shield
  - ☑ Web Shield
  - ☑ P2P Shield
  - ☑ IM Shield
  - ☑ Network Shield
  - ☑ Script Shield
  - ☑ Behavior Shield
- Language
  - ☐ Arabic
  - ☐ Belarusian
  - ☐ Bulgarian

Multiple interface languages can be installed, and it is easy to change between languages after installation using the program's settings. We were pleased to note that avast! has retained its humorous Pirate Talk "language" which makes e.g. "Scan" into "Scour the ship" and "Boot-Time Scan" into "Polish me boot buckles". The installation wizard prompts the user to restart the computer after setup has finished. After rebooting, we encountered a female voice saying "Welcome to avast!", and then informing us that an update had been completed, as the suite provides audio commentary for major events (this can be disabled in the settings). We also saw the New Network dialog box, asking us to confirm the network type – we chose "Home/Low Risk Zone".



NEW NETWORK DETECTED

The Firewall has detected a new network. Please select the appropriate firewall mode for the new network.

My local name: sevensix [192.168.1.10]

ISP: [redacted]

HOME / LOW RISK ZONE
Allow unrestricted communication on the local network.

WORK / MEDIUM RISK ZONE
Follow the application rules. This is the default mode.

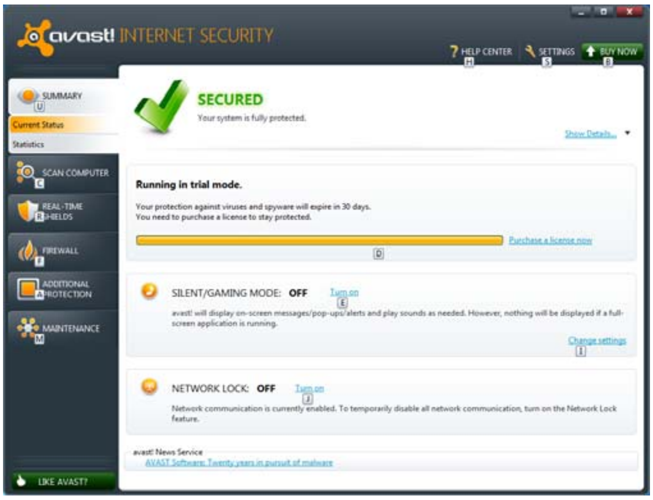
PUBLIC / HIGH RISK ZONE
Disallow any incoming connections. Don't allow any new programs.

☑ Remember my answer for this network

Looking at Windows 7’s Action Center showed us that avast! Internet Security 6.0 had registered itself as an antivirus, antispyware and firewall application. We noted that neither Windows Defender nor Windows Firewall had been disabled; we remain surprised that version 6.0, like version 5.0, leaves two firewalls running together, as Microsoft clearly recommends disabling Windows Firewall if another software firewall is used on the same computer. The suite’s uninstaller has the widest range of options we have ever seen: Change (allows components and/or languages to be added or removed), Update (installs newer program files), Repair (replaces missing or corrupted files and settings), and Uninstall (removes the program completely).

Program Interface

Anyone who has used version 5.0 of avast! Internet Security will feel at home with version 6.0, as it is all but identical to its predecessor. The program window has a familiar layout with a narrow left-hand pane containing menu buttons, and a much bigger right-hand pane to display the information and options selected. Items in the menu pane are Summary (shows system status), Scan Computer, Real-Time Shields (shows individual shields, such as File and Web, and allows individual configuration), Firewall, Additional Protection (e.g. Antispam and Site Blocking), and Maintenance (Update, Subscription, quarantine etc.). Clicking on a menu button opens up associated sub-menu items in the menu column.



SECURED

Your system is fully protected.

Running in trial mode.

Your protection against viruses and spyware will expire in 30 days.
You need to purchase a license to stay protected.

SILENT/GAMING MODE: **OFF**

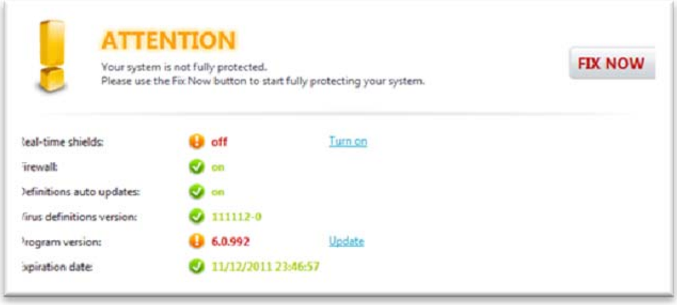
avast! will display on-screen messages/pop-ups/alerts and play sounds as needed. However, nothing will be displayed if a full-screen application is running.

NETWORK LOCK: **OFF**

Network communication is currently enabled. To temporarily disable all network communication, turn on the Network Lock feature.

avast! News Service
AVAST Software: Twenty years in pursuit of malware

The program opens by default on the Current Status page. If all is well, a big green tick (checkmark) and the word “Secured” are displayed at the top of the page. In the event of a problem, e.g. real-time protection being disabled, the program shows a big yellow exclamation mark and the word “Attention”, a big “Fix Now” button, and details of the problem:



ATTENTION

Your system is not fully protected.
Please use the Fix Now button to start fully protecting your system.

ʀeal-time shields:	off	Turn on
ɪrewall:	on	
)efinitions auto updates:	on	
/irus definitions version:	111112-0	
'rogram version:	6.0.992	Update
xpiration date:	11/12/2011 23:46:57	

In the top right-hand corner of the window are two buttons, Help Center and Settings. The latter provides detailed configuration options for all components and functions.

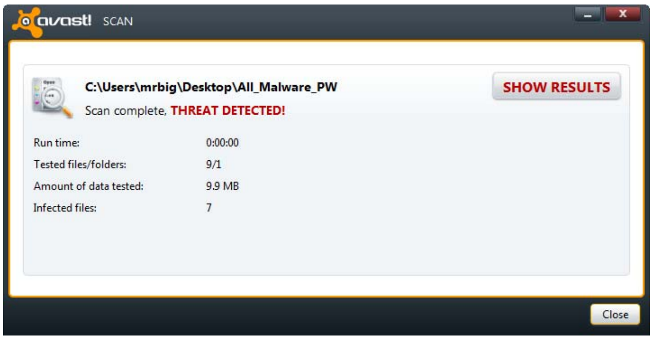
We have previously commented on the clear, easily accessible interface of avast! Internet Security 5.0, and version 6.0 retains all the good points of its predecessor.

Default settings and configuration

Scanning and malware discovery

A scheduled scan is not set up by default, but can be configured by going to Scan Computer | Scan Now | Create Custom Scan | Scheduling. We found this somewhat unintuitive and suspect it may not be easy for non-expert users to find. A boot-time scan can easily be scheduled from the Scan menu.

Running a context-menu scan or custom scan of our folder of malware samples indicated that threats had been found, but did not delete or quarantine them, or give any direct means of doing this:



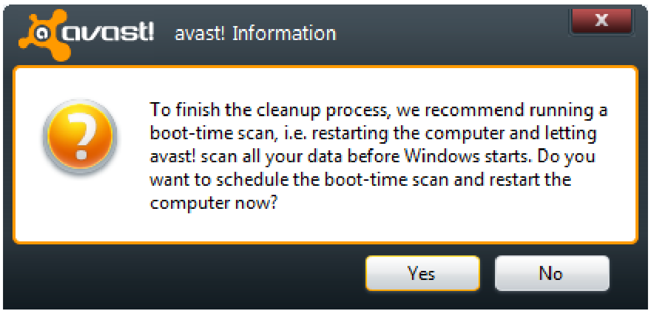
C:\Users\mrbig\Desktop\All_Malware_PW

Scan complete, THREAT DETECTED!

Run time:	0:00:00
Tested files/folders:	9/1
Amount of data tested:	9.9 MB
Infected files:	7

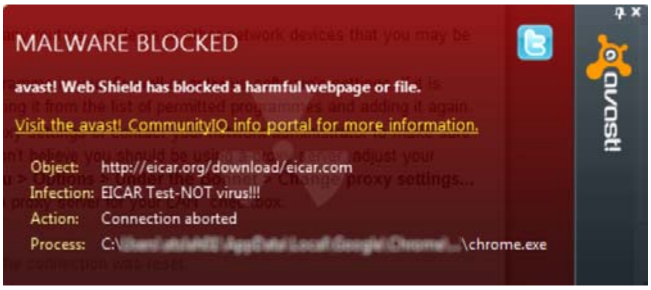
Clicking on Show Results then gives the user the options Repair, Move to Chest (quarantine) or Delete, which can be applied individually or to all threats found. Whilst these options are excellent, we are concerned that non-expert users may be confused by the initial dialog box, and simply close it without taking any action, thus rendering the scan pointless. We would suggest that avast! could make clearer to users what they need to do.

We were pleased to note that having quarantined the malware samples, avast! then suggested rebooting and running a boot-time scan:



To finish the cleanup process, we recommend running a boot-time scan, i.e. restarting the computer and letting avast! scan all your data before Windows starts. Do you want to schedule the boot-time scan and restart the computer now?

When we attempted to download the EICAR test file, avast! blocked the download and displayed the following warning:


MALWARE BLOCKED

avast! Web Shield has blocked a harmful webpage or file.

Visit the avast! CommunityIQ info portal for more information.

Object: http://eicar.org/download/eicar.com
Infection: EICAR Test-NOT virus!!!
Action: Connection aborted
Process: C:\[redacted]\chrome.exe

The warning makes clear to the user that the threat has been blocked and that no further action is required.

Inbound Firewall Settings

As mentioned previously, when rebooting after installing the program, a dialog box asks whether to regard the current network as Home, Work, or Public. We chose home, and found that we could still ping our test PC, and access its file share, from another computer on the network.

Outbound Firewall/Application Control

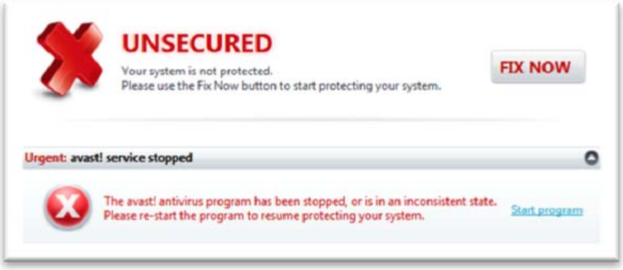
With the firewall in default mode, our firewall testing program was able to access the Internet and download the test file without any interruption or query from avast! Internet Security. We could not find any settings for the firewall which would block our firewall tester or ask for permission before allowing it.

Spam protection

Spam protection is enabled by default. It will mark suspected spam messages with the word SPAM in the subject line, and in Microsoft Outlook only will move them to a specified junk mail folder.

Safe Mode

We found that avast! Internet Security 6.0 can be used as normal to run a scan and remove malware in Safe Mode with Networking, despite a rather alarming warning message:



UNSECURED

Your system is not protected.
Please use the Fix Now button to start protecting your system.

Urgent: avast! service stopped

The avast! antivirus program has been stopped, or is in an inconsistent state.
Please re-start the program to resume protecting your system.

We are concerned that some users may assume from this message that the program is not working at all. In our test, we were unable to update the program successfully, but nonetheless ran a custom scan of our folder of malware samples, which were all detected and removed.

Help and Documentation

Clicking on the Help Center link in the program window opens the local Help window. Our searches for information on a boot-time scan and scheduled scan were both rather disappointing, in that neither produced clear instructions on how to set these up, only rather indirect references to them.

Searching the knowledge base on the www.avast.com website proved to be a somewhat hit-and-miss affair. There is an excellent video tutorial for setting up a boot scan in Internet Security 6.0, but using “Internet Security boot scan” as our search term failed to find it. However, the simple “boot scan” query uncovered it easily. Looking for instructions on a scheduled scan was more difficult still. Searching for “schedule scan” found one promising-looking article, but this applied to avast! Professional version 4.7, which has a completely different interface to Internet Security 6.0. Adding “Internet Security 6.0” to our search term was even less successful, producing no results at all.

Verdict

Overall

avast! Internet Security 6.0 is generally very easy to install and use, and has good functionality.

Plus points

Excellent installer and uninstaller with choice of components and languages; very clear, simple and elegant user interface; boot-time scan.

Minus points

Windows firewall not automatically deactivated; message box showing scan result not clear; help function could be improved.

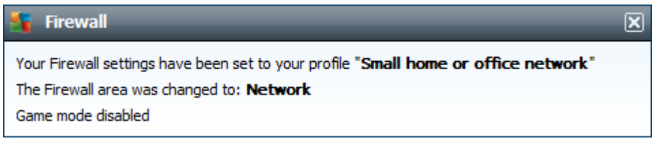
AVG Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall

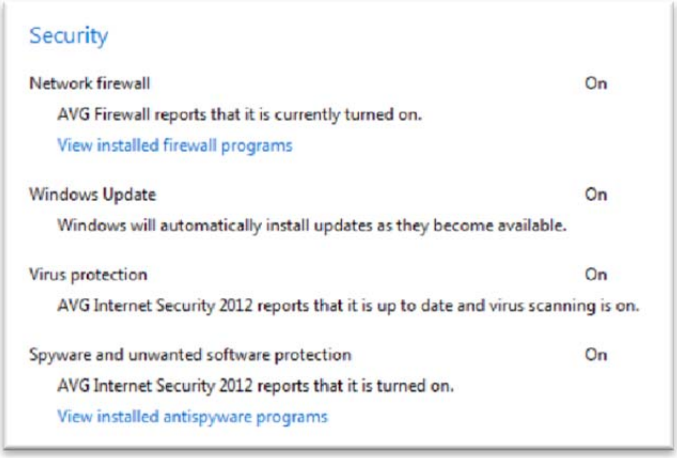
Installation

We installed AVG Internet Security from a 4 MB .exe downloader file. The wizard features a choice of language for setup, the usual licence agreement, the opportunity to enter a purchased key or use as a trial, and a custom installation, which we chose. Further options then include a detailed choice of components and interface languages to install, installation folder, and using the AVG Security Toolbar. A reboot is required when setup completes. At the first login after rebooting, AVG displayed a message box, informing us that the firewall settings had been automatically configured for “Small Home or Office Network”:



Your Firewall settings have been set to your profile "**Small home or office network**"
The Firewall area was changed to: **Network**
Game mode disabled

Looking in Windows 7’s Action Center showed us that AVG Internet Security 2012 had registered itself as an antivirus, antispyware and firewall application. Both Windows Firewall and Windows Defender had been disabled:


Security

Network firewall On
AVG Firewall reports that it is currently turned on.
View installed firewall programs

Windows Update On
Windows will automatically install updates as they become available.

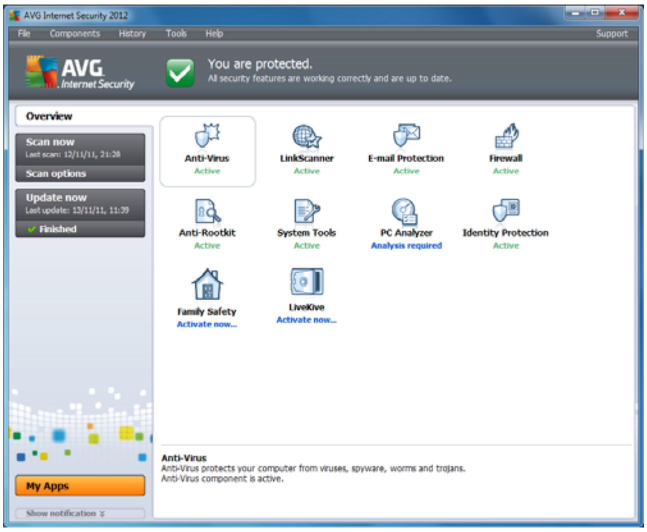
Virus protection On
AVG Internet Security 2012 reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
AVG Internet Security 2012 reports that it is turned on.
View installed antispyware programs

The uninstaller program has options to remove, repair or change the AVG suite, whereby the last of these enables program components and interface languages to be added or removed.

Program Interface

AVG Internet Security's main program window will be familiar to users of recent versions of the suite or AVG's antivirus program. There is a simple menu bar in a left-hand pane, with details displayed in a bigger right-hand pane. A horizontal strip at the top of the window shows the current security status; if there are no problems or threats, a tick (checkmark) in a green box is displayed, along with the text "You are protected":



You are protected.
All security features are working correctly and are up to date.

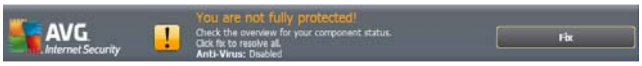
Last scan: 12/11/11, 21:28

Last update: 13/11/11, 11:39
✓ Finished

Anti-Virus: Active
LinkScanner: Active
E-mail Protection: Active
Firewall: Active
Anti-Rootkit: Active
System Tools: Active
PC Analyzer: Analysis required
Identity Protection: Active
Family Safety: Activate now...
LiveKive: Activate now...

Anti-Virus
Anti-Virus protects your computer from viruses, spyware, worms and trojans.
Anti-Virus component is active.

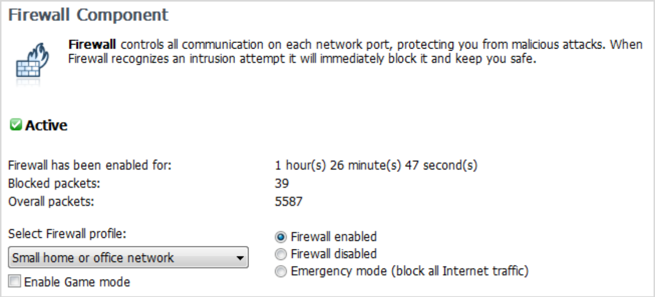
To simulate a problem, we deactivated the real-time antivirus protection; the status strip then displayed an exclamation mark in a yellow box, and the message "You are not fully protected!":



You are not fully protected!
Check the overview for your component status.
Click fix to resolve all.
Anti-Virus: Disabled

Clicking on the Fix button at the right-hand end of the strip resolves the problem by reactivating the protection. We note that a Windows 7 User Account Prompt has to be confirmed in order to do this.

The default Overview page shows all the installed components of the suite (labelled in green), plus 3 optional extras (Family Safety, PC Analyzer, LiveKive-OnlineBackup) that can be purchased separately. These are labelled in blue. Clicking on an icon for one of the installed components opens the configuration page for that item. For example, the firewall configuration page is shown below:



Firewall Component

Firewall controls all communication on each network port, protecting you from malicious attacks. When Firewall recognizes an intrusion attempt it will immediately block it and keep you safe.

✓ **Active**

Firewall has been enabled for: 1 hour(s) 26 minute(s) 47 second(s)
Blocked packets: 39
Overall packets: 5587

Select Firewall profile: Small home or office network

● Firewall enabled
○ Firewall disabled
○ Emergency mode (block all Internet traffic)

□ Enable Game mode

The other two buttons in the left-hand menu pane are Scan Now (performs a default scan), Scan Options (gives the choice of specific custom scans and the option of scheduling a scan), and Update Now.

There is a traditional menu bar at the top of the window, with File, Components, History, Tools and Help menus. Of these, the History and Help menus are the most relevant, as they contain items not accessible elsewhere in the program interface. The History menu provides access to the program's various logs, and the Help menu has links to local and online help, and the "About" item, which includes subscription information.

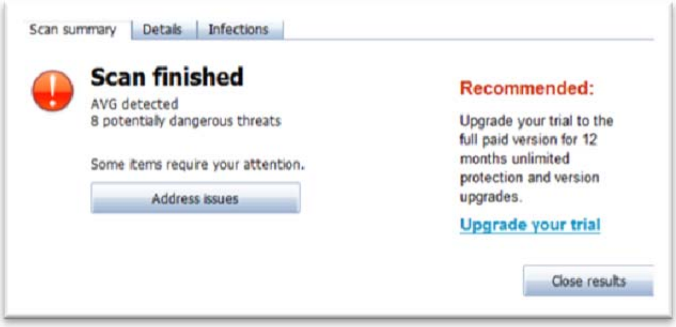
It is easy to switch between installed interface languages in the suite's advanced settings dialog box.

Default configuration

Scanning and malware discovery

A scheduled scan is not configured by default, but can be configured in the scan settings. We could not find any means of running a boot-time scan.

When we scanned our test folder of malware using custom and context-menu scans, AVG Internet Security 2012 displayed the following message:



Scan finished

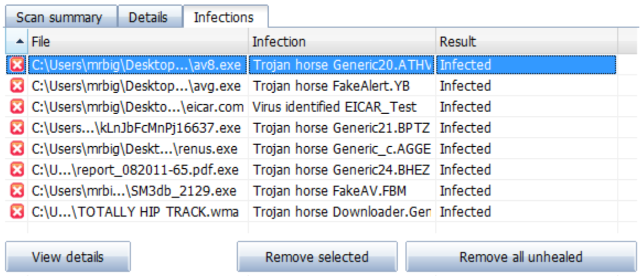
AVG detected
8 potentially dangerous threats

Some items require your attention.

Recommended:

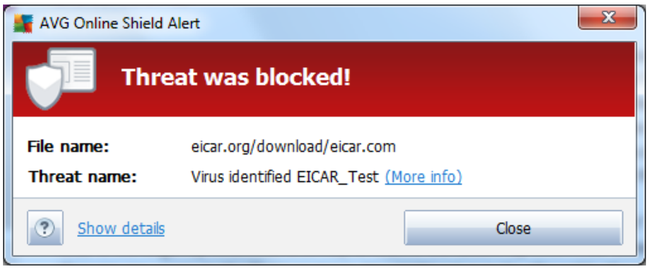
Upgrade your trial to the full paid version for 12 months unlimited protection and version upgrades.

In order to remove the threats found, it is necessary to click on "Address Issues", which then displays the following page:



File	Infection	Result
☒ C:\Users\mrbig\Desktop...\av8.exe	Trojan horse Generic20.ATHV	Infected
☒ C:\Users\mrbig\Desktop...\avg.exe	Trojan horse FakeAlert.YB	Infected
☒ C:\Users\mrbig\Deskto...\eicar.com	Virus identified EICAR_Test	Infected
☒ C:\Users...\kLnJbFcMnPj16637.exe	Trojan horse Generic21.BPTZ	Infected
☒ C:\Users\mrbig\Deskt...\renus.exe	Trojan horse Generic_c.AGGE	Infected
☒ C:\U...\report_082011-65.pdf.exe	Trojan horse Generic24.BHEZ	Infected
☒ C:\Users\mrbi...\SM3db_2129.exe	Trojan horse FakeAV.FBM	Infected
☒ C:\U...\TOTALLY HIP TRACK.wma	Trojan horse Downloader.Ger	Infected

The malware items can then be removed individually or all together. We feel that it would be better if this page were displayed automatically, as it might not be clear to non-experts what "Address Issues" means, especially if their native language is not English. Packers are not deleted, there is only a warning to the user. When we attempted to download the EICAR test file, AVG produced the following message:



AVG Online Shield Alert

Threat was blocked!

File name: eicar.org/download/eicar.com

Threat name: Virus identified EICAR_Test (More info)

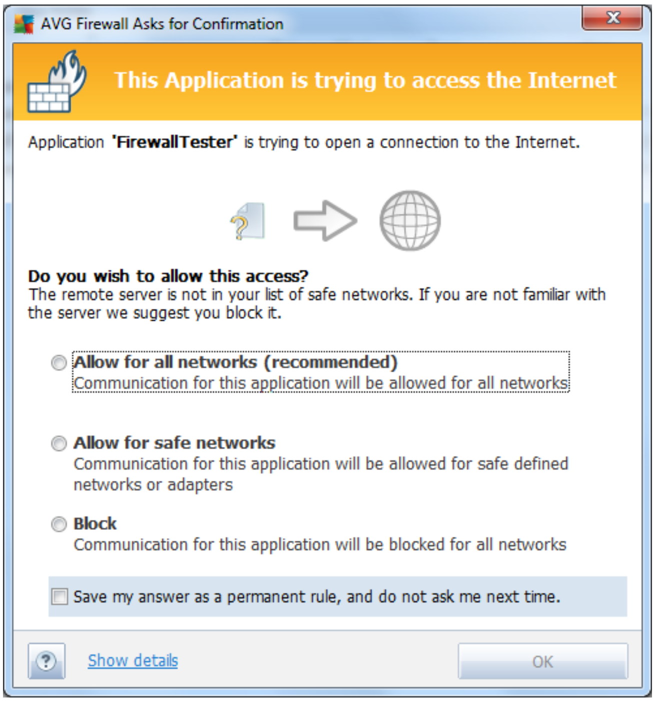
It is clear from this that no further action needs to be taken. However, we noted that AVG had not completely blocked the download, but rather stripped the content from the file. Thus we were left with a 0KB eicar.com file in our download folder; this may be a little worrying for non-expert users.

Inbound Firewall Settings

By default, the firewall's network type was set to “Small Home or Office network” our test system. We were able to ping the PC and access its file share from another computer on the same LAN.

Outbound Firewall/Application Control

When we ran our firewall testing program, AVG Internet Security 2012 produced a dialog box, asking whether we wanted to allow the program access to the Internet:



AVG Firewall Asks for Confirmation

This Application is trying to access the Internet

Application **'FirewallTester'** is trying to open a connection to the Internet.

Do you wish to allow this access?
The remote server is not in your list of safe networks. If you are not familiar with the server we suggest you block it.

○ **Allow for all networks (recommended)**
Communication for this application will be allowed for all networks

○ **Allow for safe networks**
Communication for this application will be allowed for safe defined networks or adapters

○ **Block**
Communication for this application will be blocked for all networks

□ Save my answer as a permanent rule, and do not ask me next time.

There is a recommended action (in this case, Allow), and that the answer can be saved as a rule, to avoid the dialog box appearing when the program is run again. We found it easy to view and change program access permissions in the suite's firewall settings.

When we selected the “Allow for all networks” option, our firewall tester was allowed to download its test file. However, we found that selecting “Allow for safe networks” blocked the download, even when the network type had been set to “Small Home or Office Network” and the PC had been rebooted.

Spam protection

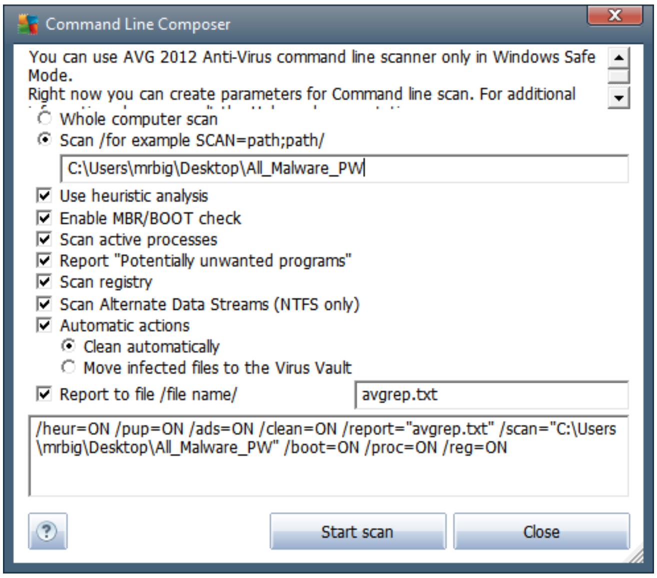
Anti-Spam is enabled by default, and marks suspected messages with [SPAM] in the subject line. It will also move spam messages to the junk folder of Microsoft Outlook, but not with other email programs.

Parental Control

The Overview page of AVG Internet Security 2012 has a link entitled Family Safety, subtitled Activate Now. However, clicking on the link opens a page which enables the user to purchase the feature; it is not included in the suite.

Safe Mode

We started our test PC in Safe Mode with Networking, and double-clicked on the AVG shortcut on the desktop. This opened AVG’s Safe Mode dialog box. This does not offer any means of updating signatures, but allows a full or custom scan to be run:



Command Line Composer

You can use AVG 2012 Anti-Virus command line scanner only in Windows Safe Mode.
Right now you can create parameters for Command line scan. For additional

○ Whole computer scan
● Scan /for example SCAN=path;path/
C:\Users\mrbig\Desktop\All_Malware_PW
☑ Use heuristic analysis
☑ Enable MBR/BOOT check
☑ Scan active processes
☑ Report "Potentially unwanted programs"
☑ Scan registry
☑ Scan Alternate Data Streams (NTFS only)
☑ Automatic actions
● Clean automatically
○ Move infected files to the Virus Vault
☑ Report to file /file name/ avgrep.txt

```
/heur=ON /pup=ON /ads=ON /clean=ON /report="avgrep.txt" /scan="C:\Users
\mrbig\Desktop\All_Malware_PW" /boot=ON /proc=ON /reg=ON
```

We chose the custom option and entered the path to the folder containing our malware collection, then started the scan. From the display, we could see that AVG was checking key Windows system files and registry entries as well as the specified folder. When the scan had finished, we checked our malware folder to see that all items had been deleted.

We found AVG’s Safe Mode solution to be a very simple and effective means of cleaning an infected PC.

Help and Documentation

The Help menu of AVG Internet Security 2012 has links to both local and online help. Searching the local Help system for “schedule scan” quickly took us to brief but clear instructions. Our local search for creating scan exceptions required more effort, but soon provided an answer. The online Help entry took us to the support page of the AVG’s website, which provided us with telephone support options, FAQ’s, forums and virus removal tools. However, the search box on this page did not find any results for our searches on scan scheduling or exceptions, and the topics were not covered in the FAQs, as far as we could see.

An extremely comprehensive manual (196 pages) is available from the AVG website, by clicking Support, Downloads. The manual is clearly written, very professionally produced, well indexed and bookmarked. It is also illustrated with abundant screenshots. We would describe it as exemplary.

Verdict

Overall

AVG Internet Security 2012 is easy-to-use, only some settings must be searched in the backend. It is a suite which is suitable for both experts and non-experts.

Plus points

Clear interface makes important information and tasks easily accessible; choice of components and interface languages in installer and uninstaller; outstanding manual

Minus points

Need to reboot after changing network type from public to private; “Allow for safe networks” setting appears not to work.

Avira Internet Security 2012

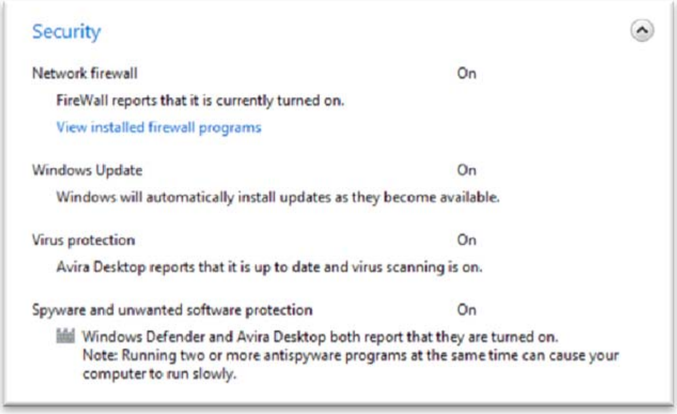
Components

- Antimalware
- Antispam
- Firewall
- Parental Controls
- Backup

Installation

We installed Avira Internet Security 2012 from an 80 MB single-language .exe file. Steps in the process include accepting a licence agreement, choosing Express or Custom installation (we selected the latter), choosing the installation folder, selecting the components of the suite to be installed, entering a licence key or opting for a trial, choosing heuristic levels and the type of threats to be detected, choosing ingoing and outgoing firewall access, whether to load real-time protection at the start of Windows' boot process, and whether to use parental controls. A reboot is required after installation. Avira probably has the longest setup routine of any of the suites we have covered in this review, but this does give the user very fine control over the components to be installed and their configuration.

Avira registers itself as an antivirus, antispyware and firewall program in Windows Action Center. Windows Firewall is disabled, Windows Defender is not:



Security

Network firewall On
FireWall reports that it is currently turned on.
View installed firewall programs

Windows Update On
Windows will automatically install updates as they become available.

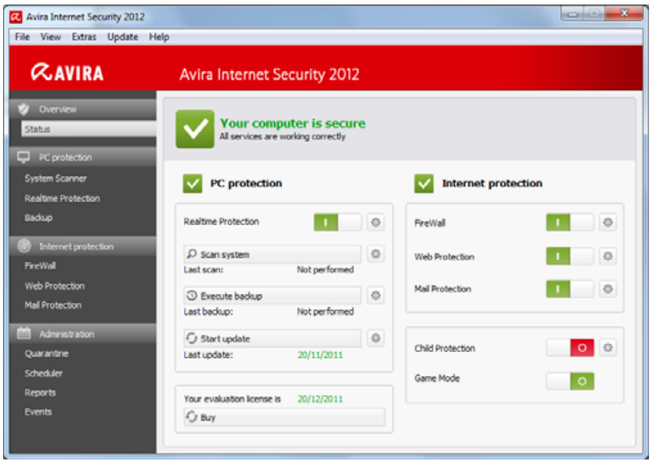
Virus protection On
Avira Desktop reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender and Avira Desktop both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

The uninstaller has a Modify option, with which individual components can be added or removed.

Program Interface

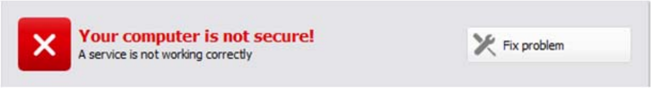
The layout of Avira Internet Security's main window uses a familiar format, with a narrow left-hand column containing menu items, and a much wider right-hand pane to show the details of the item selected. By default, the window opens on the status page, which shows the status of individual components, and the system as whole. There are also buttons to run an update, start a scan, or perform a backup:



Your computer is secure
All services are working correctly

Last scan: Not performed
Last backup: Not performed
Last update: 20/11/2011
Your evaluation license is 20/12/2011

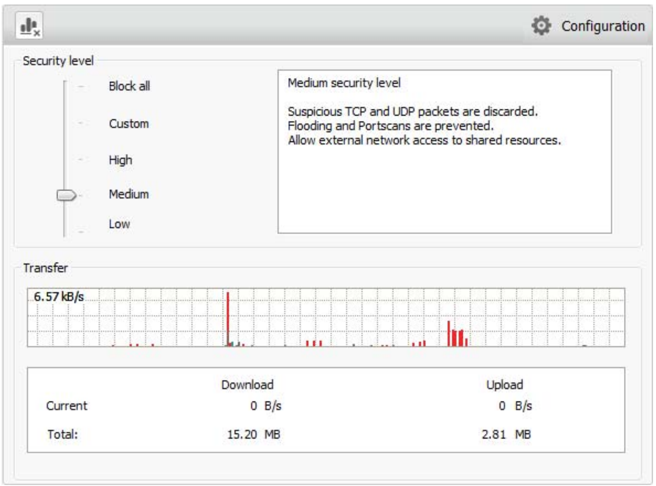
The status display shows a tick (checkmark) in a green box, along with the words “Your computer is secure”, if all is well. If an essential component such as real-time protection is switched off, the status display changes to a cross in a red box, and the words “Your computer is not secure!”:



Your computer is not secure!
A service is not working correctly

Clicking the “Fix Problem” button reactivates the component in question.

The menu pane has four sections: Overview, PC Protection, Internet Protection, and Administration. Clicking on a link opens the options for that item in the right-hand pane; many items have a “Configuration” button for more detailed options, e.g. Firewall, shown below:



Medium security level

Suspicious TCP and UDP packets are discarded.
Flooding and Portscans are prevented.
Allow external network access to shared resources.

	Download	Upload
Current	0 B/s	0 B/s
Total:	15.20 MB	2.81 MB

The Avira window also has traditional menus; some of the items in these replicate other buttons or links elsewhere in the program, while others, such as the help items, can only be found in the menu.

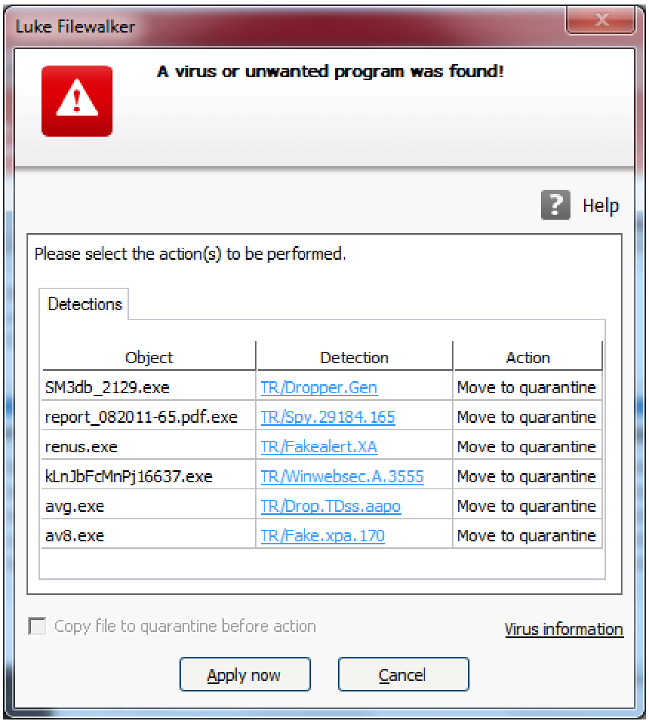
Overall, we found the interface of Avira Internet Security to be clear, simple, and easy to navigate.

Default configuration

Scanning and malware detection

A full system scan is not activated by default; however, it has been preconfigured, and can be switched on by clicking Scheduler in the menu pane, and ticking the "Enabled" box. We could not find a means of running a boot-time scan, although the setup process gives the option of loading real-time protection early in the boot process.

Running a custom or context-menu scan produced the following dialog box, the default action being to quarantine all the threats:



A virus or unwanted program was found!

Please select the action(s) to be performed.

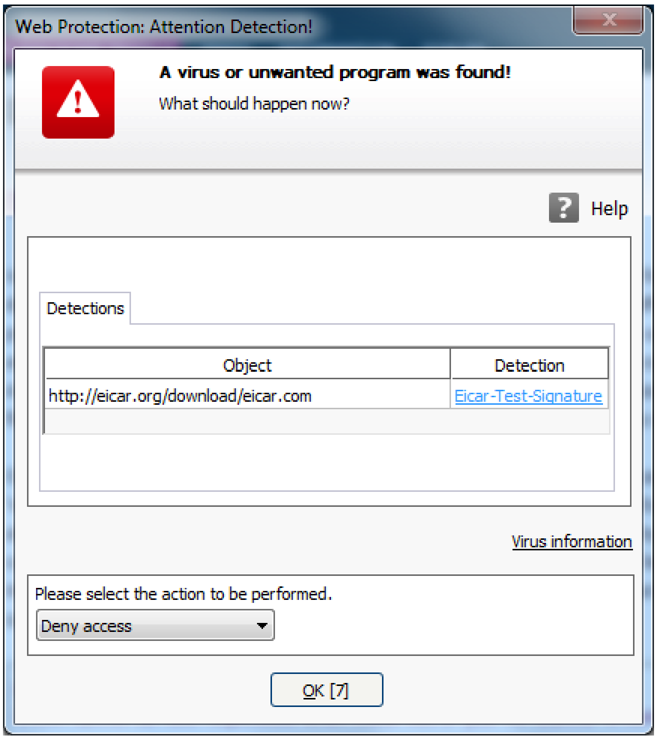
Object	Detection	Action
SM3db_2129.exe	TR/Dropper.Gen	Move to quarantine
report_082011-65.pdf.exe	TR/Spy.29184.165	Move to quarantine
renus.exe	TR/Fakealert.XA	Move to quarantine
kLnJbFcMnPj16637.exe	TR/Winwebsec.A.3555	Move to quarantine
avg.exe	TR/Drop.TDss.aapo	Move to quarantine
av8.exe	TR/Fake.xpa.170	Move to quarantine

□ Copy file to quarantine before action

Virus information

It is possible to change the default action by right-clicking an item and choosing an alternative (e.g. ignore, delete) from the shortcut menu. It is also possible to select multiple items using standard Windows techniques such as Ctrl + click or Ctrl + A, and then change the action for all of them. We feel that quarantining is an ideal default action for non-expert users, as it renders the files harmless without permanently deleting them.

When we tried to download the EICAR test file, Avira blocked the file and the page, played a warning sound, and showed the following dialog box:



Web Protection: Attention Detection!

A virus or unwanted program was found!

What should happen now?

Detections

Object	Detection
http://eicar.org/download/eicar.com	Eicar-Test-Signature

Please select the action to be performed.

Deny access

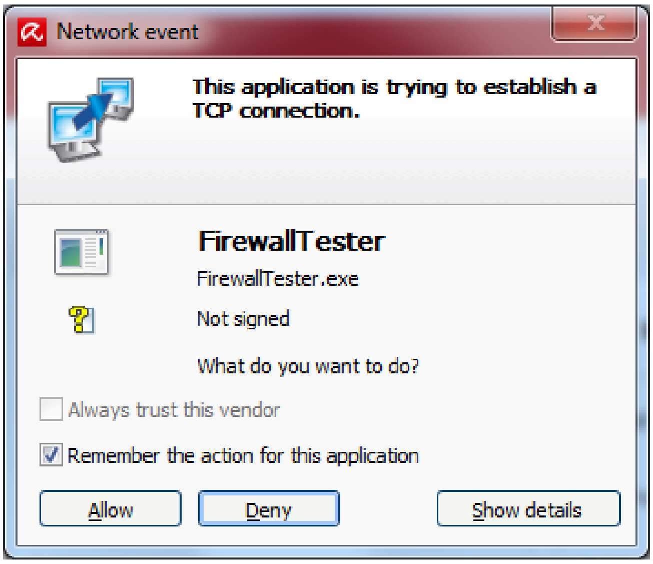
Unless the default action is changed within 10 seconds, the dialog box closes and the default action is applied.

Inbound Firewall Settings

During setup, we had selected the option to allow file and printer sharing, and the Avira firewall duly allowed us to ping our test PC and access its file share from another computer on the same LAN.

Outbound Firewall/Application Control

When we ran our firewall tester and attempted to download its test file, Avira displayed the following dialog box:



Network event

This application is trying to establish a TCP connection.

FirewallTester

FirewallTester.exe

Not signed

What do you want to do?

□ Always trust this vendor

☑ Remember the action for this application

During setup, we had selected the option to allow network access “for signed applications of trusted vendors”; however, our firewall testing program did not fit into this category. We were unable to find an option to disable all outgoing firewall prompts.

Spam protection

Spam protection is enabled by default, and marks the subject line of suspected spam mail. It is very difficult to find the configuration options, the component is so well hidden that it appears not to be present. It is necessary to switch on Expert Mode in Mail Protection settings; then Spam Protection can be seen and configured.

Parental Control

This is clearly shown as switched off by default. It can easily be configured on a Windows-user basis.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to update Avira Internet Security, but context-menu and custom scans both worked as normal and removed malware as in standard mode.

Help and Documentation

We quickly found answers to our queries on scheduling a scan, and scanning exclusions, using Avira’s local help functions. There is a comprehensive 178-page manual in .pdf format, which can be downloaded using the program’s Help menu. This is very detailed, and appears to explain every element of the interface and installation options clearly, with occasional screenshots. The “Help Me” entry in the Help menu opens Avira’s online knowledge base, which can also be searched for answers.

Verdict

Overall

Avira Internet Security 2012 is straightforward to use and is suitable for both experts and non-experts.

Plus points

Large range of configuration and installation options offered by the setup wizard, including choice of components. Clear and simple interface design makes important information and functionality easily accessible. Comprehensive manual easily found from Help menu.

Minus points

No obvious way of turning off outgoing firewall queries, other than uninstalling Avira’s firewall and using Windows Firewall instead.

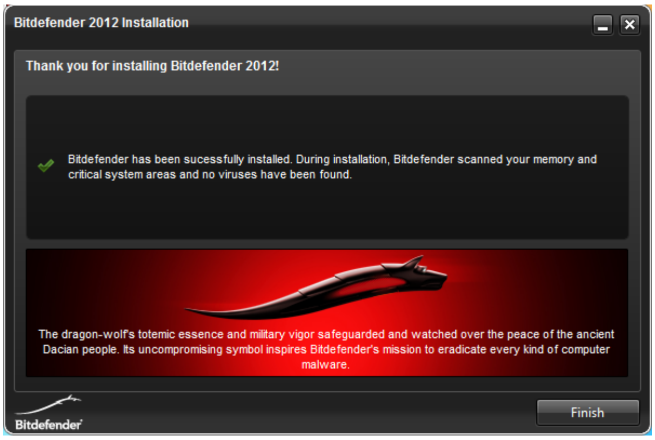
Bitdefender Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall
- Parental Controls

Installation

We installed Bitdefender Internet Security 2012 from an 848KB downloader file. The setup process consisted of the following steps: accepting the licence agreement; entering a key or choosing to use a trial; we chose to click on "Custom Settings", which additionally allowed us to change the installation folder, and decide whether to send anonymous usage reports. There is no choice of languages or components. When the setup wizard had finished, Bitdefender reported that it had run a quick scan during installation:



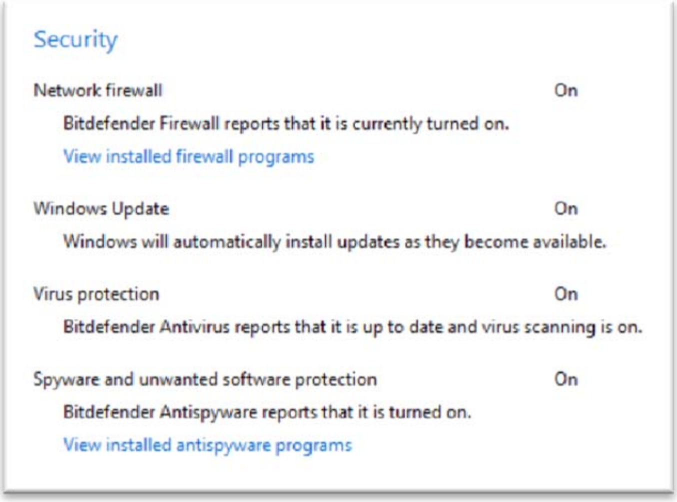
Bitdefender 2012 Installation

Thank you for installing Bitdefender 2012!

✓ Bitdefender has been sucessfully installed. During installation, Bitdefender scanned your memory and critical system areas and no viruses have been found.

The dragon-wolf's totemic essence and military vigor safeguarded and watched over the peace of the ancient Dacian people. Its uncompromising symbol inspires Bitdefender's mission to eradicate every kind of computer malware.

A reboot was not required after installation. Bitdefender Internet Security registered itself in Windows Action Center as an antivirus, antispyware and firewall application, and disabled both Windows Firewall and Windows Defender:



Security

Network firewall On

Bitdefender Firewall reports that it is currently turned on.

View installed firewall programs

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

Bitdefender Antivirus reports that it is up to date and virus scanning is on.

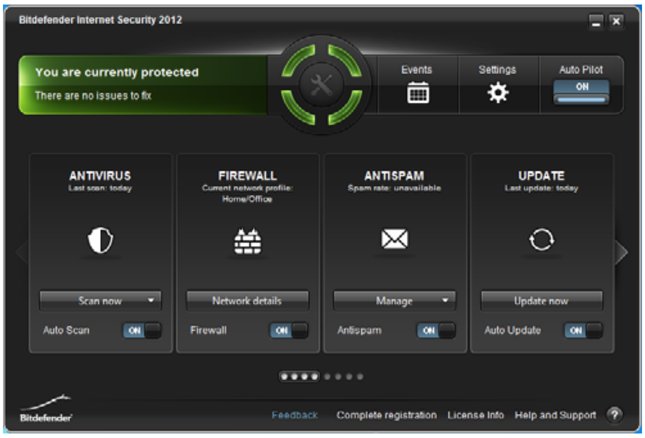
Spyware and unwanted software protection On

Bitdefender Antispyware reports that it is turned on.

View installed antispyware programs

Program Interface

The main program window is dominated by four boxes, representing Antivirus, Firewall, Antispam and Update. Each has a central icon; clicking this leads to the configuration settings of that item. A horizontal bar below each icon has either a single function, such as “Update Now” in the Update section, or a menu of options, such as different scan types in the Antivirus section. Just to the right of the Update box is an arrow pointing right; clicking on this shows further boxes for Parental Control, Privacy, Network Map, and SafeGo. We found this arrow a little bit too discreet, and it was some time before we realised that it was there and what it did.



Bitdefender Internet Security 2012

You are currently protected

There are no issues to fix

ANTIVIRUS Last scan: today

FIREWALL Current network profile: Home/Office

ANTISPAM Spam rate: unavailable

UPDATE Last update: today

Auto Scan ON

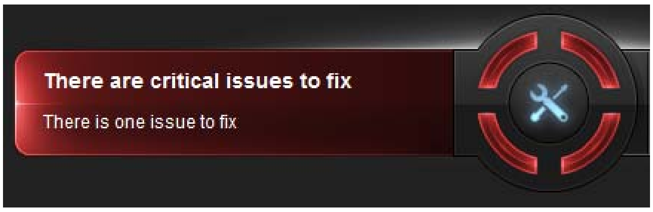
Firewall ON

Antispam ON

Auto Update ON

Auto Pilot ON

The top section of the window has a central circular icon, which is normally purely decorative as far as we can see; to the right of this are 3 buttons marked Events, Settings and Auto Pilot; to the right is the status display. When all is well, this section is green, and displays the text “You are currently protected”. When we disabled real-time antivirus protection, the status area and central circle turned red, and displayed the notice “There are critical issues to fix”:



There are critical issues to fix

There is one issue to fix

Clicking anywhere in the red status area, or the central tools icon in the circle, shows a list of the critical problems together with a button marked "Start" which resolves them.

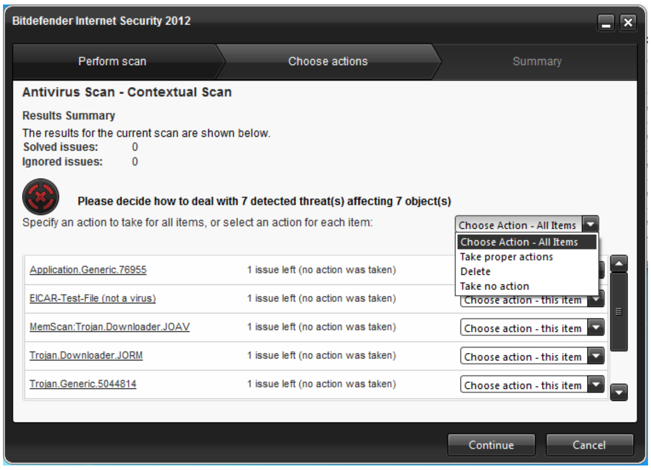
We found the program's colour scheme of white text on a black background somewhat uncomfortable to read, and would have liked an option to change to a more traditional black-on-white scheme.

Default configuration

Scanning and malware detection

We understand that Bitdefender Internet Security 2012 does not allow scheduled scans to be set, and that the feature has been replaced with "Idle-Time Scanning", which runs a scan whenever the computer is not being used. We could not find any means of running a boot-time scan.

When we ran a custom or context-menu scan on our folder of malware samples, BitDefender Internet Security 2012 showed the following dialog box:



Bitdefender Internet Security 2012
Perform scan
Choose actions
Summary

Antivirus Scan - Contextual Scan

Results Summary

The results for the current scan are shown below.

Solved issues: 0

Ignored issues: 0

Please decide how to deal with 7 detected threat(s) affecting 7 object(s)

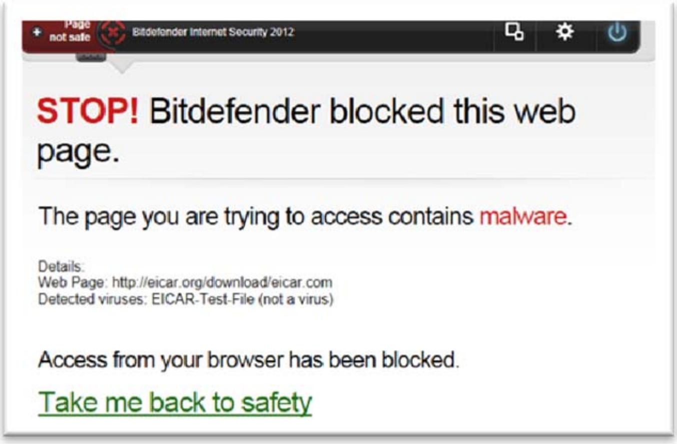
Specify an action to take for all items, or select an action for each item:

Choose Action - All Items
Choose Action - All Items
Take proper actions
Delete
Take no action

Application.Generic.76955	1 issue left (no action was taken)	
EICAR-Test-File (not a virus)	1 issue left (no action was taken)	Choose action - this item
MemScan:Trojan.Downloader.JOAV	1 issue left (no action was taken)	Choose action - this item
Trojan.Downloader.JORM	1 issue left (no action was taken)	Choose action - this item
Trojan.Generic.5044814	1 issue left (no action was taken)	Choose action - this item

It is possible to choose the action to take for each individual malware file, or to apply one action to all. We found the wording of one possible action, "Take proper action", to be a little strange; "Take recommended action" would seem more appropriate to us. We also feel that having the "Recommended" action selected by default would be easier and more reassuring for non-expert users. We note that selecting "take proper action" resulted in Bitdefender deleting one of our malware samples, and quarantining the rest.

When we tried to download the EICAR test file, Bitdefender blocked the web page, with the following message:



STOP! Bitdefender blocked this web page.

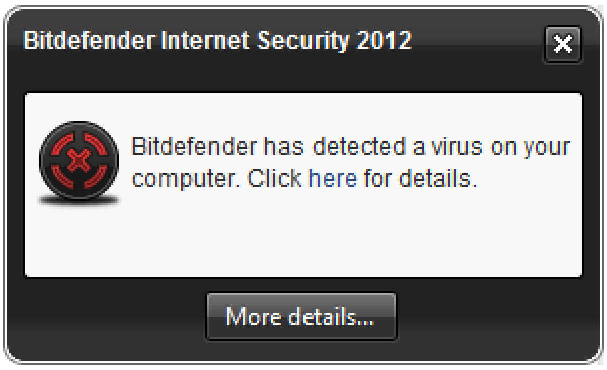
The page you are trying to access contains malware.

Details:
Web Page: http://eicar.org/download/eicar.com
Detected viruses: EICAR-Test-File (not a virus)

Access from your browser has been blocked.

Take me back to safety

The download was also blocked, and the following message box appeared:


Bitdefender Internet Security 2012

Bitdefender has detected a virus on your computer. Click here for details.

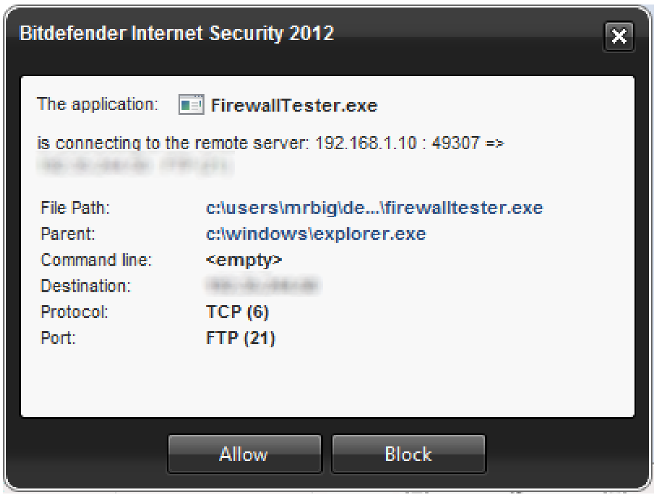
We are a little concerned that the second message box does not make clear that the malware has been blocked; clicking on "More details" only shows the malware as having been detected, not deleted; this may be worrying for non-expert users.

Inbound Firewall Settings

After installing Bitdefender Internet Security 2012, we were able to access our test PC's file share, and ping it, from another PC on the network.

Outbound Firewall/Application Control

In default mode, Bitdefender Internet Security allowed us to run our firewall tester and download the test file without hindrance or query. When we changed the firewall's settings by activating the amusingly named "Paranoid Mode", Bitdefender produced the following dialog box when we ran the firewall tester again:



The application: FirewallTester.exe

is connecting to the remote server: 192.168.1.10 : 49307 =>
[redacted]

File Path: c:\users\mrbig\de...\firewalltester.exe
Parent: c:\windows\explorer.exe
Command line: <empty>
Destination: [redacted]
Protocol: TCP (6)
Port: FTP (21)

Spam protection

Spam protection is enabled by default.

Parental Control

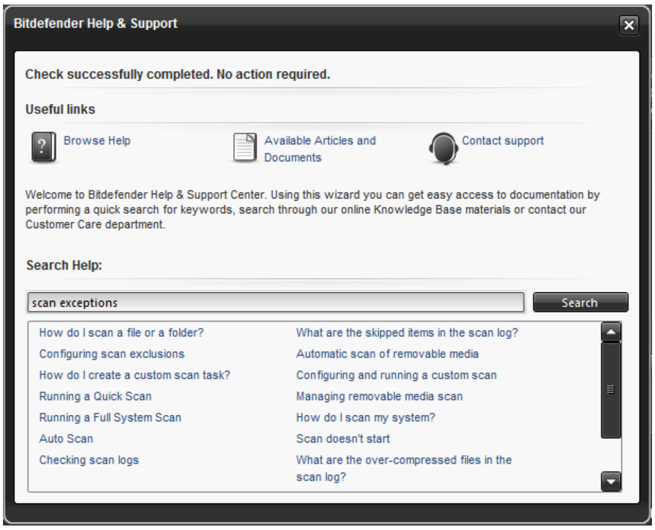
Parental Control is not shown on the main program interface, and has to be configured by going into the suite's settings. It works on a Windows-user basis, and can be enabled for individual accounts.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to update Bitdefender's virus definitions. However, we were able to run a context-menu scan on our folder of malware samples; this ran exactly as normal, detecting all the malicious programs and providing the usual options for dealing with them.

Help and Documentation

Clicking the question mark icon in the bottom right-hand corner of the Bitdefender window shows tool tips for the various elements of the interface. The Help and Support link opens a dialog that can be used to type in queries:



Check successfully completed. No action required.

Welcome to Bitdefender Help & Support Center. Using this wizard you can get easy access to documentation by performing a quick search for keywords, search through our online Knowledge Base materials or contact our Customer Care department.

scan exceptions

How do I scan a file or a folder?
What are the skipped items in the scan log?
Configuring scan exclusions
Automatic scan of removable media
How do I create a custom scan task?
Configuring and running a custom scan
Running a Quick Scan
Managing removable media scan
Running a Full System Scan
How do I scan my system?
Auto Scan
Scan doesn't start
Checking scan logs
What are the over-compressed files in the scan log?

Our test query ("scan exceptions") shown above provided a very promising-looking link entitled "Configuring scan exclusions"; clicking on this took us to Bitdefender's online manual, but unfortunately just to the title page; we then had to start searching from scratch to find our answer. We were able to find the correct page for our query after browsing for just a few moments, and it provided a concise but clear answer to the question. Our second standard query, on scheduling a scan, naturally drew a blank, as the feature is not included in the program.

Verdict

Overall

Bitdefender Internet Security 2012 is straightforward to install and use for experts or non-experts.

Plus points

Installation is very easy, with almost no questions to answer

Minus points

Slightly confusing scan results dialog box.

eScan Internet Security Suite 11.0

Components

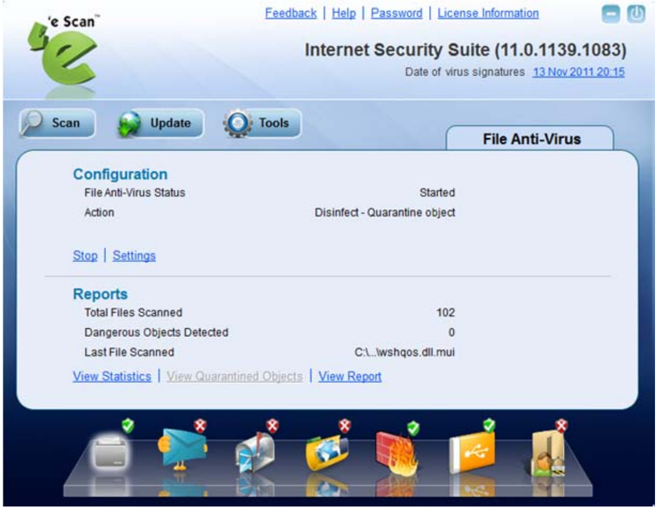
- Antimalware
- Antispam
- Firewall

Installation

We installed eScan Internet Security 11 from a 185 MB .exe file. The setup wizard offers a choice of languages and the location of the installation folder. There is no custom option or any choice of components to be installed. As usual, there is a licence agreement to accept. Additionally, the wizard shows a warning to uninstall any other antivirus software on the computer. A quick scan is run on completion of setup.

Program Interface

The version of eScan Internet Security we reviewed this year is almost identical to the one we looked at last year, and the interface is essentially identical.


'e Scan™
Feedback | Help | Password | License Information
Scan
Update
Tools
File Anti-Virus
Stop | Settings
View Statistics | View Quarantined Objects | View Report

Internet Security Suite (11.0.1139.1083)
Date of virus signatures 13 Nov 2011 20:15

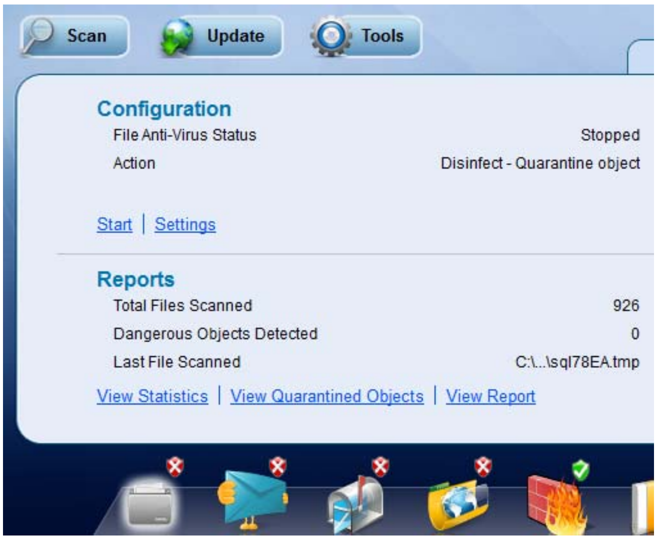
Configuration
File Anti-Virus Status Started
Action Disinfect - Quarantine object

Reports
Total Files Scanned 102
Dangerous Objects Detected 0
Last File Scanned C:\..\wshqos.dll.mui

The major components of the suite (File Anti-Virus, Mail Anti-Virus, Anti-Spam, Web Protection, Firewall, Endpoint Security, and Privacy Control) are represented by a row of icons along the bottom of the window. Whilst these icons may be considered works of art, we were confused by what many of them were supposed to represent. The Firewall icon is perfectly clear, but both Anti-Spam and Mail Anti-Virus use an envelope symbol, so we can never remember which is which. We found the other icons confusing, especially File Anti-Virus (the default page), which when selected looks remarkably like a printer. The very fact that each icon turns grey when selected is confusing in itself, as the icon gives the impression of being disabled when it is in fact the active page.

Clicking on one of the icons at the bottom opens the configuration page for that component.

There is no overall status display and no really obvious warning from the program if key components are disabled. The screenshot below shows the relevant part of the program window when real-time virus file antivirus has been disabled. This is indicated by the word "Stopped" in the top right-hand corner, and the cross in a red circle next to the File Anti-Virus symbol in the bottom left-hand corner. As the three icons to the right of it have this symbol by default, the extra cross can hardly be said to stand out.



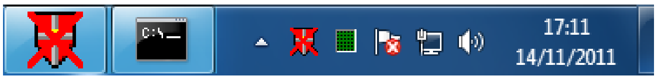
Configuration

File Anti-Virus Status	Stopped
Action	Disinfect - Quarantine object

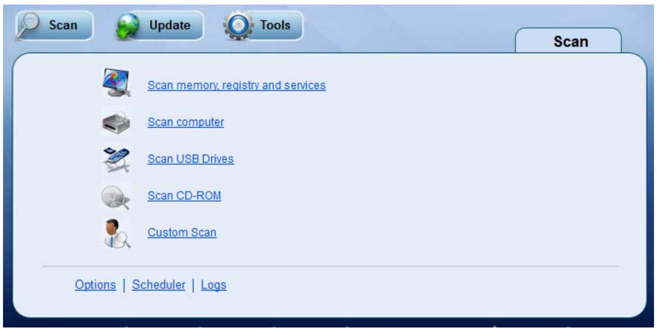
Reports

Total Files Scanned	926
Dangerous Objects Detected	0
Last File Scanned	C:\...\sql78EA.tmp

We must point out that the program's icons in the Taskbar and System Tray both acquire a red cross through them, as shown below, which does tend to indicate something is wrong. Nonetheless, we would still expect the main program window to show clearly what the problem is and how to correct it.



By contrast, the Scan, Update and Tools buttons at the top of the window are perfectly clear, as they are labelled in big, bold text. We feel that eScan would do better to mark all its buttons in this way, as it would be very much clearer what they are. Clicking on the Scan button displays the following scan options, which we found appropriate and clearly named:



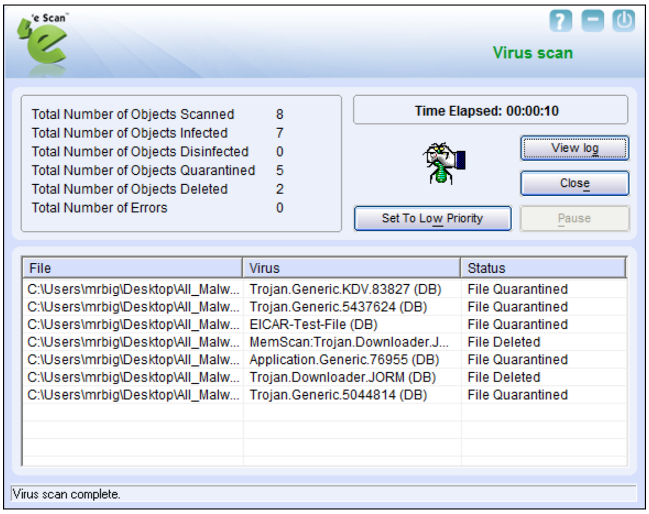
Text links at the very top of the window include Help and License Information.

Whilst a confident computer user would quickly work out what the pretty icons represent, and how to check the overall status, we feel that the interface might be very confusing for non-expert users, and that an overall status display and "Fix-All" button, along with text labels for the icons, would be a big improvement.

Default configuration

Scanning and malware discovery

No scheduled scan set is set by default, but this can be configured easily by clicking Scan/Scheduler. We could not find any means of running a boot-time scan. Running a custom or context-menu scan on our malware folder quarantined or deleted all the items without any user interaction being required:



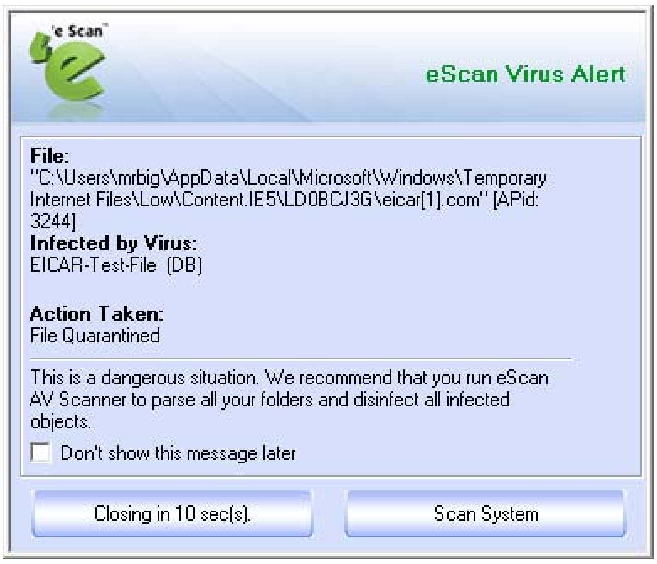
Total Number of Objects Scanned	8
Total Number of Objects Infected	7
Total Number of Objects Disinfected	0
Total Number of Objects Quarantined	5
Total Number of Objects Deleted	2
Total Number of Errors	0

Time Elapsed: 00:00:10

File	Virus	Status
C:\Users\mrbig\Desktop\All_Malw...	Trojan.Generic.KDV.83827 (DB)	File Quarantined
C:\Users\mrbig\Desktop\All_Malw...	Trojan.Generic.5437624 (DB)	File Quarantined
C:\Users\mrbig\Desktop\All_Malw...	EICAR-Test-File (DB)	File Quarantined
C:\Users\mrbig\Desktop\All_Malw...	MemScan:Trojan.Downloader.J...	File Deleted
C:\Users\mrbig\Desktop\All_Malw...	Application.Generic.76955 (DB)	File Quarantined
C:\Users\mrbig\Desktop\All_Malw...	Trojan.Downloader.JORM (DB)	File Deleted
C:\Users\mrbig\Desktop\All_Malw...	Trojan.Generic.5044814 (DB)	File Quarantined

Virus scan complete.

When we attempted to download the EICAR test file, eScan blocked the download and displayed the following message:



File:
"C:\Users\mrbig\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\LD0BCJ3G\eicar[1].com" [APid: 3244]
Infected by Virus:
EICAR-Test-File (DB)

Action Taken:
File Quarantined

This is a dangerous situation. We recommend that you run eScan AV Scanner to parse all your folders and disinfect all infected objects.

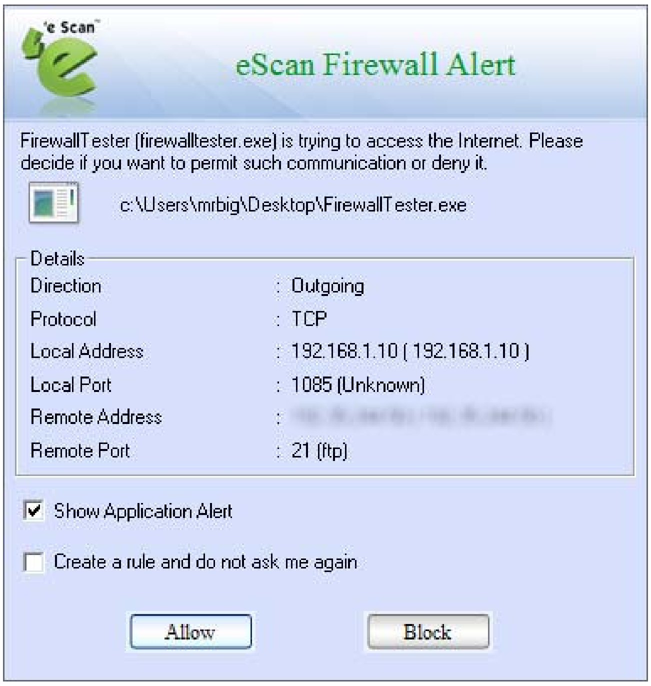
□ Don't show this message later

Inbound Firewall Settings

By default, eScan's firewall was set to Limited Filter mode. This allowed us to ping our test PC and access its file share from another computer on the network.

Outbound Firewall/Application Control

With the default firewall setting (Limited Filter), eScan Internet Security allowed our firewall tester to run and download its test file without any restriction or prompting. When we changed the setting to Interactive Filter, the following dialog appeared, asking whether we wanted to allow the program:



FirewallTester (firewalltester.exe) is trying to access the Internet. Please decide if you want to permit such communication or deny it.

c:\Users\mrbig\Desktop\FirewallTester.exe

Details

Direction : Outgoing

Protocol : TCP

Local Address : 192.168.1.10 (192.168.1.10)

Local Port : 1085 (Unknown)

Remote Address : [redacted]

Remote Port : 21 (ftp)

☑ Show Application Alert

☐ Create a rule and do not ask me again

Spam protection

The Anti-Spam service is disabled by default. It can easily be activated by clicking "Start" on the Anti-Spam configuration page. Mail considered to be spam has the prefix [Spam] added to the subject line.

Safe Mode

We could not open the main program window in Safe Mode with Networking. However, we were able to run a context-menu scan, and this removed all the malware samples exactly as it did in standard mode.

Help and Documentation

Clicking on the Help link at the top of the program window gives a choice of Live Chat, eScan Online Help, and MicroWorld Forum. As far as we can see, there is no local help function, only online. Using the search function to look for help on scheduling a scan and setting scan exceptions drew a blank;

we were not able to find any relevant articles for the Internet Security suite. There is a reasonably extensive section of FAQ, although not all the sections of this are very helpful. The eScan Configuration section appears to apply largely to the corporate edition of eScan only; the “How-to FAQs” section contains only one article, “How to update MWAV utility”; and the “eScan 11 FAQs” section contained 14 relevant-looking questions, but unfortunately none of the links on this page actually worked, so we were unable to read the answers to the questions.

We were able to find the .pdf manual for eScan Internet Security on the website, and this is comprehensive (116 pages), with all the essentials of the suite explained simply, using abundant screenshots. We would suggest that eScan might make this manual more easily accessible by placing a prominent link to it on the web page that opens when clicking on the link in the program window.

Verdict

Overall

eScan Internet Security 11 is in many ways an effective, fully-featured Internet security suite. However, we feel that the user interface might not ideally suited to non-expert users.

Plus points

Comprehensive manual

Minus points

User interface confusing for non-experts

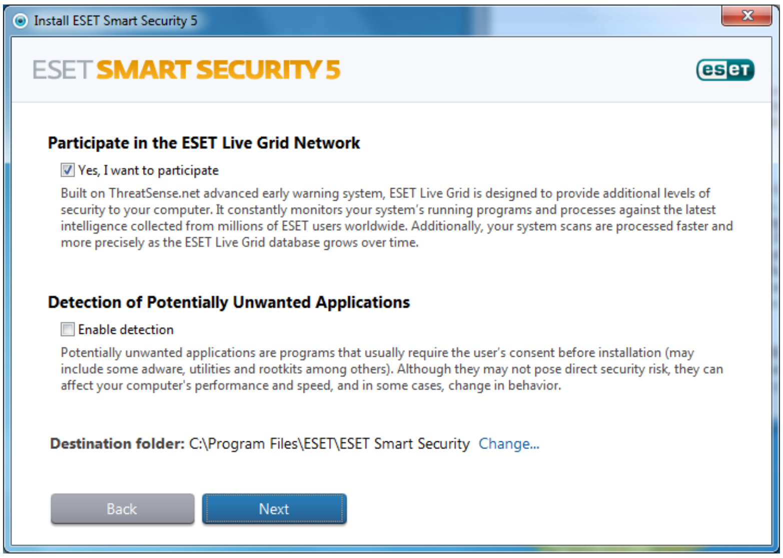
ESET Smart Security 5

Components

- Antimalware
- Antispam
- Firewall
- Parental Control

Installation

For our review, ESET provided us with their "Live Installer", a 1 MB file that downloads the latest version of the suite from the Internet. The full package, approx. 55 MB, can be downloaded from ESET's website. Installation is very simple. There is a one-time choice of languages (this cannot be changed later), and the usual licence agreement to accept. There is no custom installation as such, but the setup wizard does include an options page:



Participate in the ESET Live Grid Network

☑ Yes, I want to participate

Built on ThreatSense.net advanced early warning system, ESET Live Grid is designed to provide additional levels of security to your computer. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. Additionally, your system scans are processed faster and more precisely as the ESET Live Grid database grows over time.

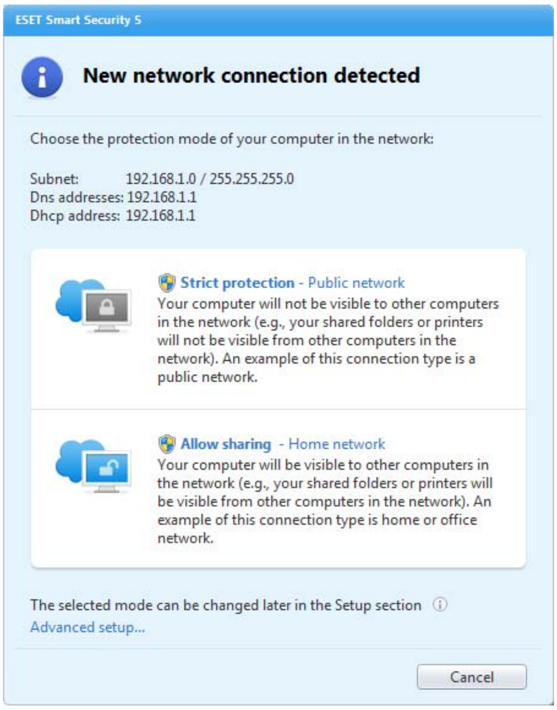
Detection of Potentially Unwanted Applications

□ Enable detection

Potentially unwanted applications are programs that usually require the user's consent before installation (may include some adware, utilities and rootkits among others). Although they may not pose direct security risk, they can affect your computer's performance and speed, and in some cases, change in behavior.

Destination folder: C:\Program Files\ESET\ESET Smart Security Change...

The choices are whether to participate in Live Grid, ESET's cloud-based service that shares information on malware (enabled by default); whether to detect potentially unwanted applications (disabled by default); and the installation folder location. The installation wizard explains to the user what Live Grid and Potentially Unwanted Applications are, to help non-expert users make the right choice for them (please see screenshot above). There is no option to choose which components of the suite to install (although the firewall and parental control can be deactivated after installation). When the desired options have been selected, installation begins. File copying completes very quickly, and then the wizard asks whether the network the PC is connected to should be regarded as public or private. There is an explanation as to what each of these options means:



ESET Smart Security 5

New network connection detected

Choose the protection mode of your computer in the network:

Subnet: 192.168.1.0 / 255.255.255.0
Dns addresses: 192.168.1.1
Dhcp address: 192.168.1.1

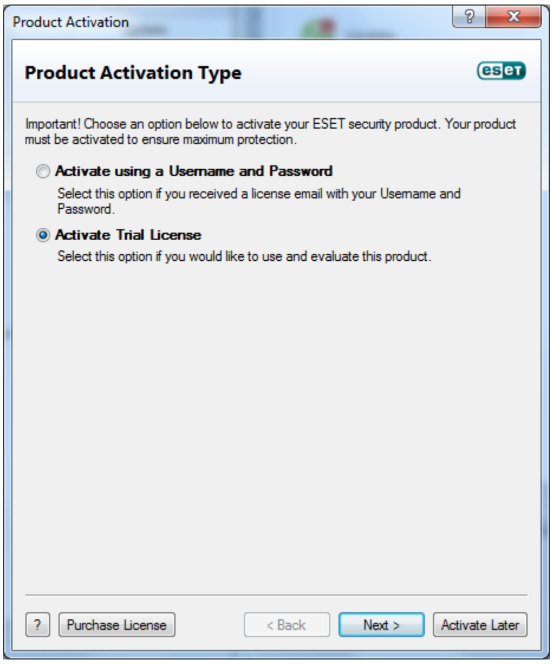
Strict protection - Public network
Your computer will not be visible to other computers in the network (e.g., your shared folders or printers will not be visible from other computers in the network). An example of this connection type is a public network.

Allow sharing - Home network
Your computer will be visible to other computers in the network (e.g., your shared folders or printers will be visible from other computers in the network). An example of this connection type is home or office network.

The selected mode can be changed later in the Setup section

For the purposes of our test, we chose “Allow sharing – Home Network”.

The final part of the setup process, activation, occurs after the installation has completed and the program is running. The first time an attempt is made to update the virus definitions, the activation dialog box appears. This gives the option of entering a username and password (equivalent to a licence key) if the product has been purchased, or activating a trial licence:



Product Activation

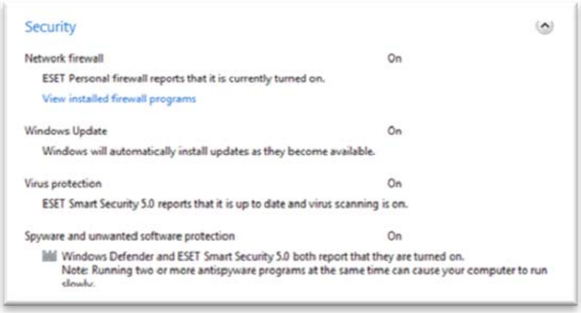
Product Activation Type

Important! Choose an option below to activate your ESET security product. Your product must be activated to ensure maximum protection.

○ Activate using a Username and Password
Select this option if you received a license email with your Username and Password.

● Activate Trial License
Select this option if you would like to use and evaluate this product.

A reboot was not required after setup had finished. ESET Smart Security 5 registers itself in Action Center as an antivirus, antispyware and firewall program. Windows Firewall is disabled, Windows Defender is not.



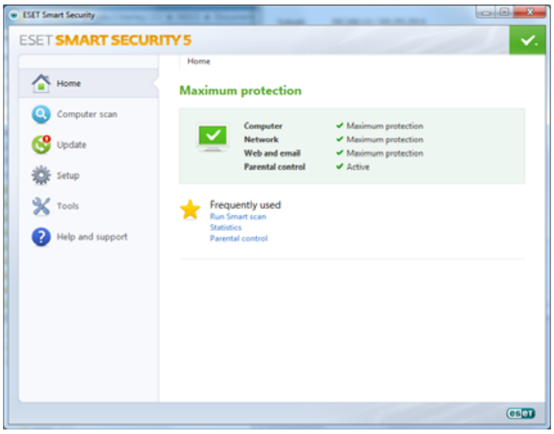
Security

Network firewall	On
ESET Personal firewall reports that it is currently turned on. View installed firewall programs	
Windows Update	On
Windows will automatically install updates as they become available.	
Virus protection	On
ESET Smart Security 5.0 reports that it is up to date and virus scanning is on.	
Spyware and unwanted software protection	On
Windows Defender and ESET Smart Security 5.0 both report that they are turned on. Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.	

We found the installation of ESET Smart Security 5 to be quick and straightforward, with a few sensible options which are clearly explained for the benefit of non-expert users. The uninstall program includes a repair option, which can be used to replace missing or corrupted files and settings.

Program Interface

The user interface of ESET Smart Security 5 will be familiar to anyone who has used version 4. The smaller left-hand pane of the window is a menu, with the items Home, Computer Scan, Update, Setup, Tools and Help & Support. Clicking on a menu item displays the relevant page in the larger right-hand pane.

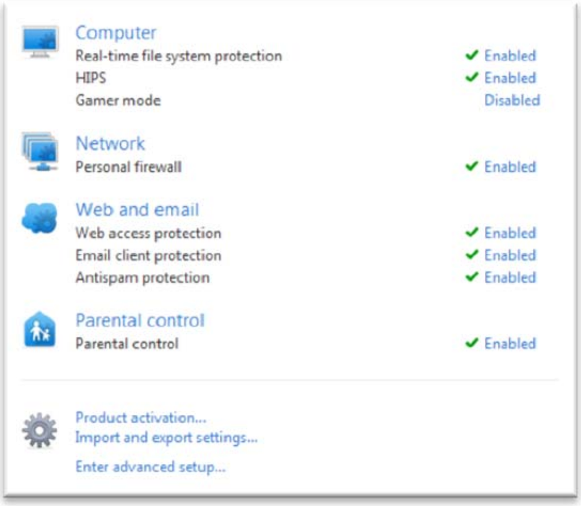


Maximum protection

Computer	✓ Maximum protection
Network	✓ Maximum protection
Web and email	✓ Maximum protection
Parental control	✓ Active

Frequently used
Run Smart scan
Statistics
Parental control

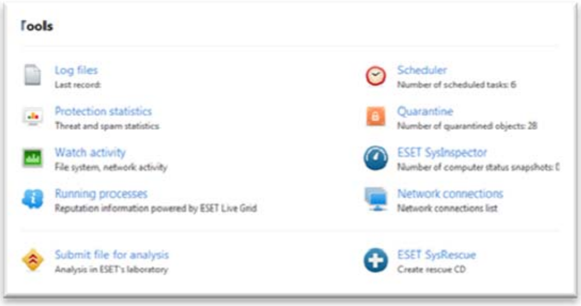
Home combines a status display of the four major components with links to Run Smart Scan, Statistics, and Parental Control. Computer Scan has links to different scan options (full/custom), and information on date and time of last scan, the virus signature version used, and number of infected files found. Update shows details of the current virus signature database, plus licence and activation status, and has a button to run a signature update. Setup lists the major protection areas and their subcomponents, with the name of each item (words in blue in the screenshot below) being a link to configure its details:



Computer	
Real-time file system protection	✓ Enabled
HIPS	✓ Enabled
Gamer mode	Disabled
Network	
Personal firewall	✓ Enabled
Web and email	
Web access protection	✓ Enabled
Email client protection	✓ Enabled
Antispam protection	✓ Enabled
Parental control	
Parental control	✓ Enabled

Product activation...
Import and export settings...
Enter advanced setup...

There is also a link to the advanced setup tree, where in-depth configuration changes can be made. Tools contains a number of items for advanced users, including scheduler, quarantine, system information and log files:

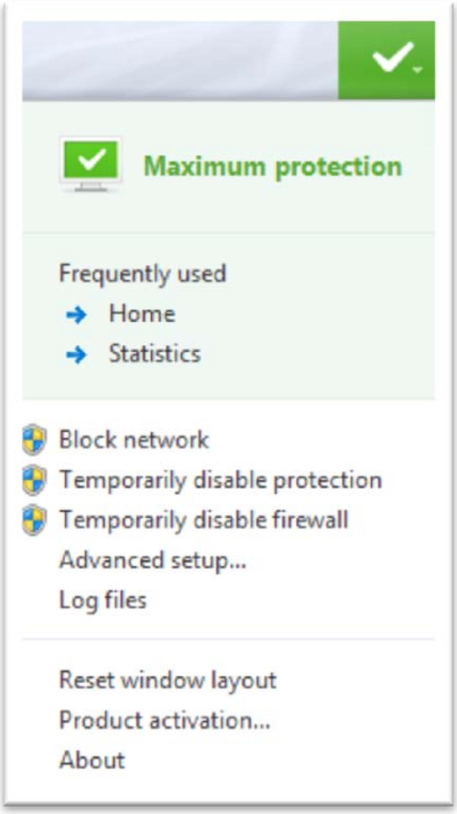


Tools

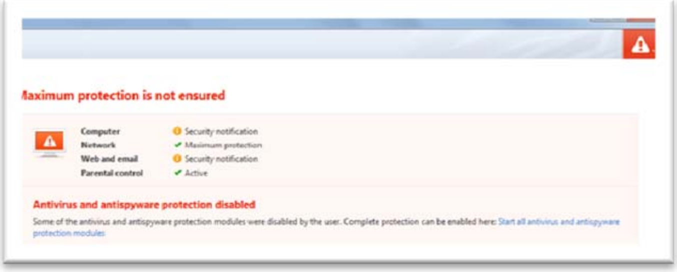
Log files Last record:	Scheduler Number of scheduled tasks: 6
Protection statistics Threat and spam statistics	Quarantine Number of quarantined objects: 28
Watch activity File system, network activity	ESET SysInspector Number of computer status snapshots: (
Running processes Reputation information powered by ESET Live Grid	Network connections Network connections list
Submit file for analysis Analysis in ESET's laboratory	ESET SysRescue Create rescue CD

Help & Support has links to both local and online help (Internet knowledge base), program information, and support request forms.

A new feature in Smart Security 5 is the big status/menu button in the top right-hand corner of the window. If all is well, it appears as a tick (checkmark) on a green background; clicking it displays a menu of useful links, including “Temporarily disable protection”:



If protection is disabled, the status/menu button changes to a warning triangle on a red background, and its menu includes options for re-enabling the protection. At the same time, the status display on the Home page changes accordingly:


laximum protection is not ensured

Computer	● Security notification
Network	✓ Maximum protection
Web and email	● Security notification
Parental control	✓ Active

Antivirus and antispyware protection disabled

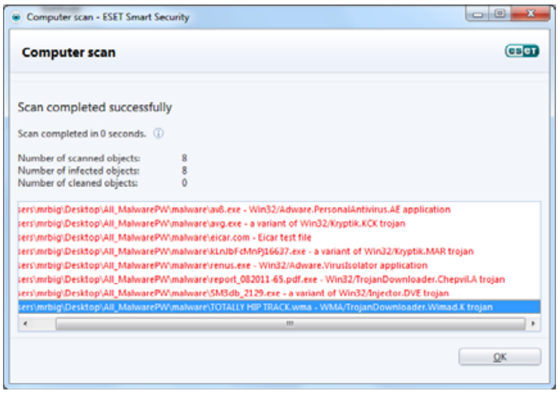
Some of the antivirus and antispyware protection modules were disabled by the user. Complete protection can be enabled here: Start all antivirus and antispyware protection modules

Default configuration

Scanning and malware discovery

A scheduled scan is not configured by default, but can be set up using Tools | Scheduler. We could not find any option to run a boot-time scan, but Smart Security is set to perform a startup scan, i.e. it checks memory when the user logs on to Windows. This can be disabled if necessary.

Running a custom scan from the main program window scans and cleans by default, although there is the option to scan without cleaning. Running a context-menu scan by right-clicking a file or folder gives the option “Scan with ESET Smart Security”. Clicking on this runs a scan, though at the end of it, the user is informed of the malware found, but not given any opportunity to clean it, and no cleaning is carried out automatically.



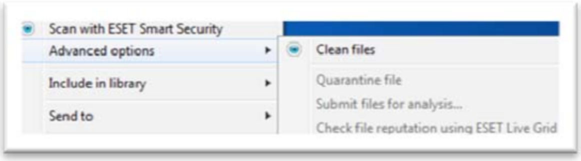
Scan completed successfully

Scan completed in 0 seconds.

Number of scanned objects:	8
Number of infected objects:	8
Number of cleaned objects:	0

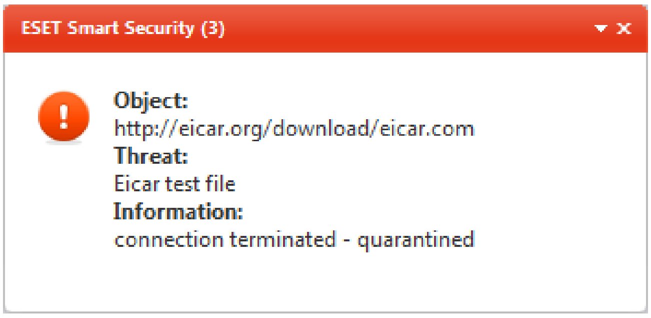
```
sers\mrbig\Desktop\All_MalwarePW\malware\av8.exe - Win32/Adware.PersonalAntivirus.AE application
sers\mrbig\Desktop\All_MalwarePW\malware\avg.exe - a variant of Win32/Kryptik.KCK trojan
sers\mrbig\Desktop\All_MalwarePW\malware\eicar.com - Eicar test file
sers\mrbig\Desktop\All_MalwarePW\malware\kLnJbFcMnPj16637.exe - a variant of Win32/Kryptik.MAR trojan
sers\mrbig\Desktop\All_MalwarePW\malware\renus.exe - Win32/Adware.VirusIsolator application
sers\mrbig\Desktop\All_MalwarePW\malware\report_082011-65.pdf.exe - Win32/TrojanDownloader.Chepvil.A trojan
sers\mrbig\Desktop\All_MalwarePW\malware\SM3db_2129.exe - a variant of Win32/Injector.DVE trojan
sers\mrbig\Desktop\All_MalwarePW\malware\TOTALLY HIP TRACK.wma - WMA/TrojanDownloader.Wimad.K trojan
```

To actually clean the malware, the user must go to the ESET sub-menu and select Clean:


Scan with ESET Smart Security
Advanced options
Include in library
Send to
Clean files
Quarantine file
Submit files for analysis...
Check file reputation using ESET Live Grid

We find this rather confusing, and suggest it would be much clearer to write e.g. “Scan without cleaning” and “Scan and clean”, so that the user knows in advance if any malware found will be cleaned or not. The default action can be changed from Scan to Clean in the advanced settings.

When we attempted to download the EICAR test file, Smart Security blocked the page and displayed the following message:



Object:
http://eicar.org/download/eicar.com
Threat:
Eicar test file
Information:
connection terminated - quarantined

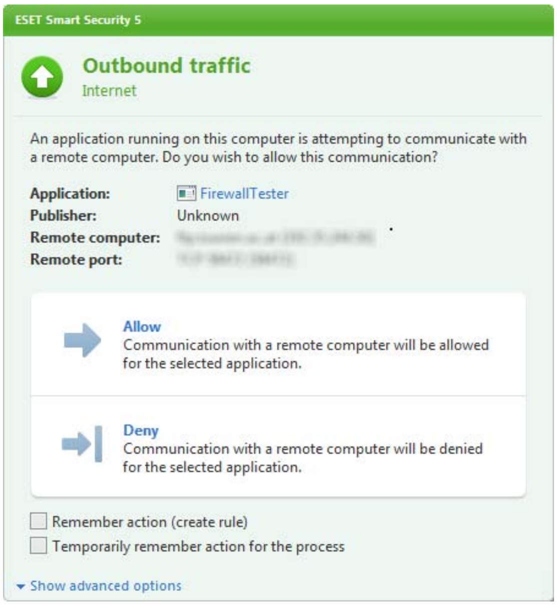
This indicated clearly that the “threat” had been quarantined and that no further action was required.

Inbound Firewall Settings

As mentioned above, the setup wizard asks whether to allow or block file sharing. The “Allow sharing” option allowed us to ping the PC and access its file share from another computer on the network.

Outbound Firewall/Application Control

Smart Security has different settings for outgoing traffic; the default is "Automatic mode", which allows "all standard outgoing connections". This allowed our firewall tester program to access the Internet and download the test file. There are 4 other modes that can be selected, including "Interactive mode"; when we selected this and ran our firewall tester, Smart Security brought up the following dialog box, asking whether to allow the outbound traffic:



ESET Smart Security 5

Outbound traffic

Internet

An application running on this computer is attempting to communicate with a remote computer. Do you wish to allow this communication?

Application: FirewallTester
Publisher: Unknown
Remote computer: [redacted]
Remote port: [redacted]

Allow
Communication with a remote computer will be allowed for the selected application.

Deny
Communication with a remote computer will be denied for the selected application.

□ Remember action (create rule)
□ Temporarily remember action for the process

▾ Show advanced options

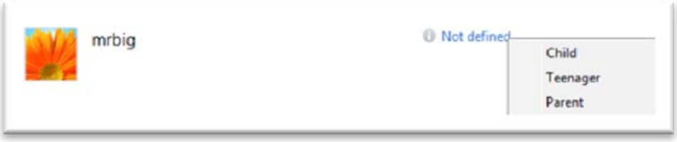
We found the default setting, Automatic Mode, to be ideal for non-expert users, as it does not require them to make any decisions about which network traffic to allow.

Spam protection

Spam protection is enabled by default, and configured to mark suspected spam messages with the prefix [SPAM]. This can be changed in the advanced settings.

Parental Control

This is enabled by default, but not configured. This means a parent has to go to the Parental Control setup page and define an age range for each Windows user:



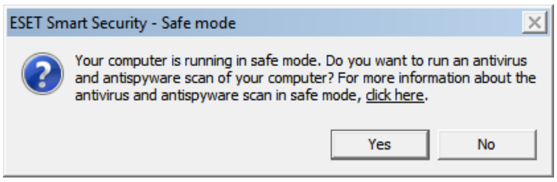
mrbig

Not defined

We feel it might be helpful if ESET were to remind users, e.g. during setup, that accounts have to be configured before Parental Control will have any effect.

Safe Mode

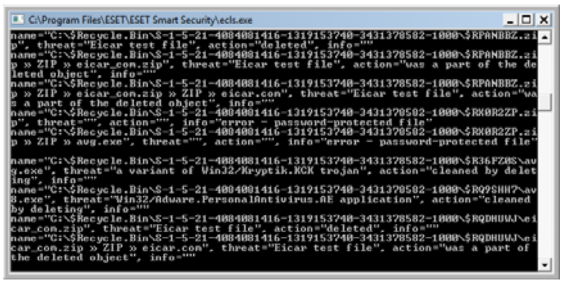
When we started our test PC in Safe Mode with Networking and attempted to open ESET Smart Security 5, the following dialog box appeared:



ESET Smart Security - Safe mode

Your computer is running in safe mode. Do you want to run an antivirus and antispyware scan of your computer? For more information about the antivirus and antispyware scan in safe mode, click here.

Clicking on “Yes” starts a scan, which displays its results in a command prompt window:



C:\Program Files\ESET\ESET Smart Security\ecls.exe

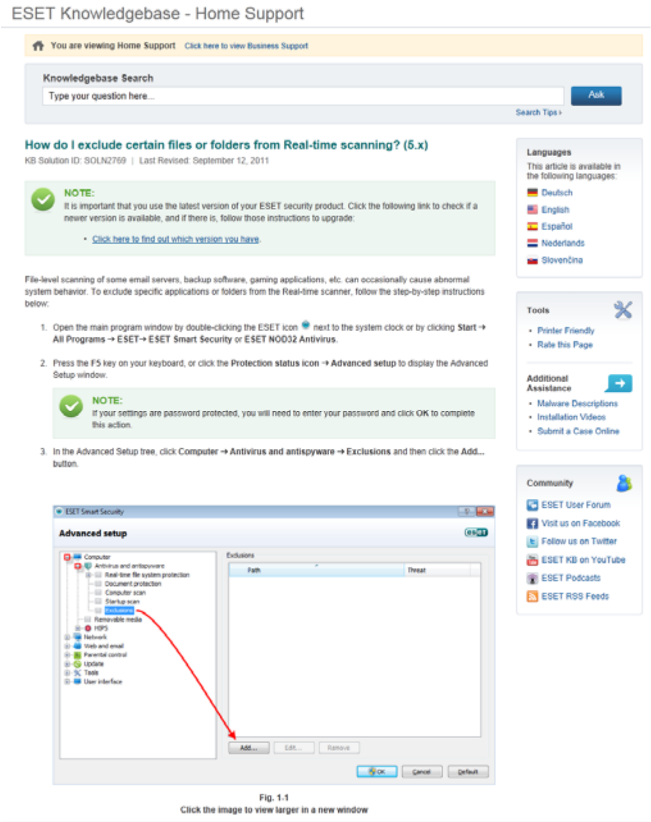
```
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RPANBBZ.zi
p", threat="Eicar test file", action="deleted", info=""
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RPANBBZ.zi
p » ZIP » eicar_com.zip", threat="Eicar test file", action="was a part of the de
leted object", info=""
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RPANBBZ.zi
p » ZIP » eicar_com.zip » ZIP » eicar.com", threat="Eicar test file", action="wa
s a part of the deleted object", info=""
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RX0R2ZP.zi
p", threat="", action="", info="error - password-protected file"
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RX0R2ZP.zi
p » ZIP » avg.exe", threat="", action="", info="error - password-protected file"

name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$R36FZ0S\av
g.exe", threat="a variant of Win32/Kryptik.KCK trojan", action="cleaned by delet
ing", info=""
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RQ9SHH7\av
8.exe", threat="Win32/Adware.PersonalAntivirus.AE application", action="cleaned
by deleting", info=""
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RQDHUWJ\ei
car_com.zip", threat="Eicar test file", action="deleted", info=""
name="C:\$Recycle.Bin\S-1-5-21-4084081416-1319153740-3431378582-1000\$RQDHUWJ\ei
car_com.zip » ZIP » eicar.com", threat="Eicar test file", action="was a part of
the deleted object", info=""
```

There is no means of updating the program before running the scan. However, the Safe Mode scan successfully removed all the malware in our collection.

Help and Documentation

The program’s Help and Support page has links to both local support and ESET’s online knowledge base. We found that both provided answers to queries on how to schedule a scan, and exclude specific files or folders from scanning. The online knowledge base must be particularly commended, however, for ease of finding a solution, and very clear, well-illustrated guides to particular tasks:



ESET Knowledgebase - Home Support

You are viewing Home Support Click here to view Business Support

Knowledgebase Search

Type your question here...

Search Tips ›

How do I exclude certain files or folders from Real-time scanning? (5.x)

KB Solution ID: SOLN2769 | Last Revised: September 12, 2011

NOTE:
It is important that you use the latest version of your ESET security product. Click the following link to check if a newer version is available, and if there is, follow those instructions to upgrade:

- Click here to find out which version you have.

File-level scanning of some email servers, backup software, gaming applications, etc. can occasionally cause abnormal system behavior. To exclude specific applications or folders from the Real-time scanner, follow the step-by-step instructions below:

1. Open the main program window by double-clicking the ESET icon next to the system clock or by clicking **Start → All Programs → ESET→ ESET Smart Security** or **ESET NOD32 Antivirus**.
2. Press the F5 key on your keyboard, or click the **Protection status icon → Advanced setup** to display the Advanced Setup window.

   NOTE:
   If your settings are password protected, you will need to enter your password and click **OK** to complete this action.

3. In the Advanced Setup tree, click **Computer → Antivirus and antispyware → Exclusions** and then click the **Add...** button.

Fig. 1-1
Click the image to view larger in a new window

Languages
This article is available in the following languages:
- Deutsch
- English
- Español
- Nederlands
- Slovenčina

Tools
- Printer Friendly
- Rate this Page

Additional Assistance
- Malware Descriptions
- Installation Videos
- Submit a Case Online

Community
- ESET User Forum
- Visit us on Facebook
- Follow us on Twitter
- ESET KB on YouTube
- ESET Podcasts
- ESET RSS Feeds

2 electronic manuals are freely available to download from ESET's main website. The Quick Start Guide is 12 pages long and covers the basics of installing and using the program. The User Guide is much more comprehensive at 119 pages, and is very well indexed and bookmarked. Both are very clearly written and illustrated with screenshots.

Verdict

Overall

We found ESET Smart Security 5 to be a well-designed and easy-to-use suite, offering sensible default settings for non-experts, and a wide range of easily accessible options for advanced users.

Plus points

Exceptionally clear, simple and elegant user interface; excellent manuals and online help.

Minus points

Confusing labelling of context-menu scans; parental control shown as active when effectively it isn't.

F-Secure Internet Security 2012

Components

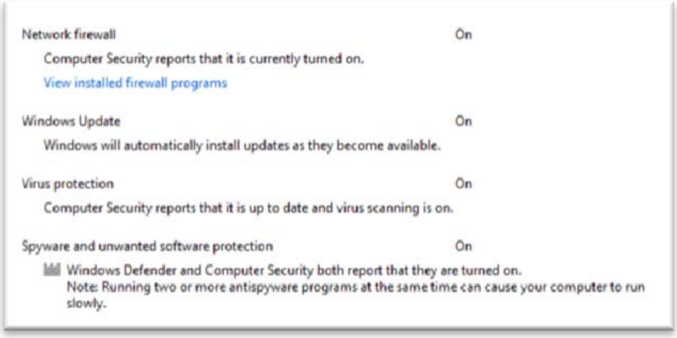
- Antimalware
- Antispam
- Firewall
- Parental Controls

Installation

We installed F-Secure Internet Security 2012 from a 1 MB downloader. Installation consists of choosing a language (a one-time choice), accepting the licence agreement, and choosing whether to send malware information to F-Secure. There is no custom option and no choice of components to be installed.

The only options in the uninstaller are whether to remove Online Safety (parental controls and browsing protection), Computer Security (the rest of the Internet Security Suite), or both.

F-Secure registers with Windows Action Center as an antivirus, antispyware and firewall program, using the semi-anonymous name "Computer Security"; we would have been more reassured to see the name "F-Secure" here. Windows Firewall is disabled, Windows Defender is not:



Network firewall On
Computer Security reports that it is currently turned on.
View installed firewall programs

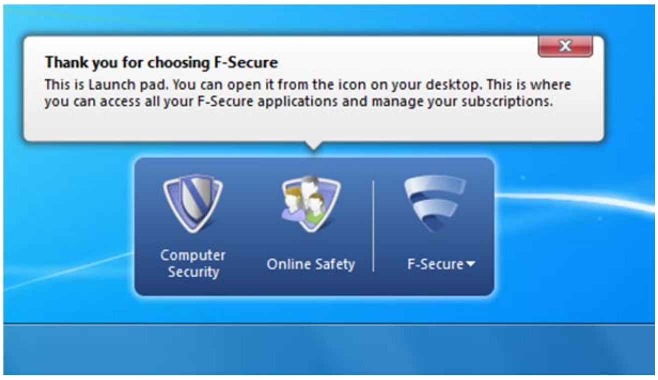
Windows Update On
Windows will automatically install updates as they become available.

Virus protection On
Computer Security reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender and Computer Security both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

Program Interface

The most obvious change from last year's program is that the F-Secure shortcuts on the desktop and in the Start Menu are now called "F-Secure Launch Pad", and clicking on one of them does not start the main program window, but rather the "Launch Pad", which is very reminiscent of a Windows Desktop Gadget:



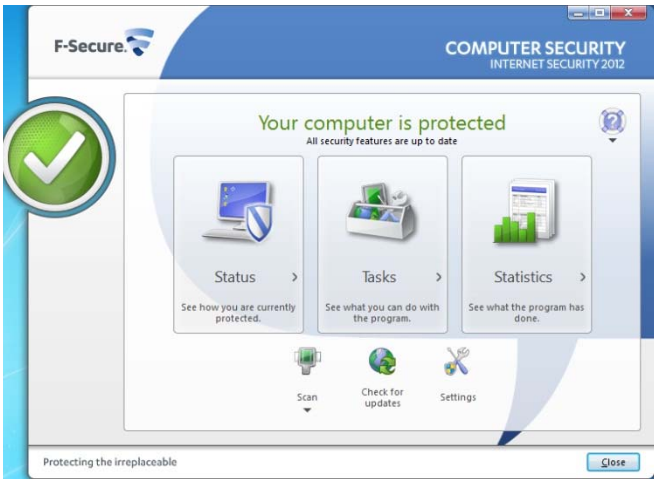
Thank you for choosing F-Secure

This is Launch pad. You can open it from the icon on your desktop. This is where you can access all your F-Secure applications and manage your subscriptions.

The Computer Security button opens the main F-Secure Internet Security window, which is very similar in appearance to last year's version. The Online Safety button opens a similar-looking window, devoted to parental controls and browsing protection. Clicking the F-Secure button produces the same shortcut menu that appears when right-clicking F-Secure's System Tray icon. The Launch Pad appears temporarily when the F-Secure shortcut is clicked, and disappears as soon as the user clicks anywhere else on the screen.

Our overwhelming feeling about the Launch Pad is that it is simply a nuisance, and requires more clicks to do the same thing. We could not find any means of starting either the Computer Security window or the Online Safety window directly, such as making direct shortcuts or pinning them to the Windows Taskbar. It is always necessary to go via the Launch Pad. We also question why it was necessary to make the Online Safety element into a separate window; other manufacturers manage to incorporate multiple components into a single window. Even if the Online Safety element is uninstalled, the Launch Pad remains, with just the two items. We find it hard to believe that any user will feel that the Launch Pad has made their life easier in any way.

The main Computer Security Window is very similar to that of F-Secure Internet Security 2011. There are three big buttons, marked Status, Tasks, and Statistics; and three small buttons, marked Scan, Check for Updates, and Settings. If all is well, the status line at the top of the window reads "Your computer is protected", and a big green circle on the left-hand side of the window shows a tick (checkmark):



Your computer is protected

All security features are up to date

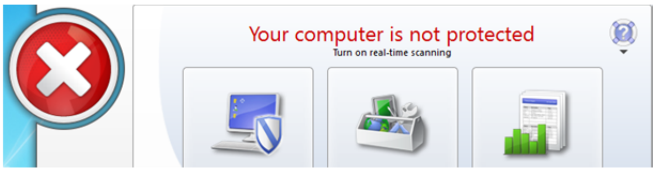
See how you are currently protected.

See what you can do with the program.

See what the program has done.

Protecting the irreplaceable

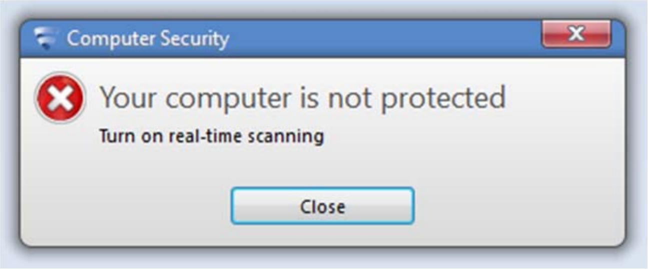
When we disabled real-time antivirus protection, the wording changed to “Your computer is not protected”, and the symbol changed to a cross on a red background:



Your computer is not protected

Turn on real-time scanning

At the same time, an F-Secure message box popped up near the System Tray:



Computer Security

Your computer is not protected

Turn on real-time scanning

We note that on neither the message box nor the main program window is there any easy means of reactivating the protection; there is no Fix All button, and the instruction “Turn on real-time scanning” gives no indication as to how this should be done. We feel that this omission makes F-Secure Internet Security less than ideal for non-expert users.

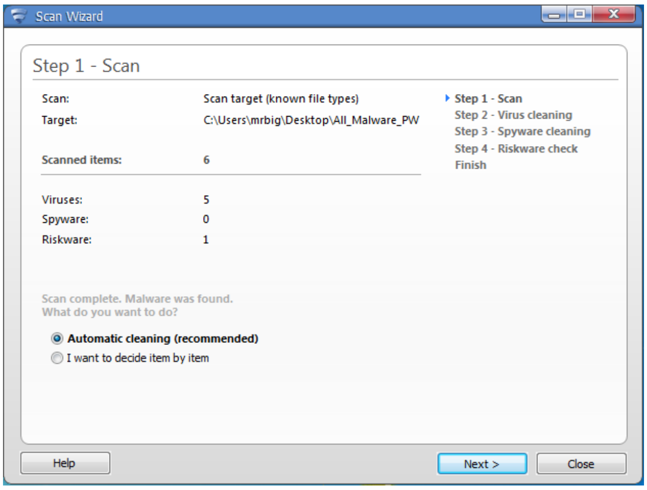
We further note that disabling or re-enabling real-time protection now requires two extra clicks each time; firstly, it is necessary to click on a new link, “Change settings on this page”, and then confirm a Windows UAC prompt. Even if most users don’t do this very often, we feel that the UAC prompt alone would provide enough security here.

Default configuration

Scanning

A scheduled scan is not configured by default, but can easily be set up by going into Settings/Scheduled Scanning. We could not find any means of running a boot-time scan.

Running a context-menu or custom scan on our collection of malware samples started a very short and simple wizard, which gave us the choice of “Automatic Cleaning (recommended)” or “I want to decide item by item”. We feel this is an excellent strategy, as there is an easy option for non-experts, while advanced users have as much flexibility as they want.

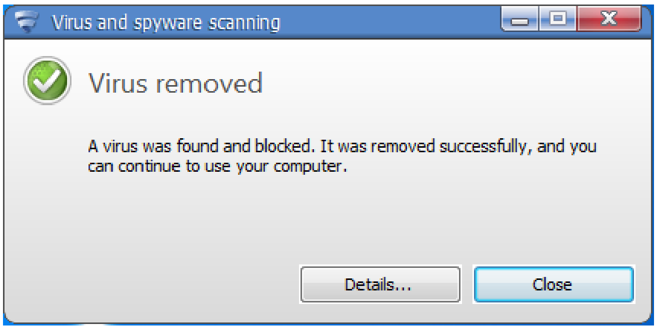


Scan: Scan target (known file types)
Target: C:\Users\mrbig\Desktop\All_Malware_PW
Scanned items: 6
Viruses: 5
Spyware: 0
Riskware: 1

Scan complete. Malware was found.
What do you want to do?

● Automatic cleaning (recommended)
○ I want to decide item by item

Clicking "Automatic Cleaning" removes the malware, and gives the user the chance to see what was found by clicking the "Show report" button on the last page of the wizard. When we tried to download the EICAR test file, F-Secure blocked the download and displayed the following message:



Virus removed

A virus was found and blocked. It was removed successfully, and you can continue to use your computer.

This makes it clear that the "threat" has been removed, and that no further action is necessary, although expert users can find more information by clicking on Details.

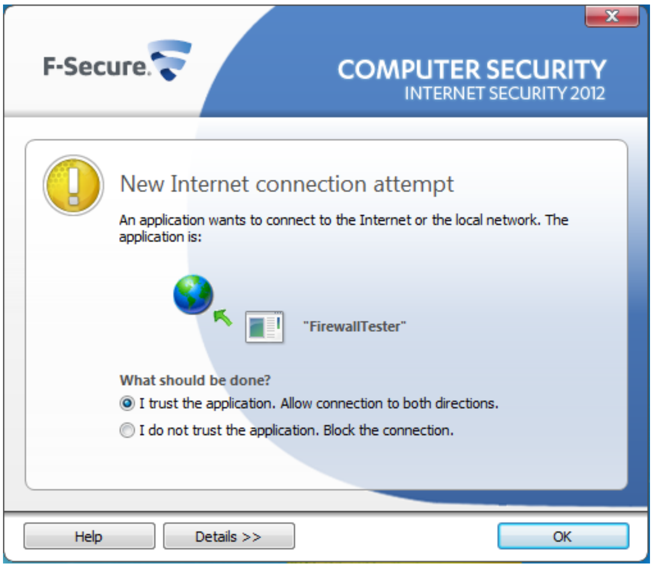
Inbound Firewall Settings

We found that pinging our test PC and accessing its File share were blocked by default.

To allow sharing, we went to Settings/Firewall/Settings/Trusted Network Adapter and set this to the LAN adapter in the PC.

Outbound Firewall/Application Control

When we ran our firewall tester and attempted to download its test file, F-Secure Internet Security 2012 produced the following dialog box:



New Internet connection attempt

An application wants to connect to the Internet or the local network. The application is:

"FirewallTester"

What should be done?

● I trust the application. Allow connection to both directions.

○ I do not trust the application. Block the connection.

F-Secure registered the choosen decision and did not ask about the firewall tester again, even after rebooting the test PC.

Deactivating Application Control in Settings prevents any such queries about permission for outgoing programs.

Spam protection

Spam protection (Email filtering) is enabled by default.

Parental Control

Parental control (Online Safety) is not enabled by default, but can easily be configured on a Windows user account basis by opening Online Safety and clicking Users.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to open F-Secure Internet Security or run any kind of scan. Clicking the F-Secure Launch Pad icon produced no visible result at all, and F-Secure's Scan entry had disappeared from the context menu.

Help and Documentation

The local Help function quickly provided clear answers to our queries about scan exceptions and scheduling a scan. However, the online support search failed to turn up an answer to either of them. We were unable to find a manual for the program on F-Secure's website.

Verdict

Overall

Despite some irritations, F-Secure is largely simple to use, and could be used by non-experts as well as experts.

Plus points

Interface is largely clear and simple

Excellent notification/choices when malware is discovered.

Minus points

No “Fix All” button

Completely non-functional in Safe Mode

Program has to be started via irritating Launch Pad

G DATA Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall
- Parental Control
- Shredder

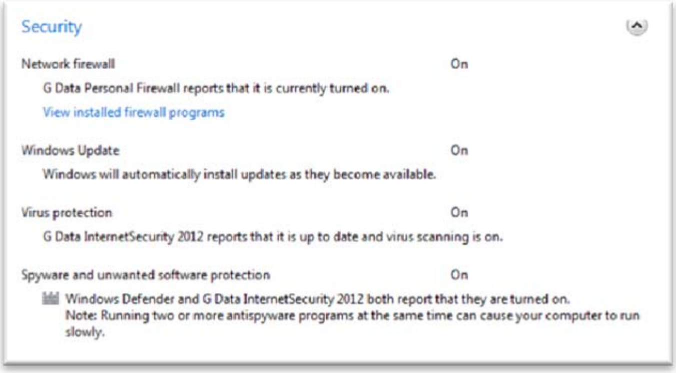
Note about the program

G Data Internet Security uses two third-party antivirus engines. By default these are usually used together, but can be disabled or enabled separately for specific functions (real-time protection, on-demand scans).

Installation

We installed G Data Internet Security 2012 from a 341 MB .exe file. It is a monoglot installer, i.e. there is no choice of language. Steps in the setup process are accepting the licence agreement, choosing whether to send malware data to G Data, opting for a full or custom installation (we chose the latter), selecting the installation folder, and entering a licence key or using the program as a 30-day trial. A restart is required when the setup wizard has finished.

We saw from Windows Action Center that G Data Internet Security had registered itself as an antivirus, antispyware and firewall program. Windows Firewall had been disabled, Windows Defender had not.



Security

Network firewall On

G Data Personal Firewall reports that it is currently turned on.

View installed firewall programs

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

G Data InternetSecurity 2012 reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

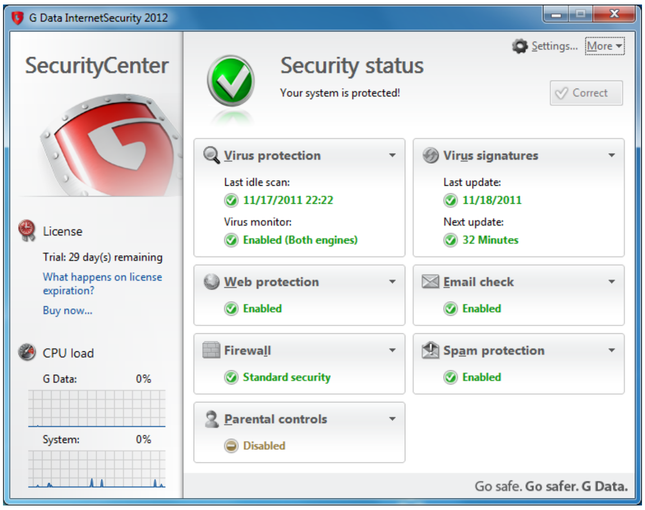
Windows Defender and G Data InternetSecurity 2012 both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

The uninstaller program has no repair option, but does allow selective removal of components.

Program Interface

The main program window of G Data Internet Security 2010 has a narrow left-hand pane containing the G Data logo, licence information, and graphs of CPU load for the G Data suite, and the system as a whole.

The right-hand pane is dominated by a horizontal status strip at the top, which shows a tick (checkmark) in a green circle, along with the words “Your system is protected!” if all is well:



Security status
Your system is protected!

License
Trial: 29 day(s) remaining
What happens on license expiration?
Buy now...

CPU load
G Data: 0%
System: 0%

Virus protection
Last idle scan: 11/17/2011 22:22
Virus monitor: Enabled (Both engines)

Virus signatures
Last update: 11/18/2011
Next update: 32 Minutes

Web protection: Enabled

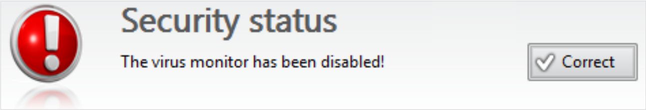
Email check: Enabled

Firewall: Standard security

Spam protection: Enabled

Parental controls: Disabled

Disabling the real-time virus protection changes the display to an exclamation mark in a red circle, with a description of the problem, namely “The virus monitor has been disabled!”. The “Correct” button to the right enables protection to be re-enabled with a single click:



Security status
The virus monitor has been disabled!

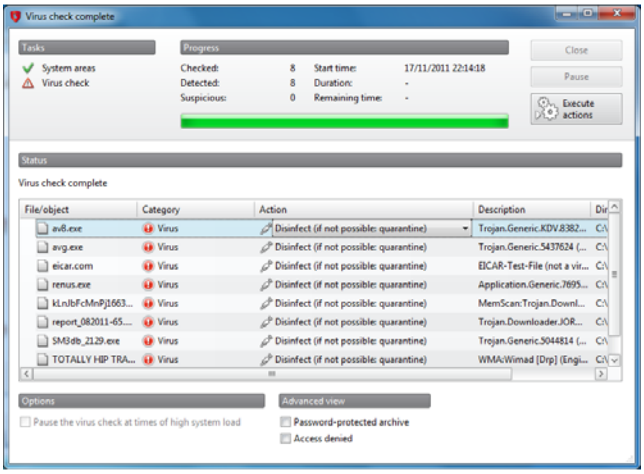
The remainder of the right-hand pane of the window is made up of boxes for the components of the suite, with status information (e.g. enabled/disabled), and links to the configuration settings for each item. We found this give a very good overview of the system and enables easy configuration of individual components.

Default configuration

Scanning and malware discovery

G Data Internet Security is set by default to run an idle-time scan, i.e. to scan the PC when it is not being used. It is possible to set up a scan to run at a specific time/day, using the advanced settings. We could not find any means of running a boot-time scan directly from the program interface, but the program includes the ability to make a boot CD for cleaning infected systems.

Running a custom or context-menu scan with G Data Internet Security produced the following dialog box:



Virus check complete

✓ System areas
⚠ Virus check

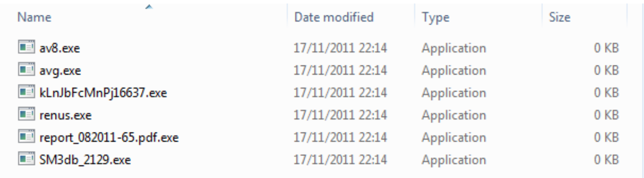
Checked: 8 Start time: 17/11/2011 22:14:18
Detected: 8 Duration: -
Suspicious: 0 Remaining time: -

Virus check complete

File/object	Category	Action	Description	Dir
av8.exe	Virus	Disinfect (if not possible: quarantine)	Trojan.Generic.KDV.8382...	C:\
avg.exe	Virus	Disinfect (if not possible: quarantine)	Trojan.Generic.5437624 (...	C:\
eicar.com	Virus	Disinfect (if not possible: quarantine)	EICAR-Test-File (not a vir...	C:\
renus.exe	Virus	Disinfect (if not possible: quarantine)	Application.Generic.7695...	C:\
kLnJbFcMnPj1663...	Virus	Disinfect (if not possible: quarantine)	MemScan:Trojan.Downl...	C:\
report_082011-65....	Virus	Disinfect (if not possible: quarantine)	Trojan.Downloader.JOR...	C:\
SM3db_2129.exe	Virus	Disinfect (if not possible: quarantine)	Trojan.Generic.5044814 (...	C:\
TOTALLY HIP TRA...	Virus	Disinfect (if not possible: quarantine)	WMA:Wimad [Drp] (Engi...	C:\

□ Pause the virus check at times of high system load
□ Password-protected archive
□ Access denied

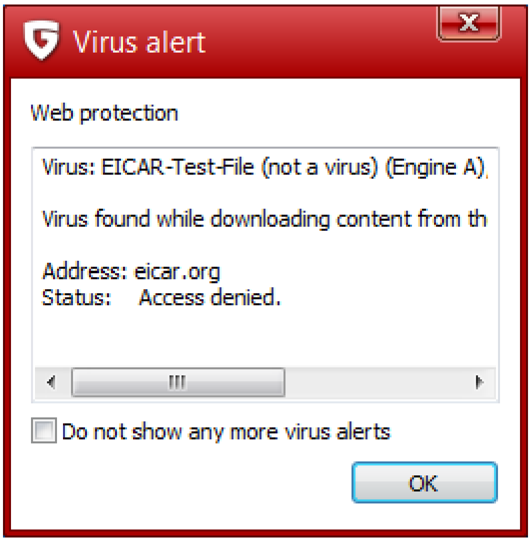
The default action for each item is “Disinfect; if not possible: quarantine”. It is possible to change this action on an item-by-item basis, but we could not find a means of changing the option for all items at once. Clicking on “Execute Actions” carries out the selected treatment of the malware. We noted that whilst all our malware samples were rendered entirely harmless, G Data actually left behind a number of 0KB .exe files, having stripped all the malicious code out of each executable:



Name	Date modified	Type	Size
av8.exe	17/11/2011 22:14	Application	0 KB
avg.exe	17/11/2011 22:14	Application	0 KB
kLnJbFcMnPj16637.exe	17/11/2011 22:14	Application	0 KB
renus.exe	17/11/2011 22:14	Application	0 KB
report_082011-65.pdf.exe	17/11/2011 22:14	Application	0 KB
SM3db_2129.exe	17/11/2011 22:14	Application	0 KB

This is not a problem for experienced users, but could be confusing to non-experts; we would suggest that quarantine would be the better default action.

When we attempted to download the EICAR test file, G Data blocked the page and the download, and displayed the following message:



Virus alert

Web protection

Virus: EICAR-Test-File (not a virus) (Engine A),

Virus found while downloading content from th

Address: eicar.org
Status: Access denied.

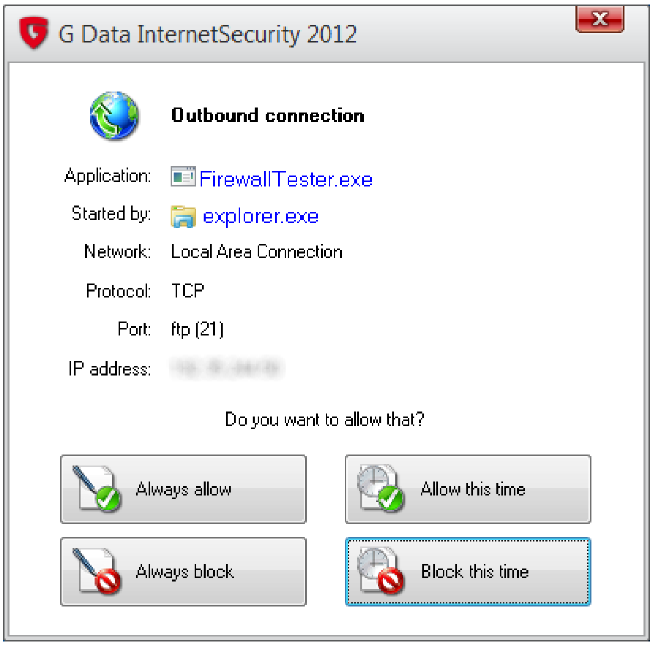
□ Do not show any more virus alerts

Inbound Firewall Settings

After Installing G Data Internet Security 2012 and rebooting, we were able to ping and access the file share on our test PC, as we had before the installation.

Outbound Firewall/Application Control

Our firewall tester ran and downloaded its test file without hindrance or query from G Data Internet Security with default configuration. When we changed the firewall's settings from the default Autopilot mode to "Create rules manually", G Data produced the following dialog box:



G Data InternetSecurity 2012

Outbound connection

Application: FirewallTester.exe
Started by: explorer.exe
Network: Local Area Connection
Protocol: TCP
Port: ftp (21)
IP address: [redacted]

Do you want to allow that?

Spam protection

Spam protection is enabled by default, the standard action being to mark the mail as spam and move to a specially created AntiSpam folder.

Parental Control

Parental Controls are clearly shown as being disabled by default, but can very easily be enabled for individual Windows accounts by clicking on the link on the home page of the program window.

Safe Mode

We were unable to run any type of scan in Safe Mode with G Data Internet Security, and all attempts to start G Data services manually failed. As noted above, the program includes the ability to make a boot CD for cleaning infected systems.

Help and Documentation

Searching the local help feature for information on making exceptions (exclusions) to scans quickly produced clear and comprehensive instructions. Looking for information on scheduling scans proved more tricky – it transpires that G Data uses the term “automatic” rather than “scheduled”. The instructions are available once you’ve found the right search term.

The “Support Center” pages on G Data’s website include options for contacting technical support and downloading support tools, but we could not find any manuals or other support documentation.

Verdict

Overall

G Data Internet Security is a very well thought-out suite, suitable for use by both non-experts and advanced users.

Plus points

Interface allows clear overview of the components of the suite and their status, with easy access to configuration settings. There is a choice of components in both the installer and the uninstaller.

Minus points

Leaving 0KB files after “cleaning” malware; inability to function in Safe Mode

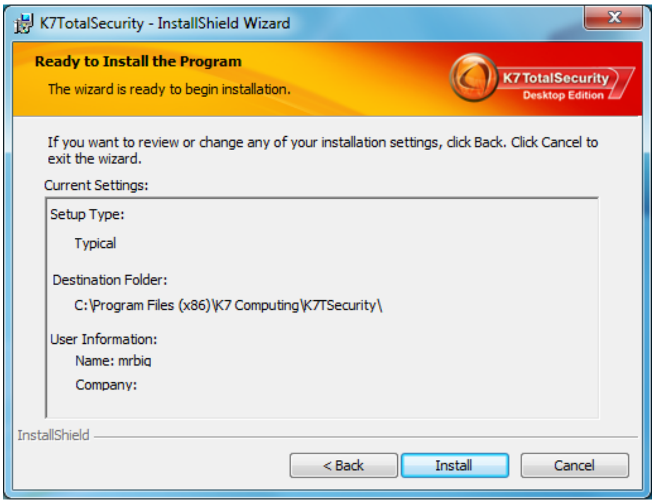
K7 Total Security 11

Components

- Antimalware
- Antispam
- Firewall
- Parental Control

Installation

We installed K7 Total Security from a 70 MB .exe file. Installing the suite is extremely simple, and really only involves accepting a licence agreement and entering a key or choosing to use the product as a trial version. There are no other options. Unfortunately, version 11 retains a pointless dialog box which we spotted in version 10 a year ago. The third page of the setup wizard shows Setup Type, Destination Folder, and User Information, and states "If you want to review or change any of your installation settings, click Back"; these elements could not be altered in the previous two steps, and clicking Back simply returns to these; there is no means of reviewing or changing any of these items at any stage. We feel that some users may find this frustrating and/or confusing.


K7TotalSecurity - InstallShield Wizard
K7 TotalSecurity Desktop Edition
InstallShield
< Back
Install
Cancel

Ready to Install the Program

The wizard is ready to begin installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Current Settings:

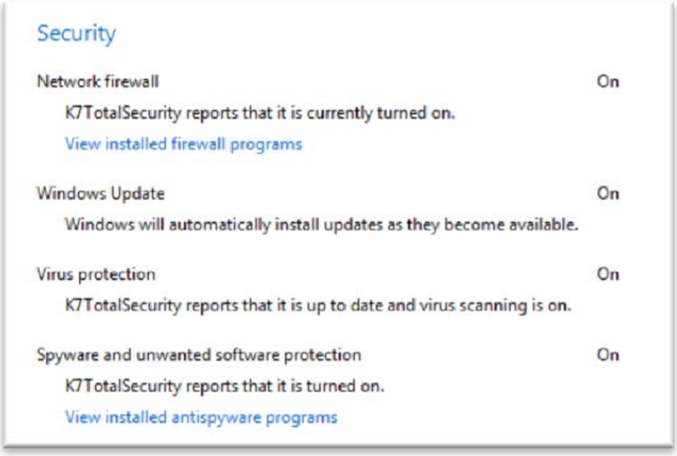
Setup Type:
Typical

Destination Folder:
C:\Program Files (x86)\K7 Computing\K7TSecurity\

User Information:
Name: mrbiq
Company:

A restart was not required when the setup wizard finished; however, we were prompted to restart the computer after updating K7 Total Security.

Consulting Windows Action Center showed K7 had registered itself as an antivirus, antispyware and firewall program, and had disabled both Windows Firewall and Windows Defender:



Security

Network firewall On

K7TotalSecurity reports that it is currently turned on.

View installed firewall programs

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

K7TotalSecurity reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

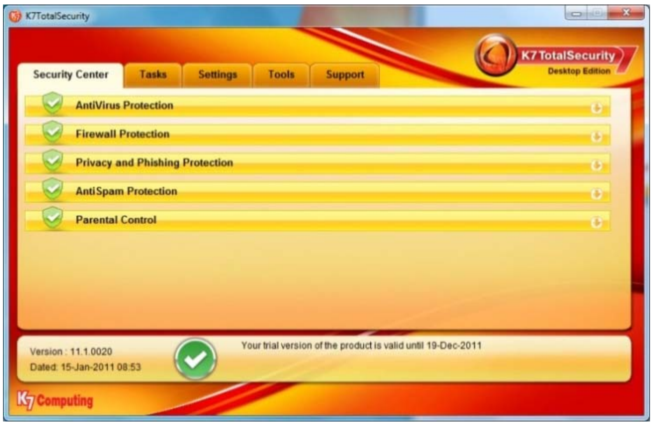
K7TotalSecurity reports that it is turned on.

View installed antispyware programs

The uninstall program has no options other than complete removal.

Program Interface

The default page of the K7 Total Security window is entitled Security Center, and it provides an overview of the protection components of the suite and their status. Each component is shown as a horizontal strip, with a shield at the left-hand end; this is green with a white tick (checkmark) if all is well:

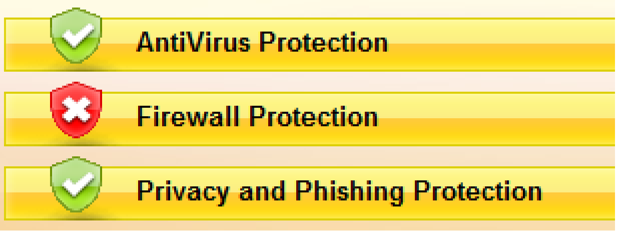


Version : 11.1.0020

Dated: 15-Jan-2011 08:53

Your trial version of the product is valid until 19-Dec-2011

The shield symbol changes to red with a white cross if a critical component is disabled:



Clicking on the strip with the warning displays all the sub-components, and enables any deactivated ones to be reactivated. There is no overall status display or fix-all button; however, we feel that the program provides perfectly adequate warning when something is wrong, and makes it straightforward to put it right.

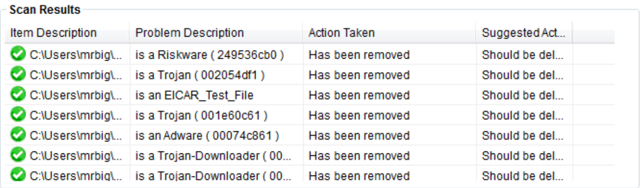
A set of tabs at the top of the window allow other pages to be selected: Tasks, which includes various scan options including scheduling; Settings, which allows detailed configuration changes to be made for each component; Tools, which includes a history cleaner, secure delete, and virtual keyboard; and Support, which includes subscription information and help and support links. Whilst we found the red and yellow colour scheme rather dazzling, we can only describe the layout of the program as very simple, clean and easy to use.

Default configuration

Scanning and malware discovery

There is no scheduled scan set by default, but it is straightforward to create one using the scheduling option under Tasks. We could not find any means of running a boot-time scan.

Running a custom or context-menu scan of our malware collection with K7 produced the following results box:

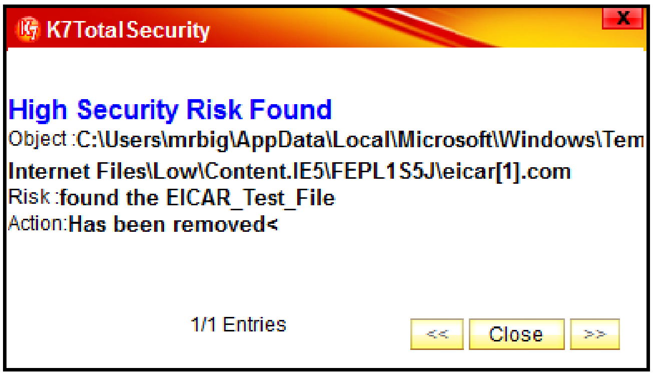


Scan Results

Item Description	Problem Description	Action Taken	Suggested Act...
✓ C:\Users\mrbig\...	is a Riskware (249536cb0)	Has been removed	Should be del...
✓ C:\Users\mrbig\...	is a Trojan (002054df1)	Has been removed	Should be del...
✓ C:\Users\mrbig\...	is an EICAR_Test_File	Has been removed	Should be del...
✓ C:\Users\mrbig\...	is a Trojan (001e60c61)	Has been removed	Should be del...
✓ C:\Users\mrbig\...	is an Adware (00074c861)	Has been removed	Should be del...
✓ C:\Users\mrbig\...	is a Trojan-Downloader (00...	Has been removed	Should be del...
✓ C:\Users\mrbig\...	is a Trojan-Downloader (00...	Has been removed	Should be del...

This shows that all the threats have been removed, and that no further action is necessary.

When we attempted to download the EICAR test file, K7 blocked the download and showed the following message:



High Security Risk Found

Object :C:\Users\mrbig\AppData\Local\Microsoft\Windows\Tem
Internet Files\Low\Content.IE5\FEPL1S5J\eicar[1].com
Risk :found the EICAR_Test_File
Action:Has been removed<

1/1 Entries

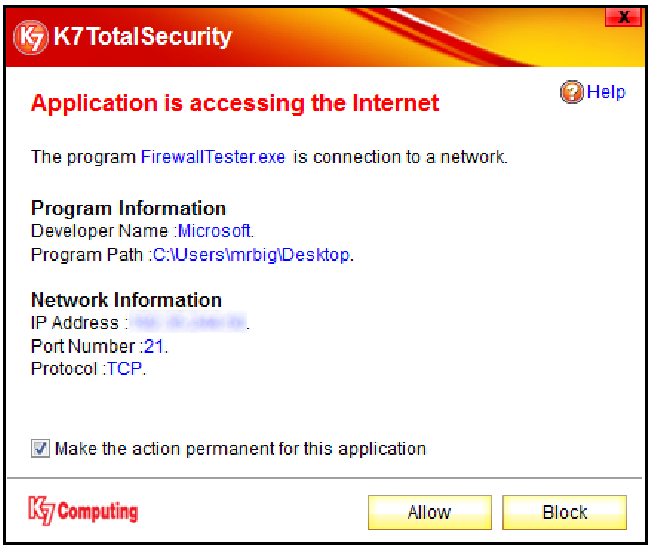
If you read this carefully, you will see that it informs the user that the threat has been removed. However, we feel the text is so cluttered that it is not immediately clear what has happened. We would suggest that hiding the exact path to the object (with a link for advanced users entitled "Details") would make it easier to see what the threat was, and that it has been dealt with. Fortunately, the message is displayed until the user clicks "Close", so there is abundant time for anyone who wants to read it to do so.

Inbound Firewall Settings

After installing K7 Total Security, we were able to ping our test PC, and access its file share over the network, exactly as before the installation.

Outbound Firewall/Application Control

With default settings, K7 Total Security allowed our firewall testing program to open and download its test file without any interruption or query. Changing the default application setting from "Allow automatically" to "Prompt for Action" brought up the following dialog box when we ran our firewall tester again:



Application is accessing the Internet

The program FirewallTester.exe is connection to a network.

Program Information
Developer Name :Microsoft.
Program Path :C:\Users\mrbig\Desktop.

Network Information
IP Address : [redacted].
Port Number :21.
Protocol :TCP.

☑ Make the action permanent for this application

Spam protection

Spam protection is enabled by default, and can be configured from the relevant link in the "AntiSpam Protection" strip on the program's home page.

Parental Control

Parental Control is shown as being enabled by default, although it effectively isn't until it is configured for each Windows user. This is however very easy to do, using the Configure link on the Parental Control strip on the home page of the program.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to update K7's virus definitions. However, running a scan of our malware samples identified and removed all of them, exactly as it would do in standard mode.

Help and Documentation

The local help service quickly provided clear answers to our search for information on scheduling a scan, and creating scan exceptions/exclusions. Documentation in the form of two .pdf manuals is available from the K7 website. There is a comprehensive 163-page manual, and a 23-page Quick Start Guide. Both are illustrated with abundant screenshots.

Verdict

Overall

K7 Total Security has a well-designed interface that could easily be used by expert or non-expert users.

Plus points

Very simple setup and user interface, largely ideal for non-experts. Concise quick-start guide, and comprehensive manual.

Minus points

Pointless page of setup wizard, which erroneously suggests certain options can be changed; cluttered text in malware discovery message; exceedingly bright colour scheme.

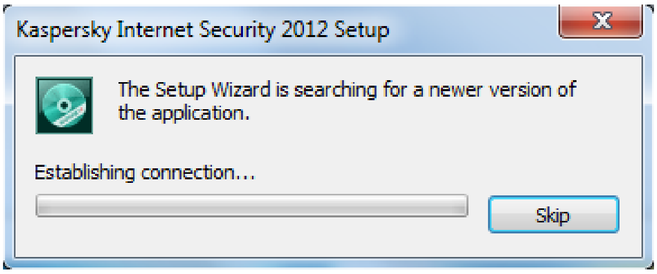
Kaspersky Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall
- Parental Control

Installation

We installed Kaspersky Internet Security from a 67 MB .exe file. Although this is a complete installation package, which could be used on a PC without an Internet connection, the setup wizard checks for a newer version of the software before installing:

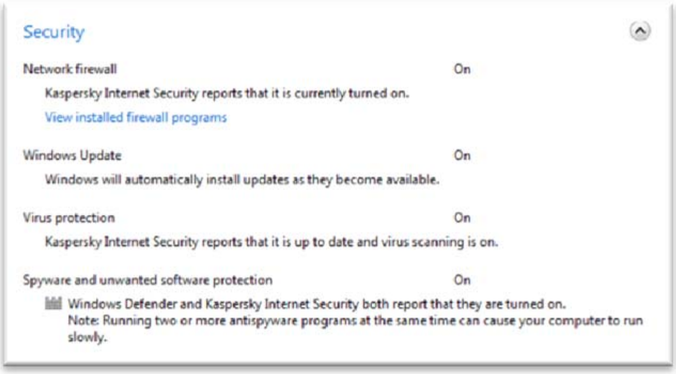


Kaspersky Internet Security 2012 Setup

The Setup Wizard is searching for a newer version of the application.

Establishing connection...

We chose the custom installation option (“Change installation settings”), which allowed us to choose whether to participate in the Kaspersky Security Network (cloud-based sharing of malware information), and the location of the installation folder. There is no choice of languages or which components to install. Naturally there is a licence agreement to accept. A reboot is not required after installation, and so the program can be started as soon as the setup wizard finishes. A dialog box immediately asks the user to enter a licence key, or activate a 30-day trial. Kaspersky Internet Security 2012 registers with Windows Action Center as an antispyware and antivirus program, and as the system firewall. Windows Firewall is deactivated, but Windows Defender is not.



Security

Network firewall On

Kaspersky Internet Security reports that it is currently turned on.

View installed firewall programs

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

Kaspersky Internet Security reports that it is up to date and virus scanning is on.

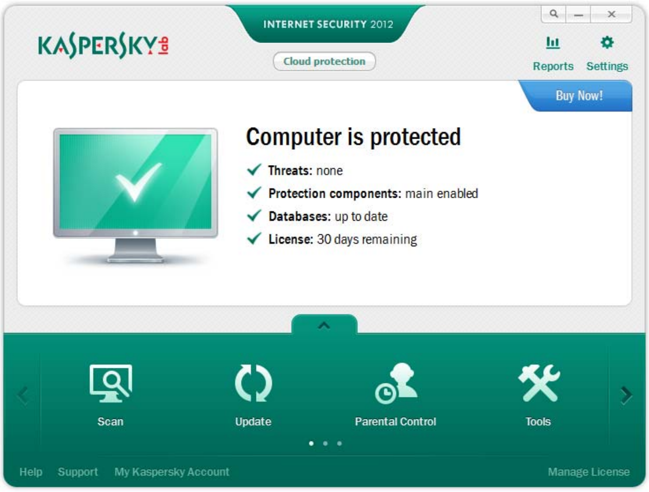
Spyware and unwanted software protection On

Windows Defender and Kaspersky Internet Security both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

The uninstall program only allows the program to be removed in its entirety, without any repair or component selection options. It does however allow activation data, settings and quarantined items to be retained.

Program Interface

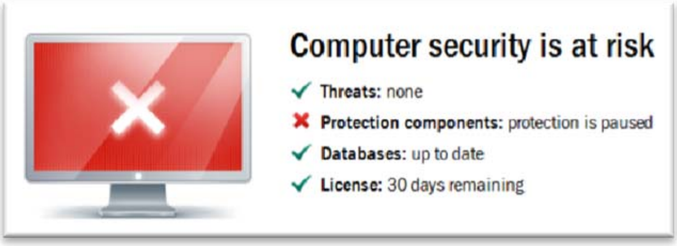
The completely redesigned interface of Kaspersky Internet Security 2012 is in our opinion very clear and uncluttered, with all the essential information and tools to hand. The window is essentially split into two horizontal panes, the upper one with status information, and the lower one with essential tools:



Computer is protected

- Threats: none
- Protection components: main enabled
- Databases: up to date
- License: 30 days remaining

The upper pane shows a computer screen with a tick on a green background if all is well. There are also text entries for Threats, Protection Components, Databases, and Licence. In the event of a security problem, such as real-time protection being enabled, the computer screen picture turns to red with a cross in it, and Protection Components shows “Protection is paused”:

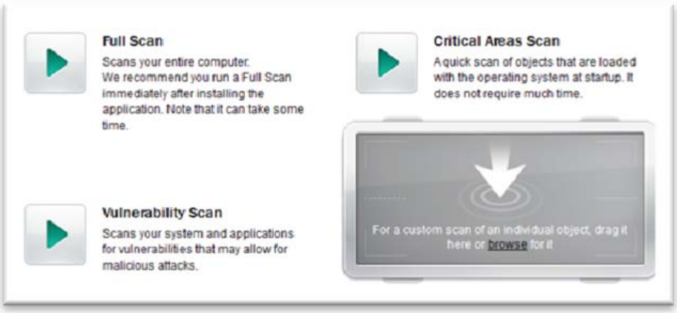


Computer security is at risk

- ✓ Threats: none
- ✗ Protection components: protection is paused
- ✓ Databases: up to date
- ✓ License: 30 days remaining

There is no “Fix All” button, but clicking anywhere in the upper pane opens a page showing the threat(s), with a button to fix each one – in this case, to reactivate the real-time protection.

The lower pane of the window has four big buttons, Scan, Update, Parental Control, and Tools. Scan opens a page of options: Full Scan, Vulnerability Scan, and Critical Areas Scan, each with an explanation, plus Custom Scan:



Full Scan

Scans your entire computer. We recommend you run a Full Scan immediately after installing the application. Note that it can take some time.

Critical Areas Scan

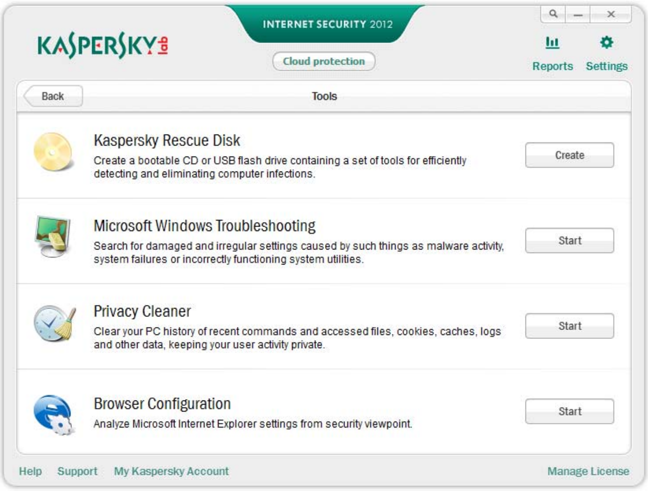
A quick scan of objects that are loaded with the operating system at startup. It does not require much time.

Vulnerability Scan

Scans your system and applications for vulnerabilities that may allow for malicious attacks.

For a custom scan of an individual object, drag it here or browse for it

Update provides details of the time of the last update and signature version, along with a button to start a manual update. Parental Control starts the configuration process for this feature, which begins with a prompt to set a password to protect the settings being changed by other users. Tools provides a variety of functions, such as making a rescue disk and deleting private information:



Kaspersky Rescue Disk

Create a bootable CD or USB flash drive containing a set of tools for efficiently detecting and eliminating computer infections.

Microsoft Windows Troubleshooting

Search for damaged and irregular settings caused by such things as malware activity, system failures or incorrectly functioning system utilities.

Privacy Cleaner

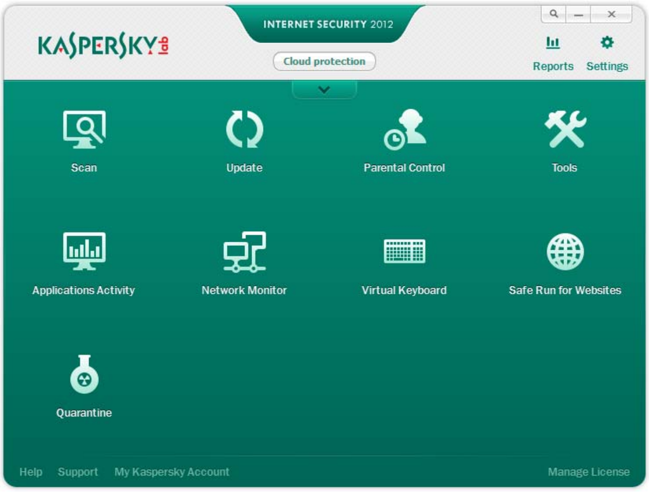
Clear your PC history of recent commands and accessed files, cookies, caches, logs and other data, keeping your user activity private.

Browser Configuration

Analyze Microsoft Internet Explorer settings from security viewpoint.

Each of the pages features a “back” button to return to the home page of the application.

At the top of the lower pane is an arrow pointing up; clicking this expands the features pane to fill the whole window, thus showing extra items such as Virtual Keyboard and Quarantine:



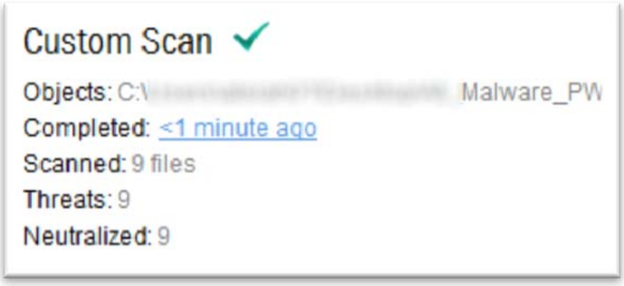
The additional items can also be accessed by using the left and right arrow buttons in the lower pane, which scroll through all the available features. Finally, there are text links in the top-right hand corner of the window to Reports and Settings, and in the bottom left-hand corner to Help, Support and My Kaspersky Account.

Default settings and configuration

Scanning and malware discovery

By default, no scheduled scan is configured. This can be set up by going into Settings, selecting the Scan tab, clicking on the scan type (e.g. Full), and then clicking Run Mode. We could not find any option to run a boot-time scan.

Both the custom scan and context-menu scan of a folder containing malware items automatically quarantined the threats, with a pop-up message informing us of this. Thus the malware is made safe without any intervention from the user being required.



Custom Scan ✓

Objects: C:\[redacted]Malware_PW

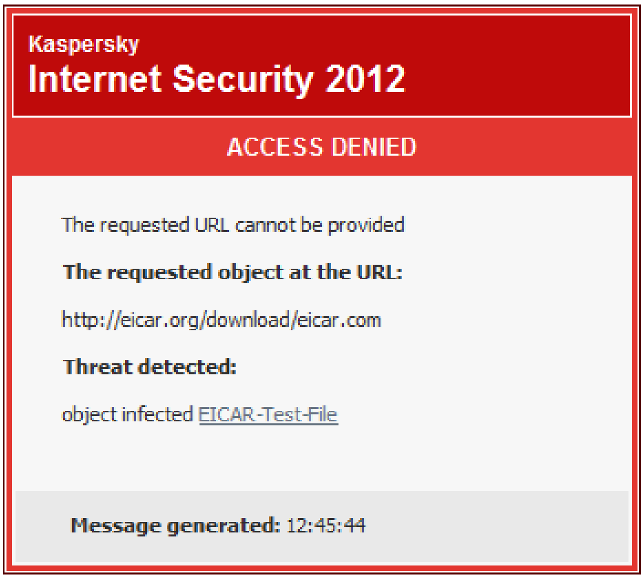
Completed: <1 minute ago

Scanned: 9 files

Threats: 9

Neutralized: 9

When we tried to download the EICAR test file, Kaspersky blocked both the download and the page, displaying the following message in the browser:



Kaspersky

Internet Security 2012

ACCESS DENIED

The requested URL cannot be provided

The requested object at the URL:

http://eicar.org/download/eicar.com

Threat detected:

object infected EICAR-Test-File

Message generated: 12:45:44

We feel that this message could make clearer to non-expert users that the threat has been neutralised, and that no action is required on their part.

Inbound Firewall Settings

By default, Kaspersky's firewall continued to allow file and printer sharing for our test PC, which we had already configured before installing the suite.

Outbound Firewall/Application Control

The default firewall and application control settings allowed our firewall testing program to access the Internet and download its test file, having correctly recognised that it was harmless. Kaspersky's Application Control works by assigning programs to the groups Trusted, Low Restricted, High Restricted, and Untrusted. By default, our firewall tester was put in the Low Restricted group, which meant that it was able to function fully. Moving it to the High Restricted group allowed the program to start, but blocked the file download; putting it in the Untrusted group meant that the program would not even start. In none of these cases did Kaspersky's suite ask whether it should allow the program to run; the decision was made automatically.

Spam protection

Spam protection is enabled by default and set to the "Recommended" level; there are two other settings, High (the most aggressive filtering method, to ensure all spam mails are caught), and Low (the least aggressive, ensuring a minimum number of false positives).

Parental Control

Parental Control has to be configured for each user account. This can be done very easily by clicking on the Parental Control button on the home page of the program window.

Safe Mode

When we started our PC in Safe Mode with Networking, we were able to open Kaspersky Internet Security, update definitions and run a scan as normal. We scanned our folder of malware, and Kaspersky found and removed all items just as it would in Windows standard mode. We were also able to start a full scan as normal.

Help and Documentation

Clicking on the Help link in the bottom right-hand corner of the program window opens the local help window. Our search for instructions on scheduling a scan quickly brought up clear (albeit brief, text-only) instructions; finding details of how to exclude a folder from scanning proved more difficult.

The kaspersky.com website has an outstanding support section for Internet Security 2012, in which we quickly found clear and simple instructions for both of our sample tasks, which were even illustrated with videos. We can only describe this as exceptionally good. Clicking on the Support link in the Kaspersky Internet Security 2012 window, then Knowledge Base, leads to a general search page for all products, meaning a lot of results for other products have to be filtered out. We wonder whether Kaspersky might not manage to link to a specific page for Internet Security, or allow users to specify the product they need help with before entering the search term.

There is an extremely comprehensive manual (226 pages) freely available to download from Kaspersky's website. It is clearly written, very well indexed and bookmarked, although screenshots are limited in number.

Verdict

Overall

We found Kaspersky Internet Security 2012 to be very easy to install and use. It is suitable for both non-experts and advanced users.

Plus points

Full installer that checks for updates if online; new interface is simple, clean, and user-friendly; updating and scanning functions are fully operational in Safe Mode; online support for the suite is superb once you find it; comprehensive manual available

Minus points

Warning message about malware download could be clearer; Support link in the program doesn't link to the optimal page of Kaspersky's website.

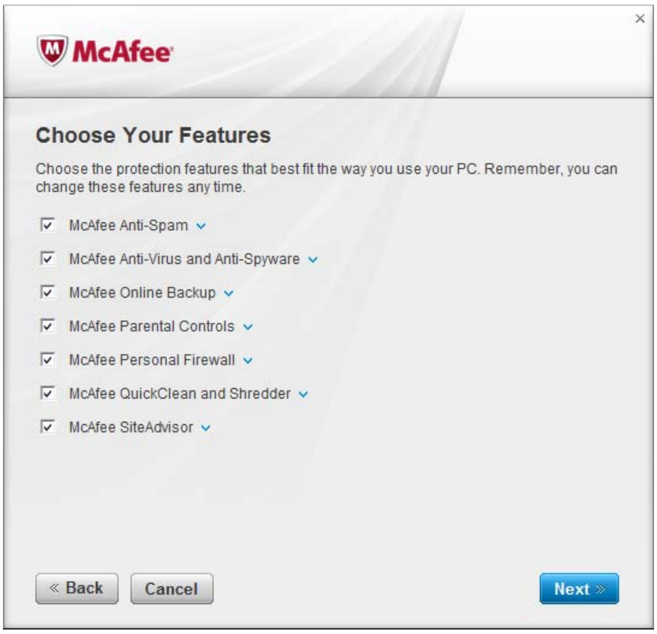
McAfee Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall
- Parental Controls
- Backup
- Shredder

Installation

We installed McAfee Internet Security 2012 from a 4 MB downloader. There is a minimum of steps to complete; a custom option is available, which allows a complete choice of the components to be installed:

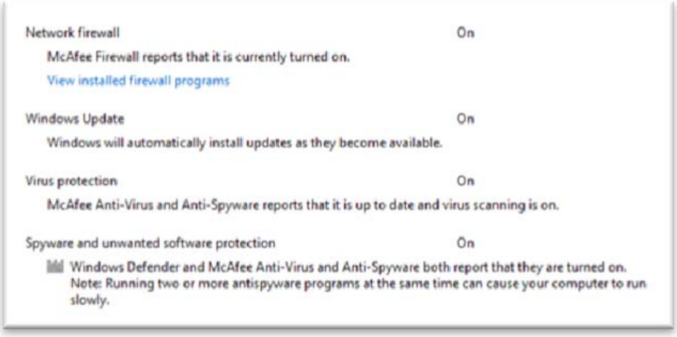


Choose Your Features

Choose the protection features that best fit the way you use your PC. Remember, you can change these features any time.

☑ McAfee Anti-Spam
☑ McAfee Anti-Virus and Anti-Spyware
☑ McAfee Online Backup
☑ McAfee Parental Controls
☑ McAfee Personal Firewall
☑ McAfee QuickClean and Shredder
☑ McAfee SiteAdvisor

There is also a choice of whether to send anonymous usage data to McAfee. No restart is needed after the installation. Windows Action Center showed us that McAfee Internet Security had registered as an antivirus, antispyware and firewall application; Windows Firewall had been disabled, Windows Defender had not.



Network firewall On
McAfee Firewall reports that it is currently turned on.
View installed firewall programs

Windows Update On
Windows will automatically install updates as they become available.

Virus protection On
McAfee Anti-Virus and Anti-Spyware reports that it is up to date and virus scanning is on.

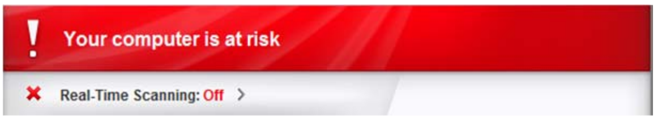
Spyware and unwanted software protection On
Windows Defender and McAfee Anti-Virus and Anti-Spyware both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

McAfee's uninstaller has no options except removing SiteAdvisor separately from the remainder of the suite.

Program Interface

McAfee Internet Security's main program window has a rather unusual design, in that it is tall and narrow.

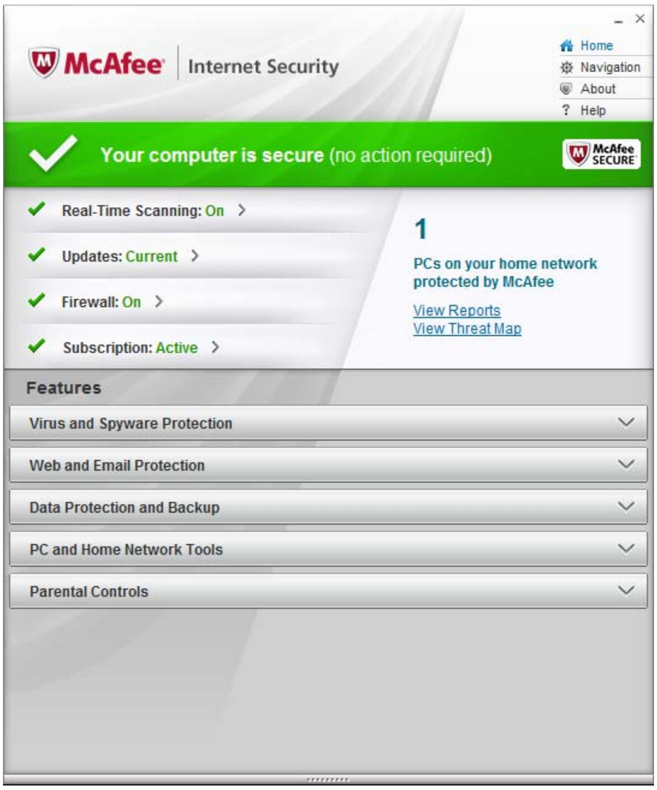
A very prominent status strip runs across the top of the window; this shows a tick (checkmark) on a green background if all is well, together with the words "Your computer is secure". In the event of a problem, such as real-time virus protection being disabled, the strip turns to red, and displays an explanation mark with the words "Your computer is at risk":



! Your computer is at risk

✗ Real-Time Scanning: Off >

While the warning is very clear, we were not able to find any means of quickly re-activating the protection; we had to go back into the settings to switch it on again. We would suggest that especially for beginners, an obvious "Fix All" button would be an improvement.



Your computer is secure (no action required)

Real-Time Scanning: On

Updates: Current

Firewall: On

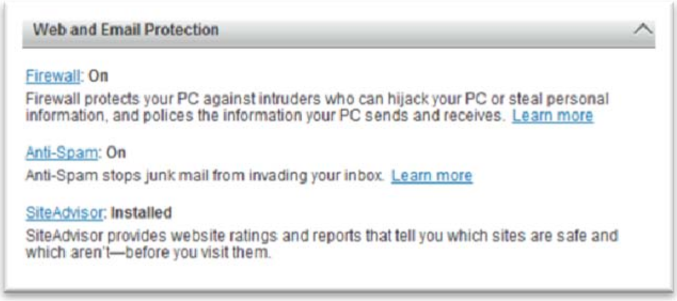
Subscription: Active

1 PCs on your home network protected by McAfee

View Reports

View Threat Map

The interface consists of a number of horizontal strips. Those in the lower half of the window represent configuration options for the major components of the suite: Virus and Spyware Protection, Web and Email Protection, Data Protection and Backup, PC and Home Network Tools, and Parental Controls. Clicking on one of these strips expands it downwards to show various links:



Firewall: On

Firewall protects your PC against intruders who can hijack your PC or steal personal information, and polices the information your PC sends and receives. Learn more

Anti-Spam: On

Anti-Spam stops junk mail from invading your inbox. Learn more

SiteAdvisor: Installed

SiteAdvisor provides website ratings and reports that tell you which sites are safe and which aren't—before you visit them.

The strips at the top of the window show the status of essential protection components: Real-Time Scanning, Updates, Firewall, Subscription. Clicking on one of these shows relevant links (e.g. Settings) in the right-hand side of the top section of the window.

Additionally, there are four small text links in the top right-hand corner of the window: Home, Navigation, About, and Help.

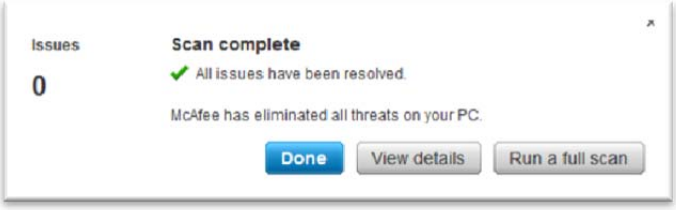
We found that McAfee's user interface took a little bit of getting used to, but it was actually simple to use once we had become accustomed to it.

Default configuration

Scanning

A scheduled scan is configured by default. It can easily be edited or deleted from links in both the Real-Time Scanning section at the top of the window, and the Virus and Spyware Protection strip. We could not find any means of running a boot-time scan.

When we ran a custom or context-menu scan on our collection of malware, McAfee detected and quarantined all of the samples with a minimum of fuss, displaying the following message:



Issues

0

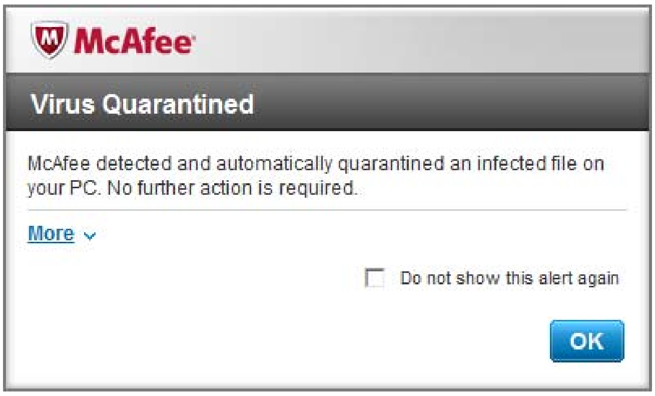
Scan complete

✓ All issues have been resolved.

McAfee has eliminated all threats on your PC.

Clicking on “View details” showed a list of the malware items that had been found and the action taken, along with details of each threat. We found the action taken and report at the end of the scan to be excellent; the message clearly informs the user that the threats have been removed and that no further action is required, while advanced users can easily find more details, and could remove any items from quarantine if necessary.

When we attempted to download the EICAR test file, McAfee Internet Security blocked the download and displayed the following message box:



Virus Quarantined

McAfee detected and automatically quarantined an infected file on your PC. No further action is required.

□ Do not show this alert again

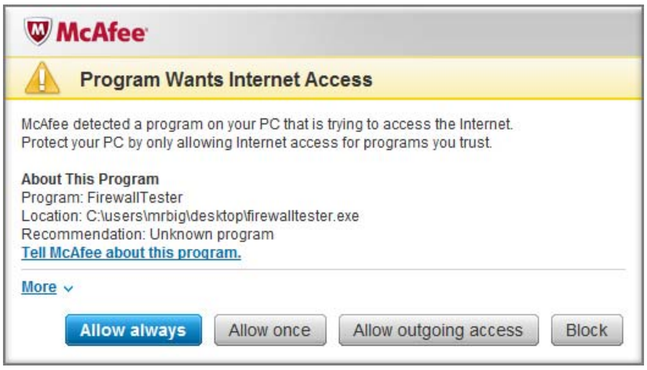
The message makes clear that the “threat” has been dealt with, and that no further action is required.

Inbound Firewall Settings

We were unable to ping our test PC or access its file share after installing McAfee Internet Security 2012. Checking the firewall showed that the network type had been set to “Work”; unlike Windows’ interpretation of a “work” network, McAfee’s does not allow file sharing. When we changed the network type to Home, pinging and file sharing became possible.

Outbound Firewall/Application Control

When we ran our firewall testing program with McAfee’s default firewall settings, it was able to download its test file without any hindrance or query from McAfee. Setting the firewall to “Stealth Mode” produced the following dialog box when running the program again:



McAfee detected a program on your PC that is trying to access the Internet.
Protect your PC by only allowing Internet access for programs you trust.

About This Program
Program: FirewallTester
Location: C:\users\mrbig\desktop\firewalltester.exe
Recommendation: Unknown program
Tell McAfee about this program.

Spam protection

Anti-Spam is enabled by default. It marks the subject line of the mail with [SPAM] and moves it to a folder marked Anti-Spam.

Parental Control

Parental Controls are not configured by default and are not shown as being active. They can easily be configured by clicking on the Parental Controls strip in the main window.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to open the McAfee program window and run an update as normal, although real-time protection was disabled. The status display in the window confirmed that the updates had been installed. We ran a context-menu scan on our collection of malware, and McAfee found and quarantined all the items just as in standard mode.

Help and Documentation

The local Help function in McAfee Internet Security 2012 has a search function which enabled us to quickly find instructions for setting a scan schedule. Searching for “exceptions” and “exclusions” drew a blank; there IS a help item on this issue, but finding it requires the specific word “excluding”; we suggest that many users might abandon their search for this particular item without finding anything.

There is an online Support page, which includes FAQs, Search, and Video Tutorial sections. We were unable to find any video tutorials at all for Internet Security. The list of FAQs appeared to be very limited (10 items). Searching for “scheduled scan” produced over 80 answers, although none appeared to be relevant. In short, the online support can only be described as a disappointment.

Verdict

Overall

McAfee Internet Security is very simple to install, and easy to use once you get used to it. It is suitable for both expert and non-expert users.

Plus points

Ability to download definition updates and scan in Safe Mode with Networking; ideal reporting and action taken when malware is discovered in a download or during a scan; complete choice of components to install is available in the setup wizard.

Minus points

No “Fix All” button to resolve problems quickly and easily. Local help is very keyword specific, online help of very limited value.

Microsoft Security Essentials 2.1

Nature of the program

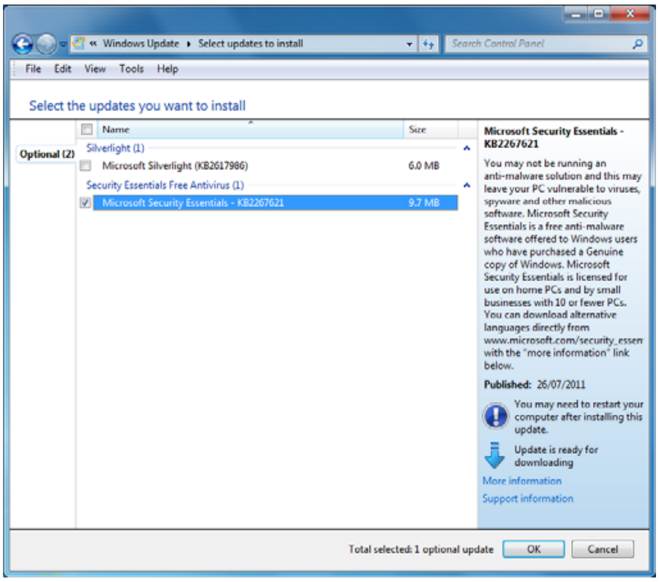
Microsoft Security Essentials is, unlike the other programs in this review, a pure and simple antimalware (antivirus and antispyware) program. It does not include a firewall, antispam protection or parental controls. Of course, the last three versions of Windows (XP, Vista and Seven) all include their own firewall, so users of Security Essentials will not need to purchase a third-party firewall to ensure their computers are protected from network attacks.

We note that Microsoft's current email programs (Outlook and Windows Live Mail) both include a spam filtering mechanism, and that Windows Live Family Safety, Microsoft's parental control program, is available as a free download.

Because Microsoft Security Essentials is not a full suite, we have omitted the sections relating to firewalls, spam protection and parental control from this report. Additionally, we have not commented on component choice in the installer or uninstaller, as there is only the one component available.

Installation

Microsoft Security Essentials (MSE) is available through Windows Update, as an optional update. It will only appear in the list of optional updates if no other antivirus program has registered with Windows Action Center. As this was the case with our test PC, we opted to install Security Essentials via Windows Update. This process is very simple. Open Windows Update, click on the link marked "...optional updates are available", and select Microsoft Security Essentials:



Select the updates you want to install

☐	Name	Size
	Silverlight (1)	
☐	Microsoft Silverlight (KB2617986)	6.0 MB
	Security Essentials Free Antivirus (1)	
☑	Microsoft Security Essentials - KB2267621	9.7 MB

Microsoft Security Essentials - KB2267621

You may not be running an anti-malware solution and this may leave your PC vulnerable to viruses, spyware and other malicious software. Microsoft Security Essentials is a free anti-malware software offered to Windows users who have purchased a Genuine copy of Windows. Microsoft Security Essentials is licensed for use on home PCs and by small businesses with 10 or fewer PCs. You can download alternative languages directly from www.microsoft.com/security_essen with the "more information" link below.

Published: 26/07/2011

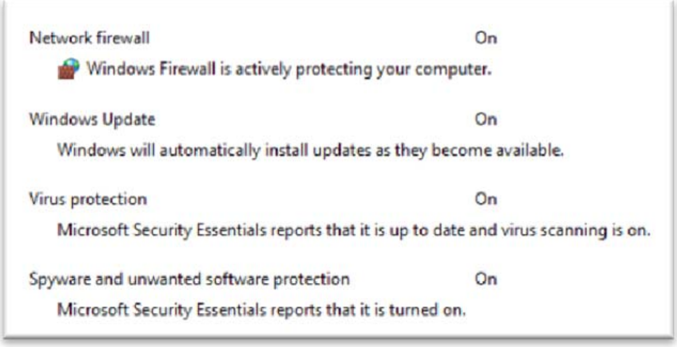
You may need to restart your computer after installing this update.

Update is ready for downloading

Total selected: 1 optional update

Click OK, and then Install Updates. Installation proceeds without any further user intervention. A restart is not required.

When we looked in Windows Action Center after installation, we saw that MSE had registered itself as an antivirus and antispyware application, and had disabled Windows Defender:



Network firewall On
Windows Firewall is actively protecting your computer.

Windows Update On
Windows will automatically install updates as they become available.

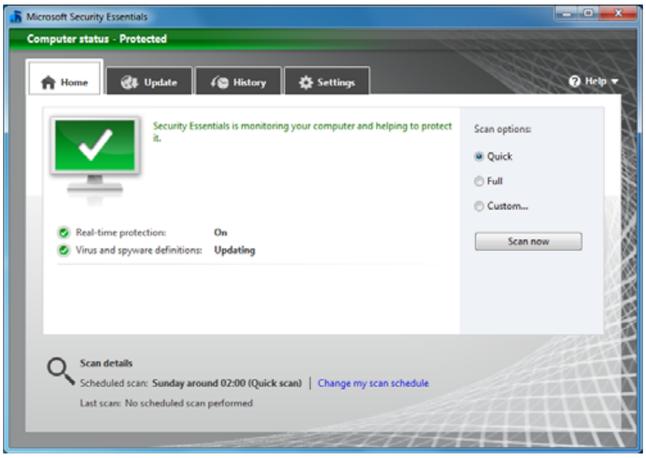
Virus protection On
Microsoft Security Essentials reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Microsoft Security Essentials reports that it is turned on.

There is no repair option in the uninstaller, only complete removal of the program.

Program Interface

The main program window of Microsoft Security Essentials 2.1 is dominated by the central status panel. This includes a computer icon and a line of text describing the security status. When all is well, the computer screen shows a tick (checkmark) on a green background, and the message reads "Security Essentials is monitoring your computer and helping to protect it". Additionally, a thin green strip along the very top of the window reads "Computer Status – Protected".



Computer status - Protected

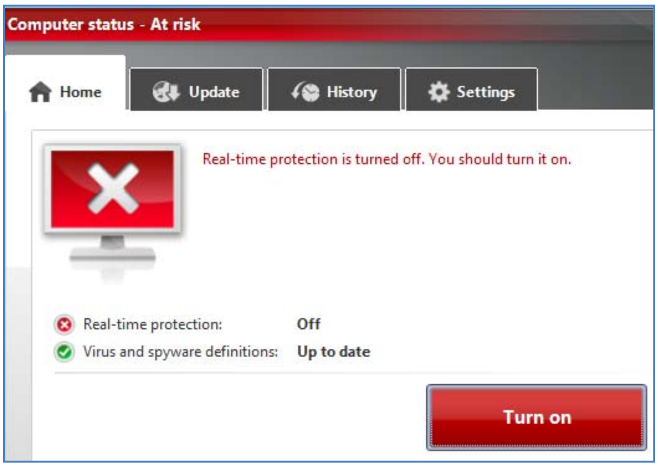
Security Essentials is monitoring your computer and helping to protect it.

Real-time protection: On
Virus and spyware definitions: Updating

Scan options:
● Quick
○ Full
○ Custom...

Scan details
Scheduled scan: Sunday around 02:00 (Quick scan) | Change my scan schedule
Last scan: No scheduled scan performed

When we switched off real-time protection, the text at the top of the window and in the status panel changed to show a warning, and the computer screen icon showed a cross on a red background. Additionally, a big button marked "Turn on" appeared in the bottom right-hand corner of the panel:



Real-time protection is turned off. You should turn it on.

Real-time protection: Off
Virus and spyware definitions: Up to date

Clicking the button restored real-time protection.

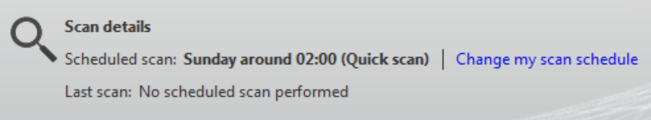
Above the status panel is a row of tabs: Home (status), Update, History (malware logs) and Settings. Finally, there is a Help menu in the top right-hand corner of the window.

When considering the user interface design, it must be noted that Microsoft Security Essentials is just an antivirus program, and so has fewer components to display than a full Internet security suite. However, we feel that it would be possible to neatly integrate items such as a firewall into the same basic interface, e.g. by adding an extra tab or two along the top of the window. Consequently, we don't think it unreasonable to compare MSE's interface design with that of Internet security suites. We found Microsoft Security Essentials to be particularly clear and simple to use, with important information and functions all very easily accessible.

Default configuration

Scanning and malware discovery

Microsoft Security Essentials displays the status of scheduled scanning, and a link to change it, clearly on the home page of the program window:



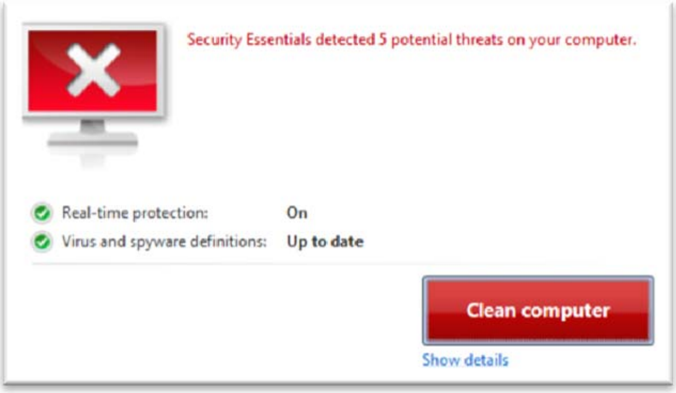
Scan details

Scheduled scan: Sunday around 02:00 (Quick scan)

Last scan: No scheduled scan performed

The scan shown in the picture, Sunday 02:00, is set by default. We could not find any means of running a boot-time scan.

When we ran a context-menu or custom scan on our folder of malware samples, MSE indicated that threats had been found, and displayed a big “Clean Computer” button:

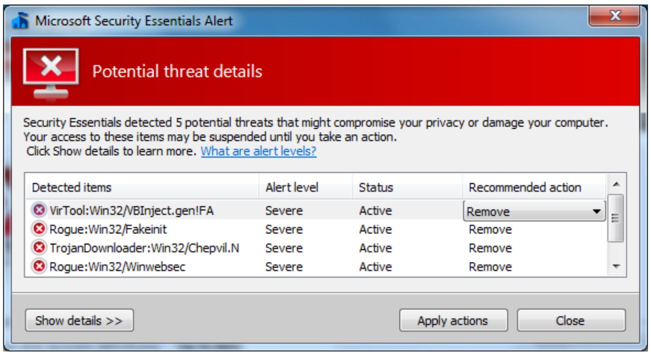


Security Essentials detected 5 potential threats on your computer.

Real-time protection: On

Virus and spyware definitions: Up to date

This then takes the default action (Remove). Clicking on the “Show Details” link below Clean Computer lets the user decide which action to take:

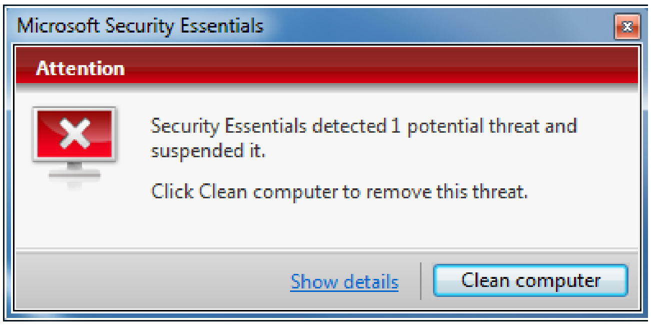


Security Essentials detected 5 potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action.
Click Show details to learn more. What are alert levels?

Detected items	Alert level	Status	Recommended action
VirTool:Win32/VBInject.gen!FA	Severe	Active	Remove
Rogue:Win32/Fakeinit	Severe	Active	Remove
TrojanDownloader:Win32/Chepvil.N	Severe	Active	Remove
Rogue:Win32/Winwebsec	Severe	Active	Remove

We feel this makes the program ideal for both non-experts (big, obvious “Clean Computer” removes malware without asking) and experts (smaller link gives options for the action to be taken with each item).

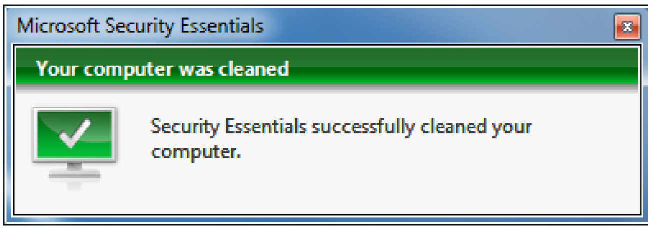
When we attempted to download the EICAR test file, MSE popped up the following dialog box:



Security Essentials detected 1 potential threat and suspended it.

Click Clean computer to remove this threat.

Clicking on “Clean Computer” then brought up a new message box:



Security Essentials successfully cleaned your computer.

This action makes it quite clear that the “threat” has been removed, and clicking “Show details” on the initial warning dialog box lets expert users decide on what to do with the file in question. However, some users might consider the process a little over-complicated for one single file.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to open the MSE window, but could not get the program to update. However, when we ran custom or context-menu scans on our folder of malware samples, MSE completed the scan and removed the malware exactly as in standard mode.

Help and Documentation

The local Help function very quickly provided clear answers to our queries on scheduling a scan, and settings scan exceptions. Searching the online help function quickly found an article on scheduling a scan, complete with Silverlight video, but nothing on scan exclusions.

Verdict

Overall

Microsoft Security Essentials may have relatively few functions, but it makes it easy to carry them out.

Outstanding points

Clear and simple user interface makes it very suitable for non-expert users.

Minor irritations

Online help could be improved.

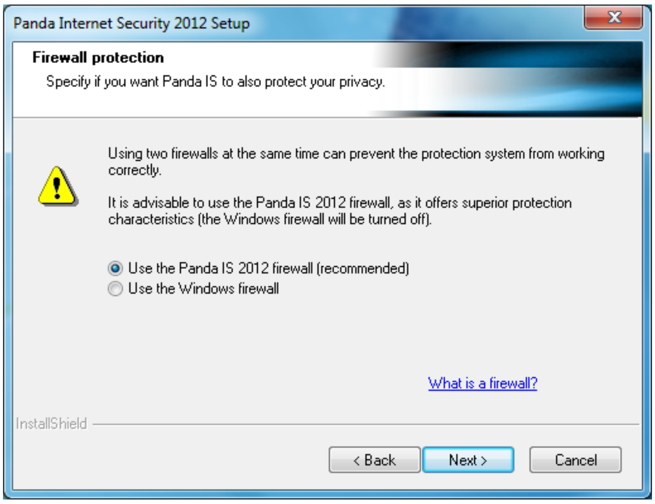
Panda Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall
- Parental Control
- Backup

Installation

We installed Panda Internet Security 2012 from a 73 MB .exe file. Steps include choosing a language (a one-time option), accepting the licence agreement, selecting the installation folder, choosing between typical and custom installation (we chose the latter), selecting the components to be installed, and deciding whether to send malware information to Panda. Two points impressed us in the setup process. Firstly, we were given the choice of using Windows Firewall or the Panda Firewall, with a link to information about what a firewall is:



Panda Internet Security 2012 Setup

Firewall protection

Specify if you want Panda IS to also protect your privacy.

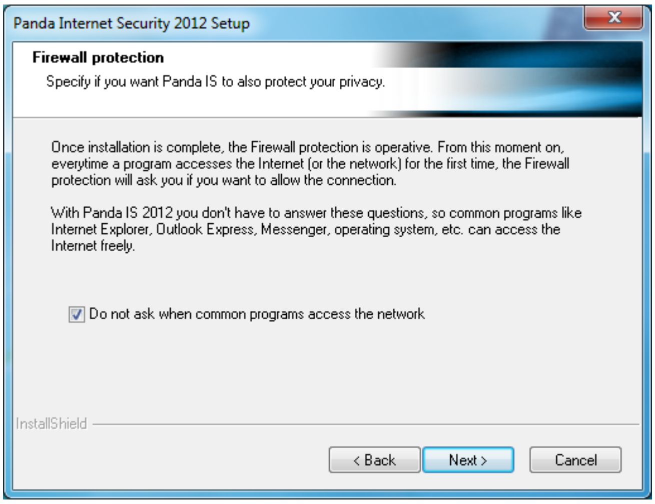
Using two firewalls at the same time can prevent the protection system from working correctly.

It is advisable to use the Panda IS 2012 firewall, as it offers superior protection characteristics (the Windows firewall will be turned off).

● Use the Panda IS 2012 firewall (recommended)
○ Use the Windows firewall

What is a firewall?

Secondly, there was an explanation of the outgoing firewall, and the chance to decide whether to allow common programs to access the Internet without query:



Panda Internet Security 2012 Setup

Firewall protection

Specify if you want Panda IS to also protect your privacy.

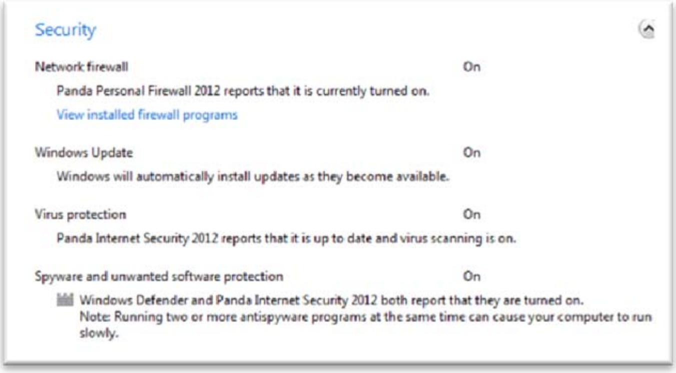
Once installation is complete, the Firewall protection is operative. From this moment on, everytime a program accesses the Internet (or the network) for the first time, the Firewall protection will ask you if you want to allow the connection.

With Panda IS 2012 you don't have to answer these questions, so common programs like Internet Explorer, Outlook Express, Messenger, operating system, etc. can access the Internet freely.

☑ Do not ask when common programs access the network

We felt that both of the above steps are valuable in educating computer users, and allowing them to make the right choice for themselves.

A reboot is required after setup finishes. Windows Action Center reported that Panda Internet Security had registered itself as an antivirus, antispyware and firewall program. Windows Firewall had been turned off (as indicated in Setup), Windows Defender had not.



Security

Network firewall On
Panda Personal Firewall 2012 reports that it is currently turned on.
View installed firewall programs

Windows Update On
Windows will automatically install updates as they become available.

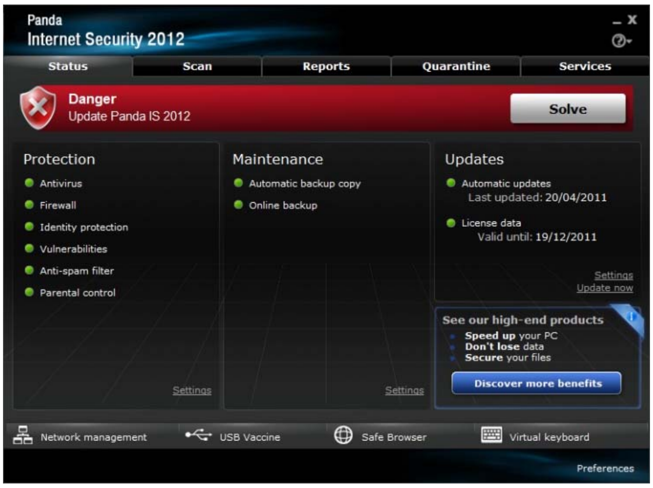
Virus protection On
Panda Internet Security 2012 reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender and Panda Internet Security 2012 both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

When we opened the program for the first time, we were given the choice of entering a licence key, or using the program as a trial. The uninstall program has no options other than complete removal (there is a separate entry in Programs and Features, namely Panda Secure Vault, which we assume is the backup service).

Program Interface

When we opened Panda Internet Security 2012 for the first time, we were greeted with an obvious warning, in the form of a big red strip across the top of the window, a shield with a cross, and the instruction “Update Panda IS 2012”:



Danger
Update Panda IS 2012

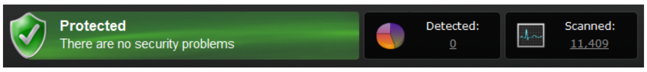
Antivirus
Firewall
Identity protection
Vulnerabilities
Anti-spam filter
Parental control

Automatic backup copy
Online backup

Automatic updates
Last updated: 20/04/2011
License data
Valid until: 19/12/2011

See our high-end products
Speed up your PC
Don't lose data
Secure your files

We clicked the prominent “Solve” button at the end of the strip, which caused the program to run an update. The status strip at the top of the program then turned to green, with the word “Protected”:



Protected
There are no security problems
Detected: 0
Scanned: 11,409

The right-hand end of the strip also includes graphical representations of the number of threats found and files scanned. The remainder of the program’s home page consists of three columns with status information: Protection, which lists the suite’s protective components; Maintenance, which shows backup components; and Updates, which shows update and licence information, and a rather small link entitled Update Now. A strip along the bottom of the program window contains buttons for various tools: Network Management, USB Vaccine, Safe Browser and Virtual Keyboard. Tabs along the top of the window allow Scan, Reports, Quarantine and Services (= Help and Tools) pages to be shown. The Scan tab has options for running a full, quick, custom or scheduled scan.

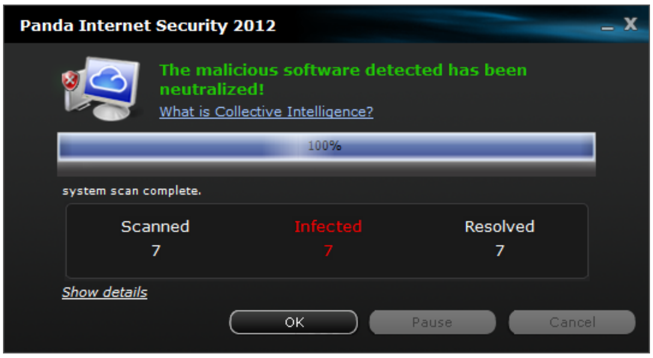
We found the layout of Panda Internet Security 2012 to be clear and straightforward, providing easy access to essential information and functions. We suspect that some people will find the white text on a black background somewhat uncomfortable to read, and would prefer an option to change to black text on white.

Default configuration

Scanning and malware discovery

A startup scan is scheduled to run every time the PC is started, but there is no scheduled full scan. This can be set up easily from the relevant link on the Scan page of the program. We could not find any means of running a boot-time scan.

Running a custom or context-menu scan on our folder of malware samples resulted in Panda Internet Security deleting all of the malicious programs without any user intervention being required:



Panda Internet Security 2012

The malicious software detected has been neutralized!

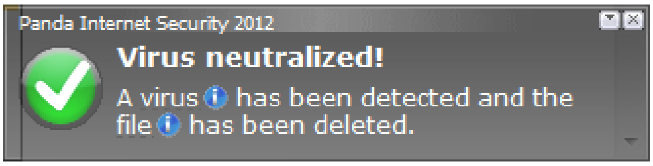
What is Collective Intelligence?

100%

system scan complete.

Scanned	Infected	Resolved
7	7	7

We noted that the suite reported connecting to the Panda server during the scan, and will warn before initiating an on-demand scan if the cloud connection is unavailable. When we attempted to download the EICAR test file, Panda blocked the download and displayed the following message box:



Panda Internet Security 2012

Virus neutralized!

A virus has been detected and the file has been deleted.

The message makes perfectly clear that the threat has been made safe, and that no further action is required.

Inbound Firewall Settings

After installing Panda Internet Security 2012, we were able to ping our test PC, and access its file share from another computer on the LAN, exactly as before installation.

Outbound Firewall/Application Control

In accordance with the choice we made during setup, i.e. to allow outgoing connections for safe programs without asking, Panda allowed our firewall testing program to access the Internet and download its test file without hindrance or query.

Spam protection

Anti-spam is enabled by default.

Parental Control

Parental control is shown as enabled by default, but an appropriate setting/age group has to be set for each user. We note that it is necessary to log on once as each user before the account will appear in the list of users in the Parental Control settings.

Safe Mode

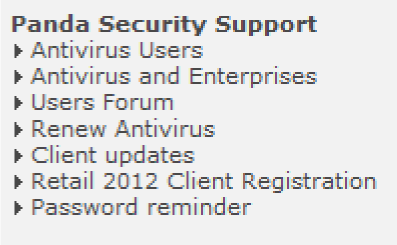
We were unable to run any sort of scan with Panda Internet Security 2012 in Safe Mode. Trying to run a context-menu scan brought up the Panda scan dialog box, but the progress bar would not go beyond 0%, and after a while the dialog box closed. All our malware samples remained intact.

Help and Documentation

We searched Panda's local help feature for information on scheduling a scan and setting scan exceptions. The first immediately found instruction for scheduling a scan, which were very clear and simple. The second query was more difficult, as the initial search term produced no relevant results. We then tried "scan exclusions", also without success; finally we tried "exclude", and this found concise instructions for settings scan exceptions.

Documentation in .pdf format available on the website is effectively limited to a brief installation guide, which would be ideal for assisting beginners with installation, but does not go beyond this.

Online help provides concise answers to a wide range of queries; we did consider that finding the right page was a little tricky. The list of support options on the website is shown below:



Panda Security Support

- Antivirus Users
- Antivirus and Enterprises
- Users Forum
- Renew Antivirus
- Client updates
- Retail 2012 Client Registration
- Password reminder

Clicking on "Antivirus Users" takes the user to a page where search queries for Internet Security 2012 can be made. We would suggest that labelling the link more clearly, e.g. "Panda home user products", might save some confusion.

Verdict

Overall

Panda Internet Security 2012 is very easy to install and use, but has a number of easily accessible advanced configuration options, making it user-friendly for both expert and non-expert users.

Plus points

Setup wizard gives choice of components to install, choice of using Panda or Windows firewall, choice of allowing outgoing program access without querying.

Minus points

Inability to run at all in Safe Mode. Parental Control shown as active before user accounts have been configured.

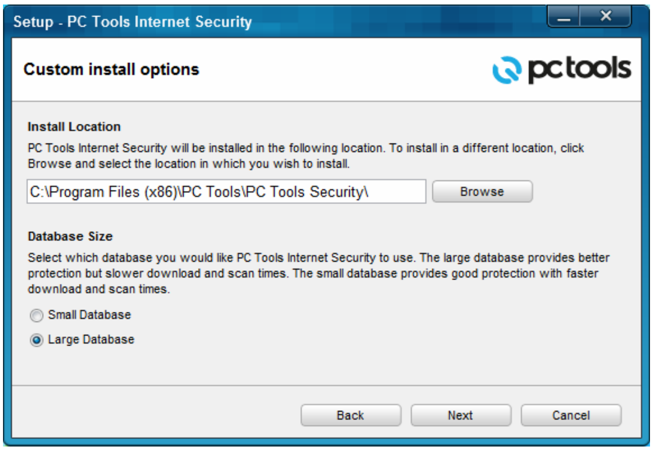
PC Tools Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall

Installation

We installed PC Tools Internet Security 2012 from 3.65 MB monolingual downloader file. Steps included accepting a licence agreement, entering a licence key or using in trial mode, choosing between Easy Install and Custom Install (we chose the latter), whether to use the PC Tools browser protection, selecting the installation folder, and a choice of large or small definition database size:



Custom install options

Install Location

PC Tools Internet Security will be installed in the following location. To install in a different location, click Browse and select the location in which you wish to install.

C:\Program Files (x86)\PC Tools\PC Tools Security\

Database Size

Select which database you would like PC Tools Internet Security to use. The large database provides better protection but slower download and scan times. The small database provides good protection with faster download and scan times.

○ Small Database

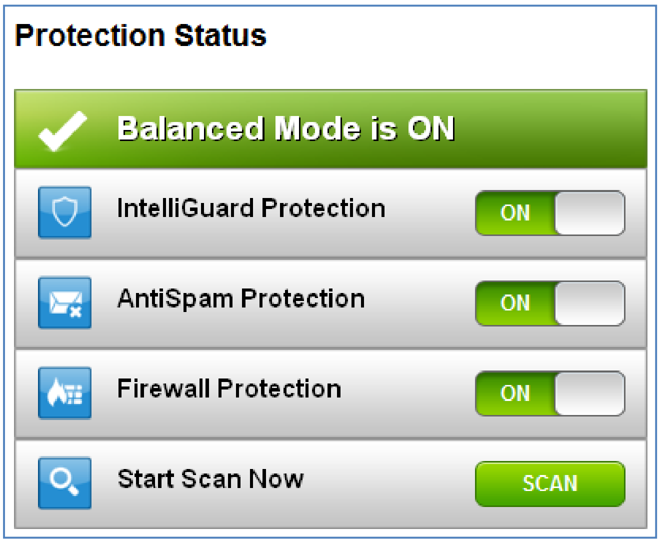
● Large Database

The wizard also asks whether to run a quick scan at the end of the installation, and whether the PC is connected to a trusted or untrusted network; we chose the former. Finally, setup asks whether Windows Defender should be disabled; we chose to do this. There is no choice of the components to be installed. A restart was required after the first update had been run.

Program Interface

The main program window of PC Tools Internet Security 2012 has a large right-hand pane and a slightly smaller left-hand pane, which displays information on threats, scans performed, update status and subscription information. 5 tabs along the top of the window allow the user to change between home (the default status page), IntelliGuard (real-time protection), Settings, Support Tools, and Start Scan Now. There is also a row of buttons along the bottom edge of the window: Report Card (report on recent threats encountered), My Account, Smart Update, and Help.

The large right-hand panel of the window is entitled Protection Status, and has on/off switches for IntelliGuard Protection (real-time protection), AntiSpam Protection, and Firewall Protection. Below these items is a fourth button marked Start Scan Now, and at the top is a strip showing the protection status. If all is well, this shows a tick and the words "Balanced Mode is ON" on a green background:



Protection Status

✓ Balanced Mode is ON

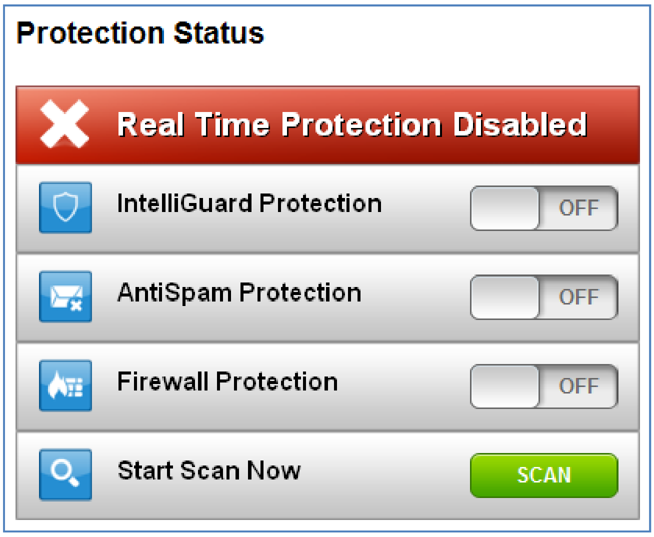
IntelliGuard Protection ON

AntiSpam Protection ON

Firewall Protection ON

Start Scan Now SCAN

In the event that **all 3** of the protection components are switched off, the status display will show a cross, and the words "Real Time Protection Disabled", on a red background:



Protection Status

✗ Real Time Protection Disabled

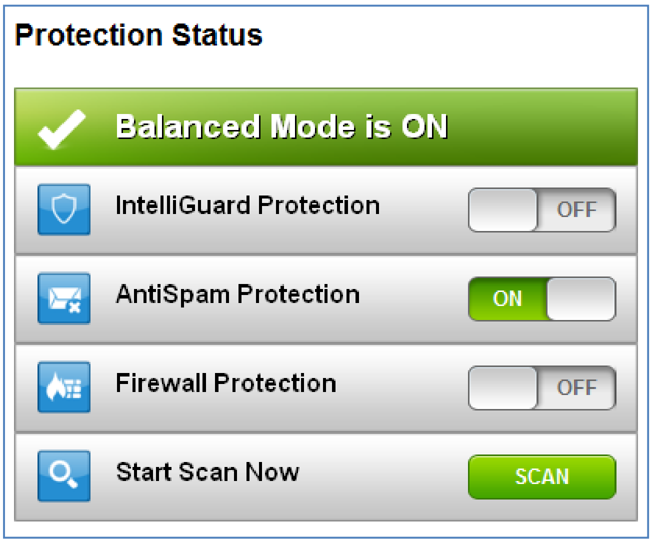
IntelliGuard Protection OFF

AntiSpam Protection OFF

Firewall Protection OFF

Start Scan Now SCAN

However, if the AntiSpam Protection is switched on, but the firewall and IntelliGuard is switched off, the status display will continue to show "Balanced Mode is ON" with a tick on a green background:



Protection Status

Balanced Mode is ON

IntelliGuard Protection OFF

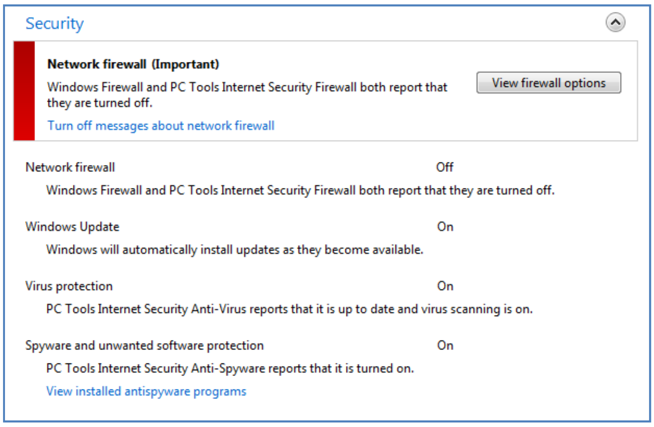
AntiSpam Protection ON

Firewall Protection OFF

Start Scan Now SCAN

In this condition, both real-time antivirus protection and the firewall are disabled; we tested the real-time protection by downloading the EICAR test file and unpacking our collection of malware from a zip file; we were able to complete both actions without any type of warning or hindrance from PC Tools.

We further note that when the real-time protection and firewall are switched off, Windows Action Center reports that the firewall has been switched off, but continues to show the antivirus and antispyware components as active:



Security

Network firewall (Important)

Windows Firewall and PC Tools Internet Security Firewall both report that they are turned off.

Turn off messages about network firewall

Network firewall Off

Windows Firewall and PC Tools Internet Security Firewall both report that they are turned off.

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

PC Tools Internet Security Anti-Virus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

PC Tools Internet Security Anti-Spyware reports that it is turned on.

View installed antispyware programs

Further experiments showed that switching off IntelliGuard (real-time protection) fails to change the “active” status of the antimalware components in Action Center, regardless of whether other components are activated or not. We found that this condition persisted after a restart.

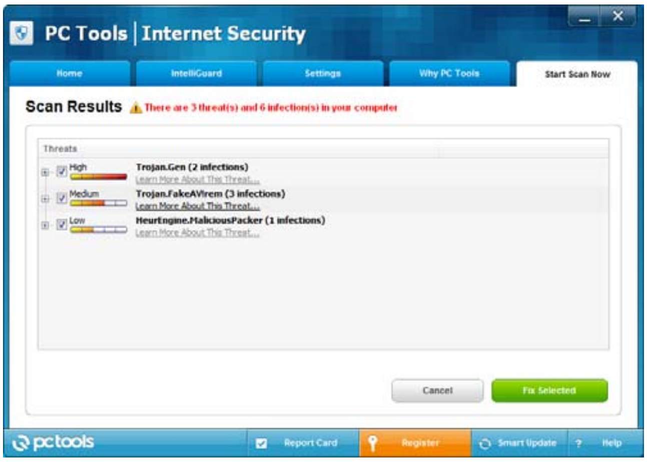
To summarise, PC Tools Internet Security 2012 will only actively warn of protection failure if all three components, including antispam, are switched off. Disabling the real-time antimalware protection, IntelliGuard, fails to produce any alert from Windows Action Center, which shows PC Tools reporting that all is well.

We can only describe the failure of PC Tools’ own warning mechanisms, combined with the inability to warn Windows Action Center about disabled real-time protection, as very alarming, and clearly below the minimum standard we would expect from a security suite intended for the general public.

Default configuration

Scanning and malware detection

A full scan is scheduled by default. It can easily be edited or deleted by going to Settings/Scheduled Tasks. We could not find any means of running a boot-time scan. When we ran a custom or context-menu scan on our folder of malware samples, PC Tools Internet Security showed the following page of scan results:

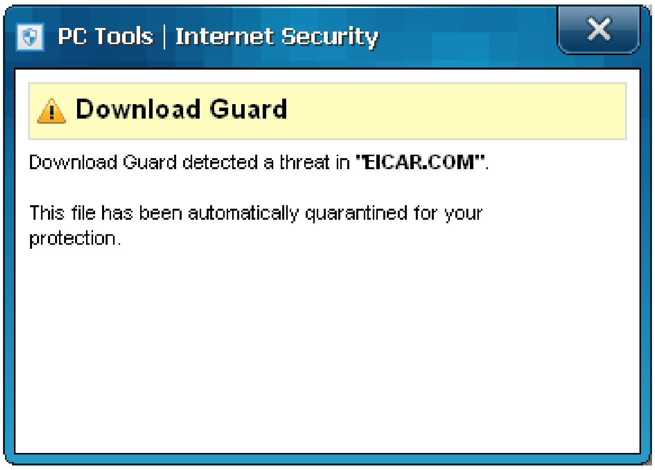


Scan Results ⚠ There are 3 threat(s) and 6 infection(s) in your computer

Threats	
☑ High	Trojan.Gen (2 infections) Learn More About This Threat...
☑ Medium	Trojan.FakeAVirem (3 infections) Learn More About This Threat...
☑ Low	HeurEngine.MaliciousPacker (1 infections) Learn More About This Threat...

Clicking "Fix Selected" removed all the malware samples.

When we attempted to download the EICAR test file, PC Tools blocked the download and showed the following message:



⚠ Download Guard

Download Guard detected a threat in "EICAR.COM".

This file has been automatically quarantined for your protection.

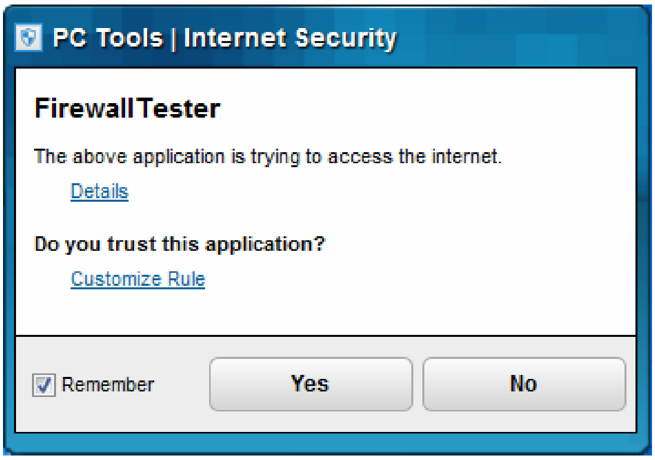
The message makes entirely clear that no further action is necessary.

Inbound Firewall Settings

During setup, we set the network type to Trusted. Having rebooted after installation, we attempted to ping our test PC and access its file share from another computer on the LAN. Whilst we were able to ping it with either IPv4 or IPv6, we were unable to access the file share at all at first. After setting the network to Untrusted and then back to Trusted, switching PC Tools' firewall off and then on again, and restarting the PC a few times, we were able to access the file share from another PC on the network.

Outbound Firewall/Application Control

When we ran our firewall testing program and attempted to download its test file, PC Tools Internet Security 2012 showed the following dialog box:



Firewall Tester

The above application is trying to access the internet.

Do you trust this application?

We were unable to find a setting which would disable queries about outgoing program access.

Spam protection

AntiSpam protection is enabled by default.

Safe Mode

When we started our test PC in Safe Mode, we noted that the PC Tools scan item had been removed from Windows Explorer's context menu. However, double-clicking the PC Tools Internet Security Icon brought up a message box asking if we wanted to enable PC Tools, to which we said "Yes". The program window then opened, and we were able to run an update successfully. The PC Tools entry re-appeared in Windows Explorer's context menu, so we were able to scan that way, or run a custom scan from the program window. Both ran and removed the malware exactly as they would have done in standard mode.

The ability to update in Safe Mode with Networking is very useful, but only found in very few antivirus programs.

Help and Documentation

The local Help function is listed as "Getting Started" in the Help menu, and contains just brief instructions for basic tasks. There is a search function, but we were unable to find answers to our questions on scan exclusions and scheduling a scan. Clicking on "Product Page" on the help menu takes the user to the sales information page; not very valuable to anyone who has already bought the program. However, clicking on the Support link at the top of the same page took us to the Resource Center page, where we were able to search for information on our two queries. Although we quickly found information on how to schedule a scan, this referred to the previous version, which has a very different interface, and so was of no help. Our search for information on scan exclusions produced no relevant answers at all. We can only describe the Help functions as disappointing.

Verdict

Overall

Although PC Tools Internet Security 2012 has in many ways been well designed, we feel that its major flaws, especially its failure to warn when real-time protection is disabled (either through its own window or in Windows Action Center), mean that we cannot recommend it in its current form.

Plus points

Simple installation; largely clear and simple interface makes it easy to use; ability to update (and scan) in Safe Mode with Networking.

Minus points

Failure to warn that real-time malware protection is disabled, either itself or via Windows Action Center; difficulty making file sharing work; poor Help functions.

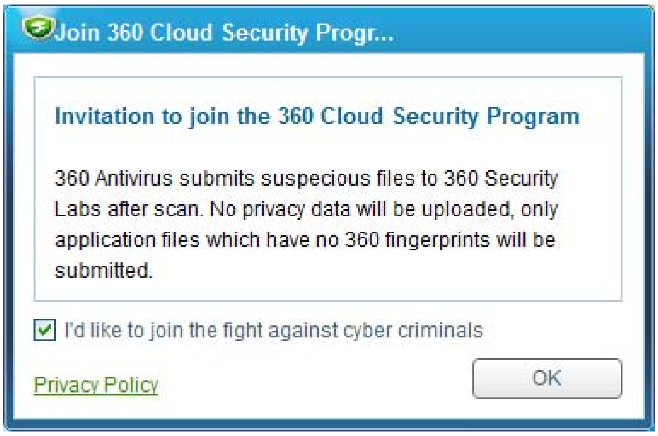
Qihoo 360 Antivirus

About the program

The program we have reviewed here is a simple antivirus program, which does not contain a firewall, antispam module or parental controls. Consequently we have omitted sections on firewall settings etc. from this report. For illustrational purposes we reviewed here the English version of Qihoo AV instead of the Chinese security suite. At this time the suite is only available in Chinese language.

Installation

We installed Qihoo 360 Antivirus from a 106 MB .exe file. We found the installation extremely simple. There is a licence agreement to accept, a choice of installation folder and Start Menu folder, but otherwise no options or custom mode. When the wizard has finished, a dialog box asks the user whether to anonymously submit malware information to the manufacturers:



Join 360 Cloud Security Progr...

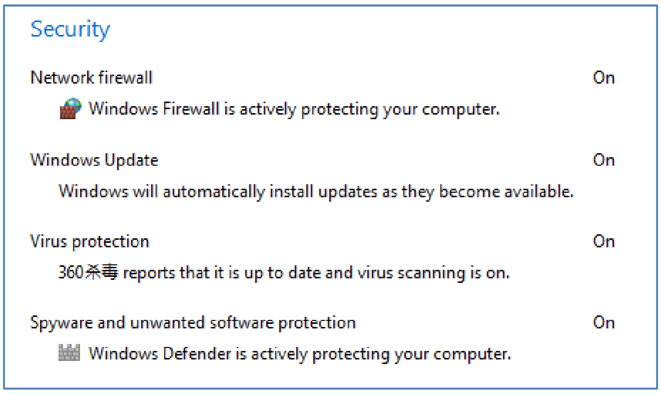
Invitation to join the 360 Cloud Security Program

360 Antivirus submits suspecious files to 360 Security Labs after scan. No privacy data will be uploaded, only application files which have no 360 fingerprints will be submitted.

☑ I'd like to join the fight against cyber criminals

A restart is not required after installation.

Qihoo 360 AV registers with Windows Action Center as an antivirus program, but not as an antispyware program. Consistently, Windows Defender is left running:



Security

Network firewall On
Windows Firewall is actively protecting your computer.

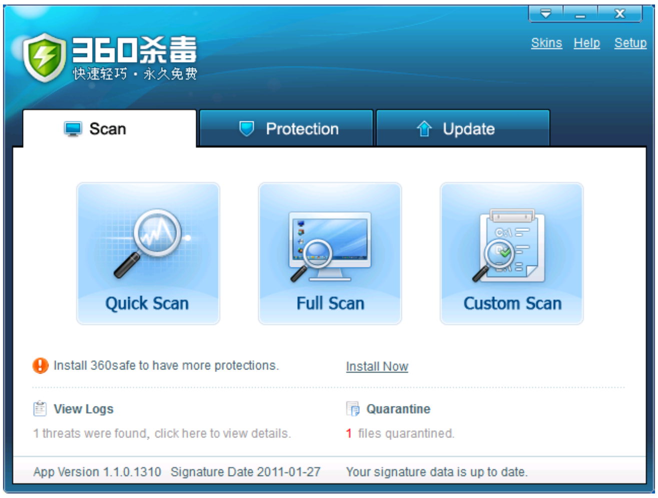
Windows Update On
Windows will automatically install updates as they become available.

Virus protection On
360杀毒 reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender is actively protecting your computer.

Program Interface

The main program window is dominated by a large display area in the lower three quarters of the window, which can be changed by clicking on tabs at the top of it: Scan, Protection and Update. By default, the program opens on the Scan tab, which shows three big buttons, namely Quick Scan, Full Scan, Custom Scan. There are also links to Logs and Quarantine:



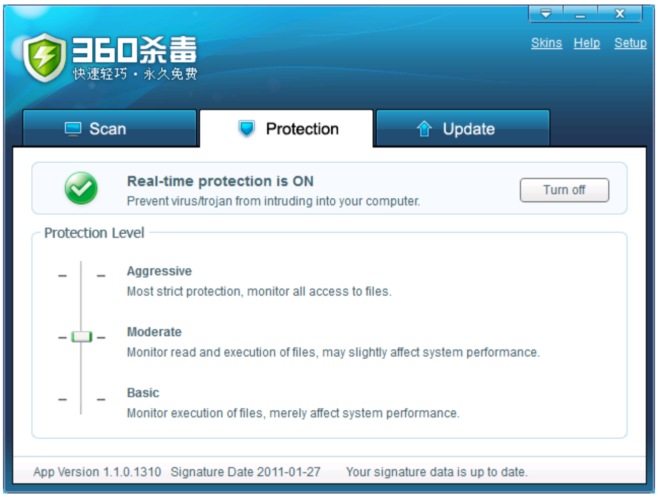
Install 360safe to have more protections. Install Now

View Logs
1 threats were found, click here to view details.

Quarantine
1 files quarantined.

App Version 1.1.0.1310 Signature Date 2011-01-27 Your signature data is up to date.

The Protection tab shows the status of real-time protection, with a button to switch this on or off, and a slider to control the compromise between protection and performance:



Real-time protection is ON
Prevent virus/trojan from intruding into your computer.

Protection Level

Aggressive
Most strict protection, monitor all access to files.

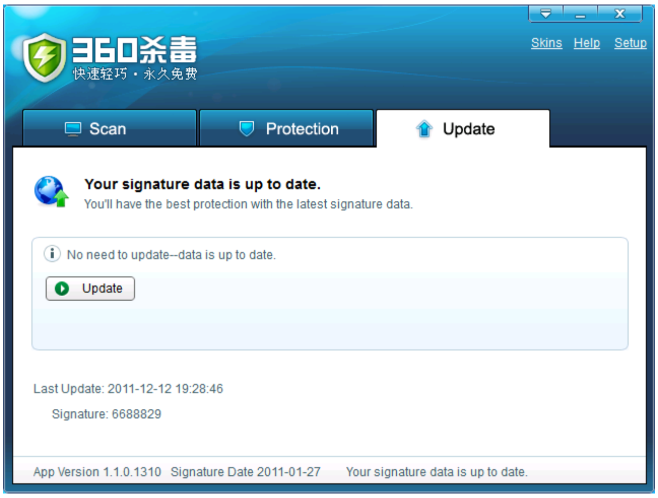
Moderate
Monitor read and execution of files, may slightly affect system performance.

Basic
Monitor execution of files, merely affect system performance.

App Version 1.1.0.1310 Signature Date 2011-01-27 Your signature data is up to date.

We would suggest that the description of Basic Protection is supposed to mean “minimal effect on system performance”.

The Update tab shows the database version of virus signatures, together with the date and time of the last update, and an Update button:



Your signature data is up to date.
You'll have the best protection with the latest signature data.

No need to update--data is up to date.

Last Update: 2011-12-12 19:28:46
Signature: 6688829

App Version 1.1.0.1310 Signature Date 2011-01-27 Your signature data is up to date.

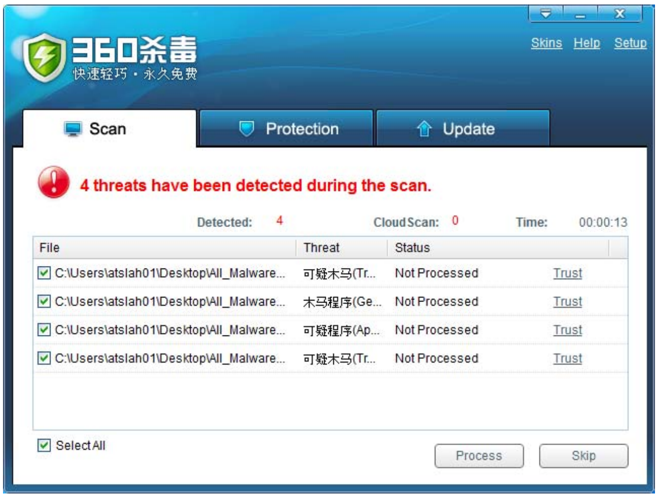
The program window also has links in the top right-hand corner of the window to Skins (allows the background image of window to be changed), Help (links to Qihoo webpage, in Chinese), and Setup, which opens the configuration options dialog box.

The interface is completed by a status bar along the bottom of the window, which shows the software version, date of last update, and an Update Now link.

Default configuration

Scanning

A scheduled scan is not configured by default, but can be set very easily from the General tab of the Settings dialog box. We could not find any means of running a boot-time scan. It is not possible to run a context-menu scan with the English version of Qihoo 360 AV, as the program does not add any entries to Windows Explorer's right-click menus. Running a custom scan on our folder of malware produced the following dialog box:



4 threats have been detected during the scan.

Detected: 4 CloudScan: 0 Time: 00:00:13

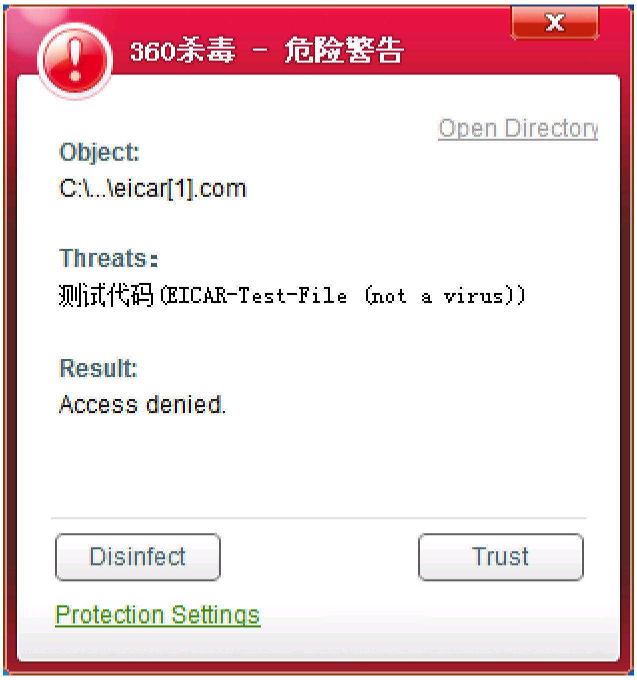
File	Threat	Status	
☑ C:\Users\atslah01\Desktop\All_Malware...	可疑木马(Tr...	Not Processed	Trust
☑ C:\Users\atslah01\Desktop\All_Malware...	木马程序(Ge...	Not Processed	Trust
☑ C:\Users\atslah01\Desktop\All_Malware...	可疑程序(Ap...	Not Processed	Trust
☑ C:\Users\atslah01\Desktop\All_Malware...	可疑木马(Tr...	Not Processed	Trust

☑ Select All

We were a little confused by the "Trust" links at the end of each line, assuming that this was the default action and that we needed to click on it to change this to e.g. "quarantine". In fact, the default action when the "Process" button is clicked is to delete the threats. The Trust link is a means of retaining an item listed in the scan results; clicking on it produces a dialog box which asks "Are you sure you want to trust this file"?

We noted that while the scan is running, there is an option available to automatically process any threats found when the scan is completed.

When we tried to download the EICAR test file, Qihoo 360 AV blocked the download and showed this warning dialog box:



360杀毒 – 危险警告

Object:
C:\...\eicar[1].com

Threats:
测试代码(EICAR-Test-File (not a virus))

Result:
Access denied.

The two options, Disinfect and Trust, are in our opinion perfectly clear. However, we feel it might be better to make the "Disinfect" button more obvious than the "Trust" button.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to open the Qihoo window, update and run a scan as normal. The scan found and removed our malware samples just as it would in standard mode.

Help and Documentation

The Help link in the main program window links directly to the Qihoo online help system in Chinese. In this system users can post product related questions.

Verdict

Overall

The tested Qihoo 360 Antivirus English version is so far not publicly available. As described above, we noticed minor differences with the Chinese version. We can confirm that Qihoo 360 AV is offering easy to use basic protection.

Plus points

Very simple interface makes essential features easy to find. Updates in Safe Mode with Networking.

Minus points

For international users, the discovery dialog box is slightly confusing malware.

Sophos Endpoint Security and Control 9.7

About the program

Sophos Endpoint Protection and Control is not a consumer Internet security suite, but rather a business endpoint protection program. It is designed to be installed, configured and maintained by a network administrator as part of a centrally managed security system. It is possible to make a stand-alone installation of the program on an individual PC, and both the antimalware and firewall components will work. However, we must stress that it is not designed or licensed for such use, and that it cannot be compared to home-user products. Any features or actions which do not comply with the standards we expect for consumer products should consequently not be regarded as failings.

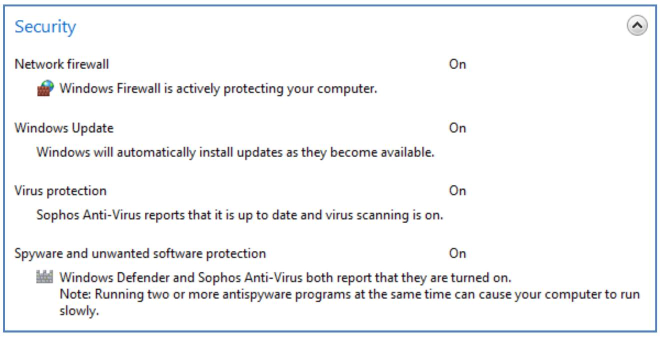
Components

- Antimalware
- Firewall

Installation

We installed Sophos Endpoint Security and Control from an 87 MB .exe file. Steps in the installation process are accepting the licence agreement, selecting the installation folder, entering update credentials (de facto licence key), choosing whether to install the Sophos Client Firewall, and choosing whether to automatically remove existing antivirus software.

Sophos registers with Windows Action Center as an antivirus, antispyware and firewall program. Windows Firewall is disabled, Windows Defender is not:



Security

Network firewall On
Windows Firewall is actively protecting your computer.

Windows Update On
Windows will automatically install updates as they become available.

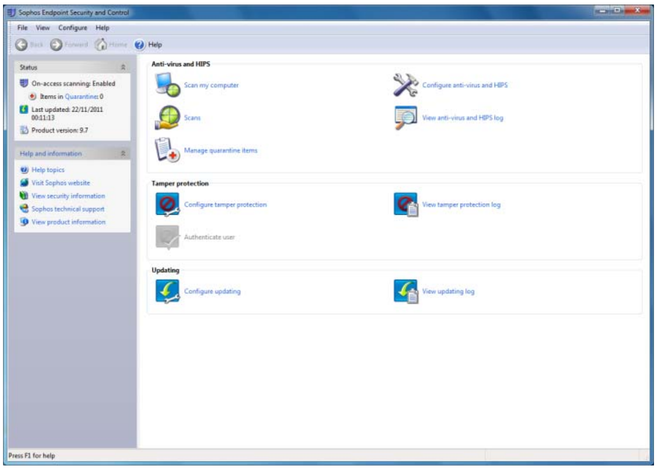
Virus protection On
Sophos Anti-Virus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender and Sophos Anti-Virus both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

There are 3 Sophos entries in Programs and Features: Sophos Anti-Virus, Sophos AutoUpdate, and Sophos Client Firewall. The only option for each of them is Uninstall.

Program Interface

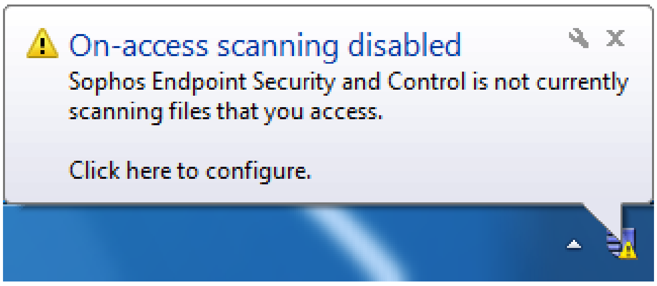
The main Sophos program window is very reminiscent of the default Control Panel window in Windows XP. There is a narrow left-hand pane with program information and links, and a much larger right-hand pane showing the individual protection components, tools and logs:



On-access scanning: Enabled
Items in Quarantine: 0
Last updated: 22/11/2011 00:11:13
Product version: 9.7

There is a toolbar with Home, Back, Forward and Help buttons, and a traditional menu bar.

There is no overall status display as such, although the top line of the left-hand pane shows whether real-time protection is enabled or disabled. Switching the protection off produces a warning message from the Sophos System Tray icon.



On-access scanning disabled

Sophos Endpoint Security and Control is not currently scanning files that you access.

Click here to configure.

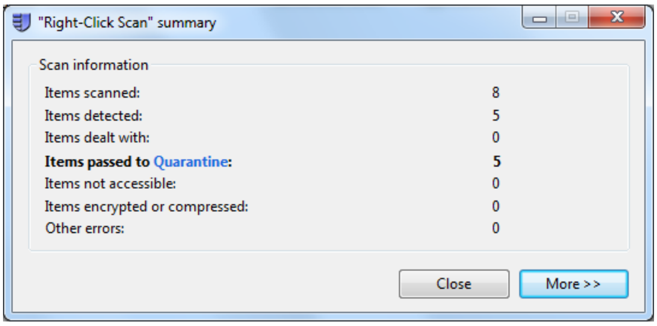
There is no update button as such in the program window, but right-clicking the System Tray icon produces a shortcut menu with an Update entry.

Default configuration

Scanning

There is no default scheduled scan, but this can easily be set up by clicking the “Scans” icon in the main pane of the window.

Running a context-menu scan on our folder of malware produced the following message box:

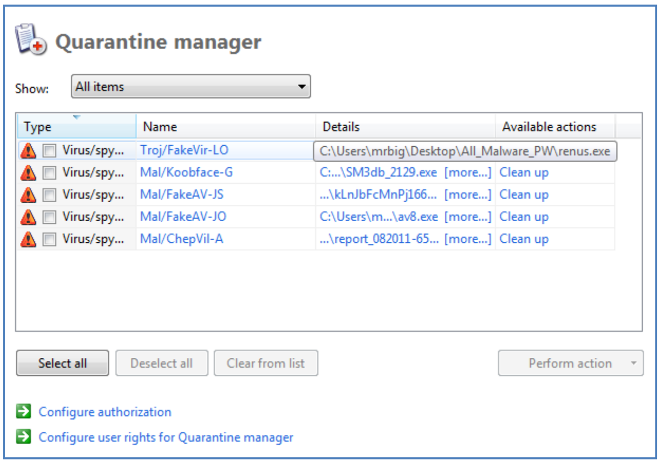


"Right-Click Scan" summary

Scan information

Items scanned:	8
Items detected:	5
Items dealt with:	0
Items passed to Quarantine:	**5**
Items not accessible:	0
Items encrypted or compressed:	0
Other errors:	0

We noted that none of the malware items in our folder had been deleted or changed in any way. We checked Sophos' Quarantine Manager, to see that the malicious programs had been listed; however, it is necessary to select an item and choose an action before anything is actually done:

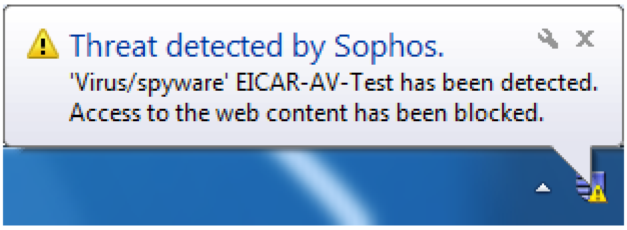


Quarantine manager

Show: All items

Type	Name	Details	Available actions
□ Virus/spy...	Troj/FakeVir-LO	C:\Users\mrbig\Desktop\All_Malware_PW\renus.exe	
□ Virus/spy...	Mal/Koobface-G	C:...\SM3db_2129.exe [more...]	Clean up
□ Virus/spy...	Mal/FakeAV-JS	...\kLnJbFcMnPj166... [more...]	Clean up
□ Virus/spy...	Mal/FakeAV-JO	C:\Users\m...\av8.exe [more...]	Clean up
□ Virus/spy...	Mal/ChepVil-A	...\report_082011-65... [more...]	Clean up

When we attempted to download the EICAR test file, Sophos blocked the download and displayed the following message:



Threat detected by Sophos.
'Virus/spyware' EICAR-AV-Test has been detected.
Access to the web content has been blocked.

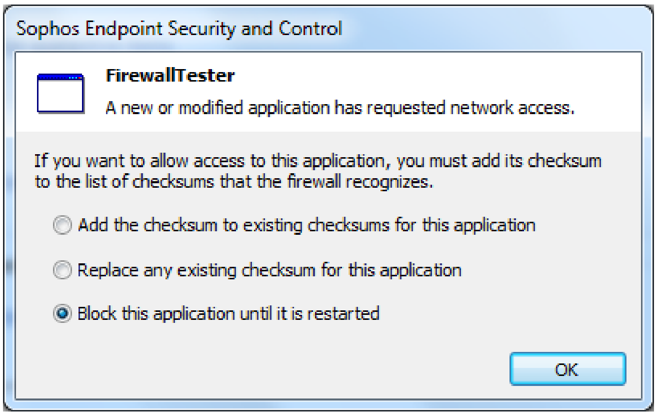
Inbound Firewall Settings

With the default firewall settings, Sophos blocked pings and file share access to our PC.

Outbound Firewall/Application Control

We noted that by default, Sophos' firewall blocked access from our test PC to the file server on the same network (configured as a workgroup, not a domain).

When we tried to open our firewall testing program, Sophos initially displayed the following dialog box:



Sophos Endpoint Security and Control

FirewallTester

A new or modified application has requested network access.

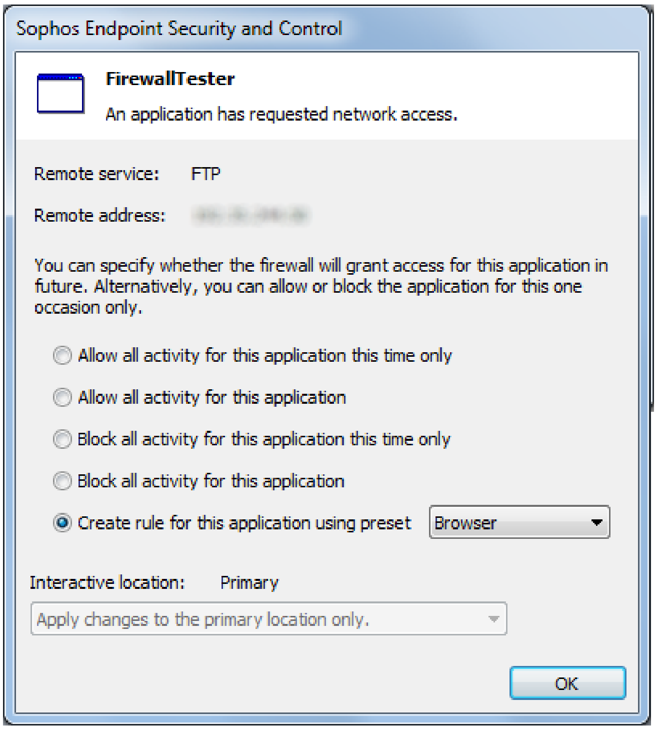
If you want to allow access to this application, you must add its checksum to the list of checksums that the firewall recognizes.

○ Add the checksum to existing checksums for this application

○ Replace any existing checksum for this application

● Block this application until it is restarted

We selected the middle option above, allowing the program to open. When we attempted to perform the download test, another dialog box appeared:



Sophos Endpoint Security and Control

FirewallTester

An application has requested network access.

Remote service: FTP

Remote address: [redacted]

You can specify whether the firewall will grant access for this application in future. Alternatively, you can allow or block the application for this one occasion only.

○ Allow all activity for this application this time only

○ Allow all activity for this application

○ Block all activity for this application this time only

○ Block all activity for this application

● Create rule for this application using preset Browser

Interactive location: Primary

Apply changes to the primary location only.

We selected the first of the options shown above, which allowed the firewall tester to complete its download.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to update Sophos' virus signatures. However, we were able to open the program window, and run custom and context-menu scans. These functioned exactly as in standard mode, marking the malware files for quarantine. We were then able to go into the Quarantine Manager and delete them from there, as normal.

Help and Documentation

Using the local help function we very quickly found clear, concise instructions on scheduling a scan and creating scan exclusions. There is a comprehensive online knowledge base; we easily found an answer to our query on setting scan exclusions, but not for scheduled scanning. The manuals we found were oriented towards overall system management rather than the client software in particular.

Verdict

Sophos Endpoint Protection and Control has a familiar interface layout, making important functions easy to find. It includes antimalware protection and an optional firewall, and the same basic features and functionality as a consumer antivirus program.

In some cases, such as the restrictive configuration of the firewall and the reaction on malware discovery, the default configuration for a stand-alone installation is clearly not suitable for a non-expert home user.

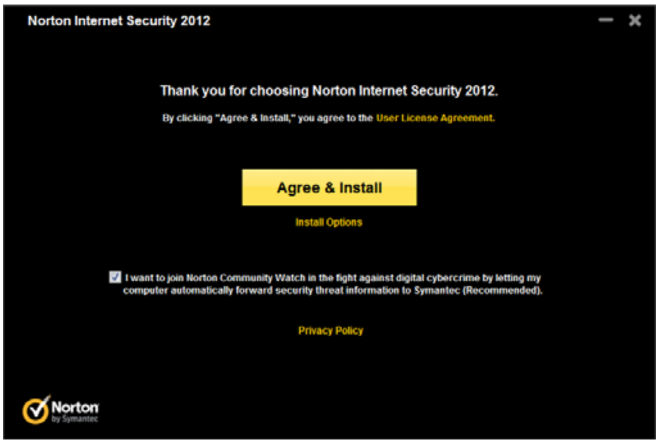
Symantec Norton Internet Security 2012

Components

- Antimalware
- Antispam
- Firewall
- Parental Controls
- Backup

Installation

We installed Norton Internet Security 2012 from a monolingual 104 MB .exe installer. The setup process is extremely simple; after double-clicking the setup file, the remainder of the installation could actually be completed with one click:



Norton Internet Security 2012

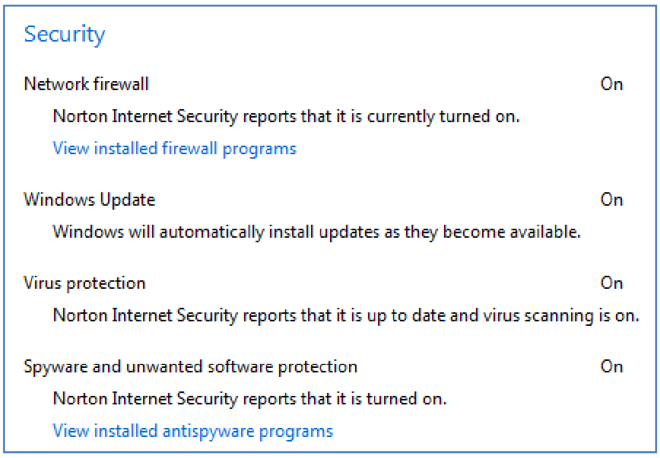
Thank you for choosing Norton Internet Security 2012.

By clicking "Agree & Install," you agree to the User License Agreement.

☑ I want to join Norton Community Watch in the fight against digital cybercrime by letting my computer automatically forward security threat information to Symantec (Recommended).

It is possible to opt out of Norton Community Watch (malware information sharing) and to change the installation folder (the only option available by clicking “Install Options”). There is no choice of components.

Setup then completes very quickly with no further interaction required. A reboot is not required. Norton Internet Security registers with Windows Action Center as an antivirus, antispyware and firewall program, and disables both Windows Firewall and Windows Defender:



Security

Network firewall On

Norton Internet Security reports that it is currently turned on.

View installed firewall programs

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

Norton Internet Security reports that it is up to date and virus scanning is on.

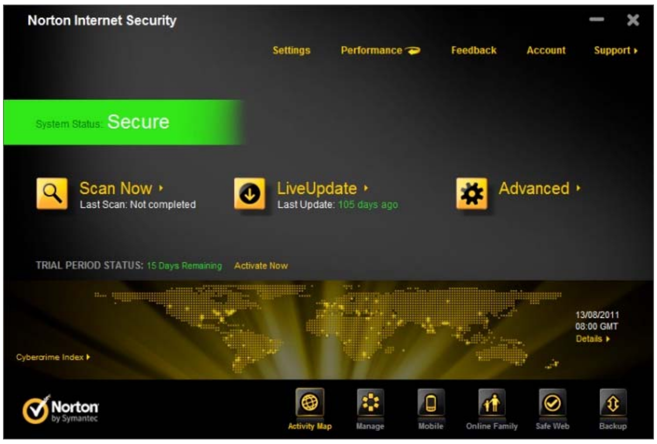
Spyware and unwanted software protection On

Norton Internet Security reports that it is turned on.

View installed antispyware programs

Program Interface

We feel it would be fair to describe the main program window of Norton Internet Security 2012 as quite complicated, in that there are numerous buttons and links displayed on the home page. However, the essentials are clearly displayed and easily accessible.



Norton Internet Security

System Status: Secure

Last Scan: Not completed

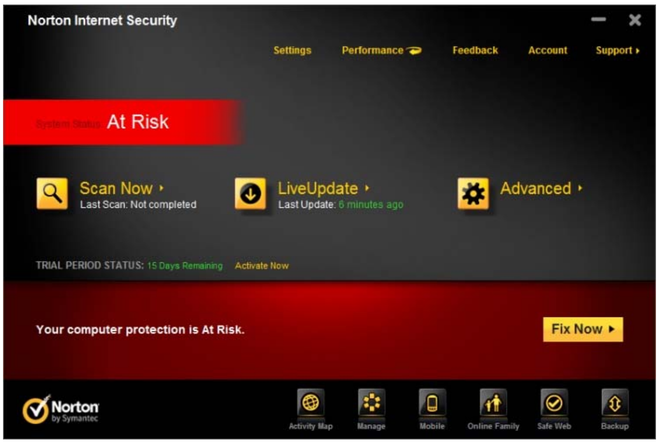
Last Update: 105 days ago

TRIAL PERIOD STATUS: 15 Days Remaining

13/08/2011
08:00 GMT

A horizontal strip in the middle of the window contains big buttons/links entitled Scan Now, Live Update, and Advanced (which shows the individual components in detail and allows them to be switched on and off).

A horizontal strip on the left-hand side of the window, towards the top, shows the protection status. If all is well, it will display “Secure” on a green background. However, when we turned off real-time protection, the strip turned red and displayed “At Risk”. Additionally, the display band at the bottom that normally shows the map changed to red, with the wording “Your computer protection is at risk”, and a very obvious “Fix Now” button:



Norton Internet Security

System Status: At Risk

Last Scan: Not completed

Last Update: 6 minutes ago

TRIAL PERIOD STATUS: 15 Days Remaining

Your computer protection is At Risk.

Clicking on Fix Now not only reactivates the real-time protection, but also runs a quick scan; we have to say that this is a sensible idea, and would be valuable in the event that a malicious program had managed to disable protection in order to proceed.

The row of buttons along the bottom of the window can be used to select the content of the broad strip just above them, which by default shows the Activity Map. Other options are Manage, Mobile, Online Family, Safe Web, and Backup.

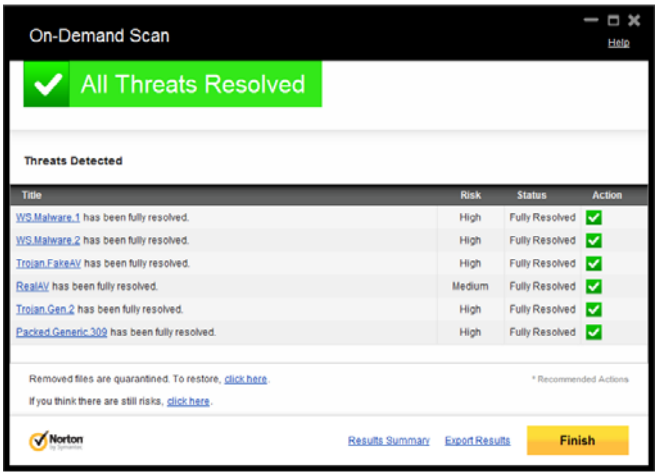
There are links along the top of the window, entitled Settings, Performance, Feedback, Account, and Support.

Default configuration

Scanning and malware discovery

A scheduled scan is configured by default; it can be edited by clicking Computer Scan, Custom Scan, Edit Scan. We found a means of enabling boot-time protection, but not an actual boot-time scan.

When we ran a custom or context-menu scan on our folder of malware, Norton Internet Security 2012 displayed the following information/dialog box:



On-Demand Scan

All Threats Resolved

Threats Detected

Title	Risk	Status	Action
WS.Malware.1 has been fully resolved.	High	Fully Resolved	✓
WS.Malware.2 has been fully resolved.	High	Fully Resolved	✓
Trojan.FakeAV has been fully resolved.	High	Fully Resolved	✓
RealAV has been fully resolved.	Medium	Fully Resolved	✓
Trojan.Gen.2 has been fully resolved.	High	Fully Resolved	✓
Packed.Generic.309 has been fully resolved.	High	Fully Resolved	✓

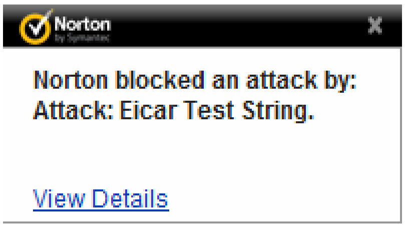
Removed files are quarantined. To restore, click here.

If you think there are still risks, click here.

* Recommended Actions

This showed clearly that all the threats had been made safe, and that no further action was necessary. All the items were quarantined, and there is a note (for advanced users) that they can be restored if necessary. We would argue that this action is optimal, for both expert and non-expert users.

When we attempted to download the EICAR test file, Norton blocked the download and displayed the following message box:



Norton blocked an attack by:
Attack: Eicar Test String.

This makes fairly clear that the threat has been stopped and that no further action is required; clicking on View Details confirms this, and gives expert users more information about the threat and its source. Again, we would describe the reaction and the information provided to be more or less ideal for users of all abilities.

Inbound Firewall Settings

After installing Norton Internet Security 2012, we were still able to ping the PC and access its file share from another computer on the LAN.

Outbound Firewall/Application Control

Our firewall tester was able to download its test file without hindrance or query. Symantec have informed that the firewall can be made to query outgoing programs, by turning off “Automatic Program Control” and enabling “Advanced Events Monitoring” in the Firewall settings. We must admit that we failed to find these settings ourselves when we looked.

Spam protection

AntiSpam is enabled by default. It can be configured by clicking Settings/Network/Message Protection.

Parental Control

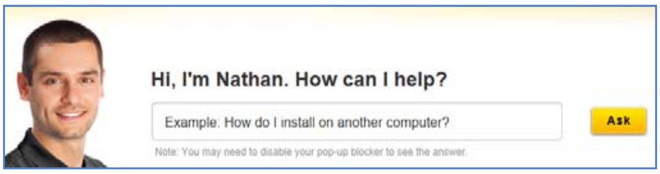
Online Family, Norton’s parental control feature, is not configured by default, and has to be installed by clicking on the Online Family icon and creating an account.

Safe Mode

When we started our test PC in Safe Mode with Networking and attempted to open the program, we were presented with a dialog box offering to run a full scan (which we declined). It is possible to run a context-menu scan as normal, and this found and removed our malware samples exactly as it did in standard mode.

Help and Documentation

Clicking on the Support link in the top right-hand corner of the window opens a browser window with Symantec's automated support agent:



Hi, I'm Nathan. How can I help?

Example: How do I install on another computer?

Note: You may need to disable your pop-up blocker to see the answer.

We typed in our first standard query: "How do I schedule a scan?". This opened up a new browser window with clear and precise instructions for scheduling a scan. We then tried our second query, "How do I exclude a folder from a scan", the service suggested exactly the same article about scheduling a scan (which doesn't mention exclusions at all). A very comprehensive manual for Norton Internet Security 2012 can be freely downloaded from the Symantec website. It is extremely detailed, being 504 pages long, well written, and has been very well indexed and bookmarked, making navigation very easy. Unfortunately, it appears not to have any screenshots at all; we feel this is a pity.

Verdict

Overall

Norton Internet Security 2012 has been well designed in most respects, and can be recommended for both expert and non-expert users.

Plus points

Very simple installation is ideal for non-expert users; action and information on malware discovery is ideal; quick scan runs when real-time protection is reactivated; comprehensive manual; good online help is available, but please see note below.

Minus points

The automated support agent, to which one's eye is naturally drawn first, is inferior to the simple "old-fashioned" search box at the top of the support page.

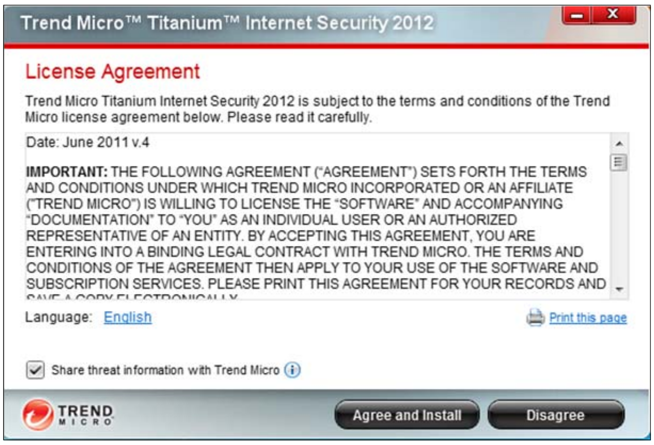
Trend Micro Titanium Internet Security 2012

Components

- Antimalware
- "Firewall Booster"
- Antispam
- Parental Controls

Installation

We installed Trend Micro Titanium Internet Security from a 2.34 MB downloader file. Full installation packages are also available. The installation process was very quick and simple once the software had been downloaded. There is a choice of entering a licence key or using a trial version, followed by an options page which combines accepting the licence agreement, choosing the language to be used, and the option of sharing threat information with Trend Micro:



Trend Micro™ Titanium™ Internet Security 2012

License Agreement

Trend Micro Titanium Internet Security 2012 is subject to the terms and conditions of the Trend Micro license agreement below. Please read it carefully.

Date: June 2011 v.4

IMPORTANT: THE FOLLOWING AGREEMENT ("AGREEMENT") SETS FORTH THE TERMS AND CONDITIONS UNDER WHICH TREND MICRO INCORPORATED OR AN AFFILIATE ("TREND MICRO") IS WILLING TO LICENSE THE "SOFTWARE" AND ACCOMPANYING "DOCUMENTATION" TO "YOU" AS AN INDIVIDUAL USER OR AN AUTHORIZED REPRESENTATIVE OF AN ENTITY. BY ACCEPTING THIS AGREEMENT, YOU ARE ENTERING INTO A BINDING LEGAL CONTRACT WITH TREND MICRO. THE TERMS AND CONDITIONS OF THE AGREEMENT THEN APPLY TO YOUR USE OF THE SOFTWARE AND SUBSCRIPTION SERVICES. PLEASE PRINT THIS AGREEMENT FOR YOUR RECORDS AND SAVE A COPY ELECTRONICALLY.

Language: English

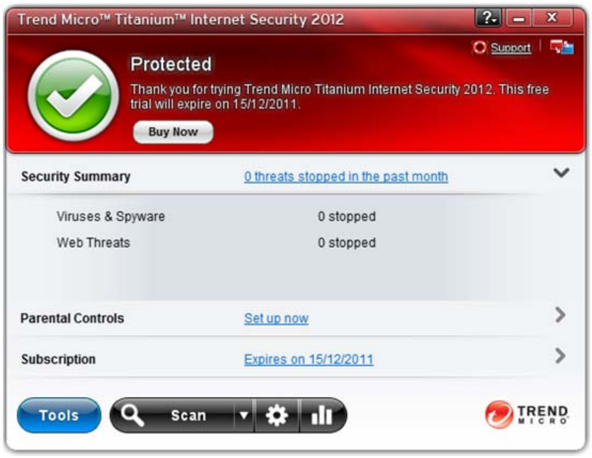
☑ Share threat information with Trend Micro

There is no custom installation as such, or choice of components. When the setup wizard has completed the installation, an email address is required, and then setup is complete and the main program window opens automatically. No reboot is needed.

Titanium Internet Security registers itself with Windows 7's Action Center as an antivirus and antispyware application, and disables Windows Defender. Unusually for an Internet Security Suite, Titanium does not have its own firewall, and so Windows Firewall remains active. Titanium does however contain a "Firewall Booster" which claims to enhance the Windows Firewall. Trend Micro's uninstall program has no options other than simple removal of the program.

Program Interface

Titanium Internet Security's program window stands out by being small, relative to most other programs in its class. A big horizontal strip along the top of the window provides a status display. When all is well, this is a tick in a big green circle, and the word "Protected". In the case of the trial version, it also includes subscription expiry information:



Protected

Thank you for trying Trend Micro Titanium Internet Security 2012. This free trial will expire on 15/12/2011.

Security Summary 0 threats stopped in the past month

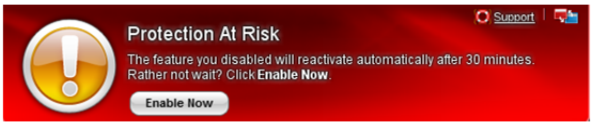
Viruses & Spyware 0 stopped

Web Threats 0 stopped

Parental Controls Set up now

Subscription Expires on 15/12/2011

In the event of a problem, such as real-time protection being disabled, the status button changes to yellow with an exclamation mark, and the wording "Protection At Risk":



Protection At Risk

The feature you disabled will reactivate automatically after 30 minutes. Rather not wait? Click **Enable Now**.

The real-time protection can be reactivated by clicking the Enable Now button.

The middle section of the window consists of three parallel strips marked Security Summary, Parental Controls, and Subscription. Clicking on the arrow at the end of each strip shows the details for that item. Security Summary, the default selection, shows the number of threats stopped. There is a link on the Parental Controls strip entitled "Set up now"; this makes clear that the feature has not been activated, and that parents who wish to use it must configure it first. The subscription strip shows the licence expiry date.

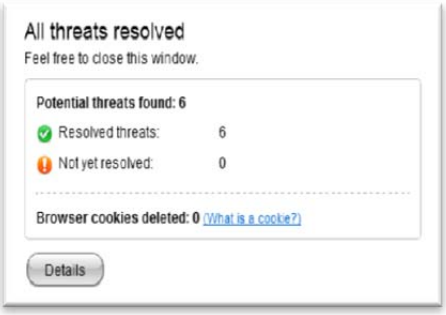
At the bottom of the window is a row of buttons. Tools, to the left, has options for configuring Parental Controls and Data Theft Protection. To the right of this is one long button divided into 3 sections: Scan, the main part of which starts a full scan, with a drop-down arrow for other options such as Quick and Custom Scans; a cogwheel, which opens the program settings dialog box; and a graph, which opens the security reports box. Conspicuous by its absence is an update button; Trend Micro even advertise that the product doesn't have one, as it uses cloud-based protection rather than local signatures. The program interface is completed by Help and Support links in the top right-hand corner of the window.

Default configuration

Scanning and malware discovery

By default, Titanium runs a Quick Scan every Friday lunchtime at 12:00. This can very easily be changed to a Full Scan or another day or time in the program's settings. We could not find any way of running a boot-time scan. However, System Startup settings allow the user to choose whether to load the security software fully, partially or not at all during booting, offering different compromises of boot time and security.

Running a custom or context-menu scan on our folder of malware samples produced the following Trend Micro dialog box, showing "All threats resolved":



All threats resolved

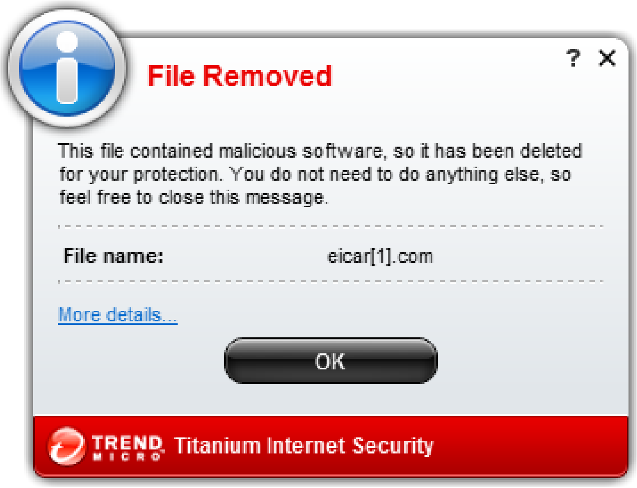
Feel free to close this window.

Potential threats found: 6

✓ Resolved threats:	6
! Not yet resolved:	0

Browser cookies deleted: 0 (What is a cookie?)

When we tried to download the EICAR test file, Titanium Internet Security blocked the download and displayed an extremely clear message, indicating that no further action was necessary:



File Removed

This file contained malicious software, so it has been deleted for your protection. You do not need to do anything else, so feel free to close this message.

File name: eicar[1].com

Firewall Settings

As mentioned, Trend Micro Titanium Internet Security 2012 does not have its own firewall, just a "Firewall Booster" which adds protection to Windows Firewall. We activated this feature, rebooted the test computer, and then tried our standard incoming and outgoing tests. The results were exactly as would be expected with the Windows Firewall configuration that we had set up before installing Titanium Internet Security: file sharing and pinging from another PC on the network worked normally, and our firewall testing program was able to complete its test without restriction or query. We should point out that we do not consider that the absence of its own firewall makes Trend Micro's suite in any way inferior. Microsoft's Windows Firewall is integrated into the system and easy to configure; many advanced users protect their computers with a simple antivirus program and rely on Windows Firewall rather than that of a third party.

Spam protection

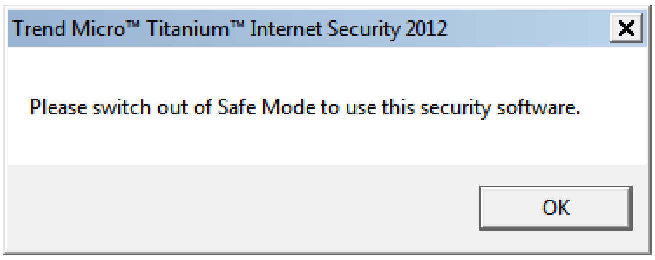
Spam protection is not enabled by default, but is very easy to switch on; there is just a single box to tick, no other configuration is possible.

Parental Control

Parental Controls are, as mentioned above, not enabled by default – the main program window makes this clear – but can be configured very easily by clicking on the appropriate link.

Safe Mode

We were unable to start Trend Micro Titanium Internet Security in Safe Mode; the following message appeared:



Trend Micro™ Titanium™ Internet Security 2012

Please switch out of Safe Mode to use this security software.

Help and Documentation

There is no manual available for the suite, as far as we could see. We could not find any local help system in the program; both the Help and Support links lead to pages of the Trend Micro website. The Support link requires a region and product to be selected, and then goes to a page with a few FAQs and a search box marked “Knowledge Base”. Both our searches, for help with scheduling a scan and setting scan exceptions, turned up the same 5 completely irrelevant answers; clicking on “Show All” extends the list of irrelevant answers to 20. A promising-looking link on the same page, entitled “Step by Step Video Guides” simply links back to the same page. In short, we found the Support link to be more or less useless.

The Help link goes to a completely different page, also with a search box. Searching for help on scheduling a scan found two articles, one of which was exactly what we wanted. Instructions were brief, but quite adequate, given how simple the procedure is. Unfortunately, our search for setting scan exceptions produced no results at all. However, we noticed that the list of help articles on the left-hand side of the page included “Exception Lists”, and this was precisely what we were looking for. We find it strange that the search was unable to find it.

Verdict

Overall

Trend Micro Titanium Internet Security 2012 has a very simple interface and is in many ways an ideal program for non-experts.

Plus points

Simple, uncluttered interface. Very easy to install and use.

Minus points

Program will not run in Safe Mode. Access to online help is confused by useless Support link and inadequate indexing of the articles found by clicking the Help link.

TrustPort Internet Security 2012

Components

- Antimalware
- Firewall
- Antispam
- Parental Control

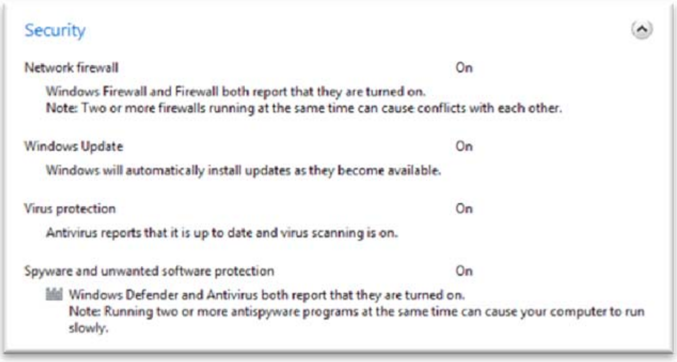
Note about the program

TrustPort Internet Security uses two third-party antivirus engines. By default these are used together for all functions, but can be disabled or enabled separately for specific functions (real-time protection, on-demand scans).

Installation

We installed TrustPort Internet Security 2012 from a 253 MB .exe file. The steps in setup are: choosing a language, accepting the licence agreement, accepting a warning about uninstalling any existing antivirus software, and choosing the installation folder. There is no custom installation option or choice of components. A restart is required. After restarting, the program has to be activated by entering a key, or opting for a trial.

Windows Action Center shows that TrustPort has registered itself as a firewall, antivirus program and antispyware program, although anonymously in all cases: the components are shown simply as "Firewall" and "Antivirus":



Security

Network firewall On

Windows Firewall and Firewall both report that they are turned on.
Note: Two or more firewalls running at the same time can cause conflicts with each other.

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

Antivirus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

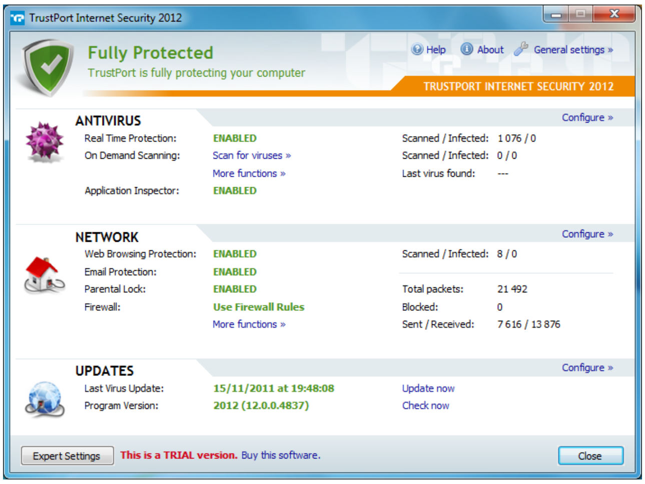
Windows Defender and Antivirus both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

We note that neither Windows Defender nor Windows Firewall was disabled by TrustPort, although Microsoft clearly recommends disabling Windows Firewall if another software firewall is used on the same computer.

The uninstall program has no options other than complete removal.

Program Interface

The main program window of TrustPort Internet Security 2012 is made up of a number of horizontal strips. The top strip is a status display, which displays a tick (checkmark) in a green shield, and the words “Fully Protected”, if all is well:



Fully Protected
TrustPort is fully protecting your computer

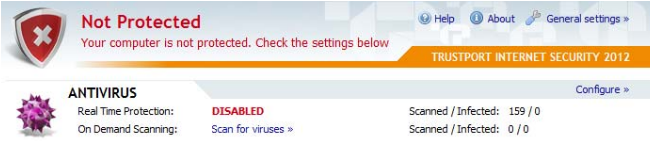
ANTIVIRUS
Real Time Protection: ENABLED
On Demand Scanning: Scan for viruses »
More functions »
Application Inspector: ENABLED
Scanned / Infected: 1 076 / 0
Scanned / Infected: 0 / 0
Last virus found: ---

NETWORK
Web Browsing Protection: ENABLED
Email Protection: ENABLED
Parental Lock: ENABLED
Firewall: Use Firewall Rules
More functions »
Scanned / Infected: 8 / 0
Total packets: 21 492
Blocked: 0
Sent / Received: 7 616 / 13 876

UPDATES
Last Virus Update: 15/11/2011 at 19:48:08
Program Version: 2012 (12.0.0.4837)
Update now
Check now

This is a TRIAL version. Buy this software.

If there is a problem, the status display at the top changes to Not Protected, with the advice to check the settings below. The problem area, in this case real-time virus protection, is shown in red text; clicking on this re-enables the protection.



Not Protected
Your computer is not protected. Check the settings below

ANTIVIRUS
Real Time Protection: DISABLED
On Demand Scanning: Scan for viruses »
Scanned / Infected: 159 / 0
Scanned / Infected: 0 / 0

At the right-hand end of this strip are the links Help, About, and General Settings, the latter allowing a licence to be registered and the interface language to be changed.

The Antivirus strip below this shows status and controls for the antivirus component, with links to enable/disable real-time protection and application control, various scan options (including full and custom), and tools such as quarantine and boot CD creation.

The Network section in the centre of the window allows Web Protection, Email Protection, Firewall and Parental Lock (parental controls) to be enabled/configured.

The Updates section below this shows details of virus signatures and the program version, with a link to run an update. Each of the main strips, Antivirus, Network and Updates, has a link entitled “Configure” to set more detailed options. An Expert Settings button in the bottom left-hand corner of the window allows advanced configuration changes to be made.

Although the number of lines of information and links may make it seem a little cluttered, we found that TrustPort Internet Security window actually made all the essential information and tasks quite easy to access.

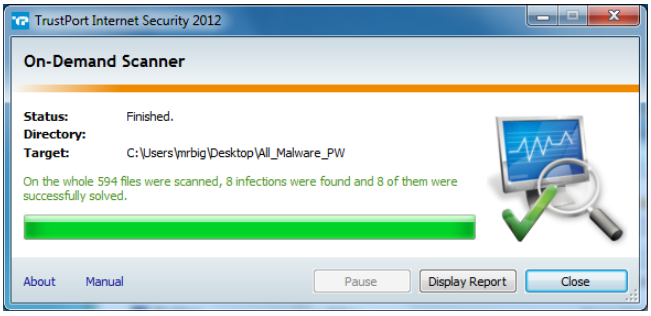
Default configuration

Scanning and malware discovery

A scheduled scan is not set up by default, but can be configured by going into Expert Settings/Antivirus/Scheduler. Whilst this should present no problem for experienced users, we felt the process might be a little challenging for non-experts.

We could not find any means of running a boot-time scan.

When we ran a context-menu or custom scan of our malware folder, TrustPort Internet Security informed us that “8 infections were found and 8 of them were successfully solved”:



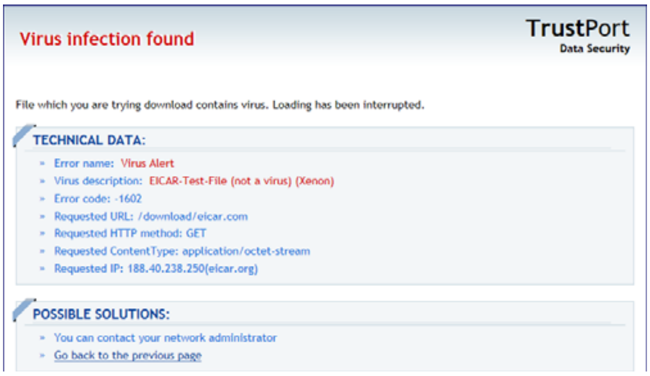
On-Demand Scanner

Status: Finished.
Directory:
Target: C:\Users\mrbig\Desktop\All_Malware_PW

On the whole 594 files were scanned, 8 infections were found and 8 of them were successfully solved.

We were a little surprised to see that rather than deleting or quarantining the malware samples, TrustPort had simply changed the .exe file endings to .0xe. Whilst this means that they can no longer be accidentally run by double-clicking them, it does not otherwise disable them (changing the file extension back renders each program fully operative again). We also feel this may be very confusing for non-expert users, and suggest that quarantining the malware programs would be safer and less worrying.

When we attempted to download the EICAR test file, TrustPort blocked the download and the web page, showing the following message in the browser window:



Virus infection found

File which you are trying download contains virus. Loading has been interrupted.

TECHNICAL DATA:

- Error name: Virus Alert
- Virus description: EICAR-Test-File (not a virus) (Xenon)
- Error code: -1602
- Requested URL: /download/eicar.com
- Requested HTTP method: GET
- Requested ContentType: application/octet-stream
- Requested IP: 188.40.238.250(eicar.org)

POSSIBLE SOLUTIONS:

- You can contact your network administrator
- Go back to the previous page

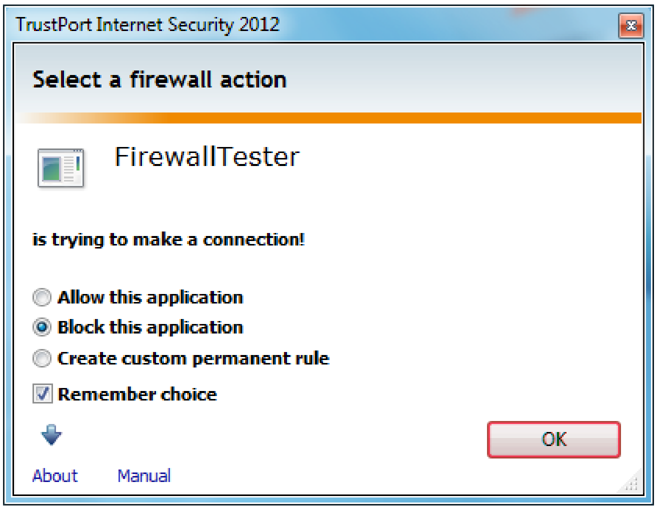
Although this will be clear enough to advanced users, we wonder whether non-expert users might find the message a little overwhelming.

Inbound Firewall Settings

TrustPort's default firewall settings for our PC continued to allow file sharing, and we were able to open, edit and save a Word document on it from another PC on the same LAN. Curiously, we were not able to ping our test PC after installing TrustPort Internet Security.

Outbound Firewall/Application Control

In the default firewall mode, "Use Firewall Rules", we were prompted twice when we tried to run our firewall tester; once on opening the program, and once when attempting to download the test file:



TrustPort Internet Security 2012

Select a firewall action

FirewallTester

is trying to make a connection!

○ Allow this application
● Block this application
○ Create custom permanent rule
☑ Remember choice

Changing the firewall setting to "Enable Outgoing Connections" allowed the firewall tester to run and download without prompting.

Spam protection

Spam protection is switched on by default. It marks suspected spam mails by adding ***SPAM**** to the subject line.

Parental Control

Parental Lock (parental control) is shown as being active by default. However, checking the advanced settings shows that the only category blocked is "Malware/Phishing", which we would expect an Internet security suite to do anyway. We would suggest that TrustPort might make clearer to users that Parental Lock needs to be configured before it can really be regarded as operational.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to get TrustPort Internet Security to update. However, we were able to run a scan on our malware folder, with exactly the same result as in standard mode: all the malware programs were identified, and the file extensions changed from .exe to .0xe.

Help and Documentation

TrustPort Internet Security appears to have no local help function, as clicking on the Help link in the program window goes directly to a page of the TrustPort website. This provides an overview of the main elements of the GUI, with abundant screenshots. The link at the bottom of the page opens a page with three further links, Graphical User Interface (the page we have just come from), TrustPort Antivirus, and TrustPort Personal Firewall. This may be confusing to non-experts, as each of these pages covers a component of the Internet Security suite as if it were a separate stand-alone application. If you can get over this hurdle, the information on each page is perfectly relevant; it is essentially an online manual, in HTML format rather than .pdf. This is comprehensive, and individual pages are easily accessible from the clearly laid-out index page. Instructions are clear and simple, and there are abundant screenshots. Our only complaint was that we could not find any sort of search feature to ask questions with.

Verdict

Overall

TrustPort Internet Security 2012 is essentially an effective program with a clear and intuitive interface, although there are a number of quirks which we feel could be improved.

Plus points

Simple program interface provides easy access to essential features and information. Good online manual.

Minus points

Default firewall/application control mode not ideal for non-experts; treatment of discovered malware is rather confusing; parental control is shown as active when effectively it is not.

Webroot SecureAnywhere Essentials 2012

Note about the program

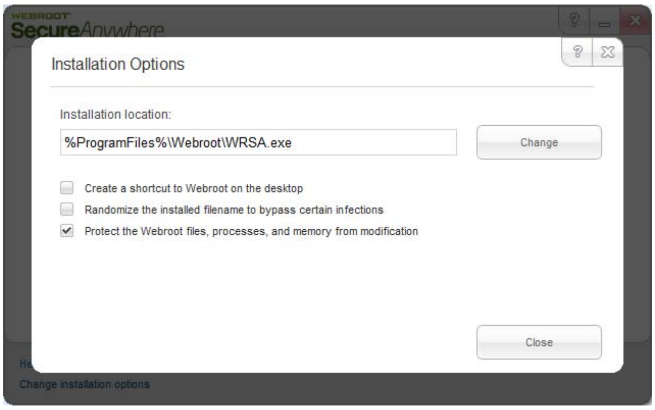
The program version described here is very new, and uses a completely different engine from the older version that was used in most of our tests. It is very possible that Webroot's results in future tests will improve as a result of the new engine.

Components

- Antimalware
- Firewall
- Backup
- Identity Shield

Installation

We installed Webroot SecureAnywhere 2012 from a 591 KB downloader file; a full installer is available, which includes language options. Installation is very quick and simple; the standard procedure just involves entering a licence key and clicking "Agree and Install". Custom options are available by clicking "Change Installation Options"; this allows the installation folder to be changed, plus a couple of other minor options:



Installation Options

Installation location:

%ProgramFiles%\Webroot\WRSA.exe

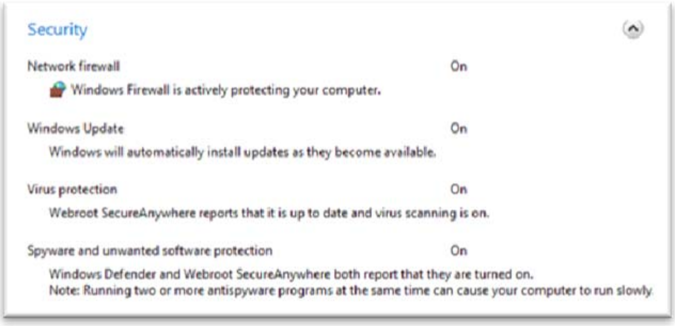
□ Create a shortcut to Webroot on the desktop

□ Randomize the installed filename to bypass certain infections

☑ Protect the Webroot files, processes, and memory from modification

There is no choice of languages or components to be installed. A reboot was not required after installation.

When we looked in Windows Action Center, we noted that Webroot SecureAnywhere had registered itself as an antivirus and antispyware application. Windows Defender had not been disabled. We were surprised to see that SecureAnywhere had not registered as a firewall; Action Center informed that Windows Firewall was active, and made no mention of any other firewall programs:



Security

Network firewall On
Windows Firewall is actively protecting your computer.

Windows Update On
Windows will automatically install updates as they become available.

Virus protection On
Webroot SecureAnywhere reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender and Webroot SecureAnywhere both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

This report remained unchanged even after rebooting the PC, and checking in SecureAnywhere's settings that the Webroot firewall was switched on.

Webroot explained this situation to us as follows:

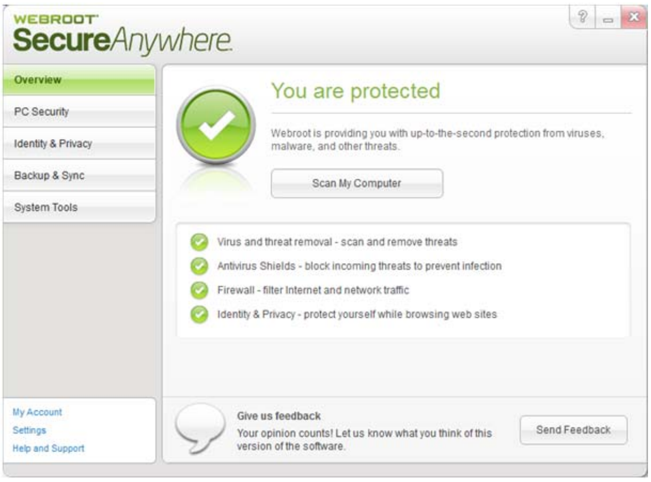
"Webroot doesn't integrate into the Security Center under the firewall because its firewall can work alongside an existing firewall if the user has one, and the presence of another firewall causes many applications to throw warnings. We've taken this unique approach to encourage layered security. Webroot doesn't use an incompatible firewall hook driver or other technologies within the OS which have a limitation of a single registered hook, and it's been designed to be as light as possible to allow it to work alongside other third party firewalls and the Windows firewall."

We feel it would be valuable if Webroot could make users aware of this, e.g. in the setup wizard, as many users might be alarmed to see that the Webroot firewall had not registered in Action Center, and assume that it was not working.

Webroot's uninstaller program has no options other than complete removal of the suite.

Program Interface

SecureAnywhere's main program window uses a familiar format, consisting of a narrow left-hand pane with menu items (Overview, PC Security, Identity and Privacy, Backup & Sync, System Tools), and a much wider right-hand pane displaying the details of each menu item. The default Overview page is a status display. If all is well, it displays a tick/checkmark in a green circle, with the wording "You are protected". The button below it is labelled "Scan My Computer", and runs a quick scan:



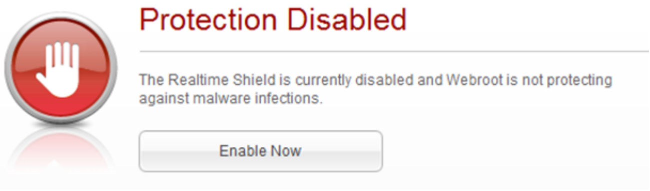
You are protected

Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

✓ Virus and threat removal - scan and remove threats
✓ Antivirus Shields - block incoming threats to prevent infection
✓ Firewall - filter Internet and network traffic
✓ Identity & Privacy - protect yourself while browsing web sites

Give us feedback
Your opinion counts! Let us know what you think of this version of the software.

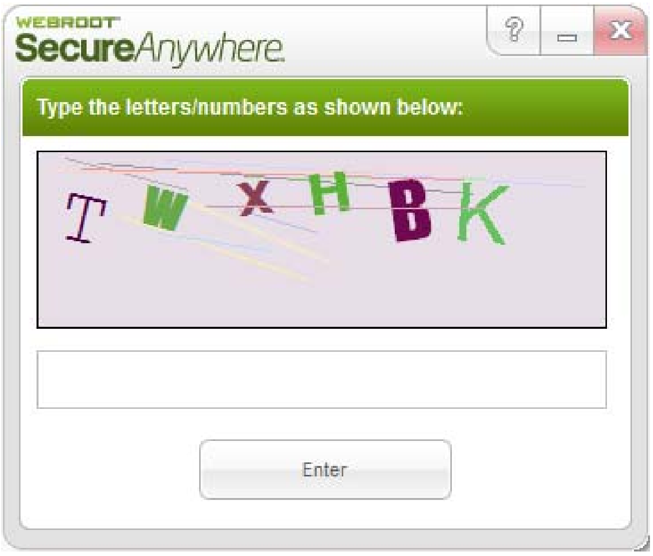
In the event that a component is disabled, this changes to a hand in a red circle, with the words “Protection disabled”:



Protection Disabled

The Realtime Shield is currently disabled and Webroot is not protecting against malware infections.

The big button now reads “Enable Now”, and allows the component to be reactivated with a single click. When disabling the real-time protection in order to test this feature, we noticed that Webroot protected this setting with a CAPTCHA screen:



Type the letters/numbers as shown below:

This feature can be turned off in the program’s settings, although we recognise that it may help to prevent malware disabling the protection. We were a little surprised to find that switching the protection back on also entails negotiating a CAPTCHA screen.

We note that there is no signature update function to be found anywhere in the suite, and Webroot’s advertising claims that it “never needs to be updated”; this is because it uses cloud-based signatures. There is an automatic software update process.

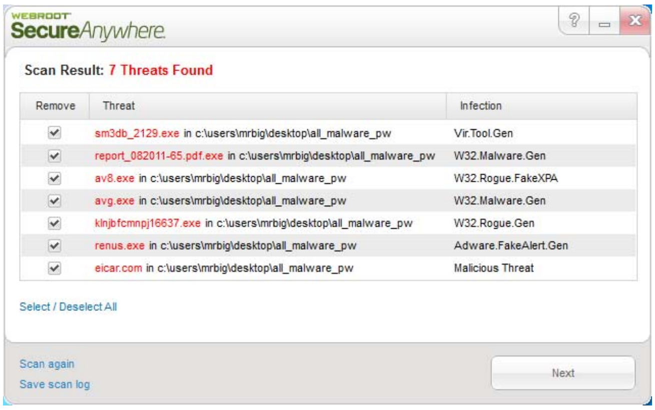
The PC Security button in the menu column has options for configuring and running a scan, including custom and scheduled scans.

Default configuration

Scanning and malware discovery

A scheduled scan is set by default, every day at 5pm “when resources are available”. A default option is “Scan on bootup if the computer is off at the scheduled time”. The scheduled scan and other scan options can easily be changed from PC Security/Scan.

Running a custom or context-menu scan of our malware folder produced the following dialog from Webroot:

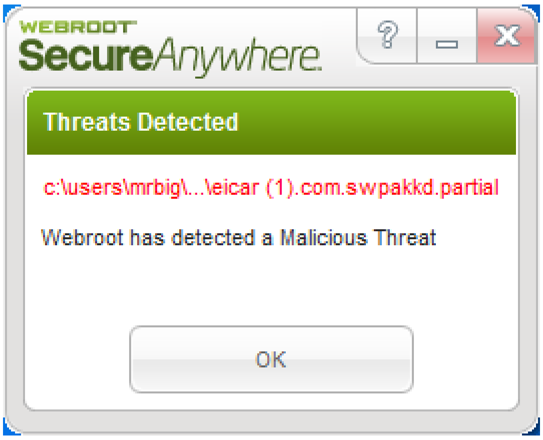


Scan Result: 7 Threats Found

Remove	Threat	Infection
☑	sm3db_2129.exe in c:\users\mrbig\desktop\all_malware_pw	Vir.Tool.Gen
☑	report_082011-65.pdf.exe in c:\users\mrbig\desktop\all_malware_pw	W32.Malware.Gen
☑	av8.exe in c:\users\mrbig\desktop\all_malware_pw	W32.Rogue.FakeXPA
☑	avg.exe in c:\users\mrbig\desktop\all_malware_pw	W32.Malware.Gen
☑	klnjbfcmnpj16637.exe in c:\users\mrbig\desktop\all_malware_pw	W32.Rogue.Gen
☑	renus.exe in c:\users\mrbig\desktop\all_malware_pw	Adware.FakeAlert.Gen
☑	eicar.com in c:\users\mrbig\desktop\all_malware_pw	Malicious Threat

Clicking Next removes the malware. We were a little bit confused by the final message box; although this confirms that all 7 threats have been removed, it also lists “Files scanned: 1” and “Total scans: 6”.

When we attempted to download the EICAR test file, we saw the following warning message from Webroot:



Threats Detected

c:\users\mrbig\...\eicar (1).com.swpakkd.partial

Webroot has detected a Malicious Threat

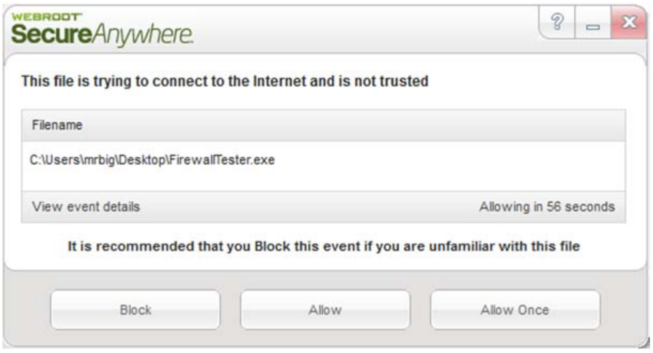
Whilst the file was deleted, the message box merely says “Webroot has detected a malicious threat”; there is nothing to indicate that it has been deleted or quarantined, and we feel this could be worrying for non-expert users. Webroot tell us that their program will run a background scan in this situation, to ensure that there is no infection.

Inbound Firewall Settings

After the installation of Webroot SecureAnywhere, we were able to ping our test PC, and access its file share, in accordance with the settings made before installing.

Outbound Firewall/Application Control

Our firewall testing program ran and downloaded its test file without any interference or queries from Webroot. Changing the firewall settings to "Warn if any new, untrusted process connects to the Internet" produces the following dialog when the firewall tester tries to download its test file:



This file is trying to connect to the Internet and is not trusted

Filename

C:\Users\mrbig\Desktop\FirewallTester.exe

View event details

Allowing in 56 seconds

It is recommended that you Block this event if you are unfamiliar with this file

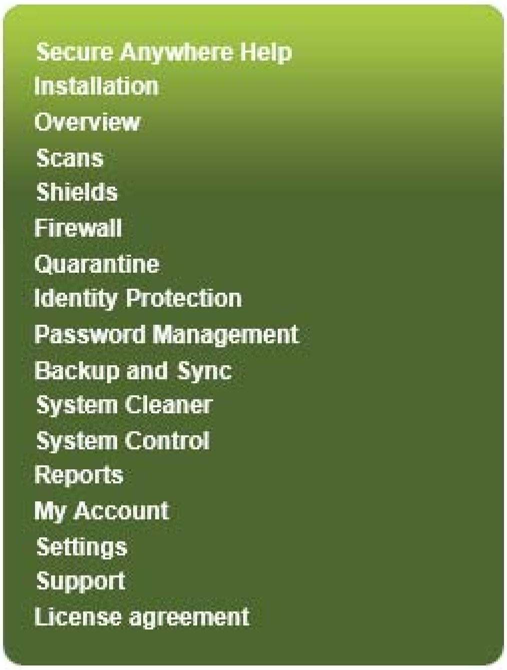
Safe Mode

We were very pleasantly surprised to discover that when we started our test PC in Safe Mode with Networking, Webroot SecureAnywhere was fully functional, including real-time protection. It scanned our folder of malware, detected and removed the threats exactly as it had done in standard mode. Moreover, simply right-clicking one of the malware files and clicking "Properties" was sufficient for Webroot's real-time protection to detect and delete the malware. Very few antivirus programs operate fully in Safe Mode, and Webroot must be given credit for making one that does.

Help and Documentation

There does not appear to be any local help function for Webroot SecureAnywhere, as clicking on either "Help and Support" or "?" in the program window open a page of Webroot's online support website. The Help and Support link opens a page with a search box, which we used for our sample searches on scheduled scanning and setting scan exceptions. The first query went straight to a clear, simple, well-illustrated page of instructions on setting a scheduled scan; the second unfortunately turned up no relevant results.

The "?" link took us to a web page best described as an online manual in HTML format. The page has a menu in the top left-hand corner with a list of components and tasks; many of these have their own submenus:



Secure Anywhere Help
Installation
Overview
Scans
Shields
Firewall
Quarantine
Identity Protection
Password Management
Backup and Sync
System Cleaner
System Control
Reports
My Account
Settings
Support
License agreement

The manual appears to be comprehensive, clearly written, and very well illustrated with screenshots.

Verdict

Overall

Webroot SecureAnywhere Essentials 2012 is straightforward to install and use and could be used by beginners or expert users.

Plus points

Very clear, simple program interface; fully functional in Safe Mode, both scanning and real-time protection; critical settings can be CAPTCHA protected.

Minus points

Some confusion over the firewall (as reported in Action Center); misleading message when malware is downloaded from the Internet.

Copyright and Disclaimer

AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss which might occur as a result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

Translation: David Lahee

AV-Comparatives e.V. (January 2011)