Anti-Virus Comparative

Summary Report 2015

Awards, winners, comments

Language: English
December 2015

Last Revision: 30th December 2015

www.av-comparatives.org

Table of Contents

Introduction

About AV-Comparatives

We are an independent test lab, providing rigorous testing of security software products. We were founded in 2004 and are based in Innsbruck, Austria.

AV-Comparatives is an **ISO 9001** certified organisation. We received the certificate of TÜV Austria for our management system for the scope: "Independent Tests of Anti-Virus Software".

http://www.av-comparatives.org/iso-certification/

AV-Comparatives is the first **certified EICAR Trusted IT-Security Lab**
http://www.av-comparatives.org/eicar-trusted-lab/

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 highlight the high-scoring products of the various tests that took place over the course of the year. Please bear in mind that this report looks at all the comparative tests of 2015, i.e. not just 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/comparatives-reviews/).

Participating Vendors

The following vendors participated in AV-Comparatives' public main test-series of 2015 and agreed to have the effectiveness of their products independently evaluated.

We are happy that this year's tests helped several vendors to find critical and other bugs in their software, and that this has contributed to improving the products.

Management Summary

Tests

In 2015, AV-Comparatives subjected 21 security products for Windows to rigorous investigation. All the programs were tested for their ability to protect against real-world Internet threats, identify thousands of recent malicious programs, and provide protection without slowing down the PC. Additionally, optional tests checked how well the products could remove malware from an infected PC, and block new and unknown threats.

Results and Awards

Whilst all of the programs in our test reached an acceptable level overall, some programs outperformed others. For details, please see "Overview of levels reached during 2015" on page 7. In order to recognise those products that achieve outstanding scores in our tests, we have given a number of awards that highlight the best results in each test and overall. The Product of the Year award and Top Rated awards are based on overall performance in the public main test series; there are also Gold, Silver and Bronze awards for each individual test type. Please see the Award Winners section for more details of the awards. The 2015 Product of the Year Award goes to Kaspersky Lab; Top Rated Products are (alphabetically) Avast, AVIRA, Bitdefender, Emsisoft, eScan, and ESET.

Overview of tested products

Here we provide a summary for each of the programs tested, with a note of each one's successes during the year. Although the user interface does not affect any awards, we have noted some of the best UI features as well.

Avast is a **Top Rated Product** this year, receiving five Advanced+ awards in the course of the year, including both Real-World Protection Tests. It wins the *Gold Award* for the Performance Test, and joint *Silver* for the Removal Test. We feel its scan-results dialog box is equally well suited to expert and non-expert users.

AVG participated in seven out of eight tests this year, and received awards in all of them, including five Advanced+. It wins the *Bronze Award* for Malware Removal. We liked the custom installation option and the quick tutorial in the setup wizard.

Avira is once again a **Top Rated Product**. It took part in seven out of eight of this year's tests, and received six Advanced+ awards, including both Real-World Protection Tests. It won *Silver Awards* for the File Detection and Performance tests, along with *Silver* for the Real-World Protection Test and joint *Bronze* for Removal. Its user interface is tried, tested, and very straightforward to use.

Baidu participated in five[1] out of eight tests this year, reaching Advanced level in both Real-World Protection Tests, and Advanced+ in the May Performance test. We liked the ability to change the program's interface language very quickly and simply.

Bitdefender is a **Top Rated Product** this year, with joint highest scores overall. It only missed Product of the Year because it won the award last year; it received Advanced+ awards in all eight main tests. It wins the *Gold Award* in Proactive Protection, joint *Gold* in File Detection, joint *Gold* in the Real-World Protection Test, and joint *Silver* in Malware Removal. Its almost instant real-time detection of malware on a flash drive stood out in our user-experience review.

BullGuard received an award in all eight tests this year, including an Advanced+ in the September File Detection Test. It wins a joint *Bronze Award* for File Detection. We liked the automatic scanning of USB drives, and fact that the program settings are password protected by default.

Emsisoft is a **Top Rated** Product this year, with four Advanced+ awards. It wins *Bronze Awards* for File Detection and Performance. We liked the information and explanations provided by its setup wizard.

---

[1] Baidu was not able to participate in the October Performance Test, due to being incompatible with Windows 10.

eScan received at least an Advanced award in all eight tests this year, and is a **Top Rated Product**. It wins a joint *Bronze Award* for File Detection. We liked the automatic scan of USB drives, which quarantines any malware found without user interaction.

ESET received six Advanced+ awards this year, and is once again a **Top Rated Product**. It wins the *Silver Award* in the False Positives category, and *Bronze* in Proactive Protection. Its refreshed graphical user is as clear as ever and there is excellent and comprehensive documentation.

Fortinet received awards in all eight tests this year, including two Advanced+. Its user interface is business-oriented but straightforward.

F-Secure reached Advanced level in all eight of our main tests this year. We liked its clear and persistent malware alerts.

Kaspersky Lab is this year's **Product of the Year**, having received Advanced+ awards in all of the year's tests. It also wins the *Gold Award* in the Malware Removal Test, and joint *Gold* in the Real-World Protection and File Detection Tests. Additional wins this year are the *Silver Award* in the Proactive Protection Test, and joint *Bronze* in Performance. We liked the real-time progress displays in its refreshed user interface, and the extensive and excellent documentation.

Lavasoft received awards in seven out of eight tests this year, including Advanced+ for the September File Detection Test. It received a joint *Bronze Award* for File Detection. We liked the option to install it as a secondary scanner.

McAfee (Intel Security) took part in six out of eight of this year's tests, and received awards in all of them, including three Advanced+. We liked the choice of components in the setup wizard, and its clear and persistent malware alerts.

Microsoft's built-in security product served as baseline. It received awards in six out of eight tests this year, and takes the *Gold Award* for Lowest False Positives. Its simple design makes it very easy to use.

Panda took part in seven out of eight of this year's tests, and received at least an Advanced award in all of them. It takes the *Bronze Award* for Lowest False Positives. We liked its new finger-friendly user interface.

Quick Heal participated in six out of eight tests this year, receiving awards in all six, including four Advanced awards. The automatic scan of USB drives ensures that any malware on such a drive will be removed.

Sophos took part in seven out of eight tests this year, and received at least an Advanced award in all of these. Its user interface is straightforward, although oriented towards business use.

Tencent took part in six out of eight tests this year, and received awards in all of them, including four Advanced+. It wins the *Bronze* Award in the Real-World Protection Test. We liked the clean and modern graphic design of the program's interface.

Threat Track Vipre received awards in five out of eight tests this year, including Advanced in the September File-Detection test. We liked sensitive real-time protection and helpful advice on upgrading to Windows 10.

Trend Micro took part in six tests this year, receiving awards in all of them, including five Advanced awards. The program interface is clean and easy to navigate, with a good status display and malware alerts.

All the 21 vendors above are AV-Comparatives Approved Windows Security Products.

Advice on Choosing Computer Security Software

There is no such thing as the perfect security program, or the best one for all needs and every user. 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.

Before selecting a security product, please visit the vendor's website and evaluate their software by downloading a trial version. Our awards are based on test results only and do not consider other factors as there are some important factors (such as available interface languages, price, and support), which you should evaluate for yourself.

Overview of levels reached during 2015

AV-Comparatives provides a wide range of tests and reviews in comprehensive reports (http://www.av-comparatives.org/comparatives-reviews/). Annual awards for 2015 are based on the public main test-series: **Real-World Protection Test**, **Performance Test**, **File Detection Test**, and **False-Alarm Test** (all compulsory), and the *Proactive Test* and *Malware Removal Test* (both optional). Vendors who choose not to have some features of their products publicly evaluated (i.e. did not participate in some of the optional tests) are still eligible for Product of the Year/Top Rated awards, but obviously have fewer opportunities to score points. Additional tests/reviews (not part of the main test-series and not relevant to the awards) included: Anti-Phishing Test, Mac Security Test/Review, Mobile Security Test/Review, Business Security Review and Parental Control Test/Review.

All the programs tested are from the reputable and reliable manufacturers. Please note that even the STANDARD level/award requires a program reach a good standard, although it indicates areas which need further improvement compared to other products. ADVANCED indicates areas which may need some improvement, but are already very competent. Below is an overview of awards reached by the various anti-virus products in AV-Comparatives' main test-series of 2015.

	File Detection Test March 2015	Proactive Test March 2015	Performance Test May 2015	Real-World Protection Test (March-June 2015)	Malware Removal Test (March-September 2015)	File Detection Test September 2015	Performance Test October 2015	Real-World Protection Test (August-November 2015)
Kaspersky Lab	***	***	***	***	***	***	***	***
Bitdefender	***	***	***	***	***	***	***	***
ESET	**	***	***	***	**	***	***	***
AVIRA	**		***	***	***	***	***	***
Emsisoft	**	*	***	**	**	***	***	***
eScan	**		***	**	**	***	***	**
Avast	*	tested	***	***	***	**	***	***
AVG	*		***	***	***	*	***	***
Tencent	**		***	***		**	***	***
Fortinet	***	*	**	***	**	**	*	**
Sophos	**		***	**	**	**	***	**
BullGuard	**	**	**	**	**	***	**	*
F-Secure	**	**	**	**	**	**	**	**
Panda	**		**	**	**	***	**	**
McAfee	***		***	*		**	***	**
Lavasoft	**	tested	**	*	**	***	**	*
Trend Micro	*		**	**		**	**	**
QuickHeal	**		*	**		**	**	*
Microsoft	tested	*	**	*	**	tested	**	*
Baidu	tested		***	**		tested		**
Vipre	*	tested	*	tested	*	**	*	tested

Key: * = Standard, ** = Advanced, *** = Advanced+

An empty box indicates that the vendor did not participate in the optional test.

Award Winners

The Product of the Year award is given to the product with the highest overall score from all the public main tests. It 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.

A number of products that reach a very high overall standard in the public main tests are given the Top Rated award.

For each of the test types[2] in the public main series (Real-World Protection, File Detection, False Positives, Performance, Proactive, Malware Removal), we give Gold, Silver and Bronze awards, for the first, second and third highest-scoring products, respectively.

---

[2] For some test types, there may be two actual tests conducted in a year; the awards are based on the combined score of both tests.

Overall winner of 2015 (Product of the Year)

For AV-Comparatives' "Product of the Year" award, all tests in the public main-test series are taken into consideration. This year, both Bitdefender and Kaspersky Lab received an Advanced+ award in all of these tests, i.e. were equally high scoring. In such cases, we use the following as a tiebreaker: the product that has not won the award before or the product that won it less recently, is given the award. On this basis, AV-Comparatives' 2015 Product of the Year award goes to Kaspersky Lab.

Kaspersky Lab

Top Rated Products 2015

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

We have used the results over the year to designate products as "Top Rated". Results from all the tests are assigned points as follows: Tested = 0, Standard = 5, Advanced = 10, Advanced+ = 15. Products with 90 points or more were given the Top Rated award, with two conditions. Firstly, any products that failed to win any award (i.e. got 0 points) in either of the Real-World Protection tests have not been considered. Secondly, good results in the performance tests cannot make up for weak results in the detection/protection tests. We intend to give the Top Rated award again next year, but the criteria may be modified.

Top Rated products for 2015 are, in alphabetical order:

Avast, AVIRA, Bitdefender, Emsisoft, eScan, ESET

Please see our summary and awards pages – links below:

http://chart.av-comparatives.org/awardslist.php?year=2015

Whole-Product Dynamic "Real-World" Protection winners

Security products include various different features to protect systems against malware. Such protection features are taken into account in the Whole-Product Dynamic "Real-World" Protection tests, which test products 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. In total, over 200,000 test cases[3] (clean and malicious) have been used.

The programs with the best overall results over the course of the year are: **Bitdefender, Kaspersky Lab, AVIRA** and **Tencent**. Kaspersky Lab and Bitdefender share the Gold Award.

AWARDS

Bitdefender, Kaspersky Lab

AVIRA

Tencent

For details and full results of the 2015 Real-World Protection tests, please click the link below:

http://www.av-comparatives.org/dynamic-tests/

---

[3] One test case = one security product tested with one clean or malicious test sample.

File Detection winners

The File Detection Test evaluates the static file scanning engine component, which is one subset of the protection features provided by security products. A high detection rate of malware - without causing too many false alarms – is, depending on the situation, one of the most important, deterministic and reliable features of an anti-virus product (as e.g. it is not heavily dependent on infection vectors or other factors).

Bitdefender and **Kaspersky Lab** earned ADVANCED+ in both tests. **AVIRA**, **Emsisoft**, **Lavasoft**, **BullGuard** and **eScan** received an ADVANCED+ award in at least one of the two tests and scored both times over 99.5%.

AWARDS

GOLD	**Bitdefender, Kaspersky Lab**
SILVER	**AVIRA**
BRONZE	**Emsisoft, Lavasoft, BullGuard, eScan**

For details and full results of the 2015 File Detection tests, please click the link below:

http://www.av-comparatives.org/detection-test/

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. AV-Comparatives carry out extensive false-positive testing as part of the File Detection Tests.

The products with the lowest rates of false positives during 2015 were *Microsoft* (0), *ESET* (1) and *Panda* (3). These figures represent the SUM of the false positives from both FP Tests.

AWARDS

 Microsoft

 ESET

 Panda

For details and full results of the 2015 False Positive tests, please click the link below:

http://www.av-comparatives.org/false-alarm-tests/

Overall Performance (Low System-Impact) winners

Security 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.

Avast, *AVIRA, Emsisoft* and *Kaspersky Lab* demonstrated a lower impact on system performance than other products.

AWARDS

Avast

AVIRA

Emsisoft, Kaspersky Lab

For details and full results of the 2015 Performance tests, please click the link below:

http://www.av-comparatives.org/performance-tests/

Proactive (Heuristic/Behavioural) Protection winners

The Proactive Test shows how good the heuristic detection and behavioural protection features of the various anti-virus products are (i.e. how good they are at protecting against new/unknown malware) without Internet access against completely new (0-day) malware. A high proactive detection/protection rate <u>must</u> be achieved with a low rate of false alarms.

The following products showed the highest proactive protection rates in the 2015 test: *Bitdefender* (99%, few FPs), *Kaspersky Lab* (92%, few FPs) and *ESET* (86%, very few FPs).

AWARDS

                    Bitdefender

                    Kaspersky Lab

                    ESET

For details and full results of the 2015 Proactive tests, please click the link below:

http://www.av-comparatives.org/retrospective-test/

Malware Removal winners

A very useful ability for an anti-virus program is the ability to remove malware, which has already infected a system.

In this year's test, five products received the Advanced+ award, these being *Kaspersky Lab, Avast, Bitdefender, AVG* and *AVIRA*:

AWARDS

Kaspersky Lab

Avast, Bitdefender

AVG, AVIRA

For details and full results of the 2015 Malware Removal test, please click the link below:

http://www.av-comparatives.org/removal-tests/

User Experience Review

Review procedure

Here we provide an overview of the main features and functionality that we have tested for this review. Programs were installed on 64-bit Windows 10 Pro, except for the International/English version of Baidu Antivirus, which does not have a compatible version, and so was tested on 64-bit Windows 8.1 Pro.

Windows Security Center

Windows versions from Windows XP SP2 onwards include a feature originally known as *Windows Security Center*. The Control Panel applet was renamed *Action Center* in Windows 7, and *Security and Maintenance* in Windows 10, although the underlying Windows Service retains the original name (which we have used here). Windows Security Center provides an overview of the system's security-related functionality and displays alerts in the event that a security feature is missing or malfunctioning. Third-party security software, when installed, should register with Security Center as providing antivirus and antispyware protection; if the security software includes its own firewall, this should also be registered. We regard Windows Security Center as a valuable means of checking a computer's security status, and so we check that the programs we test register appropriately when installed, and also that they cause Security Center to show an alert if they are disabled. To do this, we look for an option in each program's settings that will permanently disable the real-time protection, as opposed to just deactivating it for a few minutes.

Windows Defender

In Windows Vista and Windows 7, *Windows Defender* is an integrated antispyware program. In these systems, it does not provide complete malware protection, and needs to be supplemented by an antivirus program. In Windows 8, 8.1 and 10, it can be regarded as a full antimalware program in itself. Windows 10 includes a new security mechanism, which we feel is valuable: if a third-party antivirus program reports to Windows Security Center that it is disabled or ineffective, Windows Defender will be reactivated in order to ensure that the system is protected against malware. We regard this as a helpful addition to system security, and so check that Windows Defender will be re-enabled if the security program being tested is switched off.

Windows Firewall

Windows Firewall is integrated into Windows versions from XP onwards. We do not regard it as being necessarily any better or any worse than the third-party firewalls included in some security suites. A third-party security program that does not include its own firewall should leave Windows Firewall

running, but if the security suite *does* include a firewall of its own, we would normally expect its setup wizard to disable Windows Firewall, in order to avoid conflicts. In the event that the third-party firewall is disabled, we feel the suite should cause Windows Security Center to show an alert and reactivate Windows Firewall. Please note that with a few security suites, the third-party firewall is designed by the manufacturer to supplement the Windows Firewall rather than replace it, and so Microsoft's firewall is left running. In such cases, which we have noted in the text of the review, we do not regard it as necessary that the suite should cause Action Center to show an alert if its own firewall is disabled. Please note that in the case of products that do not include their own firewall, we have stated that the product "uses Windows Firewall", meaning that if the product is installed, Windows Firewall is not deactivated and continues to provide the firewall protection for the computer.

Deinstallation/deactivation from a standard user account

All NT-based versions of Windows, i.e. from Windows XP onwards, provide two different types of user account, namely *Standard* and *Administrator*. Standard user accounts allow users to run installed programs and configure their own user profiles, e.g. by changing their desktop wallpaper or the location of their personal folders. Administrator accounts can additionally change system settings, such as the network configuration, and install/uninstall programs. With a family PC, parents may use administrator accounts themselves, but create standard user accounts for their children, to prevent them e.g. changing security settings. Likewise, the owner of a small business may set up standard user accounts for his//her employees, for the same reasons. We feel that security programs should follow the same principle, either by making their settings inaccessible to standard users, or by password-protecting the configuration. If the latter method is used, we regard it as ideal if the program's setup wizard prompts the user to set up password protection immediately.

Main program window

We feel that security programs should make certain features easily accessible from the home page of the main program window. A status display should show clearly whether the real-time protection is switched on, and malware signatures are up to date. If the product includes its own firewall, the status display should also indicate that this is functioning appropriately. A scan button should be provided, so that the user can check the computer for malware. Although automatic updates are now a standard feature of security programs, we feel it is ideal for the program to include an easy means of running a manual update, so that the user can ensure that the program has the very latest definitions before running a scan. A help button should also be easy to find. In the case of paid-for programs, it is helpful if licence expiry information is displayed, so that the user can renew the subscription before it expires. Power users may also be interested in finding logs, quarantine and settings.

Status alerts

If the security program's real-time protection is disabled for any reason, or malware definitions are out of date, we expect the program's status display to show a clear warning to this effect. We feel the program should also provide an easy means of rectifying the problem, e.g. a "Fix-All" button that will carry out the necessary action(s) to ensure optimal security. The same principles apply to the program's own firewall if there is one.

Malware alerts

If the user encounters malware whilst using the computer, we feel the security program should inform the user clearly that this has happened, and take appropriate action that does not require the user to make a decision. To check the alerts shown by each program, we used three test scenarios. Please note that the alerts shown here may only represent a few of the many possible warnings shown by a program in different situations.

1. We attempted to download a malware sample from a web server to the test PC, using Internet Explorer. We used our own http server for this test, to ensure that all programs display a malware alert as opposed to a URL-blocker alert.

2. We connected a flash drive with malware samples to our test PC, opened the drive in Windows Explorer, and then attempted to copy the samples to the Desktop folder.

3. We connected a flash drive with malware samples to our test PC and ran an on-demand scan.

For each scenario, we have provided a screenshot of the alert shown and noted what user action, if any, is provided. If in our Real-World Protection Test a program produced a user-dependent alert in more than 1% of all test cases, we have additionally included a screenshot of the dialog box shown in such situations. These days, almost all of the programs we test produce clear default notifications that do not require a user decision. We also performed a functionality test, in which we attempted to copy malware samples from a read-only network share to an empty flash drive connected to the test PC. In the event that that any of the samples appeared to have been copied successfully to the drive, we then removed the drive and checked to see if there were any intact malware samples on it. We performed this test twice, once by simply pulling the drive out of the USB port, and once by using Windows' *Safely eject hardware* function, and waiting until the message *device can now be safely removed* was shown. We have only reported the results of this test for those programs that allowed the flash drive to be removed with at least one malware sample intact.

AV
comparatives

Additional points covered in the review

The review also covers a few other points, which may be of interest to some readers. Firstly, we note whether the product uses any third-party protection components. In the event that one product in a manufacturer's range (e.g. *Antivirus*) uses different third-party components from another product (e.g. *Internet Security*), we also report this. Next, we look to see what options, if any, are included in the product's setup wizard. We also checked whether the program's uninstaller includes any options other than complete removal of the product. All the products in the review add their own icon to the Windows System Tray; we show a screenshot of the menu displayed by right-clicking this icon, so readers can see what functions it makes available. Most products also add at least one entry (scan) to the Windows Context Menu, shown when a file, folder or drive is right-clicked in Windows Explorer; we include a screenshot of this. Finally, we note whether the product adds a toolbar to Internet Explorer, changes its default search service (Bing), or adds ratings to its search results (typically an icon added to the headline of each result, to show whether the page is deemed to be safe or not).

Avast Free Antivirus 11.1
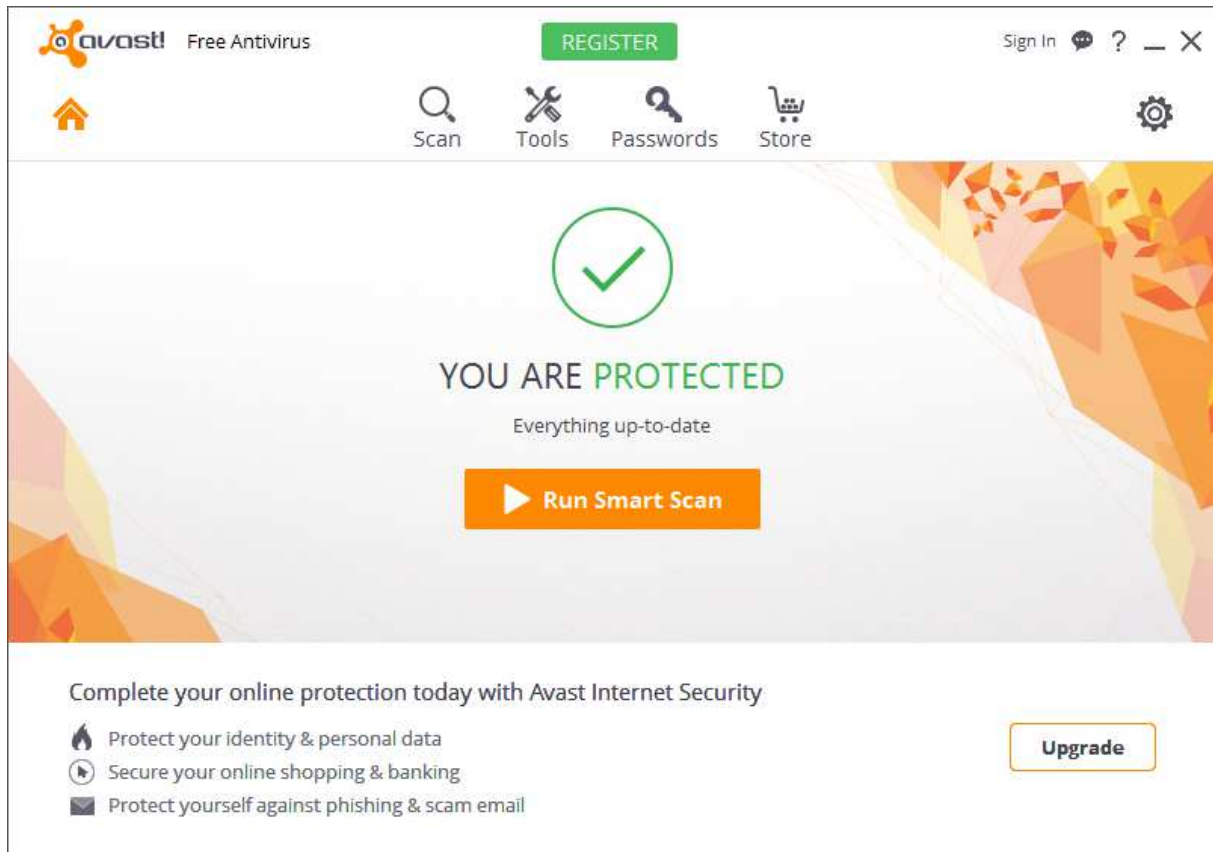
Supported operating systems
Windows XP, Vista, 7, 8, 8.1, 10

Firewall
Avast Free Antivirus uses Windows Firewall.

Product page on vendor's website
https://www.avast.com/compare-antivirus

Help
There is a local help feature, accessible from the main program window, and an online FAQ page is provided for the product[4].

---

[4] https://www.avast.com/en-us/support

Good points

We liked Avast's custom installation option. The program interface is clearly laid out and makes almost all the important functions easy to find. Malware alerts are good, providing the option to report the detection of a download as a false alarm. We also felt that the scan results dialog provides an easy, one-click option to clean up malware automatically, whilst power users can change the action taken for individual files if they want.

Suggestions for improvement

Two minor possible improvements could be to make the manual update a little easier to find, and prompt the user during setup to password-protect the settings.

Installation, deinstallation, deactivation

Installation options

There is a standard installation option, which does not require the user to make any decisions, and a custom option. With the latter, the user can choose the location of the installation folder and program components to be installed.

Deinstallation options

The uninstaller additionally lets the user update the program to the newest version, change components, or repair the installation.

Deinstallation/deactivation from a standard user account

A user with a standard Windows user account cannot uninstall the product, but is able to deactivate protection components. It is possible to password protect the settings to prevent this.

Windows Security Center, Windows Defender

Avast Free Antivirus integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window

Security Status, scans, settings and help can all be found on the home page. A manual update can be run by clicking *Settings, Update*. Logs and quarantine can be found under Tools, *Statistics*, *Component Status*; quarantine is named *Virus Chest*.

System Tray menu
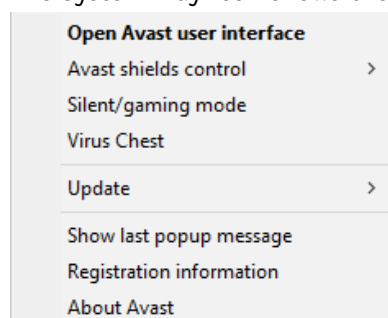
The System Tray icon shows the following menu:

Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:
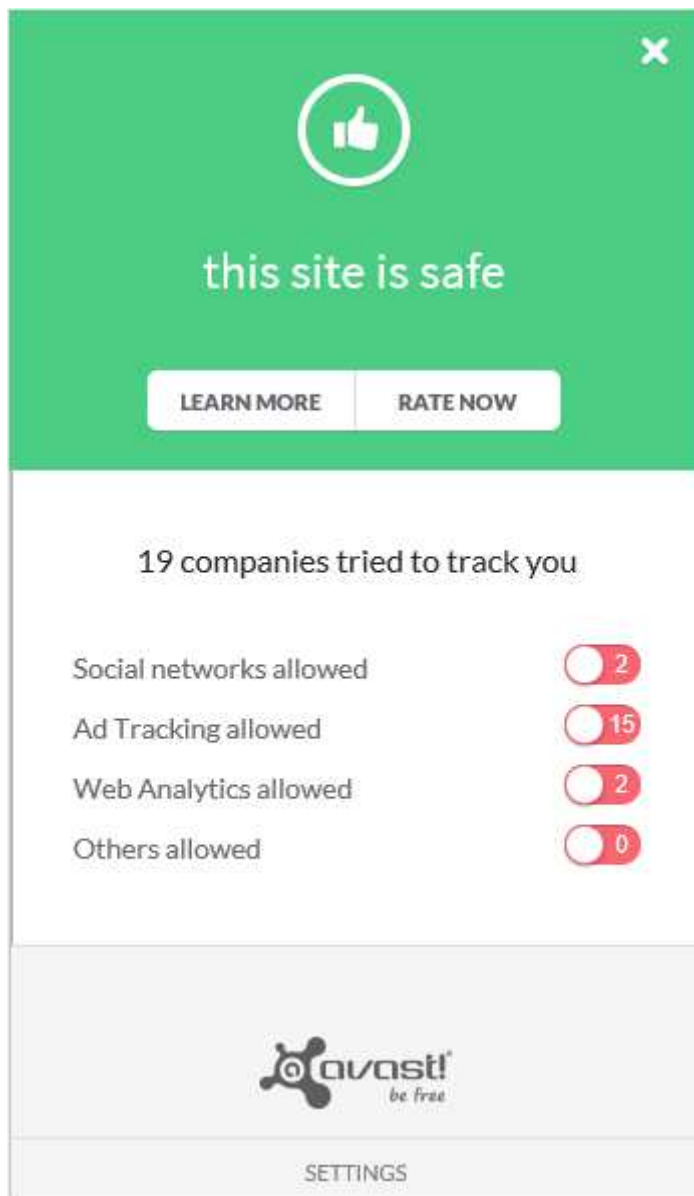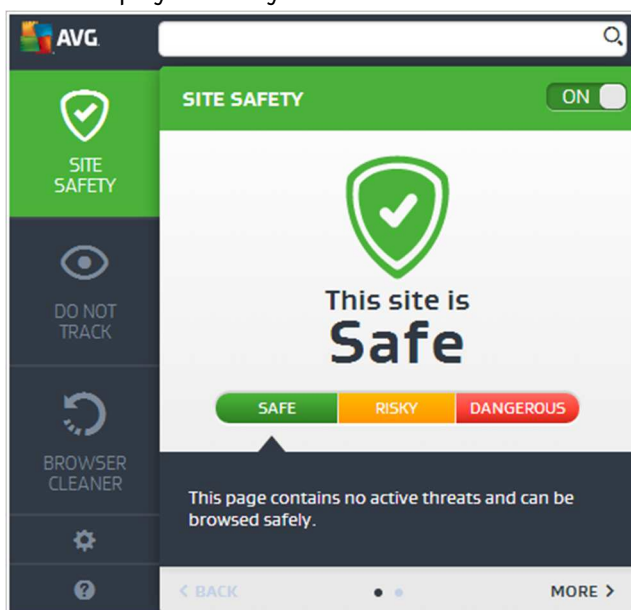

Internet Explorer

Toolbar

An Avast icon is added to the symbols in the top right-hand corner of the Internet Explorer window:

Clicking the icon displays security information about the web page currently being displayed:

Search service

The default search service in Internet Explorer is not changed.

Search ratings

Search ratings for search engine results are not displayed.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:
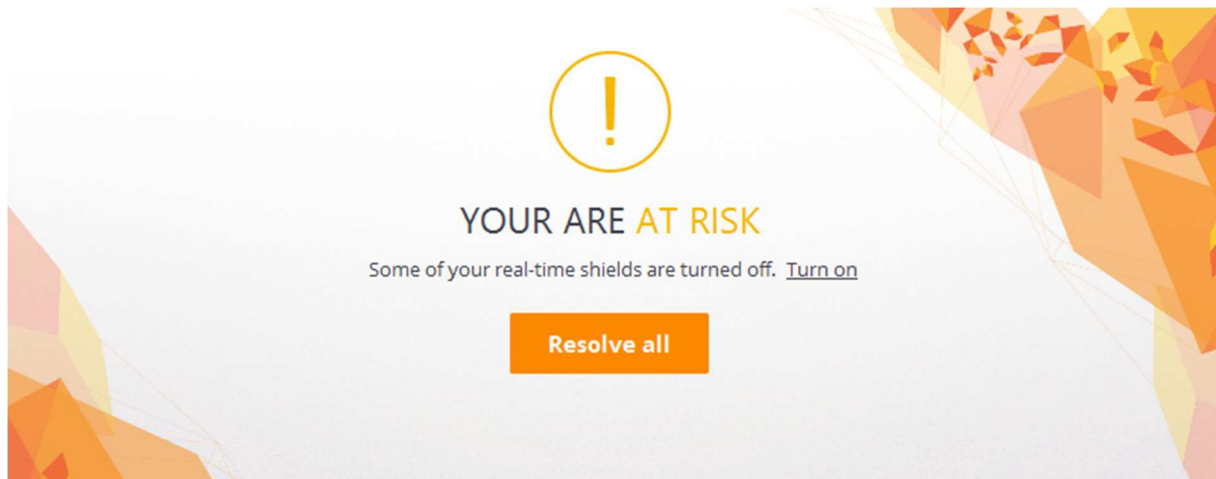

Protection can be reactivated by clicking *Resolve All*.

Malware alerts

Web

If malware is downloaded via Internet Explorer, the following Avast alert is shown:
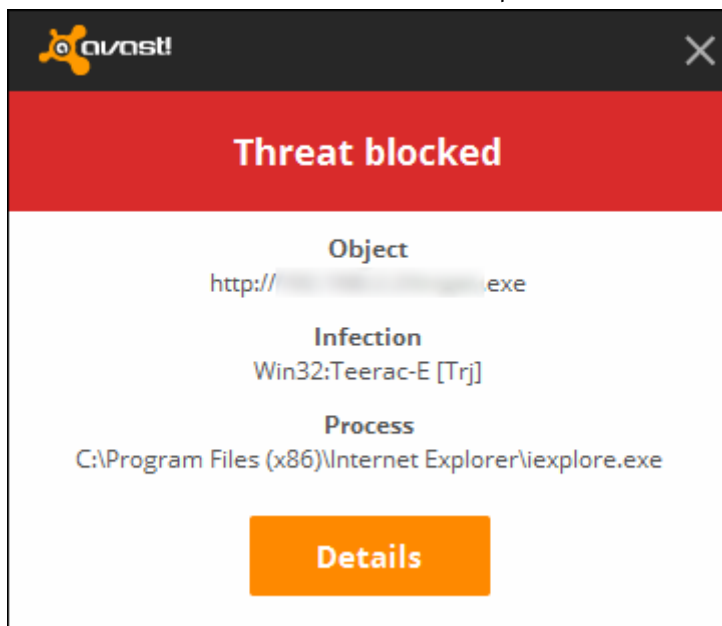
No user action is required.

USB on-access

If the user attempts to copy an infected file from a USB flash drive to the computer's hard disk, Avast displays the following alert:
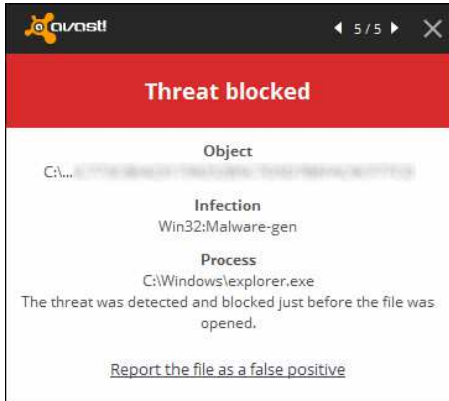
No user action is required. Note that the malware is not automatically deleted from the flash drive.

USB on-demand

Running an on-demand scan of a flash drive containing malware shows the resultant detections and lets the user choose what action to take. By default, *Fix Automatically* is selected for all items, and there is an explanation of what this means:

The user only needs to click *Apply* to render the malware harmless.

AVG Internet Security 2016

Supported operating systems
Windows XP, Vista, 7, 8, 10

Firewall
AVG Internet Security includes its own firewall.

Product page on vendor's website
http://www.avg.com/eu-en/internet-security

Help
A local help feature is provided, and an FAQ page is available on the manufacturer's website[5].

Good points
We liked the custom installation option and the quick tutorial in the setup wizard. The status display is detailed but clear, and the most important functions are easily found in the main program window. Malware alerts are clear, and removing detected malware is intuitive.

---

[5] https://support.avg.com/support_Internet_Security?l=en_US

Suggestions for improvement

We feel that if the AVG Firewall is deactivated for whatever reason, this should be reported to Windows Security Center – meaning that Windows Firewall will then be re-enabled.

Installation, deinstallation, deactivation

Installation options

There is standard installation options, with no choices to be made, or a custom option, which allows the user to select components and change the location of the installation folder:
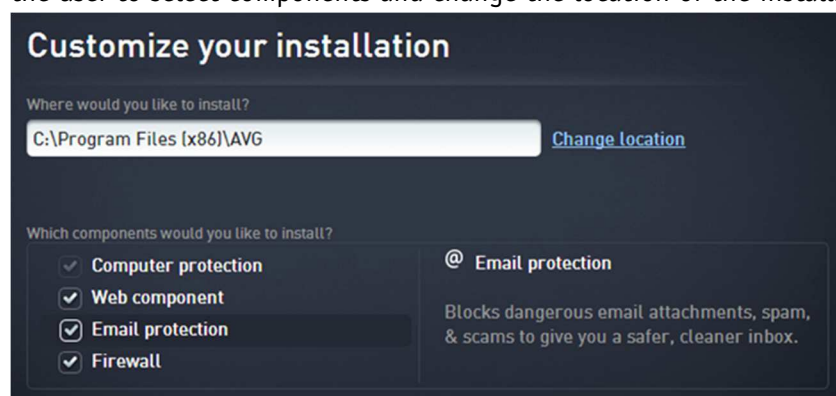
Deinstallation options

A Repair option is provided in addition to deinstallation.

Deinstallation/deactivation from a standard user account

The product cannot be uninstalled, nor can protection be disabled, with a standard user account.

Windows Security Center, Windows Defender

If the AVG Firewall is disabled, an alert is shown in the program itself. It appears to not inform Windows Security Center, which continues to state *AVG Internet Security is currently turned on*. As a result, Windows Firewall is not automatically activated, and a quick test demonstrates that no firewall protection is provided in this case.

User Interface

Main program window

This has a clear overall status display, with individual tiles for each component additionally showing the status for that component. Scan and update (*Protection is up-to-date*) buttons are shown on the home page; help and quarantine (*Virus Vault*) can be found in the *Options* menu in the top right-hand corner of the window; logs can be seen by clicking the *Reports* button at the top of the window. To find the options for a particular component, such as the Firewall, the user clicks on the component's tile on the home page and the cogwheel icon which is then displayed. Licence information can be seen by clicking *Options, About AVG, License and Support*.

System Tray menu

This shows the following menu:
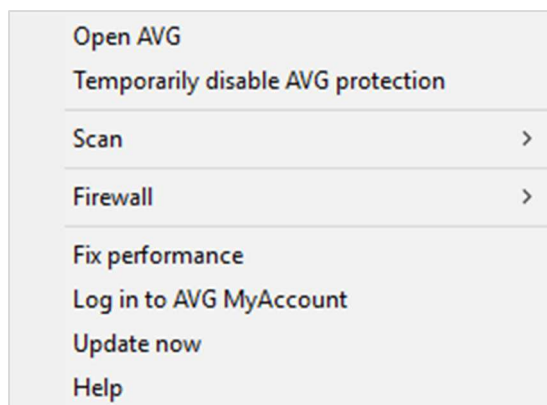
Open AVG
Temporarily disable AVG protection

Scan   >

Firewall   >

Fix performance
Log in to AVG MyAccount
Update now
Help

Windows Explorer context menu

The following entries are added to the menu shown when a file is right-clicked in Windows Explorer:

Scan with AVG
Permanently shred with AVG
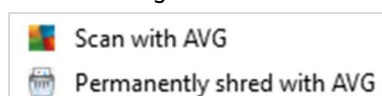
The second option allows files to be securely deleted.

Internet Explorer

Toolbar

We found that while there is no toolbar, AVG adds an icon to the window frame of Internet Explorer, which displays security information for the current web page:

Search service

The default search service in Internet Explorer is changed to AVG's own Yahoo-based search service.

Search ratings

No obvious search ratings are displayed.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

Protection can be reactivated by clicking *Fix Now*.

Firewall

A corresponding alert and reactivation button are shown if the AVG Firewall is disabled.

Malware alerts

Web

The following alert is shown if malware is downloaded from a web page:
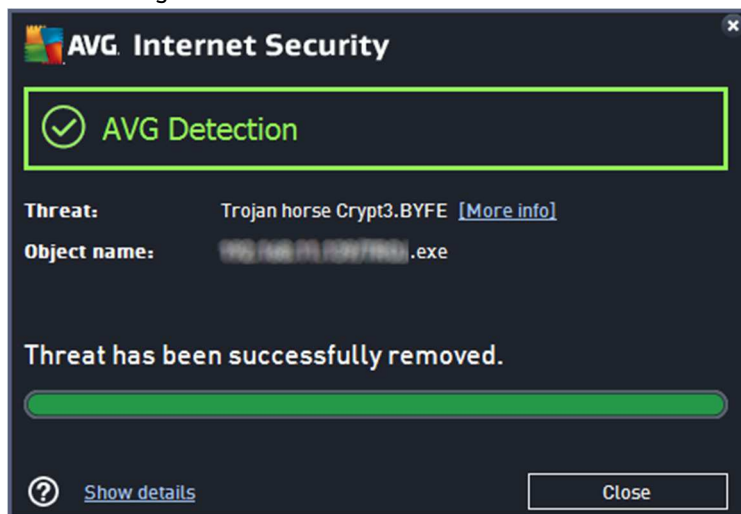
No user action is required.

USB on-access

If the user attempts to copy malware from a flash drive to the local hard drive, the alert below is shown:

The user need only click *Remove All* to delete the threats.

USB on-demand

If a flash drive is scanned and malware detected, the following alert is shown:
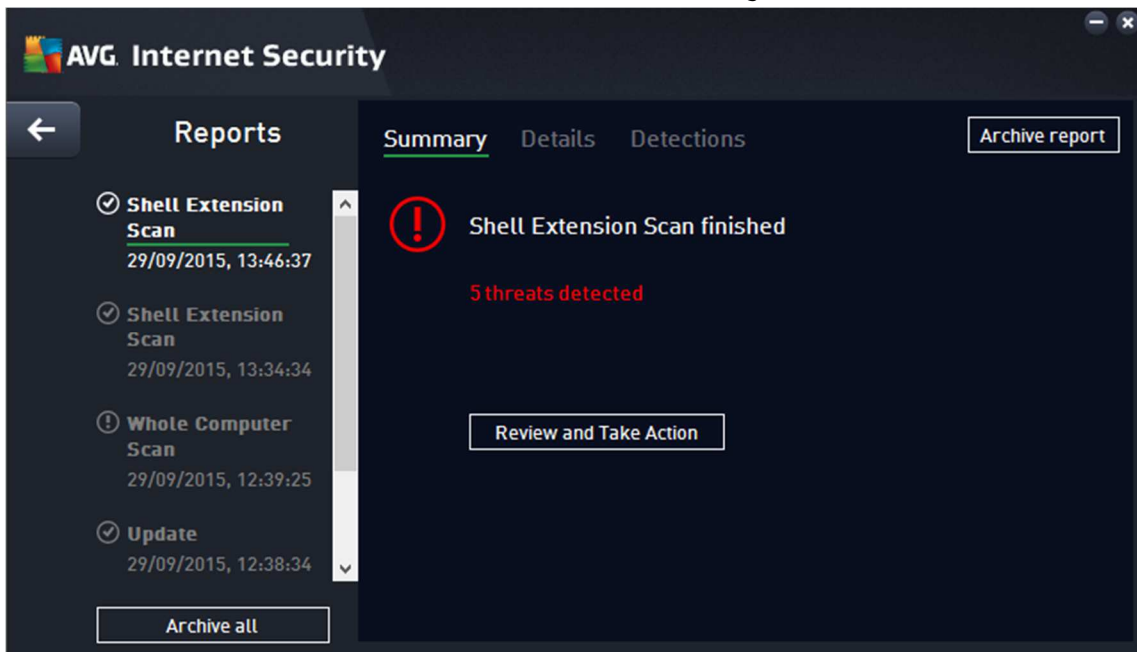
Clicking *Review and Take Action* lets the user see and delete the items found.

Additional comments

During our test, we noticed that AVG prompts the user to run an initial scan, and to set up browser protection:
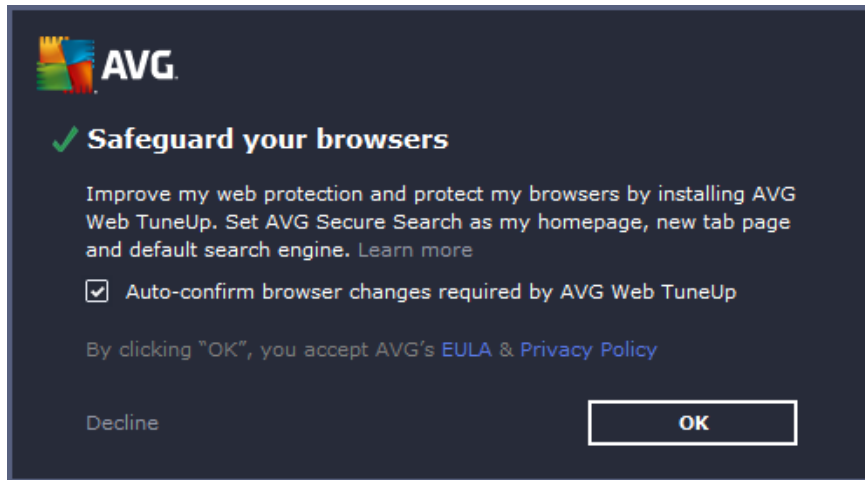
The setup wizard provides a brief explanation of the status display on the home page:

Avira Antivirus Pro 15.0
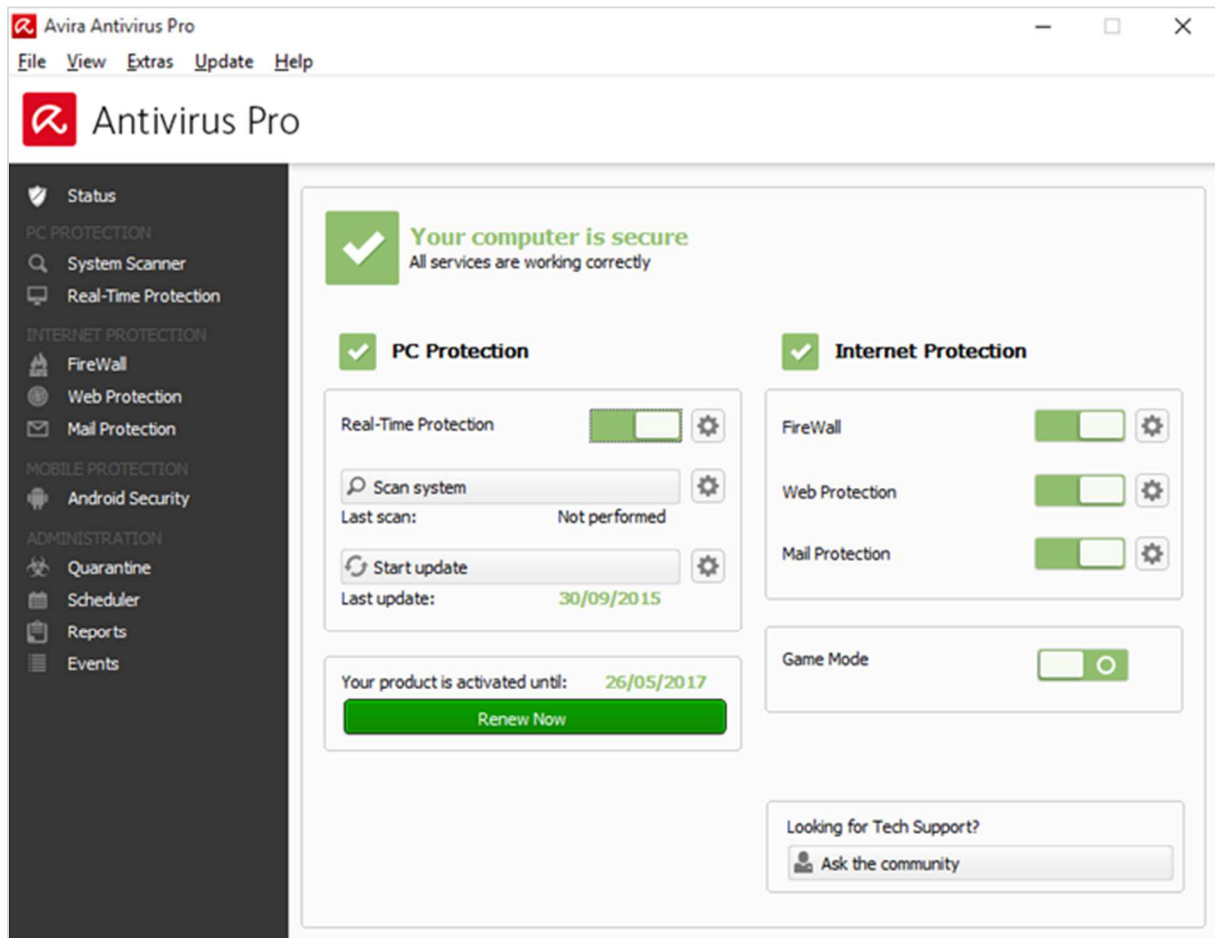
Supported operating systems
Windows 7, 8, 8.1, 10, all 32 and 64-bit

Firewall
Avira Antivirus Pro uses Windows Firewall.

Product page on vendor's website
http://www.avira.com/en/avira-antivirus-pro

Help
A local help file is provided, and a searchable FAQ page is provided on the manufacturer's website[6].

---

[6] http://www.avira.com/en/support

Good points

We found that the main program window of Avira Antivirus Pro makes all important functions and information easily accessible. The status display and malware alerts are clear, and make it easy for the user to keep the computer secure.

Suggestions for improvement

We feel that the setup wizard should make clear that the *SafeSearch Plus* browser add-on does not work with Internet Explorer. Avira informed us that the *Avira Launcher* allows users "to quickly access all Avira related products as well as the Management backend". However, we feel that in its current form, it serves principally to advertise other Avira products, and question whether this is appropriate in an otherwise very professional product that the user has paid for. Note that it is possible to download Avira Antivirus Pro separately from the Avira Launcher[7].

Installation, deinstallation, deactivation

Installation options

There is an option to install *Avira SafeSearch Plus*:
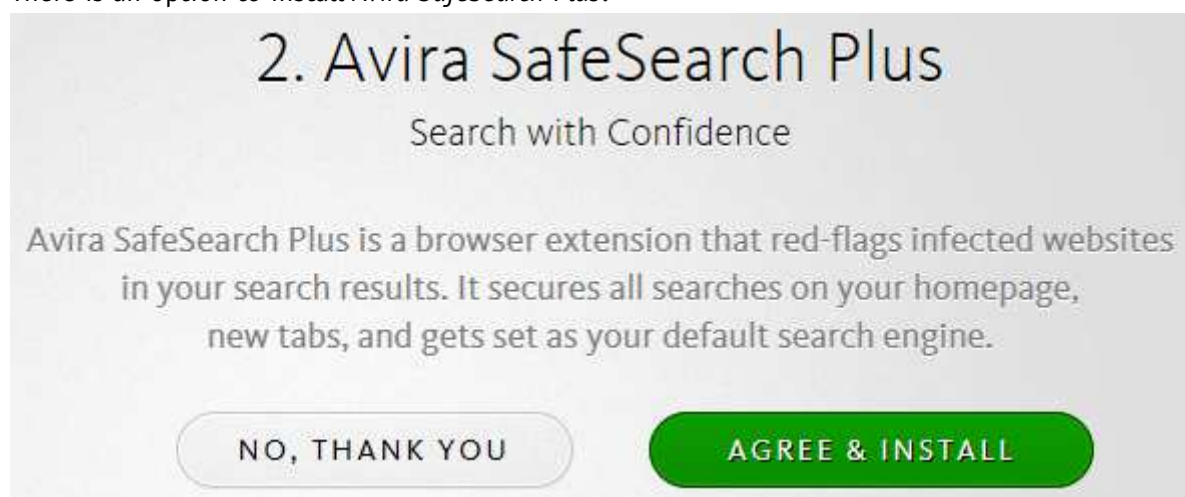
Deinstallation options

There is an option in the uninstaller to change the installed components.

Deinstallation/deactivation from a standard user account

The program cannot be deactivated or uninstalled without entering administrator credentials.

Windows Security Center, Windows Defender

Avira Antivirus Pro integrates with Windows Security Center and Windows Defender exactly as expected.

---

[7] http://www.avira.com/de/download/product/avira-antivirus-pro

User Interface

Main program window

The main window includes a status display, update and scan links, a help menu, licence information, and links to quarantine and logs (*Reports*). Each of the components shown on the home page has its own cogwheel icon, which opens the settings for the respective component; settings can also be accessed by clicking the *Extras* menu, *Configuration*.

System Tray menu

The System Tray icon displays the following menu when right-clicked:
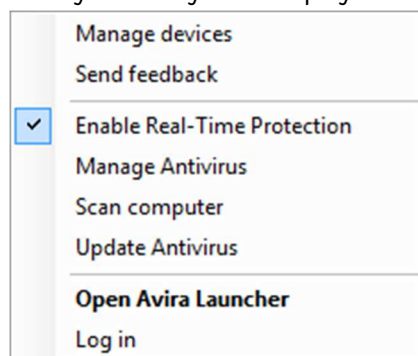
To open the main program window, the user needs to click on *Manage Antivirus*.

Windows Explorer context menu

The following entry is added to the menu shown when a file, folder or drive is right-clicked in Windows Explorer:

Internet Explorer

Toolbar, search service and search ratings

Although we opted to install the *SafeSearch Plus* component during setup, we found that no changes were made to Internet Explorer, its default search engine, or the search results displayed. When we asked Avira about this, they informed us that the component currently only works with Google Chrome and Mozilla Firefox.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

Additionally, the System Tray icon changes from an open umbrella to a closed umbrella. Clicking *Fix Problem* in the main window's status display allows the user to reactivate the protection.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown in the browser window:
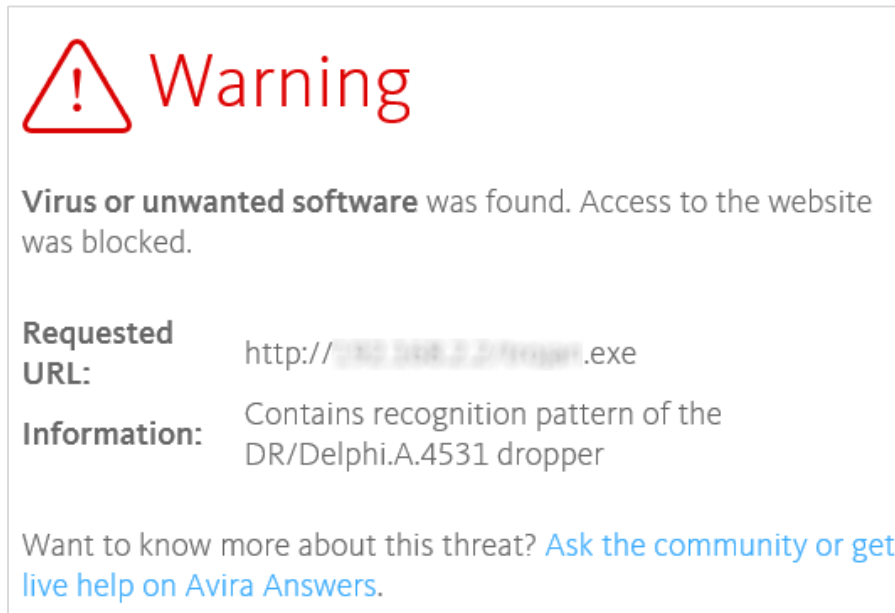
USB on-access

If the real-time protection detects malware on a USB flash drive, the alert below is displayed:
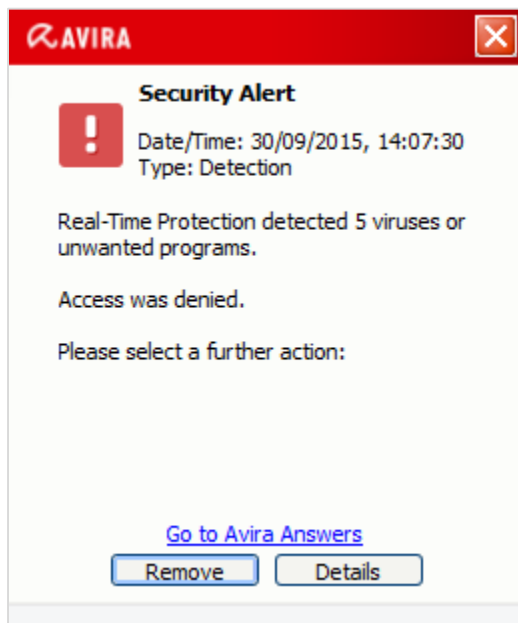
The user only needs to click *Remove*.

USB on-demand

Running an on-demand scan of a flash drive containing malware produces this warning:
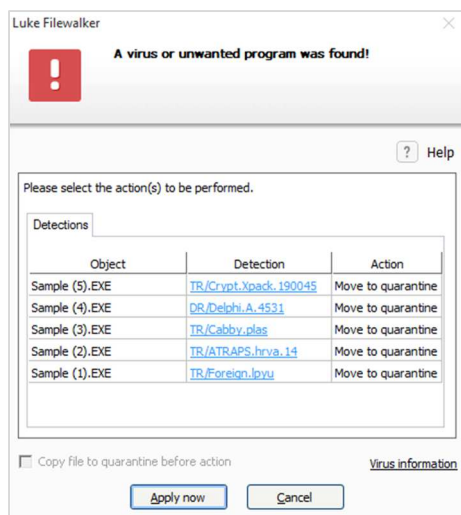
Clicking *Apply now* quarantines the malware found.

Additional comments

Clicking the System Tray icon (left-click) displays the *Avira Launcher*:
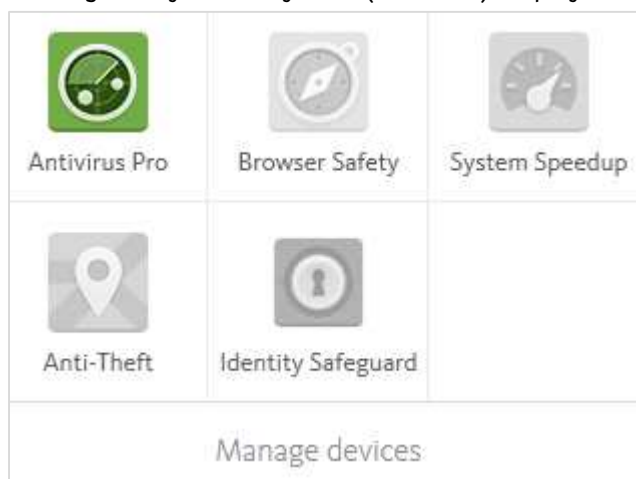
Manage Devices opens Avira's web management console, which allows administration of all registered Avira products. *Browser Safety* is a free plug-in for Windows browsers, which unfortunately does not work with Internet Explorer under Windows 10[8]. *System Speedup* is a system optimizer for Windows, which is installed as a trial version, and can be used only once before the user has to pay for it. Both *Anti-Theft* and *Identity Safeguard* are for products for mobile operating systems (Android/iOS).

---

[8] https://www.avira.com/en/support-for-home-knowledgebase-detail/kbid/1777

Baidu Antivirus 5.4.3 (International/English version)
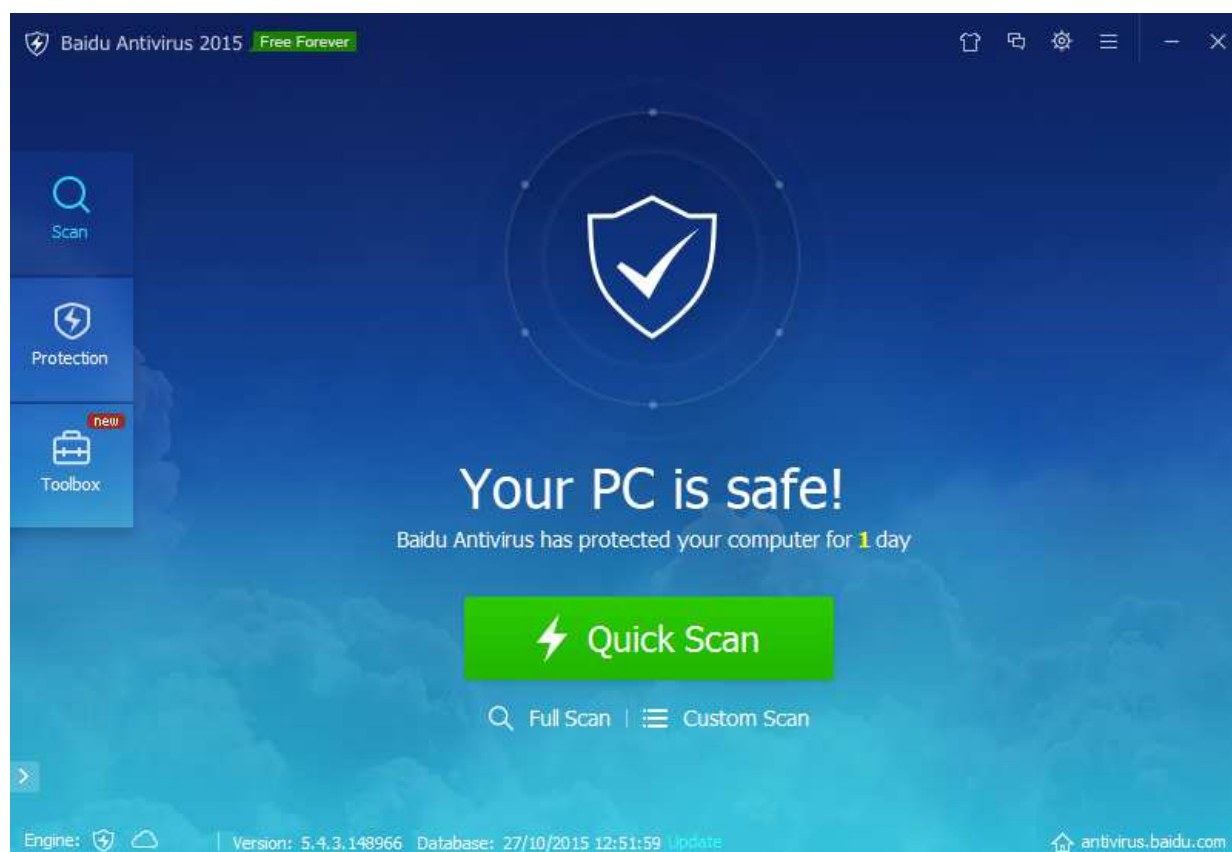
Supported operating systems
Windows XP, Vista, 7, 8, all 32 and 64-bit

Note about Windows 10 compatibility
We feel that the information about the Windows versions supported is not very prominent, as it is at the bottom of the program's FAQ page. We note that Baidu Antivirus can be installed under Windows 10 without any obvious problems or error messages. However, our Windows 10 compatibility test showed that the program does not provide adequate protection with this operating system, and that malware (even samples for which the program has definitions) can be copied to the PC, and even executed, without Baidu providing any sort of warning.

Due to the incompatibility with Windows 10, we have tested the program on Windows 8.1 for the purposes of this review. Baidu informed us that they currently have no plans to develop the international English version further, and so only the Chinese-language version will be made compatible with Windows 10.

Firewall
Baidu Antivirus uses Windows Firewall.

Third-party components

The international English version of Baidu Antivirus includes some scanning components provided by Avira.

Product page on vendor's website

http://antivirus.baidu.com/en/

Help

There is a forum on the manufacturer's website.[9] An FAQ page is also provided[10]; this is accessed by clicking *PC Knowledge* on the program's home page.

Good points

The program's interface is largely clean and easy to navigate. We liked the ability to change the interface language very quickly and simply.

Suggestions for improvement

We feel that if a user attempts to install the program under Windows 10, the setup program should warn that it is not compatible with this OS. Additionally, the download page itself should make clear which operating systems are supported.

If (under a supported operating system) the real-time protection is disabled, the program should report appropriately to Windows Security Center that both antispyware and antivirus components are disabled.

Installation, deinstallation, deactivation

Installation options

The interface language can be changed; there is also a custom installation option, which lets the user choose the location of the installation folder, and whether to join the *User Experience Program* (the default setting is not to do so).

Deinstallation options

There are none, although Baidu attempts to persuade the user not to uninstall the product:

---

[9] http://forum.antivirus.baidu.com
[10] http://antivirus.baidu.com/en/computer-knowledge/list.php?category=bavfaq

Deinstallation/deactivation from a standard user account

The program cannot be installed using a non-administrator account, although it is possible to disable the protection. This can be password-protected in the settings.

Windows Security Center, Windows Defender

In our test, we found that if real-time protection is disabled, Windows Security Center reports that only spyware protection is turned off:
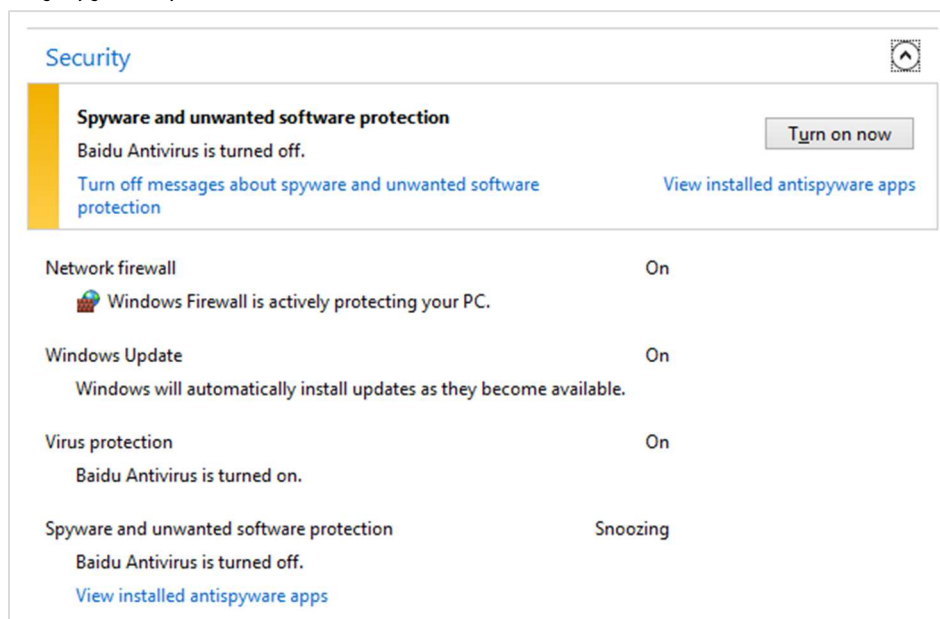
User Interface

Main program window

This includes a status display, buttons/links for three types of scan, an update link, and settings button. Logs and quarantine can be found in a small menu in the bottom left-hand corner of the window. There is a (not very prominent) update link at the bottom of the window. We could not find a help link nor button, although there is a link to the vendor's website.

System Tray menu

The System Tray icon displays the following menu – the sub-menu for real-time protection is also shown:
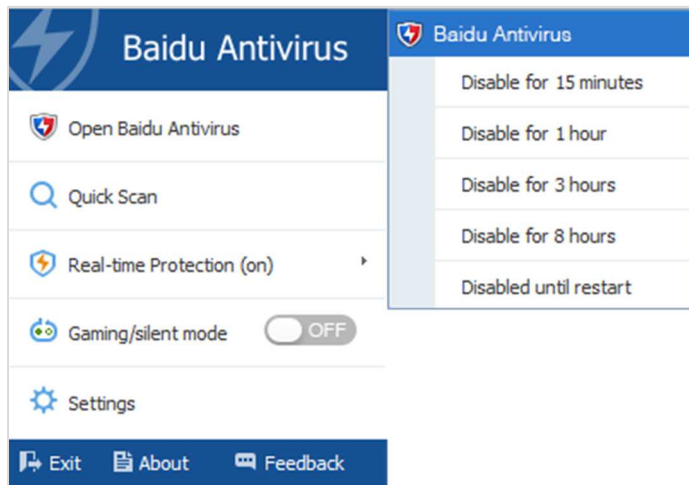
Windows Explorer context menu

The following entries are added to the menu shown when a file, folder or drive is right-clicked in Windows Explorer:
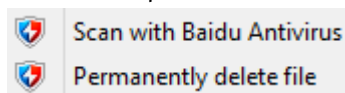
The *Permanently delete file* entry is a secure delete function.

Internet Explorer

Toolbar, search service, search ratings

Baidu does not add a toolbar to Internet Explorer, change the search service or add search ratings.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

The user only needs to click *Get Full Protection* to reactivate the component.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown:
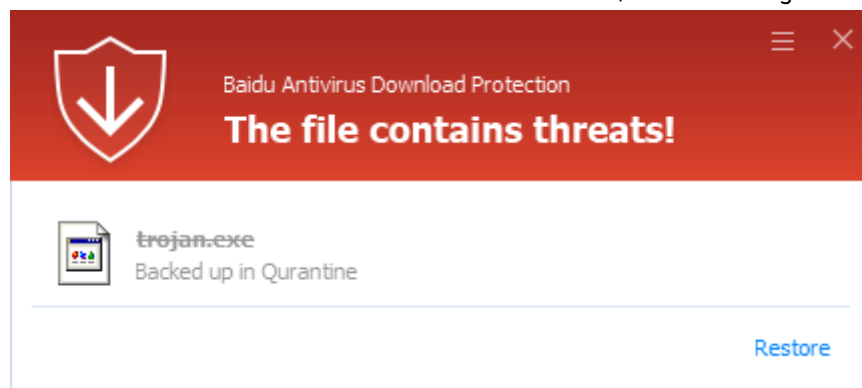
No user action is required.

USB on-access

If a USB flash drive containing malware is connected to the PC, a scan is run automatically. The action taken is thus identical to that for an on-demand scan, described below.

USB on-demand

Running an on-demand scan of a flash drive containing malware produces this warning:
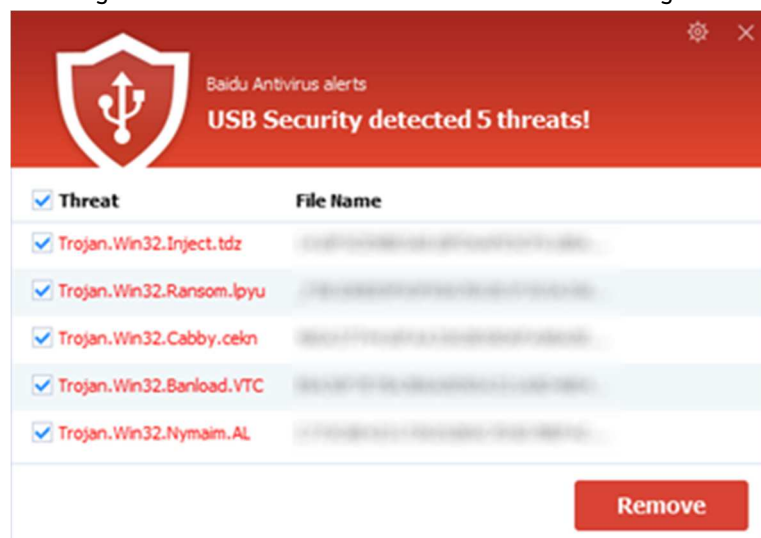
The user simply has to click on *Remove*.

Additional comments

The user can change the interface language from the menu (three horizontal lines) in the top right-hand corner of the window. It is also possible to change the theme (background picture) of the main window, from a button at the top of the window, which looks to us like a T-shirt.

Bitdefender Internet Security 2016

Supported operating systems

Windows 7, 8, 8.1, 10

Firewall

Bitdefender Internet Security includes its own firewall.

Product page on vendor's website

http://www.bitdefender.com/solutions/internet-security.html

Help

The *Help & Support* link in the program's menu has links to a searchable online manual[11] and knowledge base[12].

Good points

We found Bitdefender's almost instantaneous proactive detection of malware on a USB flash drive to be excellent. The interface is very straightforward to navigate, and the main program window makes important functions and information easy to find.

---

[11] http://www.bitdefender.com/media/materials/user-guide/en-US/InternetSecurity/current/html/index.html
[12] http://www.bitdefender.com/support/internet-security-2016/functionality.html

Suggestions for improvement
We feel that if the product's own firewall is disabled, Windows Firewall should be reactivated.

Installation, deinstallation, deactivation
Installation options
The user can decide whether to send anonymous usage reports to Bitdefender. A custom installation option is available, which additionally allows the choice of installation folder location and proxy settings.

Deinstallation options
There is a repair option in addition to removal.

Deinstallation/deactivation from a standard user account
 The product cannot be uninstalled or disabled without entering administrator credentials.

Windows Security Center, Windows Defender
If the Bitdefender Firewall is disabled, an alert is shown in Windows Security Center, but Windows Firewall is not reactivated.

User Interface
Main program window
The home page provides a status display, update and scans buttons, and licence information. The menu, accessed from the symbol to the left of the minimise button, has links to help and logs (*Events*). Quarantine and settings can both be accessed from the *Modules* button in the bottom left-hand corner of the window.

System Tray menu
The System Tray icon shows the following menu:
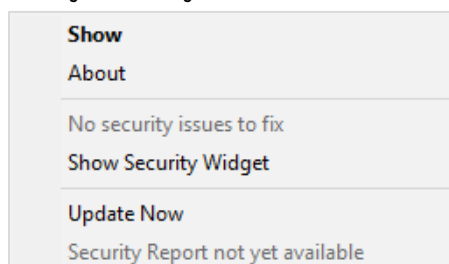
> **Show**
> About
>
> No security issues to fix
> **Show Security Widget**
>
> **Update Now**
> Security Report not yet available

Windows Explorer context menu

The following entries are added to the menu shown when a file is right-clicked in Windows Explorer:
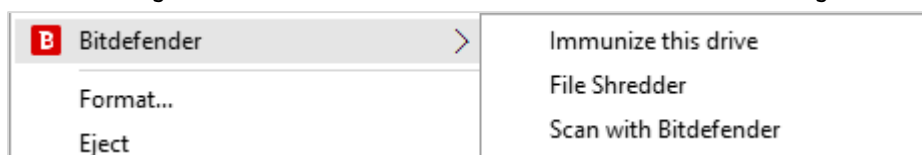
The *Immunize this drive* entry can be used to disable autorun on a USB drive, while *File Shredder* can be used to securely delete sensitive data.

Internet Explorer

Toolbar

A toolbar for Bitdefender Wallet (password manager) is added to Internet Explorer.

Search service

The default search service in Internet Explorer is not changed.

Search ratings

Security ratings are applied to web searches by means of an icon at the beginning of each entry:
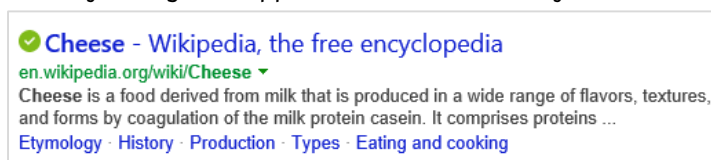
Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:
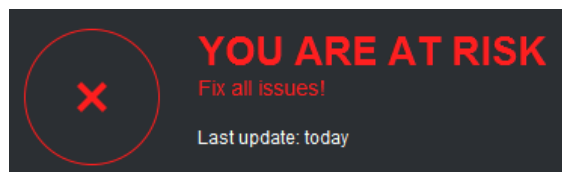
Clicking *Fix all issues* allows the user to reactivate the protection. A similar alert and fix button are displayed if the firewall is disabled.

Malware alerts

Web

If malware is downloaded using a web browser, the following alert is shown as a web page in the browser window:
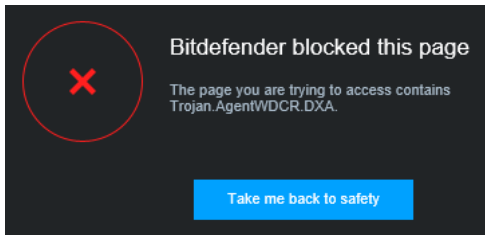
No additional action is required; clicking *Take me back to safety* will go back to the previous web page.

USB on-access

If a USB flash drive containing malware is connected to the PC, Bitdefender displays the following alert after just a couple of seconds:
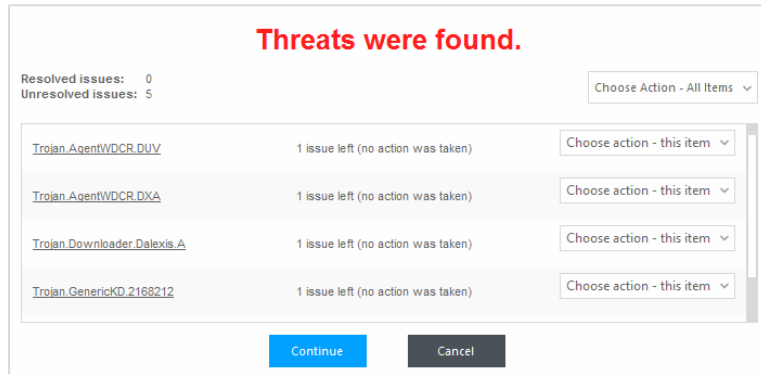
The user needs to choose an action for individual items or all items, the choices being *Take proper actions, Delete,* and *Take no action*. Clicking *Continue* will then carry out the user's choice.

USB on-demand

An on-demand scan of a USB flash drive containing malware brings up the same dialog box as for on-access, shown above.

Additional comments

The user has to create a "Bitdefender Central" account to access the product's interface.

BullGuard Internet Security 15.1
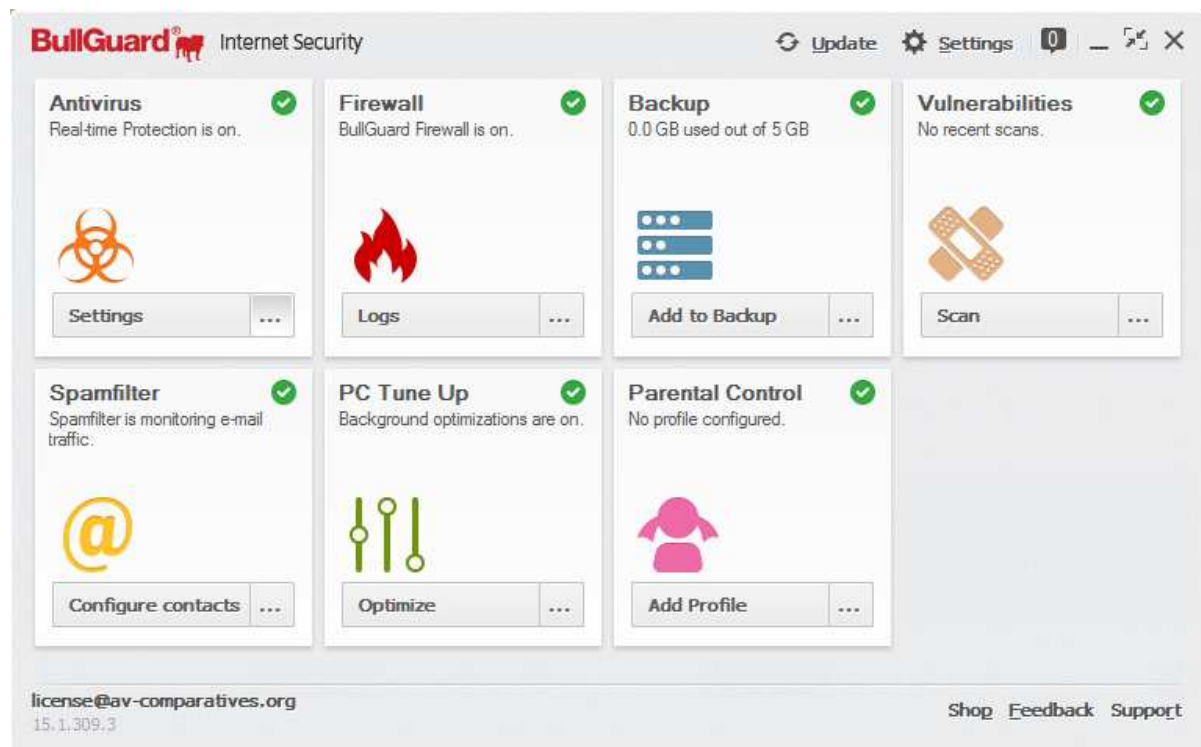
Supported operating systems

Windows XP, Vista, 7, 8, 8.1, 10

Firewall

BullGuard Internet Security provides its own firewall; this is an addition to, rather than a replacement of, the Windows Firewall.

Third-party protection components

BullGuard Internet Security includes some malware-protection components provided by Bitdefender.

Product page on vendor's website

https://www.bullguard.com/products/bullguard-internet-security.aspx

Help

The *Support* link on the home page opens the product's online support page[13].

Good points

We found BullGuard Internet Security to be largely well designed and easy to use. We particularly liked the automatic scanning of USB drives.

---

[13] https://www.bullguard.com/support/product-guides/bullguard-desktop-protection-guides/getting-started.aspx

Suggestions for improvement

A minor improvement might be to add a dedicated "Scan" button, as it is not immediately obvious how to run a scan from the program's home page. It would also be helpful if licence expiry information were displayed on the home page.

Installation, deinstallation, deactivation

Installation options

There are no choices to be made during setup.

Deinstallation options

The user can choose to retain settings when uninstalling the product.

Deinstallation/deactivation from a standard user account

A standard user cannot uninstall the program without entering Windows administrator credentials. During setup, the user is prompted to enter a password, which must be entered to change any settings (such as disabling protection).

Windows Security Center, Windows Defender

The setup process does not disable Windows Firewall, which then runs in parallel with the product's own firewall. BullGuard informed us that this is by design, and that the two firewalls are entirely compatible.

User Interface

Main program window

An overall status display is shown for a few seconds when the program window is first opened. The home page shows status for individual components, plus buttons for help (*Support*), updates, settings, and logs (button between settings and minimise buttons).

System Tray menu
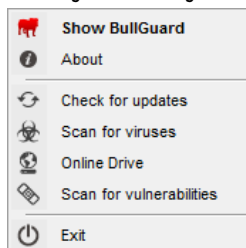
The System Tray icon displays the following menu:

Windows Explorer context menu

The following entries are added to the menu shown when a file is right-clicked in Windows Explorer:


The context menu also allows files or folders to be backed up.

Internet Explorer

Toolbar

BullGuard does not add a toolbar to Internet Explorer.

Search service

The default search service in Internet Explorer is not changed.

Search ratings

Bing search results show security ratings in the form of an icon before each page title:

BullGuard informed us that these are also applied to Google and Yahoo searches, and Facebook content.

Status alerts

Real-time protection and Firewall

If either of these protection components is disabled, the following alert is shown in the respective tile in the main window:

In either case, the user simply has to click *Enable* to reactivate the protection.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown:

No user action is required.

User-dependent test cases

In a number of the Real-World Protection Tests this year, BullGuard Internet Security produced a significant number of user-dependent decisions. The alert displayed in such cases is shown below. However, we note that as of October this year, the program no longer shows such alerts, but rather blocks the malware automatically.

USB on-access

If a USB flash drive is connected to the PC, a scan is started automatically, so the result is the same as for an on-demand scan.

USB on-demand

Running an on-demand scan of a flash drive containing malware produces this warning:
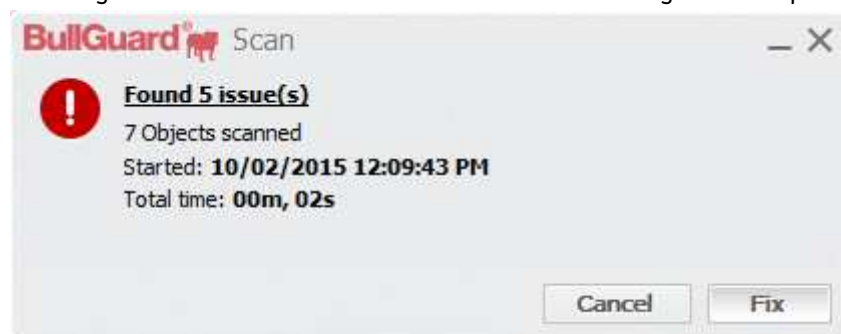
The user merely has to click *Fix* to remove the threats.

Additional comments

The setup wizard introduces the user to some of the program's features, such as backup, spam filter, vulnerability scanner, parental control and *PC TuneUp:*

Emsisoft Anti-Malware 11.0
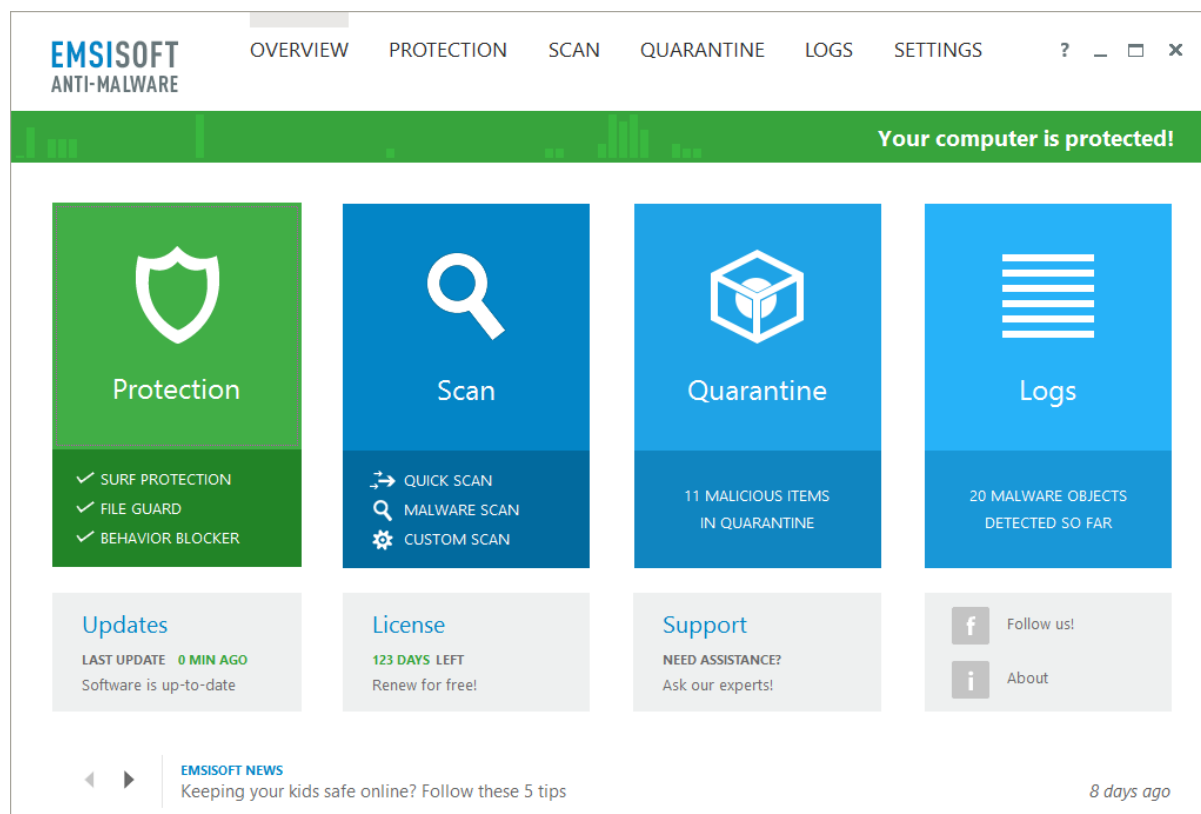
Supported operating systems

Windows 7, 8, 10

Firewall

Emsisoft Anti-Malware doesn't come with a firewall.

Third-party components

Emsisoft Anti-Malware includes some scanning components provided by Bitdefender.

Product page on vendor's website

http://www.emsisoft.com/en/software/antimalware/

Help

Clicking the *?* symbol in the top right-hand corner of the window opens a local help file. An online forum is also provided[14].

---

[14] http://support.emsisoft.com/

Good points

The program's modern interface makes all important functions and information easily accessible from the home page. We also liked the information and explanations provided by the setup wizard, such as the illustration of PUAs and advice on updating/scanning/checking real-time protection, and feel these would be very helpful to non-expert users.

Suggestions for improvement

We feel that the *Thorough* setting for *File Guard* (real-time file-system protection) would be more suitable for non-expert users than the default *Balanced* setting.

Installation, deinstallation, deactivation

Installation options

The setup wizard lets the user choose whether to join the *Emsisoft Anti-Malware Network* data-sharing scheme. There is also a choice as to whether to enable detection of PUAs.

Deinstallation options

There are none.

Deinstallation/deactivation from a standard user account

A standard Windows user cannot uninstall the product without entering administrator credentials. It is possible to disable the protection as a standard user, however.

Windows Security Center, Windows Defender

Emsisoft Anti-Malware integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window

The home page of the program includes a detailed status display, and buttons/links for updates, 3 types of scan, help, logs, quarantine and settings. Licence information is also displayed.

System Tray menu

The System Tray icon displays the following menu:
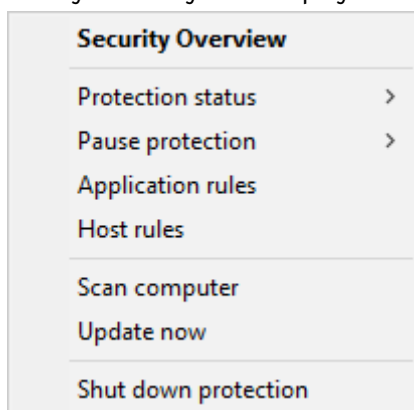
Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:
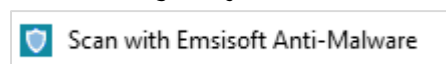
Internet Explorer

Toolbar, search service, search ratings

Emsisoft Anti-Malware does not make any modifications to Internet Explorer or its default search service, or provide ratings for search results.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:
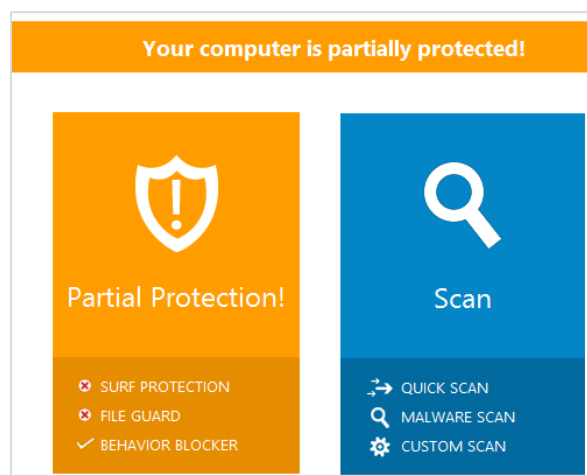
To reactivate protection, the user has to click on each of the sub-components shown as disabled; this opens a dialog box for the sub-component, from which protection can be reactivated.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown:
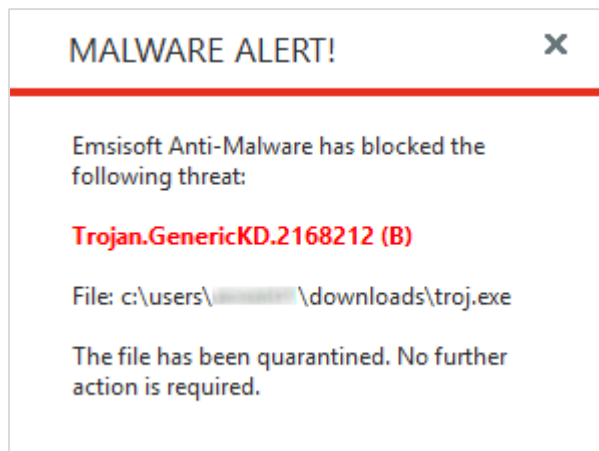
No user action is required.

User-dependent test cases

In a number of the Real-World Protection Tests this year, Emsisoft Anti-Malware produced a significant number of user-dependent decisions. The alert displayed in such cases is shown below.
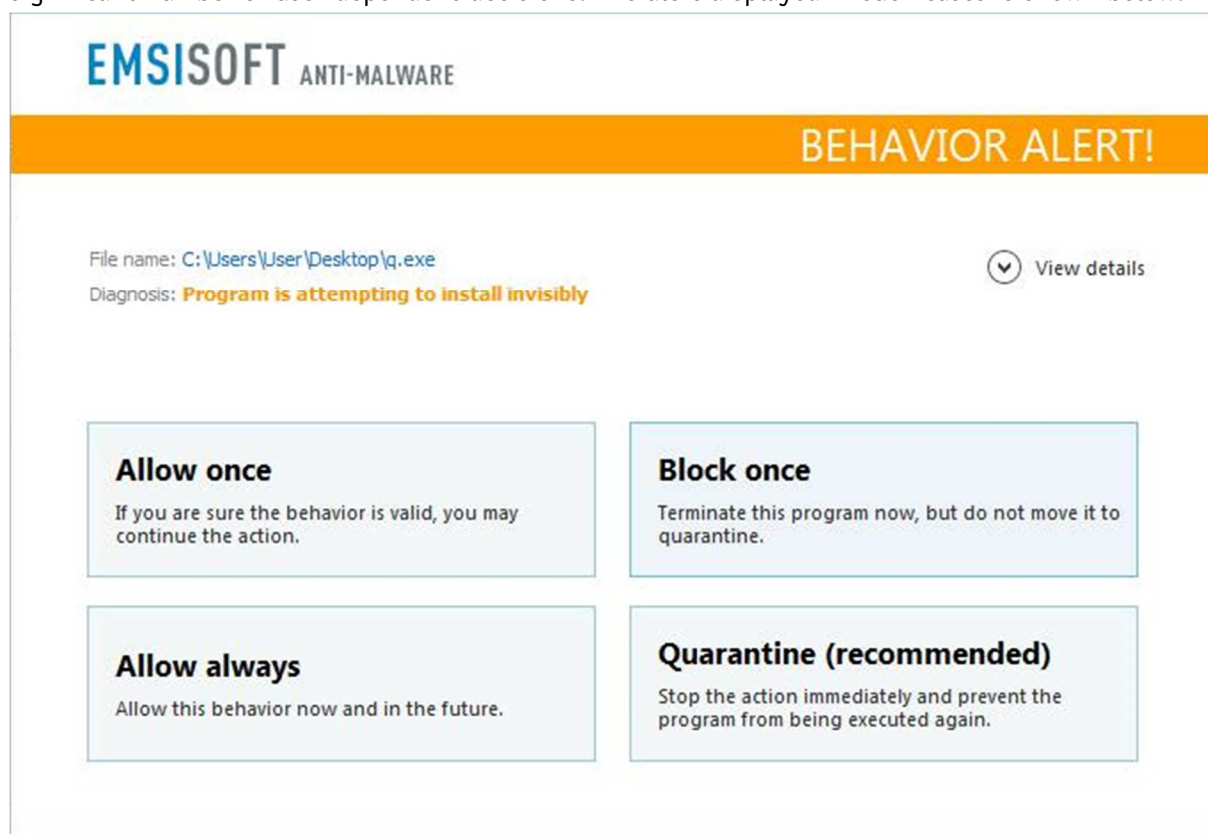
USB on-access

When testing Emsisoft Anti-Malware with default settings, we found that it was possible to copy malware from a USB flash drive to the Desktop. After a few seconds, the malware on the desktop was detected and deleted by Emsisoft Anti-Malware, which displayed the following alert:
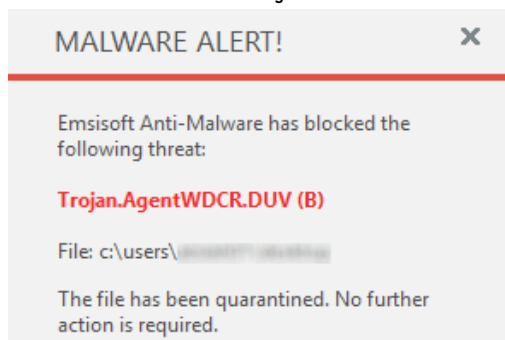
No user action was required to remove the copied malware on the desktop. However, the malware on the flash drive was not detected by the real-time protection.

We also found that it was possible to copy a few malware samples from a network drive onto a flash drive, and then immediately pull the flash drive out of the PC (without using Windows' *Safely Eject Hardware* function) with all the samples intact. If the flash drive is not removed immediately after copying is complete, the malware is detected and deleted after a few seconds.

Emsisoft informed us that switching the program's *File Guard* settings to *Thorough – Scan files when they are read* will immediately detect the malware and prevent it being copied at all. We were able to verify this in an additional test.

USB on-demand

Running an on-demand scan of a flash drive containing malware displays this dialog:
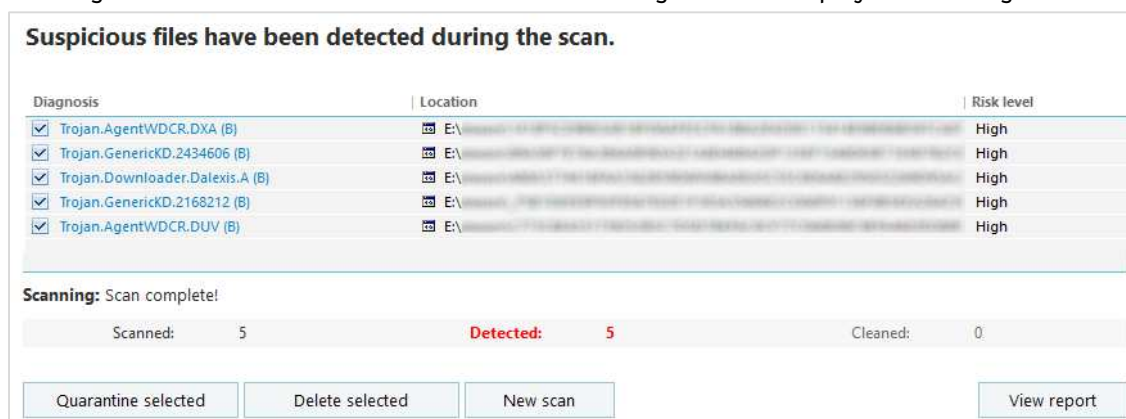
The user can choose to quarantine or delete the selected files. If *Delete* is chosen, Emsisoft displays a confirmation prompt:

Emsisoft Anti-Malware   ✕

Do you really want to delete the selected objects? If you aren't sure that these objects are unwanted, please use Quarantine instead, as deleted objects can not be recovered. Delete now?

[Yes]   [No]
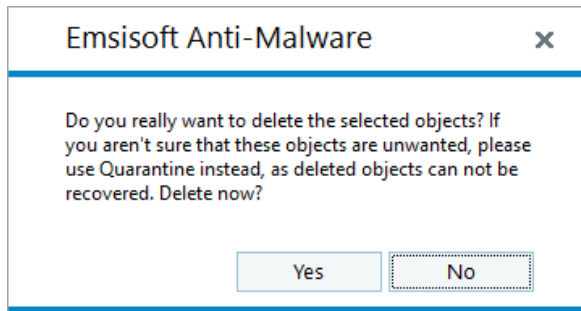
Additional comments

The setup wizard provides quite comprehensive explanations of the Emsisoft Anti-Malware Network, signature updates and their importance, and PUAs, the latter being illustrated with a picture of a browser window overloaded with multiple add-on toolbars. There is also an illustrated explanation of how to run scans and check that real-time protection is active:
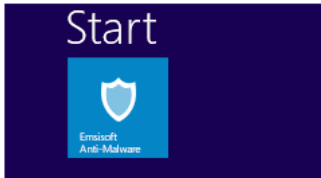
Your computer is protected now!

Emsisoft Anti-Malware is now ready to protect your computer from viruses, trojans, bots, rootkits, worms, spyware and all other sorts of malicious software.

Important: Ensure that the Emsisoft Anti-Malware real-time protection is always active!

How can I scan my drives?

On the windows start screen, locate the group of Emsisoft Anti-Malware tiles and select the "Emsisoft Anti-Malware" tile. Ensure that all available online updates are installed and scan the hard disk for Malware using the Scanner.

Start

Emsisoft Anti-Malware

How do I know that real-time protection is active?

The Emsisoft Anti-Malware real-time protection is active if you can see the Emsisoft Anti-Malware shield icon next to your system clock in taskbar. Right click on the icon to get a little menu with shortcuts to the most important components of the software.

17:17
18.02.2014

eScan Internet Security Suite 14.0

Supported operating systems

Windows XP, Vista, 7, 8, 8.1, 10

Firewall

eScan Internet Security Suite includes its own firewall.

Third-party components

eScan Internet Security includes some scanning components provided by Bitdefender.

Product page on vendor's website

http://www.escanav.com/en/windows-antivirus/internet-security-suite.asp#systemsupport

Help
Clicking the *?* symbol in the top right-hand corner of the main window displays a link to the program's online help[15].

Good points
We liked the clear, tiled layout of the homepage, and the automatic scan of USB drives, which quarantines any malware found without user interaction.

Suggestions for improvement
We feel that if a protection component (real-time protection or firewall) is disabled, the relevant Windows component (Windows Defender or Windows Firewall) should be reactivated to ensure the system remains protected.

Installation, deinstallation, deactivation
Installation options
There are none.

Deinstallation options
There are none.

Deinstallation/deactivation from a standard user account
The software cannot be deactivated or uninstalled without entering administrator credentials.

Windows Security Center, Windows Defender
If eScan's antivirus component is disabled, Windows Defender is not automatically reactivated. Likewise, Windows Firewall is not switched on again if the eScan firewall is turned off. This state persists even after a system restart.

---

15 http://wiki.escanav.com/wiki/index.php/Escan/english/escan14/epc
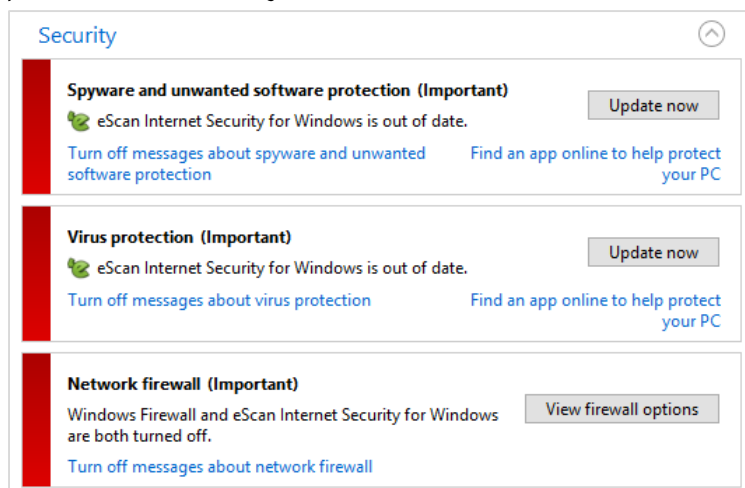
User Interface

Main program window

The home page of the program includes status displays for each of the individual protection components, as well as scan, update and helps buttons, and links to logs (*Reports*) and licence information. Quarantine can be found by clicking the *file anti-virus* tile, then *View quarantine objects*.

System Tray menu
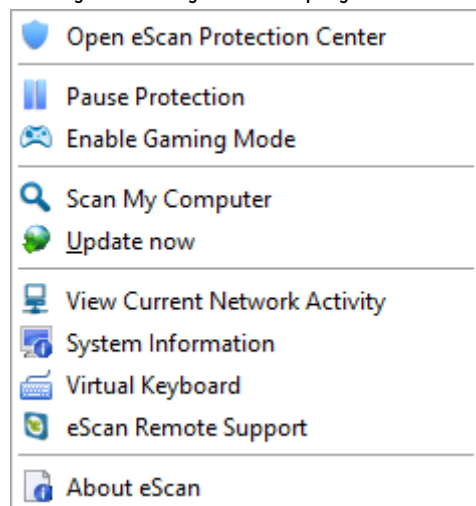
The System Tray icon displays the following menu:

Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:
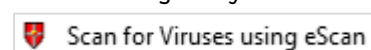

Internet Explorer

Toolbar, search service, search ratings

No changes are made to Internet Explorer or the search service. Search ratings are not displayed in eScan's Internet Security product.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:
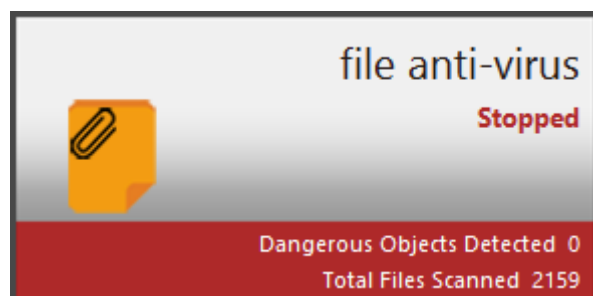
The protection can be reactivated by clicking the *file anti-virus* tile, and then *Start* in the subsequent dialog box:

Configuration	
File Anti-Virus Status	Stopped
Proactive Behaviour Monitor Status	Enabled
Action	Disinfect - Quarantine object
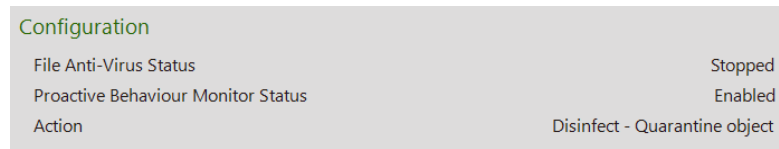
Firewall

A similar alert and reactivation process are provided if the eScan firewall is disabled.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown:
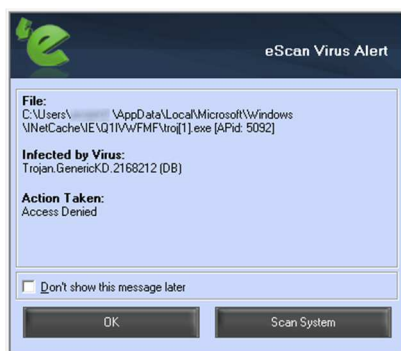
The user only needs to click *OK* to close the alert.

USB on-access/on-demand

If a USB flash drive is connected to the PC, eScan automatically runs a scan and quarantines any malware found:
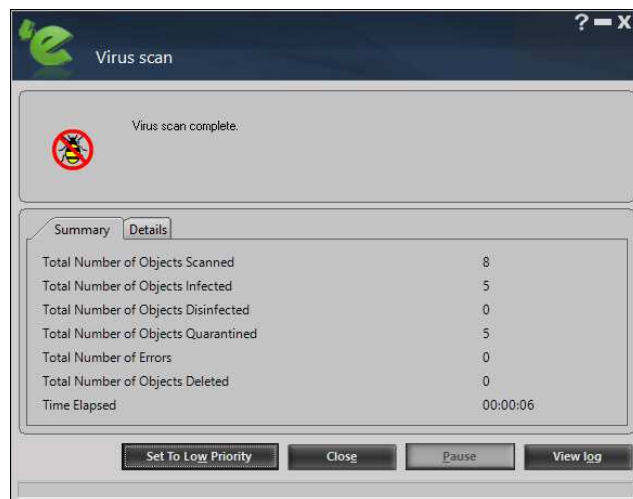
ESET Smart Security 9.0
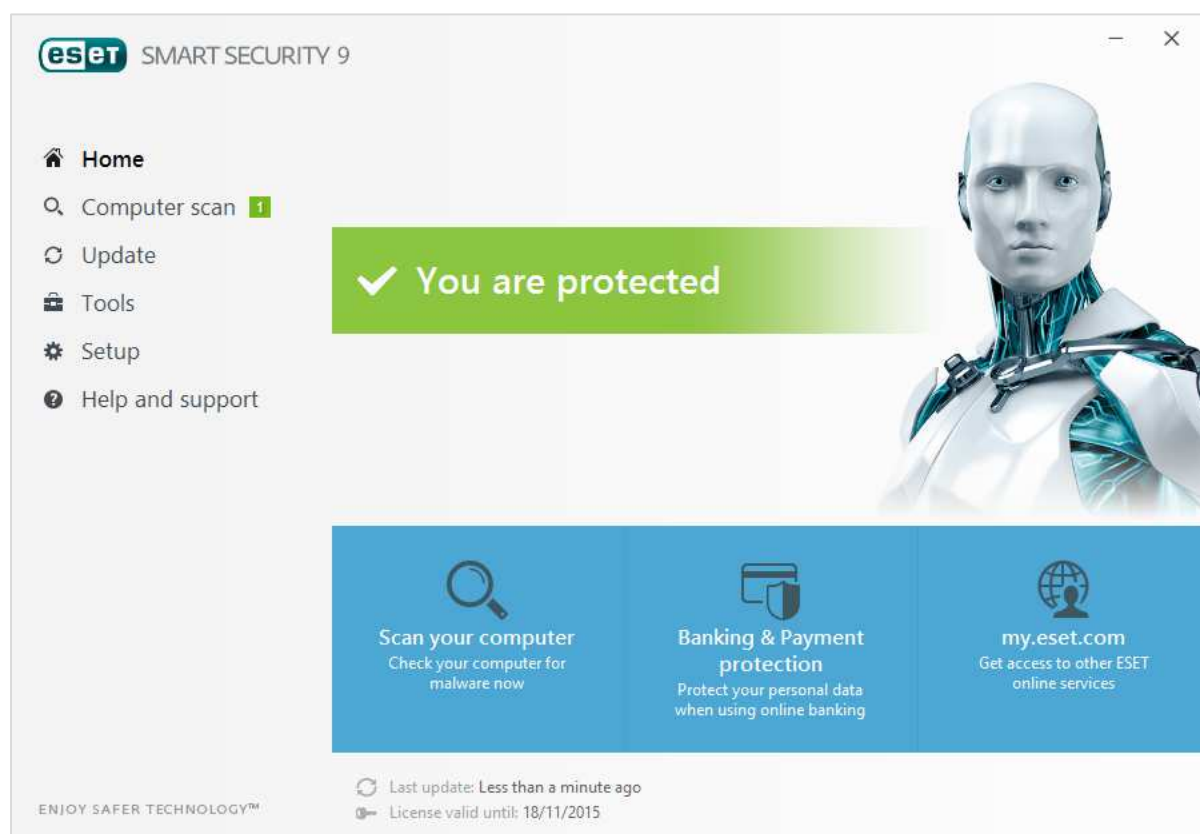
Supported operating systems

Windows XP, Vista, Home Server, 7, 8, 8.1, 10

Firewall

ESET Smart Security includes its own firewall, which is activated by default. An expert user who preferred to use Windows Firewall could neatly and cleanly disable the ESET Firewall in the advanced configuration dialog. We like the fact that ESET have made this option available to power users.

Product page on vendor's website

http://www.eset.com/int/home/products/smart-security/

Help

Two manuals are available from the product's download page[16]. There is also a searchable knowledge base[17] and local help feature.

---

[16] http://www.eset.com/int/download/home/detail/family/5/
[17] http://support.eset.com/?segment=home

Good points

ESET Smart Security 9 retains the clean, practical layout of previous versions, with a new graphic design and finger-friendly controls suitable for use on touchscreens. Documentation is comprehensive and produced to a very high standard.

Installation, deinstallation, deactivation

Installation options

Two types of installation file are provided, a live installer (downloader), and a complete installation package. We used the latter in our test. The user can choose whether to join ESET LiveGrid (data-sharing scheme) and if PUAs should be detected.

Deinstallation options

There is a repair option in addition to removal.

Deinstallation/deactivation from a standard user account

A standard user cannot deactivate protection or uninstall the product without entering administrator credentials.

Windows Security Center, Windows Defender

ESET Smart Security integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window

The home page has a status display, licence information, buttons for update, scan, help, and settings (*Setup*. Logs and quarantine can be found by clicking *Tools*.

System Tray menu
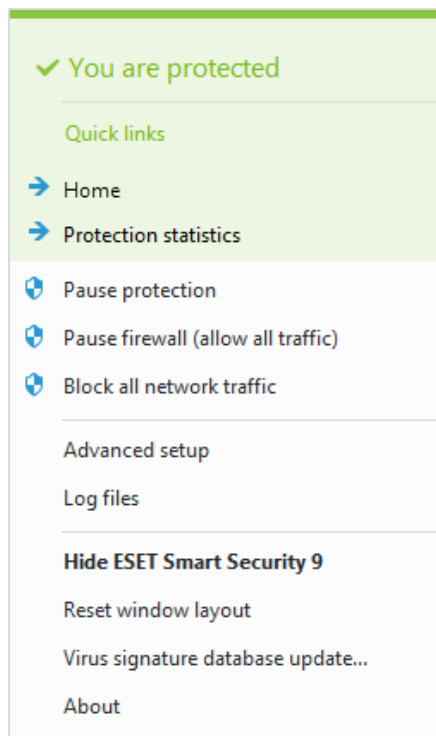
The system tray icon displays the following menu:

✔ You are protected

Quick links

→ Home

→ **Protection statistics**

🛡 Pause protection

🛡 Pause firewall (allow all traffic)

🛡 Block all network traffic

Advanced setup

Log files

Hide ESET Smart Security 9

Reset window layout

Virus signature database update...

About

Windows Explorer context menu

The following entries are added to the menu shown when a file is right-clicked in Windows Explorer:
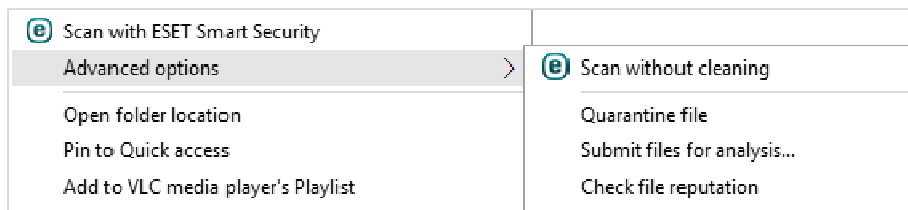
## Internet Explorer

Toolbar, search service, search ratings

No changes are made to Internet Explorer or the search service, and search ratings are not shown.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert[18] is shown in the status section of the main window:
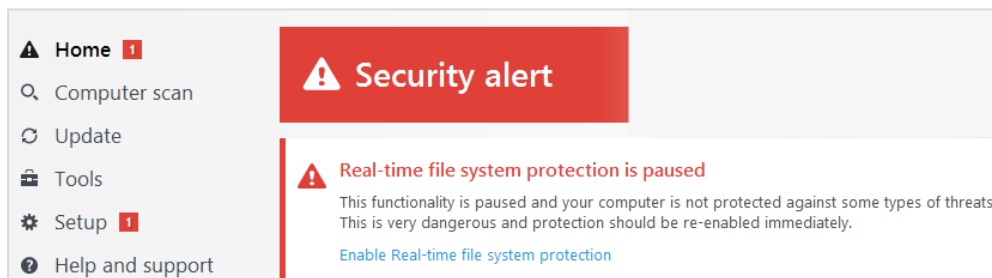
To reactivate the protection, the user just needs to click *Enable Real-time file system protection*.

Firewall

Similar alerts/reactivation link are shown if the firewall is disabled.

Malware alerts

Web

If malware is detected in a download, the following alert is shown:
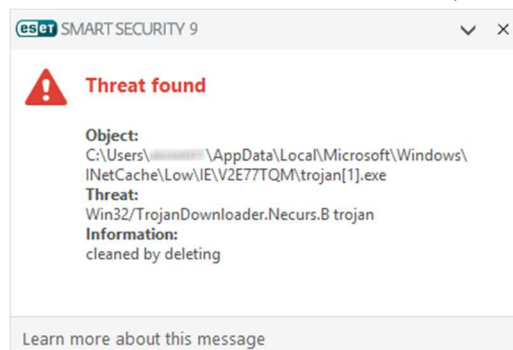
No user action is required.

---

[18] For convenience, we have removed some empty space between items in this screenshot

USB on-access

If malware on a flash drive is detected by real-time protection, the alert below is shown:
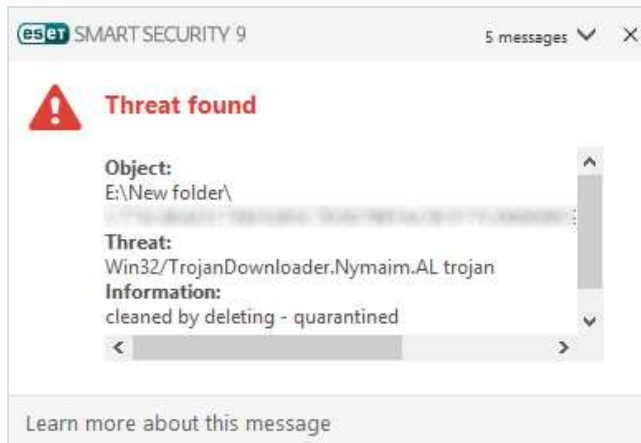
No user action is required.

USB on-demand

If a USB flash drive containing malware is scanned, the following report is shown in the main program window:
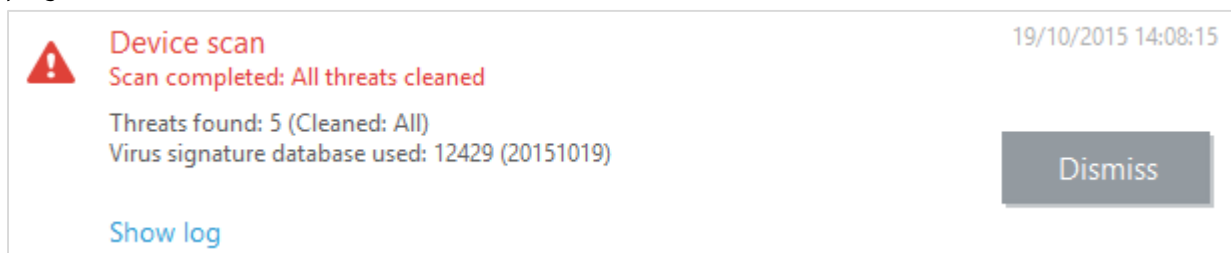
No user action is required.

Additional comments

After installation, the program asks the user whether the current network should be regarded as private or public (so as to configure the firewall appropriately). The product also has to be activated; users with an existing licence in username/password format have to convert this to a new format (product key), but this is easily and quickly done using the link in the activation dialog box.

F-Secure Internet Security 16.0
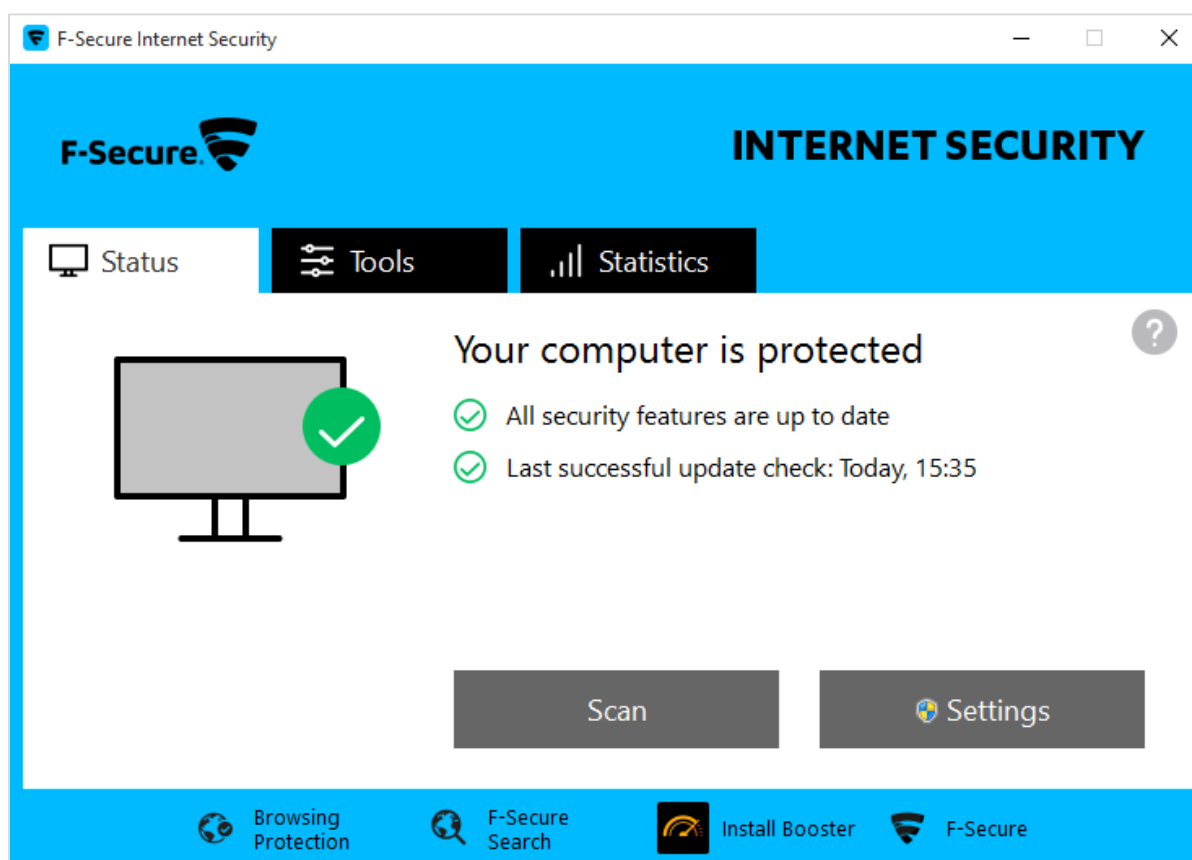
Supported operating systems
Window XP (32-bit only); Windows Vista, 7, 8, 8.1, 10

Firewall
F-Secure Internet Security uses Windows Firewall.

Third-party protection components
F-Secure Internet Security uses some protection components provided by Bitdefender.

Product page on vendor's website
https://www.f-secure.com/en/web/home_global/internet-security

Help
A manual is provided in PDF format[19]. There is also a local help feature and an online forum[20].

Good points
We liked the status display, and clear malware warnings that persist until closed by user.

---

[19] https://www.f-secure.com/documents/10192/1068122/F-Secure_Internet_Security_2015_manual_eng.pdf
[20] https://community.f-secure.com/t5/English/ct-p/EN?skin=default

Installation, deinstallation, deactivation

Installation options

The user can choose whether to join *Security Cloud* (F-Secure's data sharing scheme).

Deinstallation options

It is possible to remove the *Browsing Protection* and *Antivirus* components independently of each other.

Deinstallation/deactivation from a standard user account

A standard user cannot deactivate or uninstall the program without entering administrator credentials.

Windows Security Center, Windows Defender

F-Secure Internet Security integrates with Windows Security Center and Windows Defender exactly as expected. We note that F-Secure Internet Security registers with Security Center simply as "Antivirus". F-Secure tell us that this is because the product is resold by e.g. some Internet service providers using their own brand names.

User Interface

Main program window

The program's home page has a status display, and buttons for scan, settings, and help. Updates and quarantine can be found on the *Tools* tab, while the *Statistics* tab provides a simple log. Licence information can be found by in the help menu (*?* symbol).

System Tray menu

The System Tray icon displays this menu:
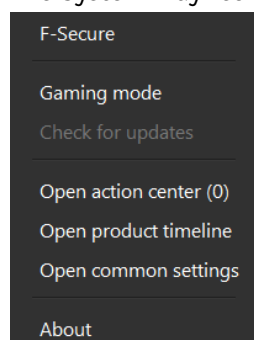
Windows Explorer context menu

The following entries are added to the menu shown when a file, folder or drive is right-clicked in Windows Explorer:
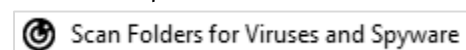
Internet Explorer

Toolbar, search service

F-Secure Internet Security does not add a toolbar to Internet Explorer or change the default search service.

Search ratings

Security ratings for search results are provided in the form of a symbol in front of the headline of each result:
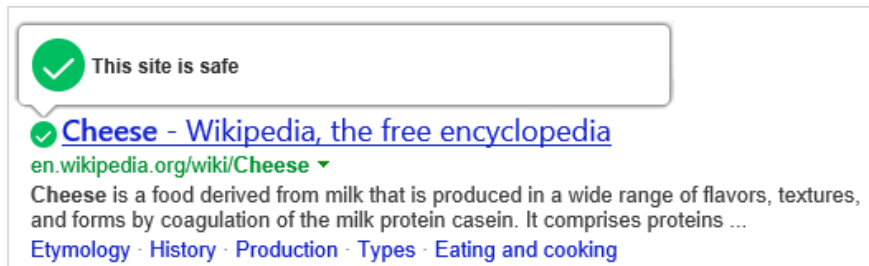
Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:
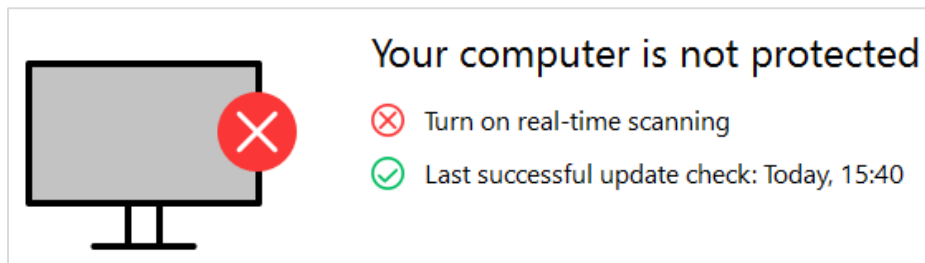
An alert is displayed in the bottom right-hand corner of the screen, with a *Turn on* button, which immediately re-enables the component:
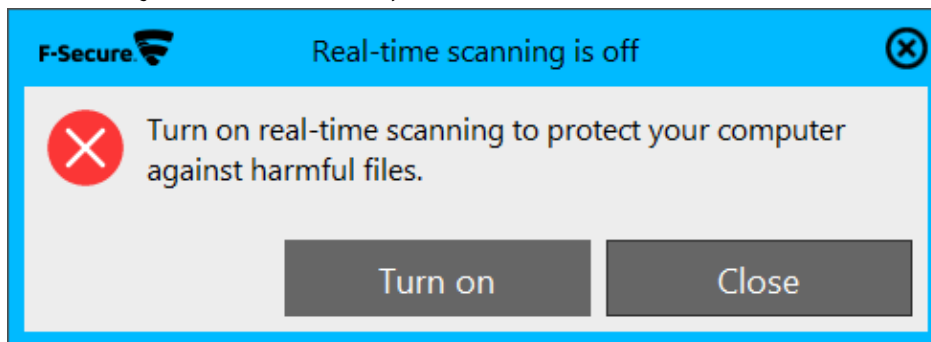
If the protection is disabled when the computer is (re)started, the same dialog box is displayed when the user logs on.

Malware alerts

Web

If malware is detected in a download, the following alert is displayed.
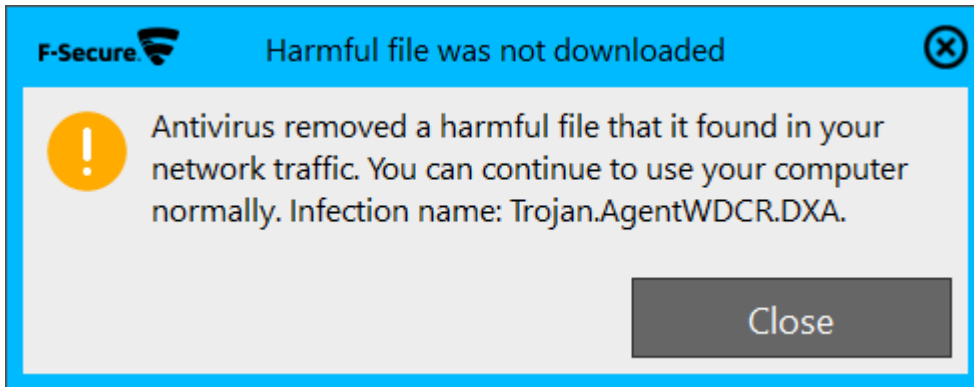
No user action is required. The alert persists until closed by the user.

User-dependent test cases

In a number of the Real-World Protection Tests this year, F-Secure Internet Security produced a significant number of user-dependent decisions. The alert displayed in such cases is shown below.
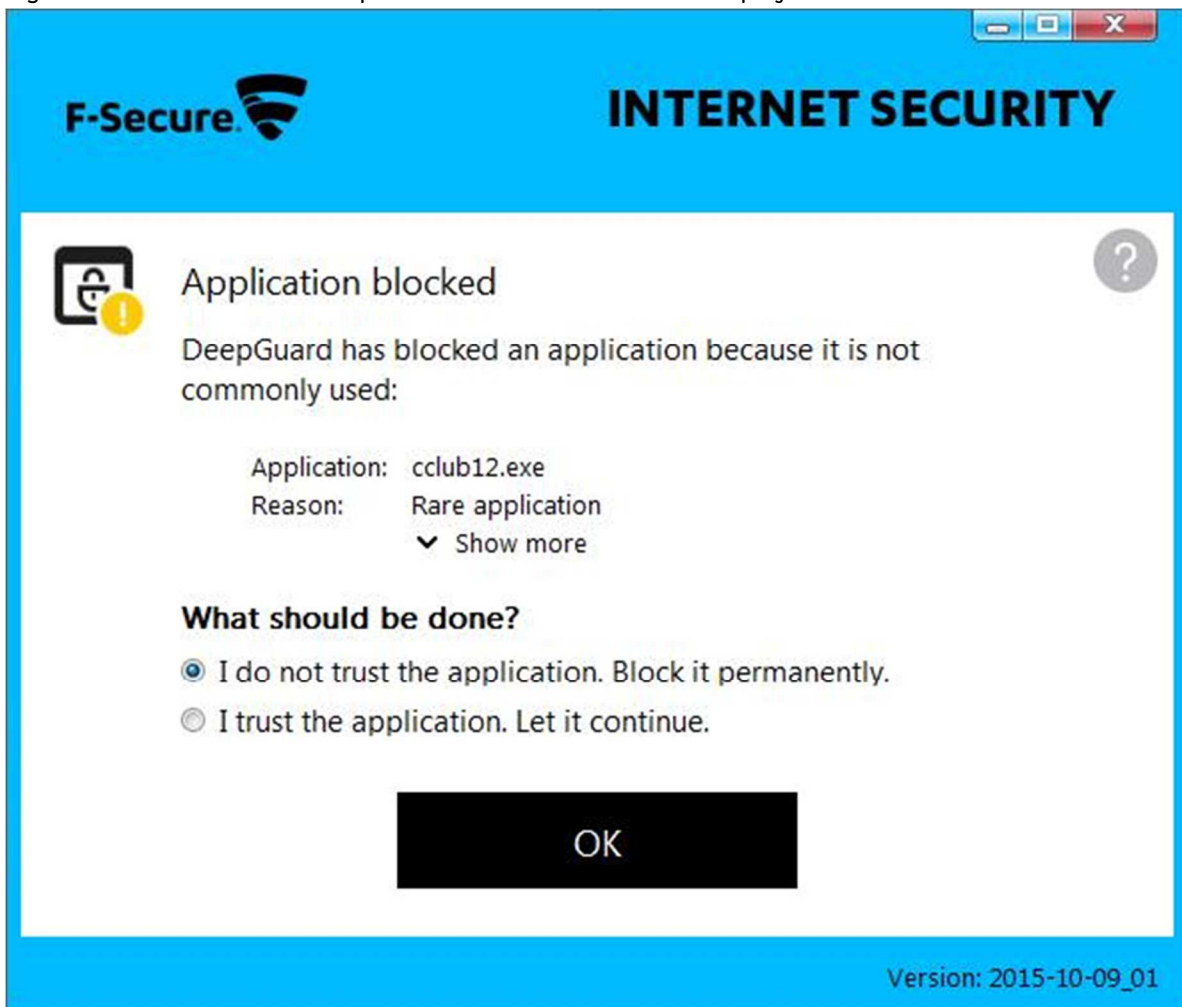
USB on-access

If a USB flash drive containing malware is viewed in Windows Explorer, the malware is automatically removed, and the following alert is shown:
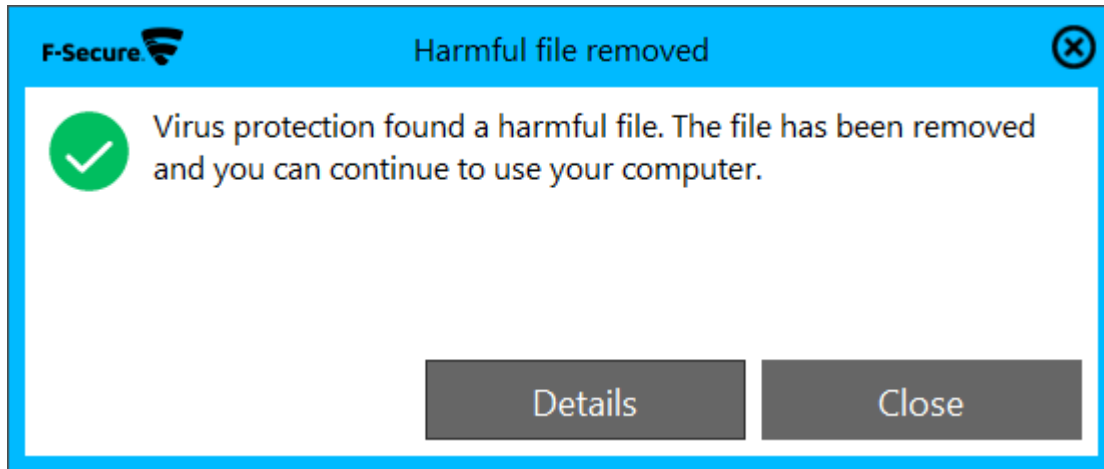
No user action is required.

USB on-demand

If malware is found on a flash drive by an on-demand scan, the following alert is shown in the main program window:
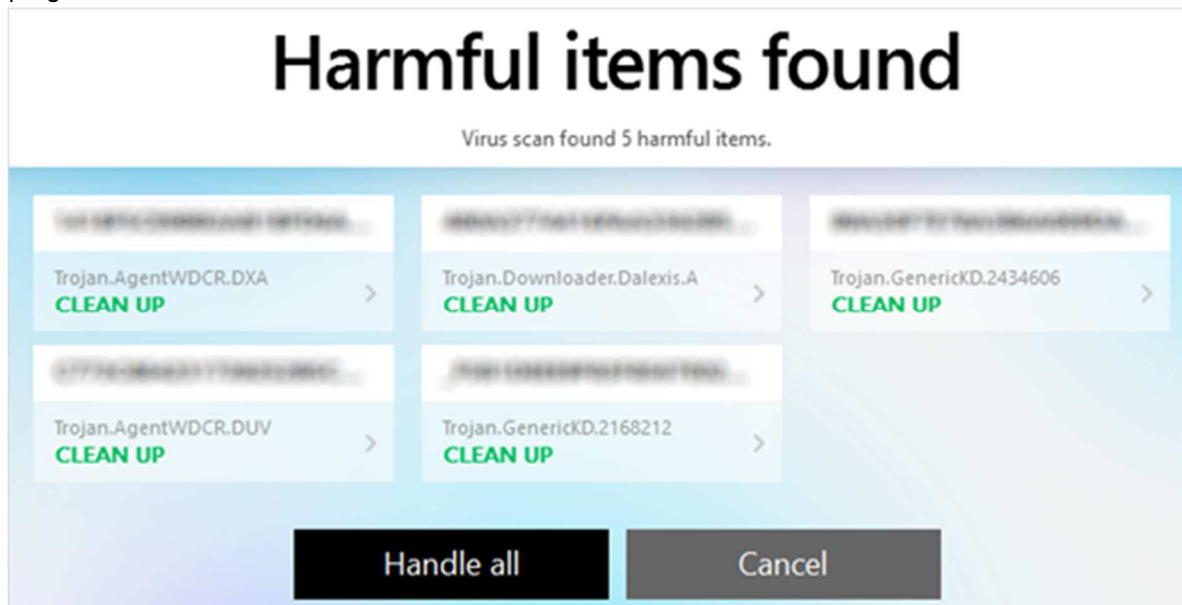
Clicking *Handle All* carries out the default action (*Clean Up*).

Additional comments

1. When the setup wizard has completed, a pop-up appears with information on network security:
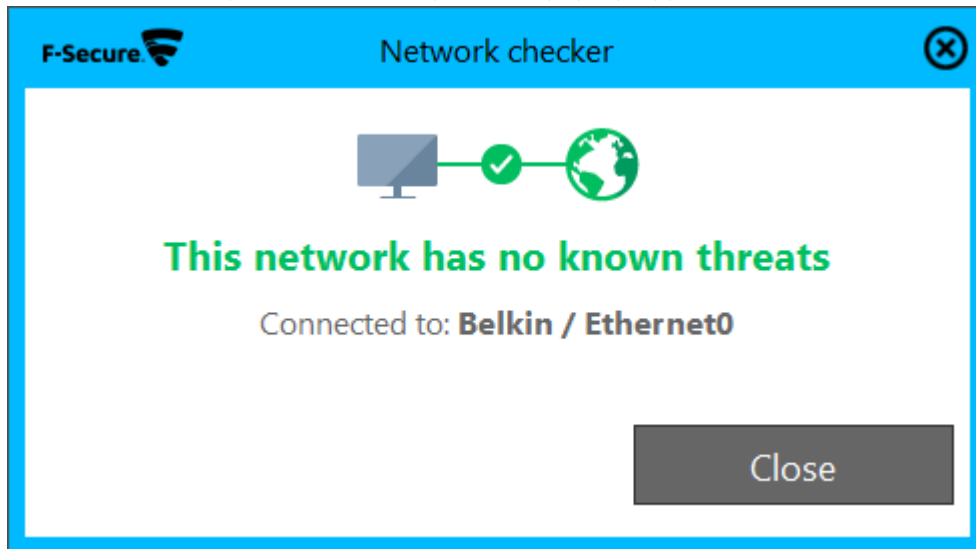
2. When we performed initial testing of F-Secure Internet Security for this review, we discovered a bug in the program, which under some circumstances could allow malware to be copied undetected from a network drive to a USB flash drive. We informed F-Secure of this, and to their credit, they immediately investigated and rectified the problem. The updated program version will be installed automatically without any user action being required.

Fortinet FortiClient 5.2.4 (with FortiGate)

Supported operating systems

Windows XP or higher

Firewall

Fortinet FortiClient uses Windows Firewall.

Note regarding the nature of the program

Fortinet FortiClient is intended for use in business networks, in conjunction with a FortiGate security appliance (which improves malware protection). Consequently, its features and interface may differ from those of a typical consumer security product. For our tests, we register the program to a FortiGate appliance.

Product page on vendor's website

http://www.forticlient.com

Help

An online knowledge base is provided[21]. This is very much oriented towards management by system administrators rather than everyday use by end users.

Good points

We feel the program's interface is suitable for its intended use in businesses. Users can see the status, and run scans and updates.

Suggestions for improvement

We wonder whether it might be possible to avoid rebooting the computer when malware is detected in a download.

Installation, deinstallation, deactivation

Installation options

The user can change the location of the installation folder.

Deinstallation options

There are none.

Deinstallation/deactivation from a standard user account

The program cannot be uninstalled or deactivated without entering administrator credentials.

Windows Security Center, Windows Defender

FortiClient integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window

There is a status display, update link and scan button on the program's home page. Logs/quarantine can be accessed from the *Threats Detected* link, also on the home page, and help functions are found in the *Help* menu. Settings can be accessed from the *File* menu.

System Tray menu

The System Tray icon displays the following menu:
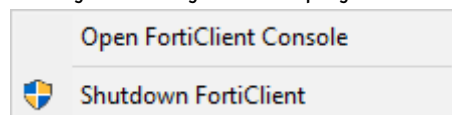
Open FortiClient Console

Shutdown FortiClient

Windows Explorer context menu

The following entries are added to the menu shown when a file, folder or drive is right-clicked in Windows Explorer:

Scan with FortiClient AntiVirus

Submit for analysis

---

[21] http://kb.fortinet.com/kb/microsites/msbrowse.do
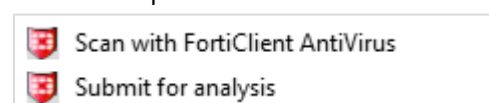
Internet Explorer

Toolbar, search service, search ratings

No modifications are made to Internet Explorer or the default search service, and search ratings are not displayed.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:
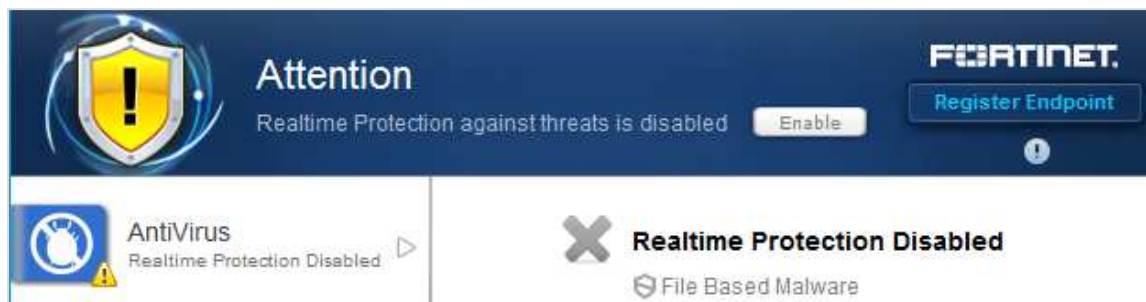
Clicking *Enable* reactivates the protection.

Malware alerts

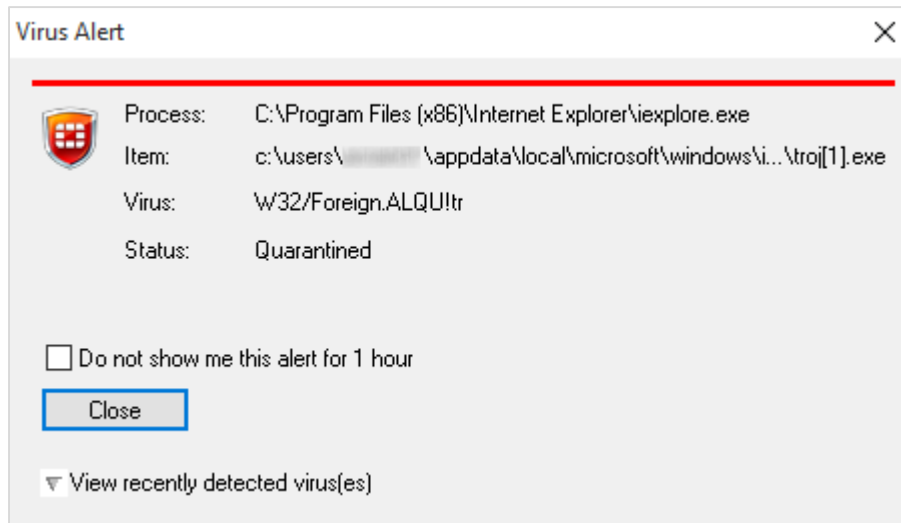### *Web*

If a malicious file is downloaded from the Internet, the following warning is shown:
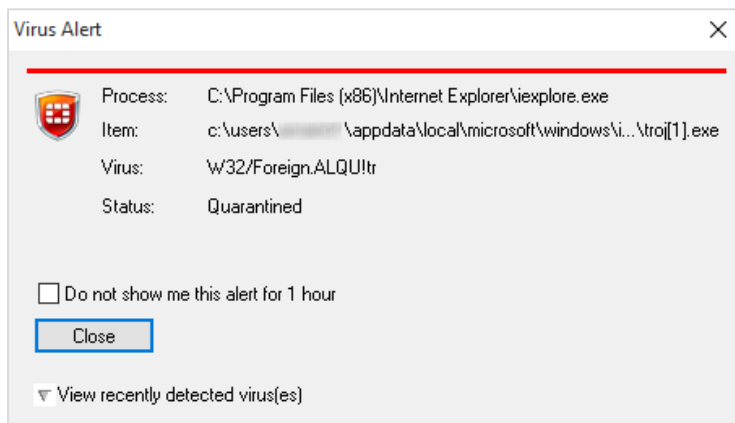
The user is then prompted to reboot the PC:
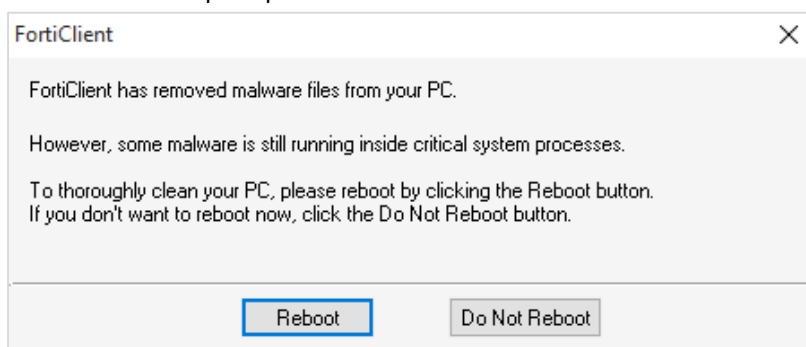
USB on-access

If the real-time protection detects malware on a USB flash drive, the alert below is displayed:

No user action is required.

USB on-demand

Running an on-demand scan of a flash drive containing malware produces this dialog:
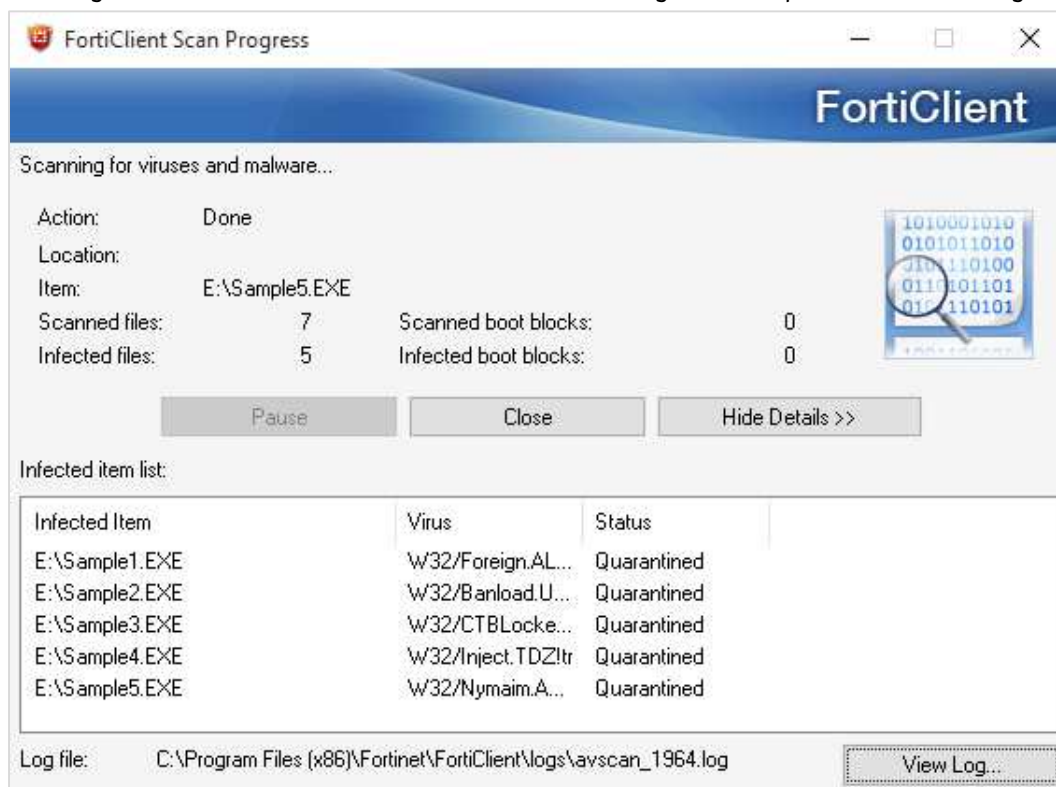
The user merely has to close the dialog.

Additional comments

The FortiClient Virus Cleaner is run before the installation commences:
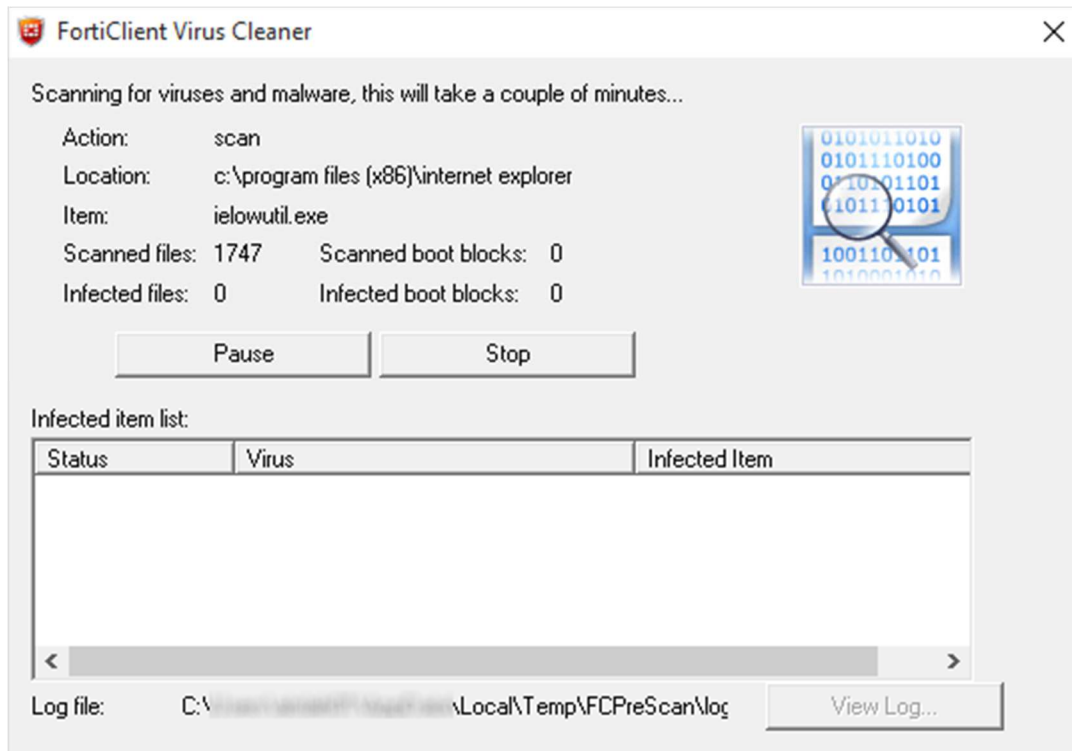
Kaspersky Internet Security 16.0
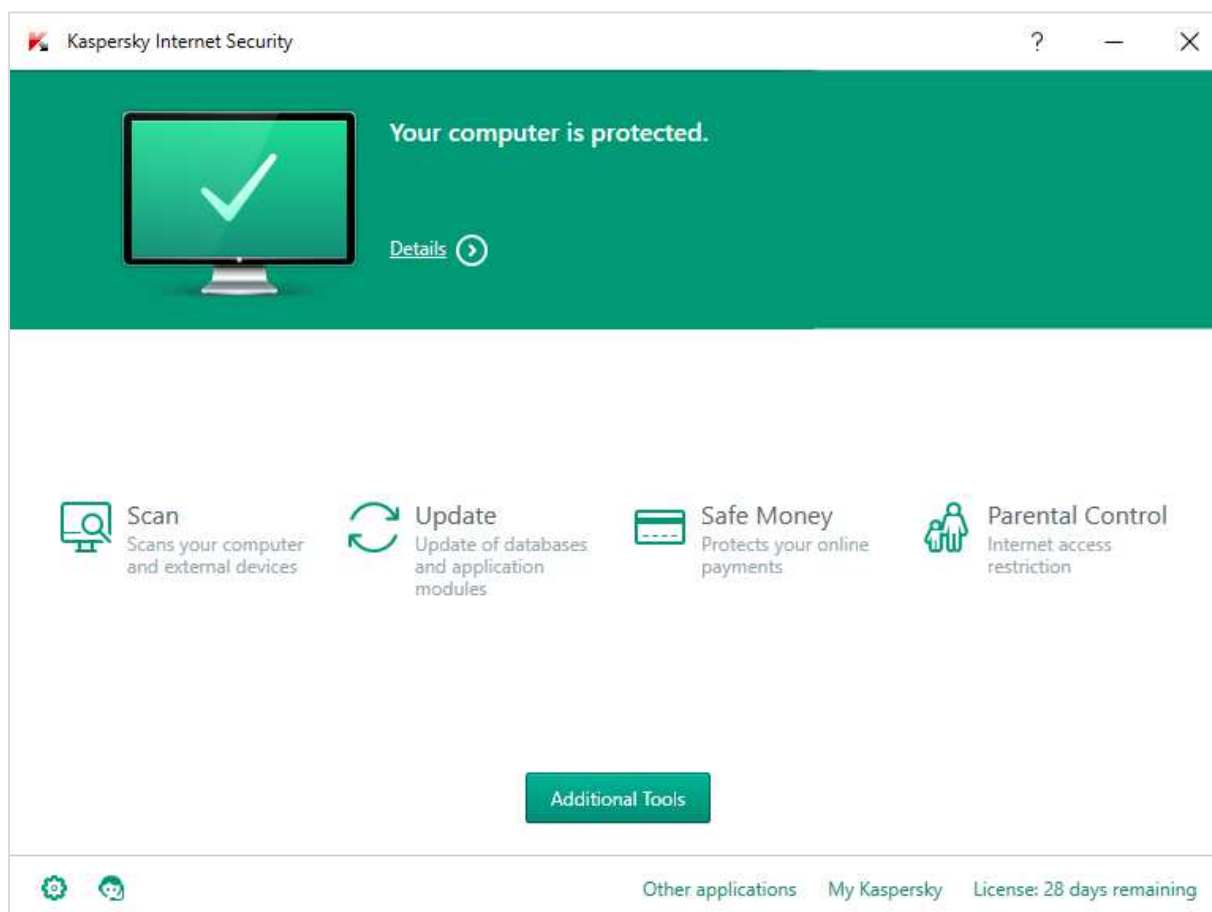
Supported operating systems
All 32 and 64-bit versions of Windows XP, Vista, 7, 8, 8.1, 10

Firewall
Kaspersky Internet Security includes its own firewall.

Product page on vendor's website
http://www.kaspersky.com/internet-security#Feature0

Help
There is a local help feature, a manual[22] and a knowledge base[23].

---

[22] http://www.kaspersky.com/downloads/internet-security
[23] http://support.kaspersky.com/kis2016

Good points

We found the user interface of KIS 2016 to be very well designed and user friendly. The main program window makes all important components and information easy to find, and provides clear status warnings and an easy means of reactivating any disabled components. The System Tray and Explorer context menus are useful, while malware detection does not require any user interaction. Help facilities are excellent.

Suggestions for improvement

We feel it would be helpful if the setup program pointed out that the website blocking and password-protection features need to be enabled if the user wishes to deploy them.

Installation, deinstallation, deactivation

Installation options

The user can decide whether to join the Kaspersky Security Network (data-sharing scheme).

Deinstallation options

The user can choose whether to retain some data, such as settings, licence info and quarantined items.

Deinstallation/deactivation from a standard user account

A user without administrator privileges cannot uninstall the program, but can disable protection components such as real-time protection or firewall. It is possible to prevent this with password protection; this could be valuable e.g. to parents who want to ensure their children do not deactivate the protection.

Windows Security Center, Windows Defender

KIS integrates with Windows Security Center and Windows Defender as expected.

User Interface

Main program window

The home page of the program includes a status display, update button, scan button, help button, and licence information. Quarantine and logs (*Report*) are easily accessible via the *Additional Tools* button. Settings can be accessed from the cogwheel icon on the home page.
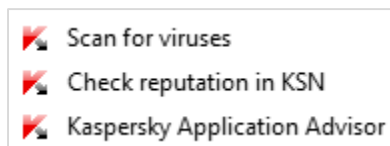
System Tray menu

This is shown below:
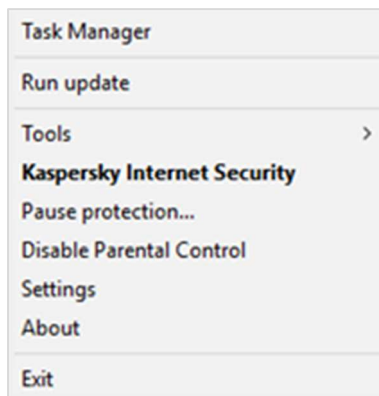
Windows Explorer context menu

The following entries are added to the menu shown when a file is right-clicked in Windows Explorer:

The *Check reputation in KSN* shows an info box with reputation information for a particular file:
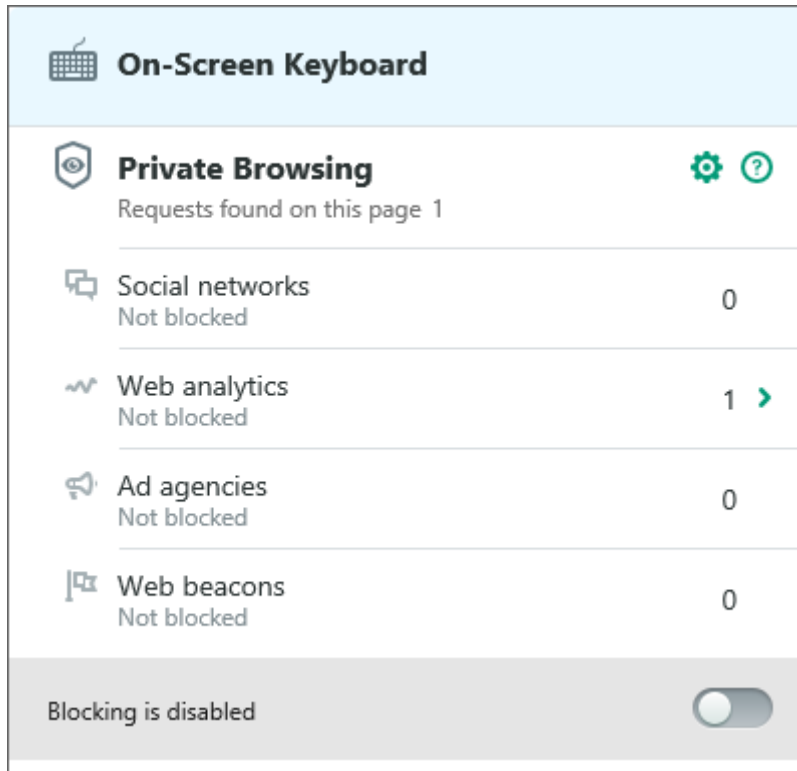

Clicking *Kaspersky Application Advisor* in the context menu opens a web page that shows more security information for a file.

Internet Explorer

Toolbar

A toolbar is added to Internet Explorer; there is just one icon, which opens the following menu:

We note that by default, the blocking function is disabled.

Search service

The default search service in Internet Explorer is not changed.

Search ratings

Google search results show a small icon to the right of the page title, in green for safe sites:
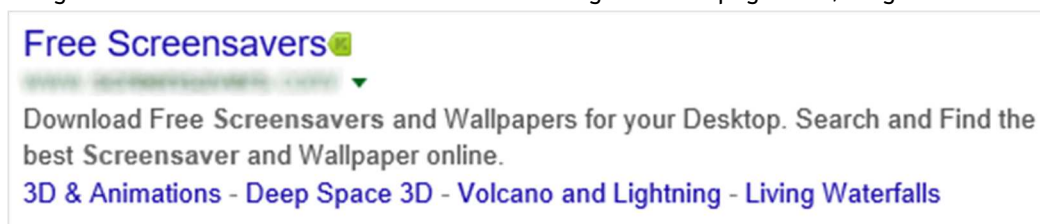
Status alerts

Real-time protection

If the real-time protection is disabled, the following alert is shown in the status section of the main window:

Protection can be reactivated by clicking on *Details*; this opens the configuration page, from which the component can easily be reactivated:
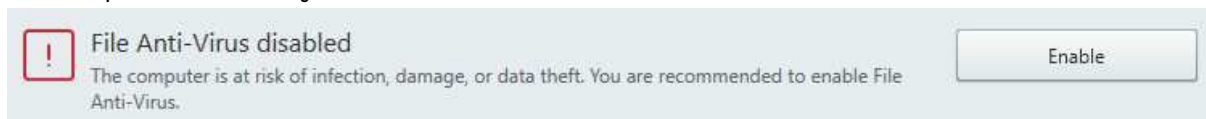
Firewall

If the firewall is disabled, a similar alert (in orange) and reactivation option are displayed.

Malware alerts

Web

If malware is detected when a file is downloaded from the web, the following alert will be shown:
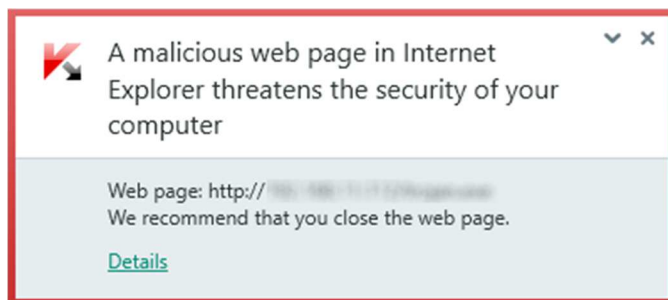
No user action is required. An additional alert is shown in the browser window.

USB on-access
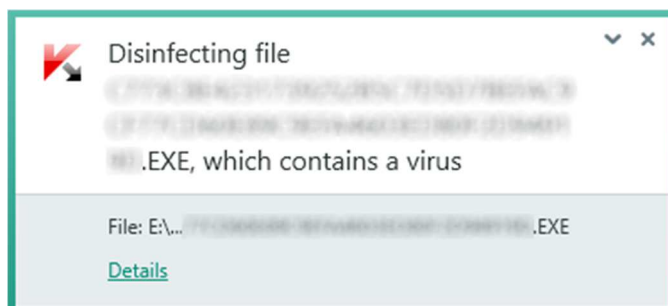
No user action is required.

USB on-demand
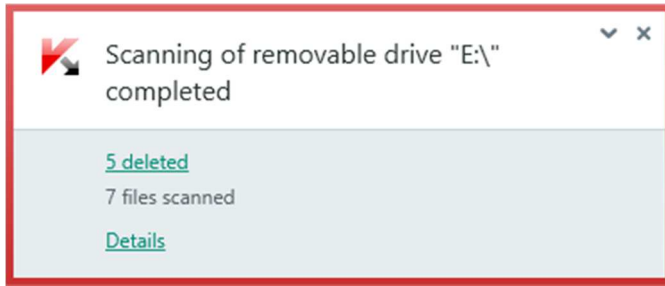
No user action is required.

Additional comments

Both the *Scan* and *Update* panels on the home page show progress bars when an operation is in progress:
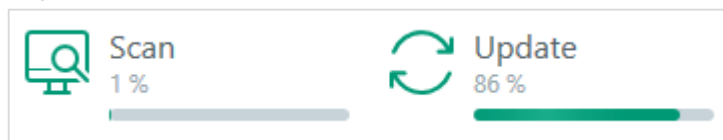
Lavasoft Ad-Aware Free Antivirus+ 11.9
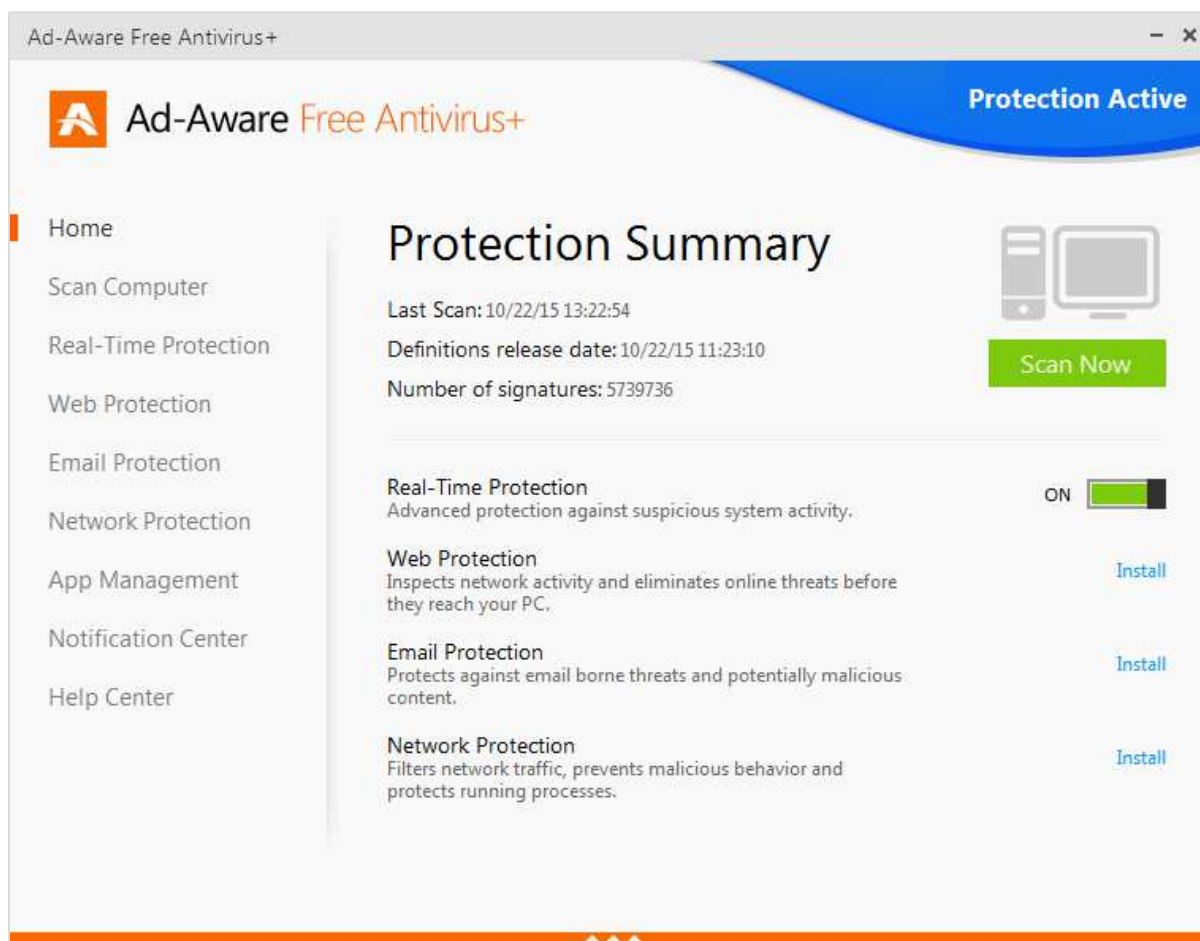
Supported operating systems

Windows XP (32-bit only); Windows Vista, 7, 8, 8.1, 10

Firewall

Ad-Aware Free Antivirus+ does not provide its own firewall.

Third-party components

Ad-Aware Free Antivirus includes some scanning components provided by Bitdefender. We note that two of the products in the Ad-Aware range (*Pro Security* and *Total Security*) additionally include a Bitdefender behaviour blocker; consequently, we would expect these to perform better than the *Free Antivirus* in our Real-World Protection Test.

Product page on vendor's website

http://www.lavasoft.com/products/ad_aware_free.php?t=features

Help

The *Help Center* provides links to the program's FAQ page[24] and documentation page, from which a manual can be downloaded[25].

Good points

We liked the opportunity to install the product as a secondary malware scanner without real-time protection. The program window is clearly laid out, malware alerts are simple and clear, and the help function has been made very accessible in this version.

Suggestions for improvement

We feel that the update function could be made much more accessible.

Installation, deinstallation, deactivation

Installation options

The user can change the location of the installation folder, choose the interface language, and decide whether to join *ThreatWork* (data-sharing scheme). There is also an option to install the program as a second line of defence only, without real-time protection. Additionally, Ad-Aware Web Companion, a URL blocker, can be installed (the default option, which we accepted, is to install it). There are further options to set the default search service and browser home page to Bing. Finally, the user can enter a PIN to protect the program's settings.

Deinstallation options

There is a *Repair* option in addition to removal.

Deinstallation/deactivation from a standard user account

We were unable to uninstall the program using a standard user account. Assuming the user sets a PIN during setup to protect the settings, the protection cannot be disabled without entering this, regardless of whether the user has Windows admin rights.

Windows Security Center, Windows Defender

Lavasoft Free Antivirus+ integrates with Windows Security Center exactly as expected.

When testing an earlier version of the product, we discovered a bug, which lead to the Windows 10 Firewall being deactivated (but not replaced) by Free Antivirus+. We reported this to Lavasoft, who have since rectified the problem.

## User Interface

Main program window

The home page includes a status display, scan button, and a link to help features. Settings, logs (*Report List*) and quarantine can be found by clicking *Scan Computer*. If the user clicks on *Modify Settings* under the *Definition Files* on the *Scan Computer* page, it is possible to perform a manual update.

---

[24] http://lavasoft.com/mylavasoft/support/supportcenter/technicalproblems/faq/?source=inapp&culture=en
[25] http://www.lavasoft.com/mylavasoft/support/supportcenter/product_manuals?source=inapp&culture=en
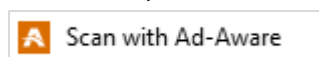
AV
comparatives

System Tray menu

The System Tray icon displays the following menu:
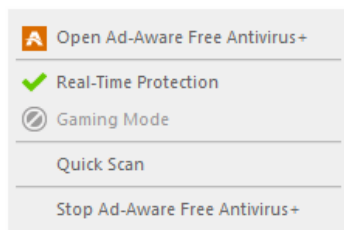
Windows Explorer context menu

The following entries are added to the menu shown when a drive, folder or file is right-clicked in Windows Explorer:

Internet Explorer

Toolbar

No toolbar is added.

Search service

Assuming the user accepts the default options during setup, the search service in Internet Explorer is set to Bing, although this is of course the default in Windows 10 anyway.

Search ratings

Ratings for search results are not shown.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown at the top of the main window:

The protection can easily be reactivated from the slider button on the home page.

Malware alerts

Web

If malware is detected in a download, the following alert is shown:
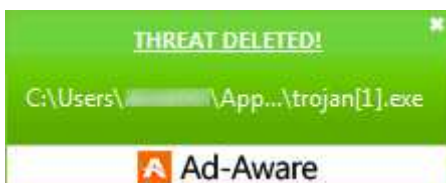
No user action is required.

USB on-access

When Ad-Aware Free Antivirus+ detects malware on a flash drive, the alert below is displayed:
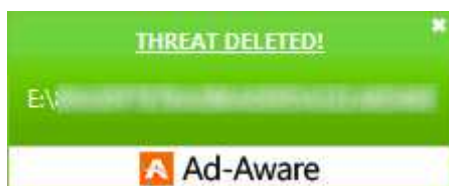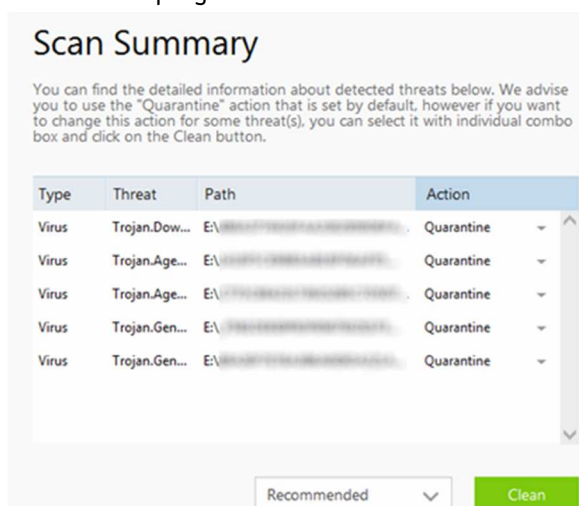
No user action is required.

USB on-demand

If an on-demand scan is run of a flash drive containing malware, Ad-Aware displays the alert shown below:

To remove the malware, the user needs to click on *View Details*. The following dialog is then shown in the main program window:

Clicking *Clean* then carries out the recommended action, i.e. quarantining the malware.

Additional comments

The main program window's left-hand menu panel displays links to *Web Protection, Email Protection* and *Network Protection*. These features are not available in the free version, but can be installed by upgrading to a paid-for version of the product.

McAfee Internet Security 14.0
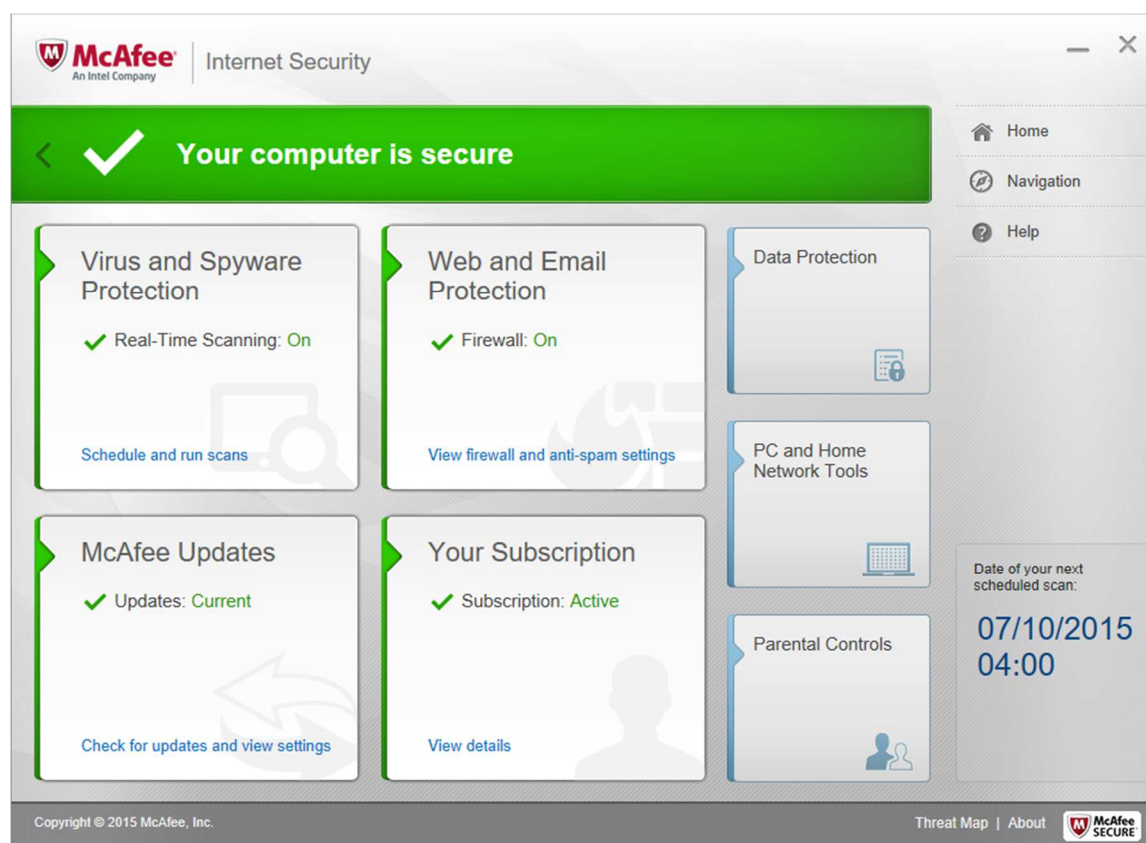
Supported operating systems

7, 8, 8.1, 10, all 32 and 64-bit

Firewall

McAfee Internet Security includes its own firewall.

Product page on vendor's website

http://home.mcafee.com/store/internet-security

Help

There are extensive online help pages, which may be described as on online manual, accessible from the *Help* button in the top right-hand corner of the program window[26].

Good points

We liked the option in the setup wizard to select which components to install. The online help pages explain the various components of the suite and to large extent security software in general very well. The main program window makes important functions easy to find, and the malware alerts are clear and persistent.

---

[26]   https://smarthelp.mcafee.com/help/mcafee/14.0/total%20protection/en-us/GUID-CDB29714-9C0B-42B1-8D83-8EF7D80B1AD2.html

Suggestions for improvement

We feel the convenient *Turn On* button provided to reactivate disabled real-time protection should be displayed immediately, as opposed to the next time the computer is restarted. We would also say that if McAfee's antivirus or firewall components are deactivated, Windows Defender and Windows Firewall, respectively, should be reactivated.

Installation, deinstallation, deactivation

Installation options

The user can decide whether to send anonymous usage information to McAfee. There is a custom installation option, which allows the user to choose the components to be installed:

Deinstallation options

It is possible to uninstall the web protection separately from the other components.

Deinstallation/deactivation from a standard user account

It is not possible to uninstall or deactivate the program without entering administrator credentials.

Windows Security Center, Windows Defender

If McAfee's real-time protection and firewall are disabled, neither Windows Defender nor Windows Firewall is reactivated.
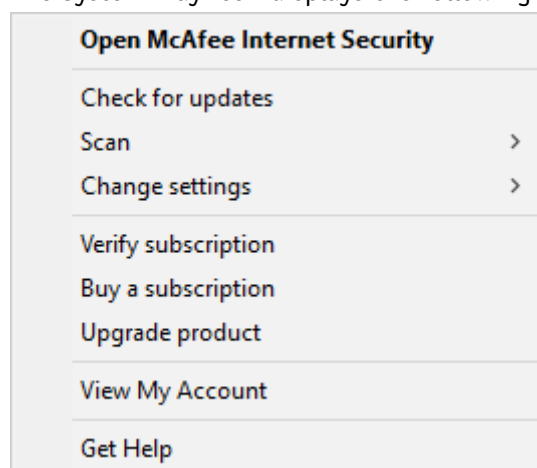
User Interface

Main program window

The main program window includes a status display, and buttons for scans, updates, logs (*Security Report*) and help. Settings for each individual component can be found by clicking on the respective tile on the home page. We found quarantine by clicking on the *Navigation* button on the home page.
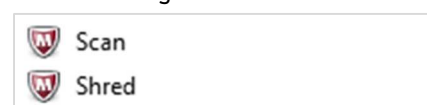
System Tray menu

The System Tray icon displays the following menu:

Open McAfee Internet Security

Check for updates
Scan   >
Change settings   >

Verify subscription
Buy a subscription
Upgrade product

View My Account

Get Help

Windows Explorer context menu

The following entries are added to the menu shown when a file is right-clicked in Windows Explorer:

Scan
Shred

The *Shred* entry securely deletes files.

Internet Explorer

Toolbar

No toolbar is added to Internet Explorer.

Search service and search ratings

When Internet Explorer is first started after the McAfee installation, the following prompt is shown:

McAfee WebAdvisor

Secure Search is off — be careful

Secure Search steers you away from risky sites in your search results.

Want to stay ahead of the bad guys with extra search protection?

☑ Yes, turn Secure Search on after I restart my browser.
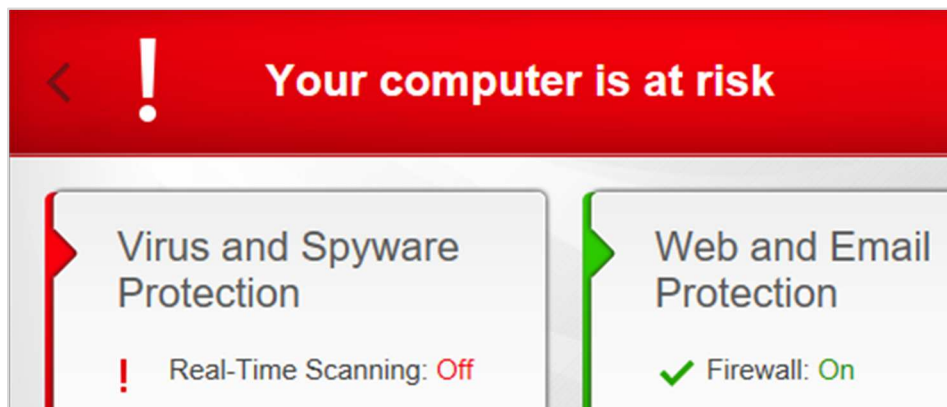
Done
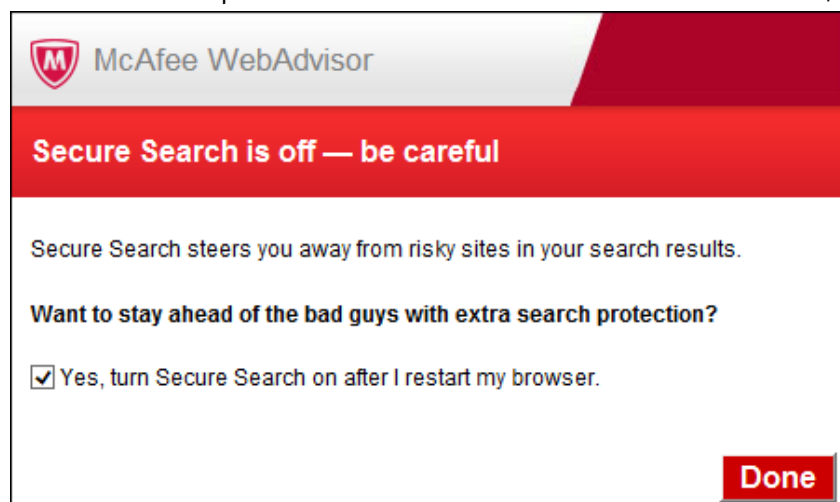
If the user accepts the default option to use McAfee Secure Search, the search service is changed to a Yahoo-based service, and search ratings are provided in the form of an icon at the end of each headline:

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

The next time the computer is restarted, an additional overlay will be shown, with a button to reactivate the protection:

Firewall

If the firewall is disabled, a similar warning is shown, and the overlay with the *Turn On* button is displayed immediately.

Inevitably, we ask why the *Turn On* button is not also provided immediately for the real-time protection, but only appears after a system reboot.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown:
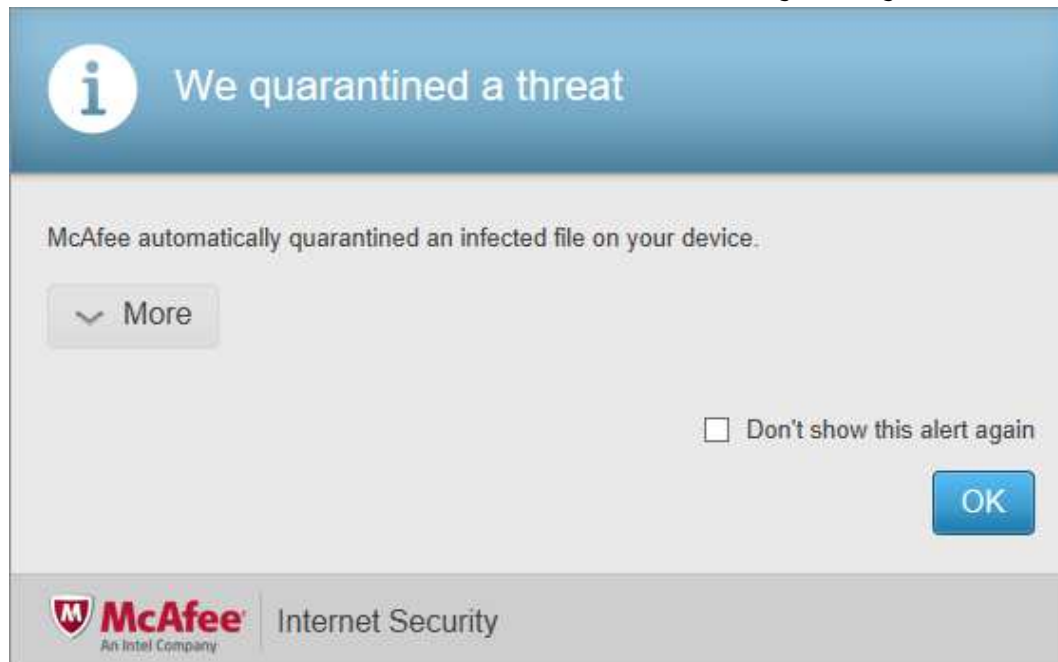
No user action is required. An additional alert is shown in the browser window:
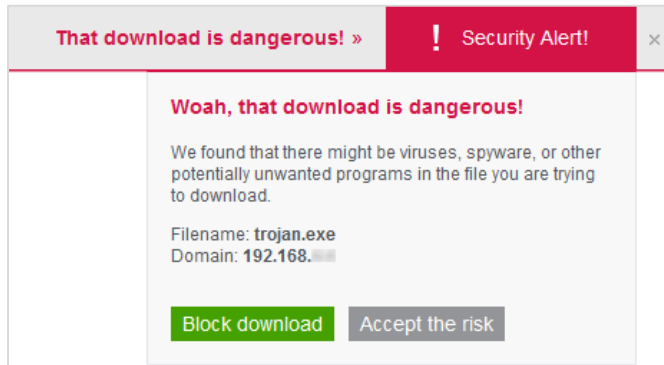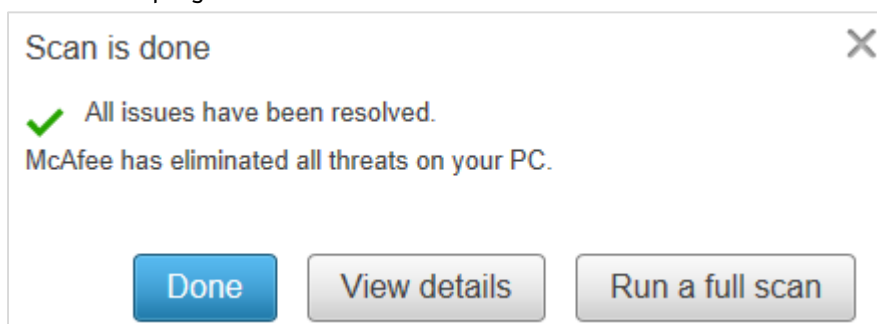

USB on-access

If the real-time protection detects malware on a USB flash drive, the alert below is displayed:
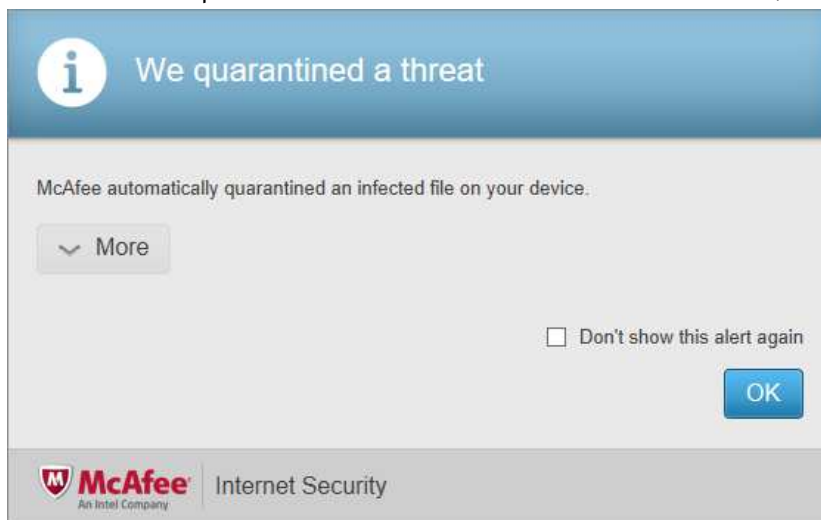
No user action is required. The alert persists until closed by the user.

USB on-demand

Running an on-demand scan of a flash drive containing malware displays the following notification in the main program window:
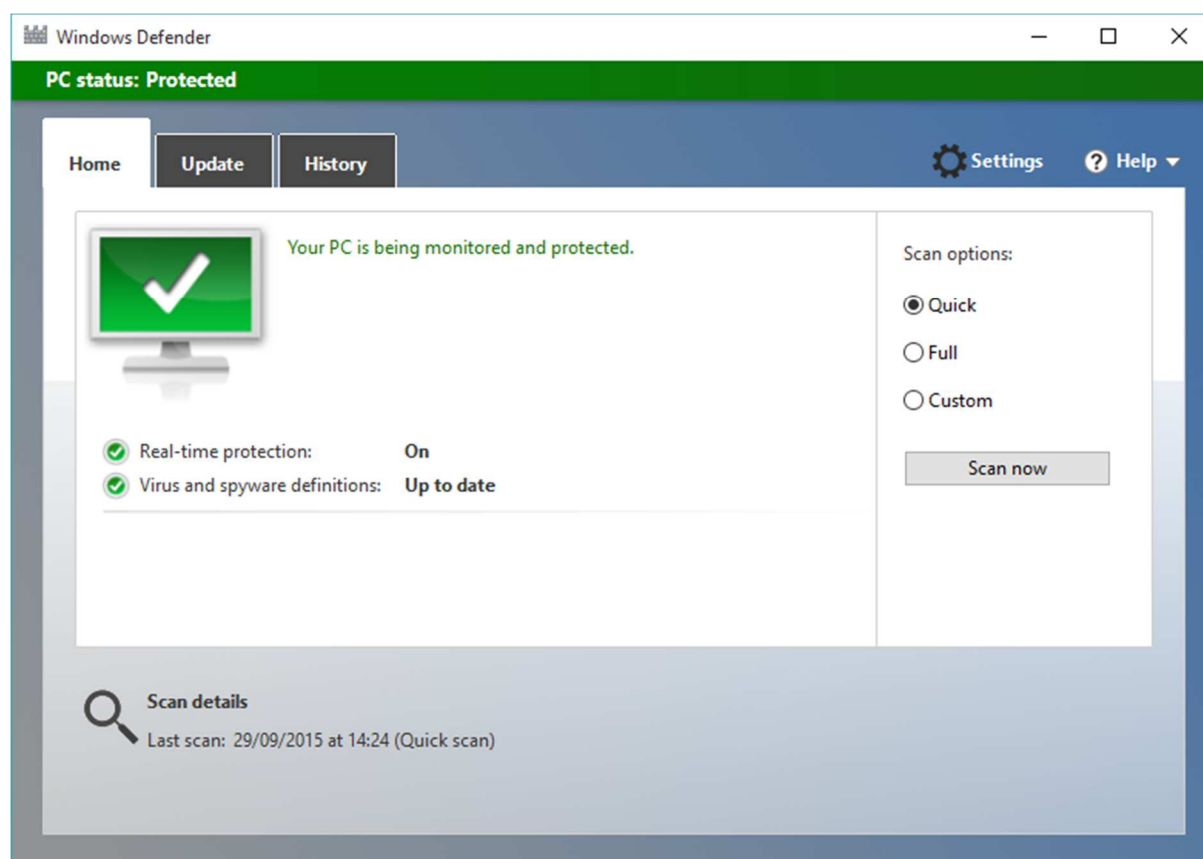

Details of the malware found can be seen in the pane below the notification, or by clicking *View Details*. No user action is required, other than clicking *Done*.

Additional comments

The setup wizard performs a scan for existing malware before installing the product.

Microsoft Windows Defender 4.9 for Windows 10

Nature of the program

Windows Defender for Windows 10 is incorporated into the operating system, as is the Windows Firewall. Both can be deactivated by third-party security programs when appropriate, in order to avoid conflicts. Note that Microsoft also includes other security-related features, such as Smart Screen (which includes e.g. reputation checking) in its operating systems.

Help

Clicking the *Help* link in the program window opens the product's online help page[27].

Good points

Windows Defender's clear and simple layout makes it easy to find important functions and information, whilst alerts are clear and provide easy options for rectifying security issues.

---

[27] http://answers.microsoft.com/en-us/protect/forum/protect_defender

Suggestions for improvement

Regarding the points we have looked at in this (very limited) review, we did not find anything in the program's interface that we felt was in obvious need of improvement. However, note that the name *Windows Defender* for both the antispyware program in Windows 7, and the full antimalware program in Windows 10, may confuse users as to what level of protection they have by default.

Deactivation from a standard user account
Protection cannot be deactivated from a non-administrator account.

User Interface

Main program window
The program's home page includes a status display, 3 scan options, links for help and settings, an *Update* tab and a *History* tab, which provides access to logs and quarantine functions.

System Tray menu
The System Tray icon displays a menu with just one item, *Open*.

Status alerts

Real-time protection
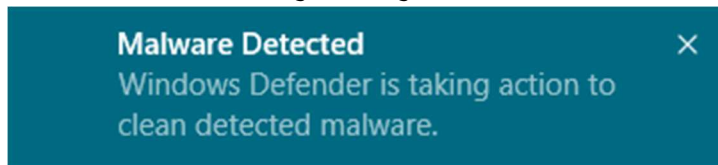If real-time protection is disabled, the following alert is shown in the status section of the main window:

Clicking the *Turn on* button reactivates the protection.
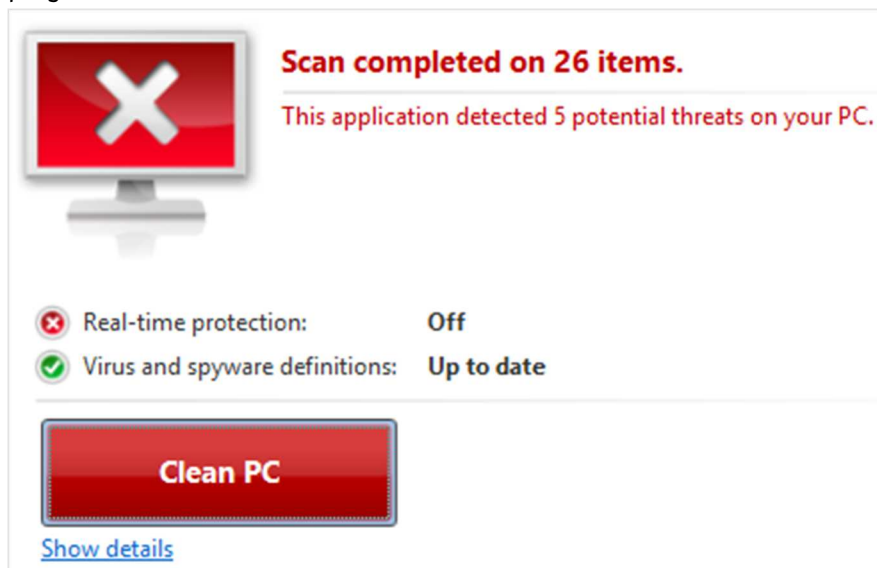
Malware alerts

Web, USB on-access

If a malicious file is downloaded from the Internet, or detected by the real-time protection on a USB flash drive, the following warning is shown:

Malware Detected   ✕
Windows Defender is taking action to
clean detected malware.

No user action is required.

USB on-demand

Running an on-demand scan of a flash drive containing malware displays this alert in the main program window:

Scan completed on 26 items.

This application detected 5 potential threats on your PC.

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

Clean PC

Show details

The user only needs to click *Clean PC* in order to remove the malware.

Panda Free Antivirus 16.0
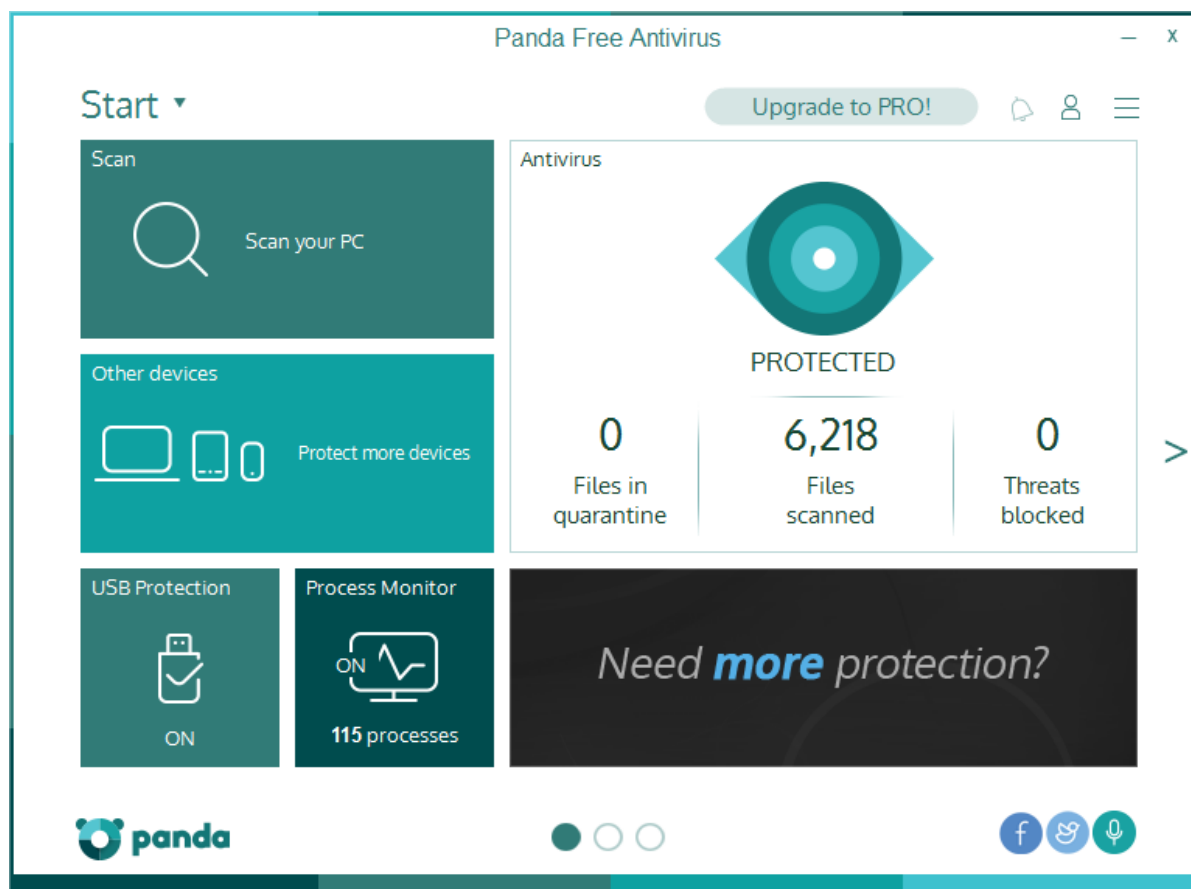
Supported operating systems

Windows XP (32-bit only), Windows Vista, 7, 8, 8.1, 10

Firewall

Panda Free Antivirus uses Windows Firewall.

Product page on vendor's website

http://www.pandasecurity.com/usa/homeusers/solutions/free-antivirus/

Help

Clicking *Help* in the program's menu opens the online help feature[28].

---

[28] http://www.pandasecurity.com/homeusers/downloads/docs/product/help/av/2016/en/r16_en.htm

Good points

We found the new interface to be easy to navigate, with an eye-friendly colour scheme and finger-friendly controls, well suited to use on a touchscreen.

Suggestions for improvement

We are concerned that the program's real-time protection allows (quick) users to copy malware from one drive to another. We also feel that if the product's own real-time protection is disabled, Windows Defender should be automatically reactivated.

Installation, deinstallation, deactivation

Installation options

The user can choose the location of the installation folder, language, whether to install the Panda Security Toolbar, and whether to change to a Yahoo-based browser home page and search service.

Deinstallation options

There are none.

Deinstallation/deactivation from a standard user account

A standard user cannot uninstall the product without entering administrator credentials. It is possible to disable the protection with a non-administrator account, although these settings can be password protected.

Windows Security Center, Windows Defender

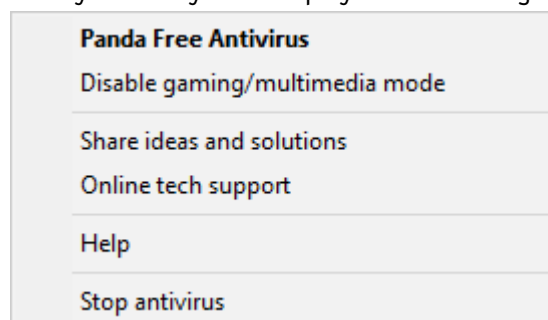If Panda's real-time protection is disabled, Windows Defender is not automatically reactivated.

User Interface

Main program window

The home page includes a status display, quarantine and logs display/link, and a scan button. Help and settings can be found in the menu ("hamburger" icon in the top right-hand corner of the window). An update button can be found under *Settings | General*.

System Tray menu

The System Tray icon displays the following menu:

Panda Free Antivirus
Disable gaming/multimedia mode

Share ideas and solutions
Online tech support

Help

Stop antivirus

Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:

Scan with Panda Free Antivirus

Internet Explorer

Toolbar, home page, search service

Assuming the user accepts the default options during setup, Panda adds a toolbar to Internet Explorer, and changes the search service and homepage to Yahoo-based variants:
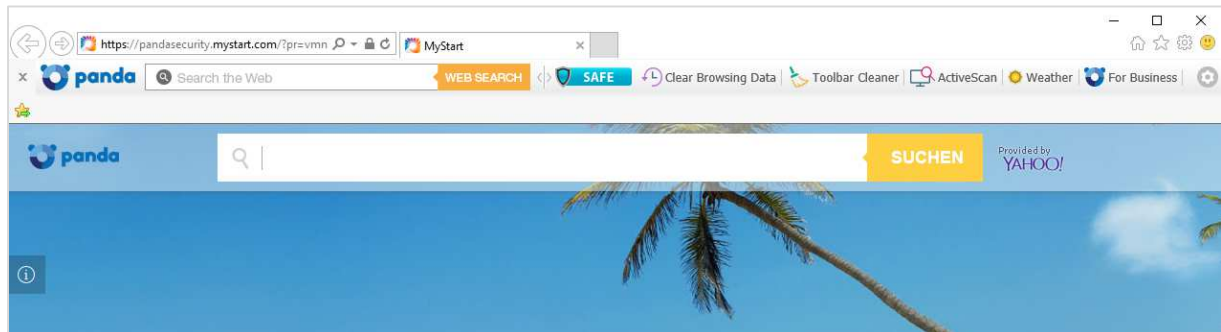
Search ratings

Search ratings are not provided.

Status alerts

Real-time protection

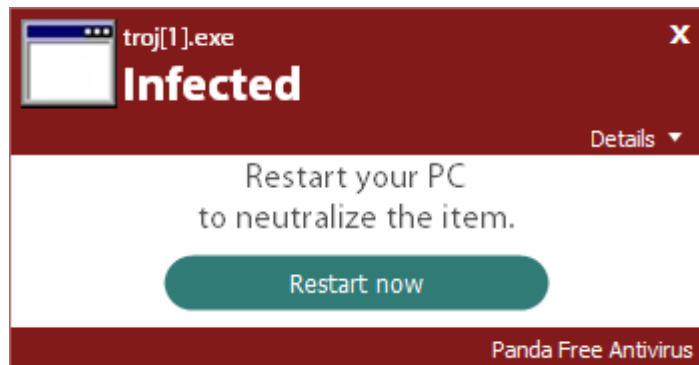If real-time protection is disabled, the following alert is shown in the status section of the main window:

Clicking anywhere in the *Antivirus* panel opens the component's configuration page, from which the component can be switched on again.

Malware alerts

Web

If a malicious file is downloaded from the Internet, the following warning is shown:

The alert prompts the user to restart the computer, although the inspecting the Downloads folder reveals that the only trace of the malware is a 0 KB file.

USB on-access

In our test, we found that it was possible to copy malware from a USB flash drive to the Desktop. After a few seconds, the malware on the desktop was detected and deleted by Panda Free Antivirus, which displayed the following alert:
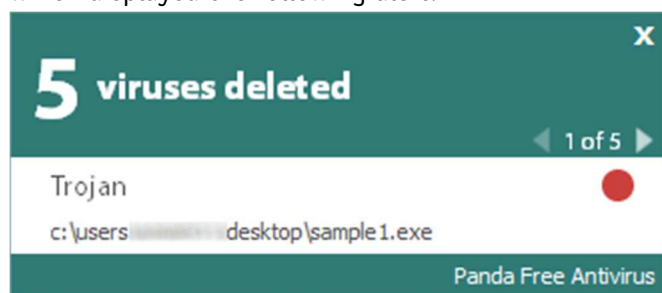
No user action is required.

In this test, the malware on the flash drive itself was not detected by the real-time protection. We also found that it was possible to copy 5 malware samples from a network drive onto a flash drive, and then remove the flash drive from the PC with all 5 samples intact, without Panda detecting it (albeit by simply pulling the drive out without using Windows' *Safely Eject Media* process. If the flash drive is not removed immediately after copying is complete, the malware is detected and deleted after a few seconds.
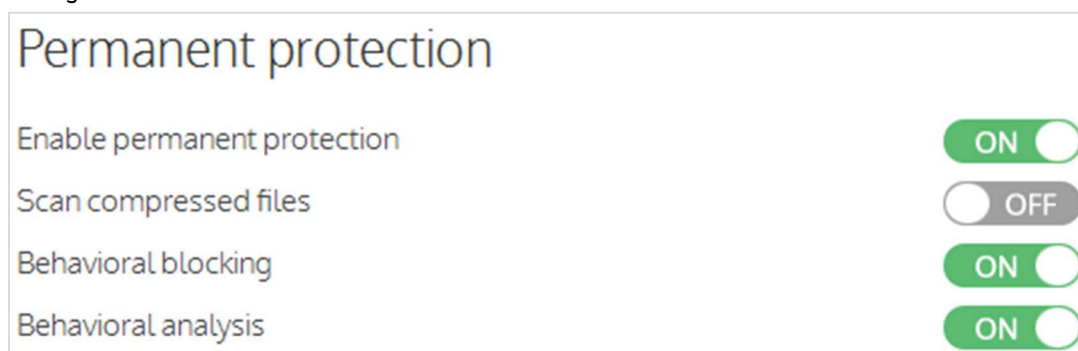
USB on-demand

Running an on-demand scan of a flash drive containing malware produces this message box:
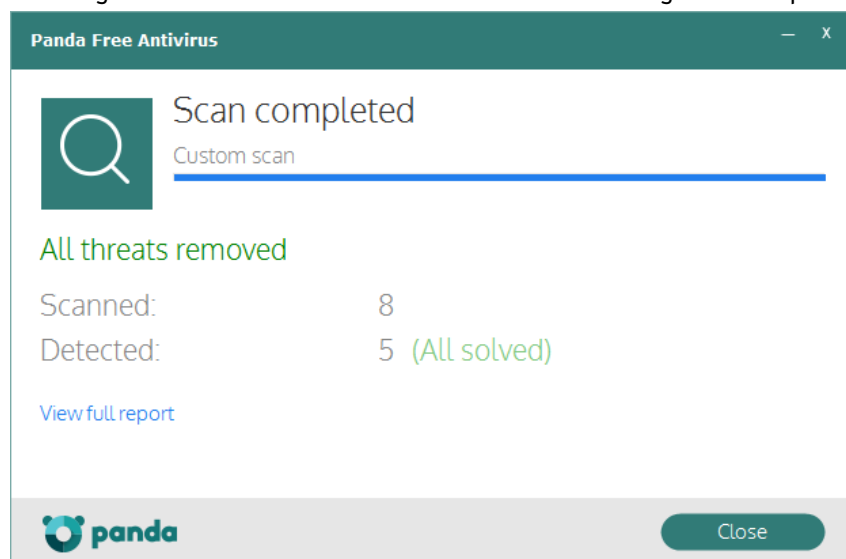
No user action is required.

Additional comments

The status window is configurable; tiles can be rearranged by dragging. The program interface is very suitable for use on a touchscreen, as illustrated by the finger-friendly buttons in the settings dialog below:

In our Real-World Protection Test, a number of cases were observed in which Panda Free Antivirus blocks malware but does not display an alert. Only by searching the advanced logs can the detection be confirmed.

Quick Heal Total Security 16.0

Supported operating systems

Windows 2000, XP, Vista, 7, 8, 8.1, 10

Firewall

Quick Heal Total Security includes its own firewall.

Third-party protection components

Quick Heal Total Security includes some protection components provided by Bitdefender. We note that all the other products in Quick Heal's home-user range (e.g. *Internet Security*) use only Quick Heal's own components. It is thus possible that these products will score differently from Total Security in some of our tests.

Product page on vendor's website

http://www.quickheal.com/quick-heal-total-security

Help

There is a local help feature, and an FAQ page on the Quick Heal website[29].

Good points

We found the interface clean, easy to navigate, and well suited to use with touchscreens. The automatic scan of USB drives ensures that any malware on such a drive will be removed.

Suggestions for improvement

We feel that Windows Defender should be reactivated if the product's real-time protection is disabled.

Installation, deinstallation, deactivation

Installation options

The user can change the location of the installation folder.

Deinstallation options

The user can choose to keep quarantined items, licence information, malware definitions, logs and similar information when uninstalling.

Deinstallation/deactivation from a standard user account

If logged on with a standard Windows user account, a user cannot disable or uninstall the product.

Windows Security Center, Windows Defender

If Quick Heal's real-time protection is disabled, Windows Defender is not reactivated.
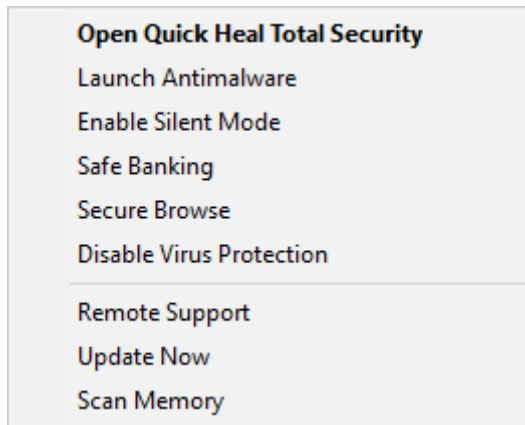
User Interface

Main program window

The product's home page includes a status display, scan button, link to logs (*Reports*) and general settings, and help menu. Licence information can be found by clicking *Help, About*, while quarantine is accessed by clicking on the *Files and Folders* tile. A manual update can be run from the System Tray icon, or by clicking the *Quick Update* shortcut in the program's folder in the Windows Start Menu. The settings for each individual component can be found by clicking on the respective tile on the home page.

---

[29] http://www.quickheal.com/faq-avists

System Tray menu

The System Tray icon displays the menu shown below:

> **Open Quick Heal Total Security**
> Launch Antimalware
> Enable Silent Mode
> Safe Banking
> Secure Browse
> Disable Virus Protection
>
> Remote Support
> Update Now
> Scan Memory

Windows Explorer context menu

The following entries are added to the menu shown when a file, folder or drive is right-clicked in Windows Explorer:
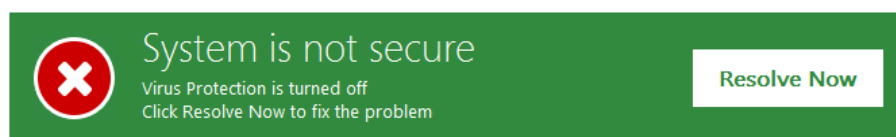
> **Q** Quick Heal Total Security Scan

Internet Explorer

Toolbar, search service, search ratings

Quick Heal Total Security does not add a toolbar to Internet Explorer, change the default search engine, or add search ratings. Quick Heal informed us that their web protection is browser-independent and so does not use toolbars or plugins.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

> ❌ System is not secure
> Virus Protection is turned off
> Click Resolve Now to fix the problem
> **Resolve Now**

Clicking *Resolve Now* immediately reactivates the protection.

Firewall

If the Quick Heal Firewall is disabled, an alert is shown in the component's tile on the home page:

> 🌐❗
> Internet
> & Network

Note that in this case, Windows Firewall is immediately reactivated. Consequently, we feel that this (less-prominent) alert is entirely adequate and appropriate.
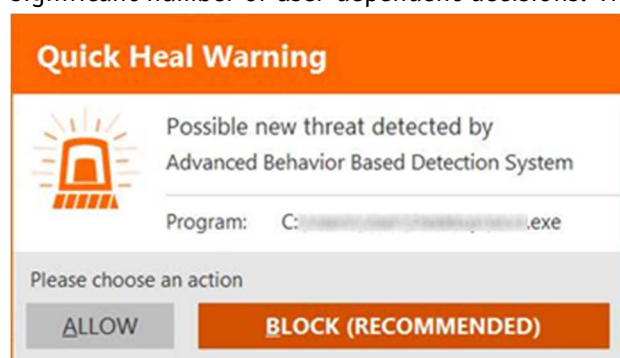
AV comparatives

Malware alerts

Web

If malware is detected in a download, the following alert is displayed:

Quick Heal Total Security
Virus Protection

Detected: Trojan.Inject.013126
File: C:\Users\⬛⬛⬛⬛\AppDat...\trojan[1].exe

Access denied

No user action is required.

User-dependent test cases

In a number of the Real-World Protection Tests this year, Quick Heal Total Security produced a significant number of user-dependent decisions. The alert displayed in such cases is shown below.

Quick Heal Warning

Possible new threat detected by
Advanced Behavior Based Detection System

Program: C:⬛⬛⬛⬛⬛⬛⬛⬛⬛⬛.exe

Please choose an action

ALLOW   BLOCK (RECOMMENDED)

USB on-access

If a USB flash drive is connected to the PC, a scan of the device is started automatically. Results are thus the same as for an on-demand scan.

USB on-demand

If malware is detected by an on-demand scan of a USB flash drive, the following alert is shown:

Quick Heal Total Security
Virus Protection

Detected: Ransom.Nymaim.rw5
...\⬛⬛⬛⬛⬛⬛⬛⬛⬛⬛⬛⬛⬛⬛

File successfully repaired

The malware is quarantined automatically; no user action is required.

Additional comments

A pop-up message advertises Webinars, such as "Safety tips to avoid online scams this festive season". The Parental Control tile is shown with an alert on the home page; this does not mean that it is malfunctioning, but that parents who wish to use it need to configure it appropriately for their children. Quick Heal has a News feature, which from time to time informs users about current cyber threats, good security practices and other relevant topics.

Sophos Endpoint Security and Control 10.3
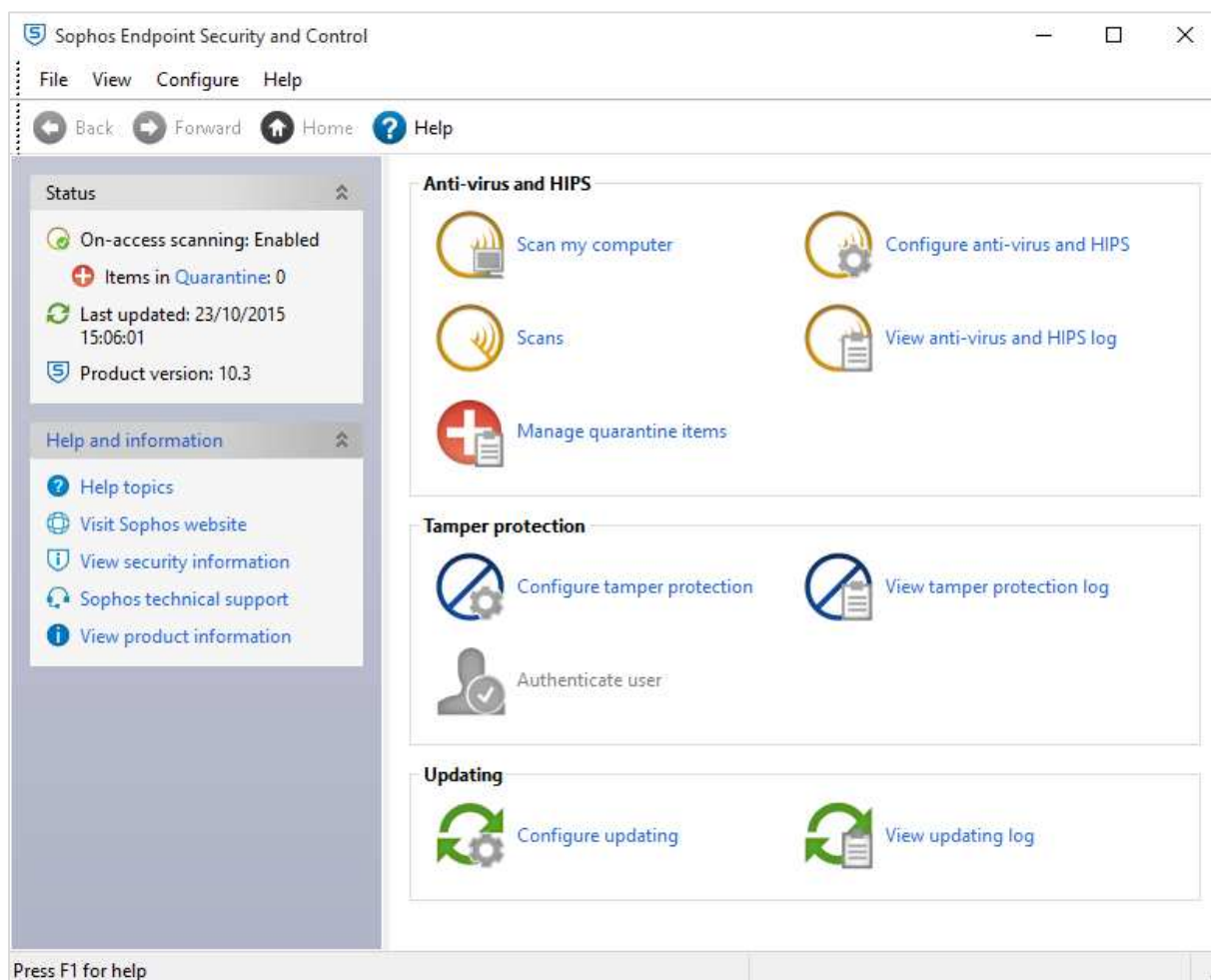
Supported operating systems

Windows XP, Vista, 7, 8, 8.1, 10

Firewall

Sophos Endpoint Security and Control includes the Sophos Client Firewall, which can be installed as an option in the setup wizard. We used the default setting, which does not install it, in our test; in this case, Windows Firewall is left running.

Product page on vendor's website

https://www.sophos.com/en-us/products/endpoint-antivirus.aspx

Note regarding the nature of the program

Sophos Endpoint Security and Control is designed for use in a managed business network, and so its user interface may vary from that of a typical consumer security product.

Help

There is a local help feature, 2 manuals[30], and a searchable knowledge base[31].

Good points

We would say the program's interface is suitable for its intended use in managed business networks. Documentation is comprehensive.

Suggestions for improvement

We feel that the program's graphic design, very similar to Windows Explorer in Windows XP, could do with being refreshed.

Installation, deinstallation, deactivation

Installation options

The user can change the location of the installation folder, enter details of a proxy server for use with the update function, and choose to remove third-party security software.

Deinstallation options

There are none.

Deinstallation/deactivation from a standard user account

The program cannot be deactivated or uninstalled without entering administrator credentials.

Windows Security Center, Windows Defender

Sophos Endpoint Security and Control integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window

This includes status text for real-time protection, links to scans, logs and quarantine, configuration links for individual components, and a help button. Definitions can be updated using the System Tray menu shown below.

---

[30] https://www.sophos.com/en-us/support/documentation.aspx
[31] https://www.sophos.com/en-us/support.aspx
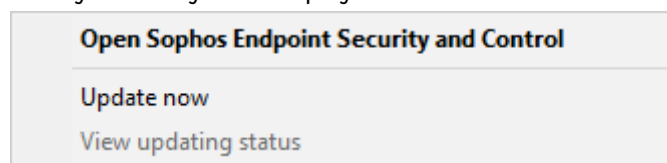
System Tray menu

The System Tray icon displays the menu below:

> Open Sophos Endpoint Security and Control
>
> Update now
>
> View updating status

Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:

> Scan with Sophos Anti-Virus

Internet Explorer

Toolbar, search service, search ratings

Sophos does not add a toolbar, change the search service, or provide search ratings.

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

> On-access scanning: Disabled
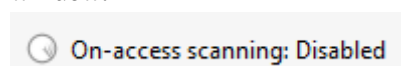
To reactivate protection, the user has to go into the settings of the antivirus component.

Malware alerts

Web

If malware is detected in a download, the following alert is shown:

> **High risk website blocked** ✕
> Virus/spyware 'Mal/Generic-L' has been detected on this site.

No user action is required. An additional alert is shown in the browser window:

> Malicious Content Blocked
>
> Location: _____/trojan.exe
>
> The requested location contains malicious content, identified as *Mal/Generic-L* and was blocked from downloading.
>
> Return to the page you were previously viewing.
>
> Return to previous page
>
> sophos web protection
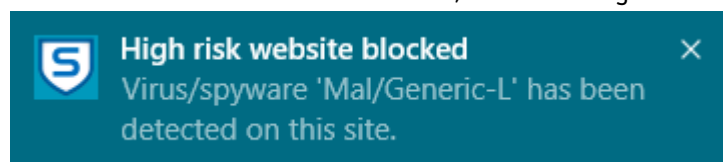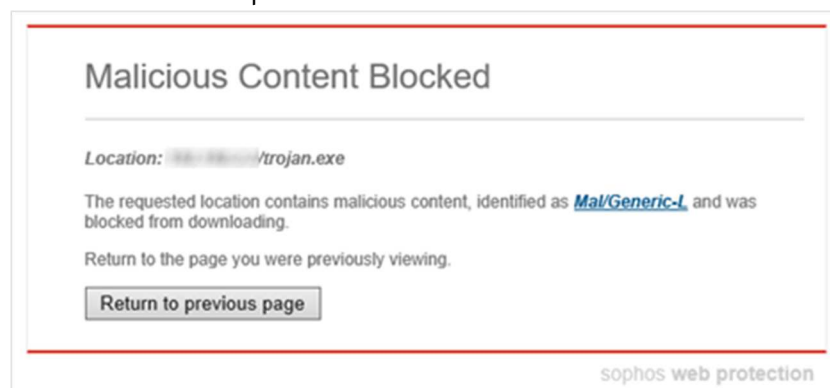
USB on-access
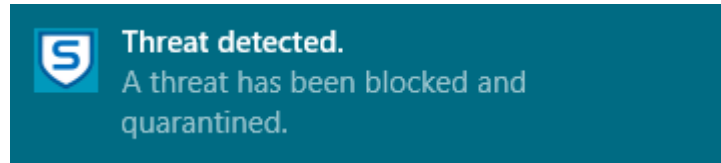
No user action is required.

USB on-demand

If an on-demand scan is run of a USB flash drive containing malware, the dialog below is shown:
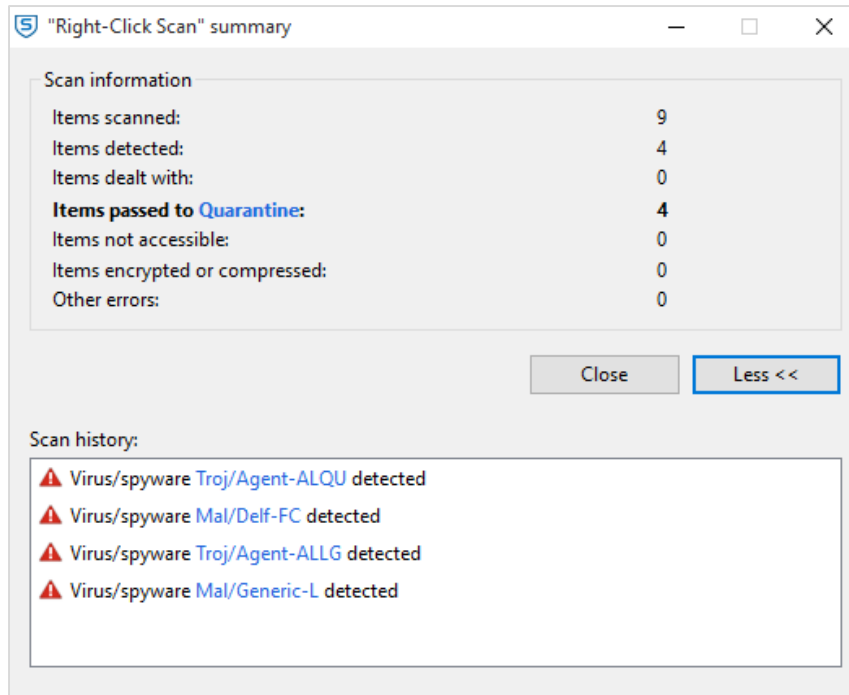
No user action is required.

Tencent PC Manager 11.0 (International/English version)
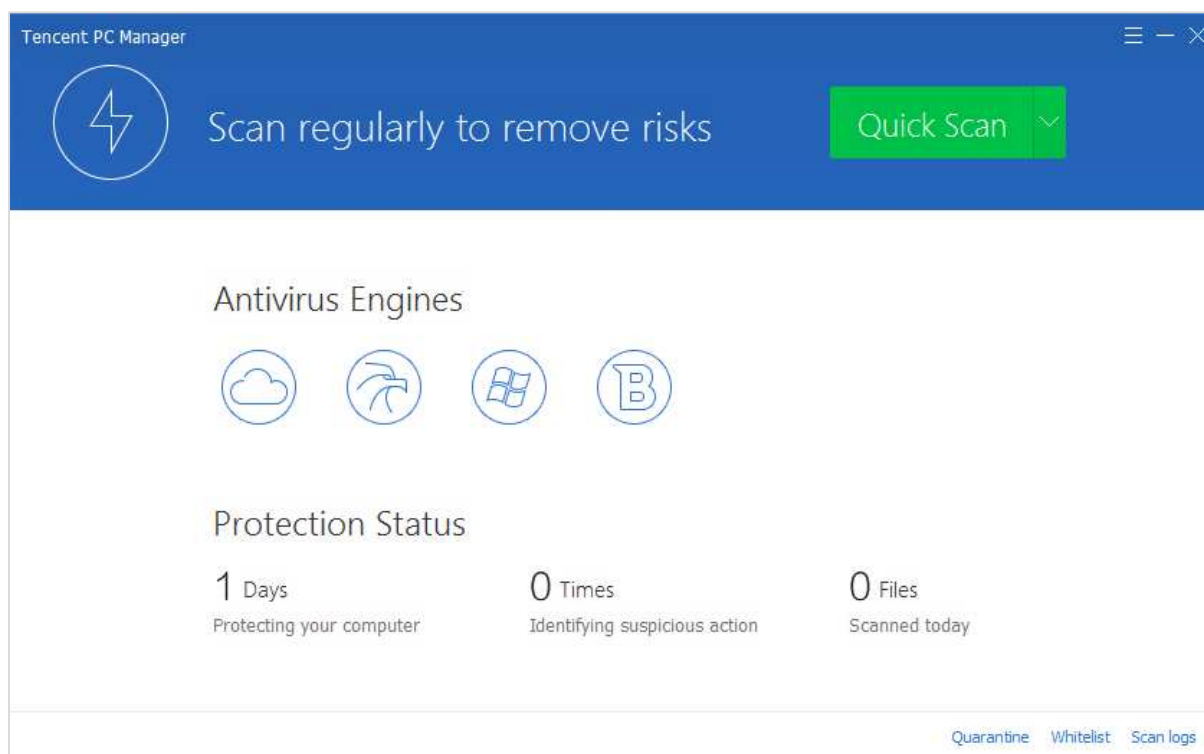
Supported operating systems

We could not find any information about this on the manufacturer's website.

Firewall

Tencent PC Manager uses Windows Firewall.

Third-party components

The tested version, released on 30th October 2015, includes some scanning components provided by Bitdefender. Previous versions used some scanning components provided by Avira (in place of the Bitdefender components).

Product page on vendor's website

http://pcmgr-global.com/

Help

We could not find any help features within the product or on the manufacturer's website.

Good points

We liked the clean and modern graphic design of the program's interface.

Suggestions for improvement

We regard the program's default real-time protection settings, which allow malicious PE (executable) files to be copied from a network share to the local hard drive without them being deleted, and without any alert being shown, as not ideal for the average PC user, who could unwittingly spread malware this way. We also feel that the descriptions of the different settings for real-time protection could be much clearer (please see *Additional Comments*). Additionally, we recommend that the main program window show a clear alert in the event that real-time protection is completely disabled. Finally, we feel that a help feature, and information on supported operating systems, would be useful.

Installation, deinstallation, deactivation

Installation options
The user can change the location of the installation folder.

Deinstallation options
There are none.

Deinstallation/deactivation from a standard user account
It is not possible to uninstall or disable the program using a non-administrator account. A Windows User Account Control prompt appears, demanding administrator credentials, if a standard user merely tries to open the program window.

Windows Security Center, Windows Defender

Tencent PC Manager integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window
There is no status display relating to real-time protection in the main window. The window does include a scan button, links to logs and quarantine, and a menu (three horizontal lines in top right-hand corner of window) in which settings and update links are provided. We could not find any sort of help feature in the program's interface.

System Tray menu
Clicking the System Tray icon displays the following menu:
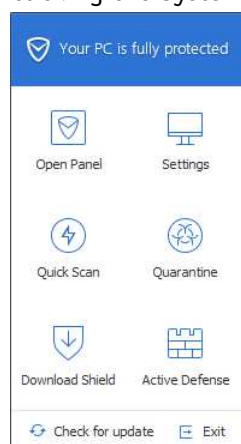
Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:

Scan(PC Manager)

Internet Explorer

Toolbar, search service, search ratings

Tencent PC Manager does not add a toolbar to Internet Explorer, change the search service, or provide search ratings.

Status alerts

Real-time protection

If real-time protection is disabled, no alert of any description is shown in the main window. The System Tray icon (hidden by default) acquires a small exclamation mark and the tool tip "PC Manager: Not all protection are active" [sic] is displayed if the mouse is moved over it. The System Tray menu, however, continues to state "Your PC is fully protected":
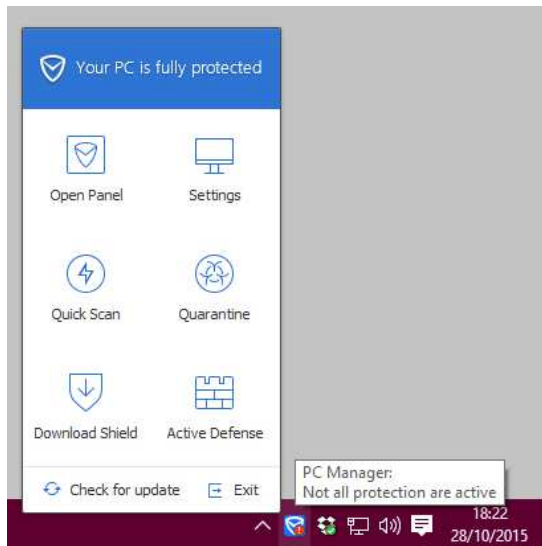
Assuming that the user realises the protection has been disabled, he/she will have to reactivate it manually; there is no "Fix-All" button anywhere.

Malware alerts

Web

If malware is detected in a download, the following alert is displayed:
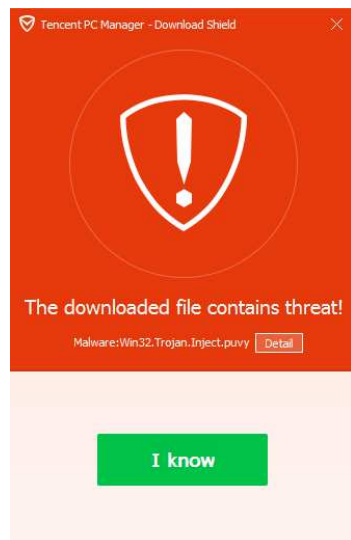
The user just has to click "I know" to close the alert.

Network share

In our test, we found it was possible to copy malware from a network share onto the local hard drive without it being quarantined or deleted, and without any sort of warning being shown by Tencent.

USB on-access

We were able to copy malware from a USB flash drive to the Windows Desktop folder (local hard disk) without the program deleting or quarantining it or showing any sort of warning.

USB on-demand
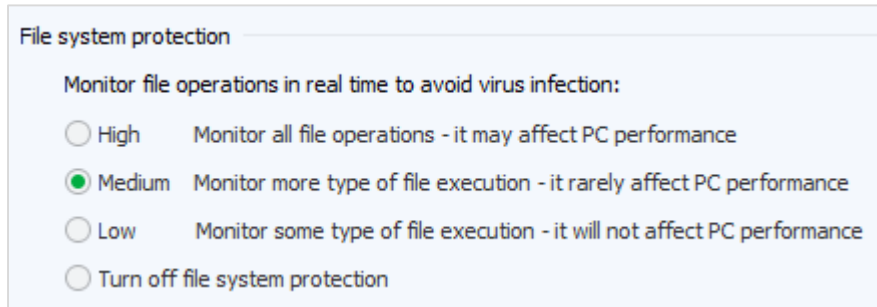
If an on-demand scan is run of a flash drive containing malware, the main program window displays the following dialog:
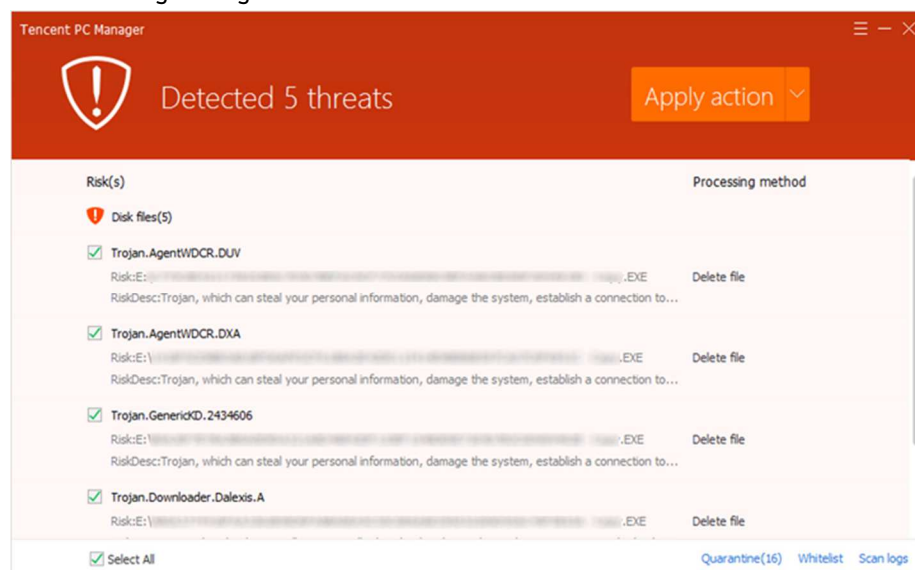
The user merely has to click *Apply action* to delete the malware.

Additional comments

The default settings for PC Manager's real-time protection are shown below:

We would describe the description of the *High* setting, *Monitor all file operations*, as both grammatically correct and clear. However, we find the descriptions used for the *Medium* and *Low* settings are neither.

Our test established that the default *Medium* setting only detects the download and execution of executable files, allowing malicious executable files to be moved or copied between the local hard disk, USB drives and network drives without detection. Tencent evidently make this the standard setting in order to reduce the impact of their software on the performance of the computer.

We repeated the file-copying tests using the *High* setting, and found that Tencent then behaves in the same way as the other programs in the test, i.e. detects the malware samples when they are moved or copied.

ThreatTrack VIPRE Internet Security 2016
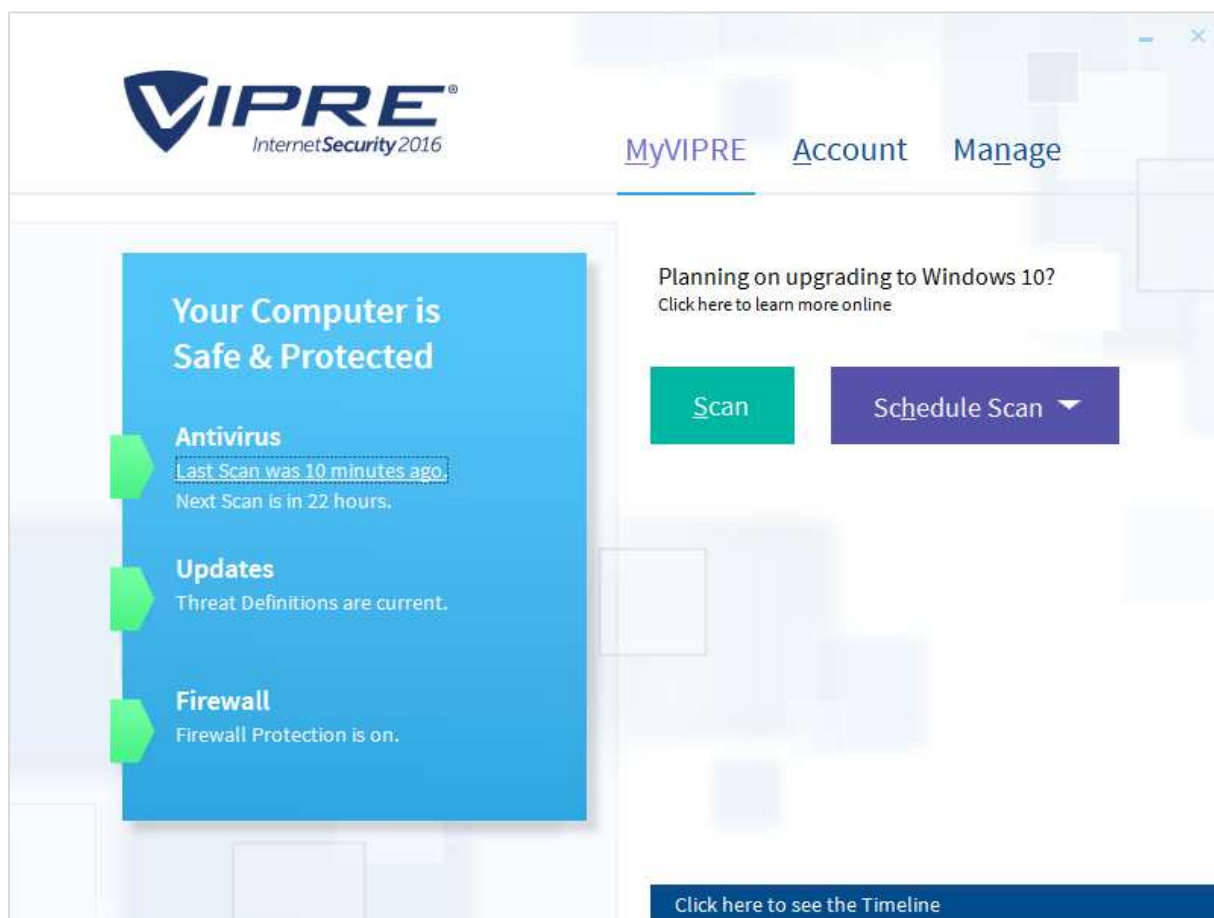
Supported operating systems
Windows XP, Vista, 7, 8, 10, all 32 and 64-bit

Firewall
VIPRE Internet Security includes its own firewall.

Product page on vendor's website
http://www.vipreantivirus.com/VIPRE-internet-security/

Help
There is a local help feature, online knowledge base[32] and a forum[33].

---

[32] http://support.vipreantivirus.com/support/solutions
[33] http://support.vipreantivirus.com/support/discussions

Good points

We found VIPRE Internet Security's interface to be clean and easy to navigate. The real-time protection is very sensitive, and detects malware on a flash drive as soon as the drive is opened in Windows Explorer. We also found the advice on upgrading the system to Windows 10 (a link is displayed on the program's home page) to be helpful. We note that this appears even if the program is installed directly onto a Windows 10 system.

Suggestions for improvement

We feel it should be possible to password-protect the settings, to prevent unauthorised users from disabling the protection.

Installation, deinstallation, deactivation

Installation options

The user can change the location of the installation folder. There is also an option to join *ThreatNet*, the manufacturer's data-sharing scheme.

Deinstallation options

There is a *Repair* option in addition to removal.

Deinstallation/deactivation from a standard user account

A standard user cannot uninstall the program, but is able to deactivate the protection.

Windows Security Center, Windows Defender

VIPRE Internet Security integrates with Windows Security Center and Windows Defender exactly as expected.

User Interface

Main program window

The home page includes a status display, scan button, update button, and log feature. The latter is accessed by clicking *Click here to see the Timeline* on the program's home page. Subscription information and help features can be accessed by clicking *Account* at the top of the window, while settings are found on the *Manage* tab. Quarantine is accessed from the settings of the *Antivirus* component.

System Tray menu

The System Tray icon displays the following menu:
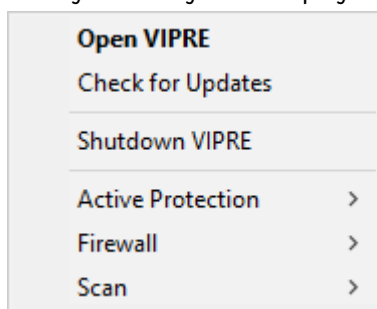
The *Firewall* and *Active Protection* submenus allow the respective components to be enabled or disabled.

Windows Explorer context menu

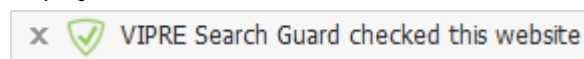The following entries are added to the menu shown when a file, folder or drive is right-clicked in Windows Explorer:
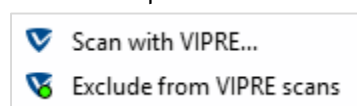
The menu allows the user to set scan exceptions, as well as running a scan.

Internet Explorer

Toolbar

A toolbar is added to Internet Explorer, which shows the security rating for the site currently displayed in the browser's window:

Search service

The default search service in Internet Explorer is not changed.

Search ratings

Search ratings are shown, in the form of an icon at the end of each headline:
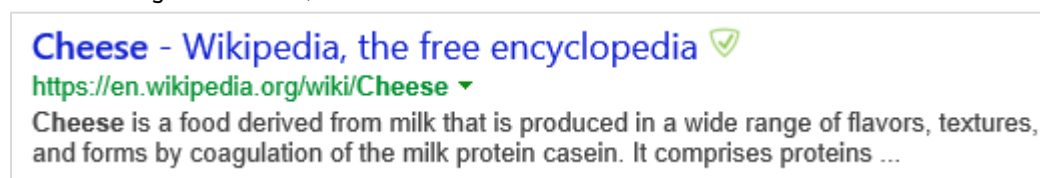
Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

The component can be reactivated by clicking *Turn On*.

Firewall

A similar alert and reactivation link are shown if the firewall is disabled.

Malware alerts

Web

If malware is detected in a download, the following alert is shown:
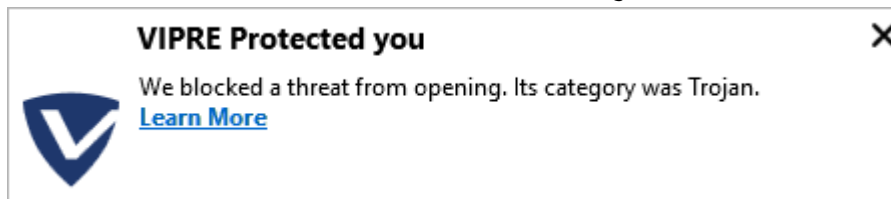
No user action is required. An additional message is shown in the browser window:
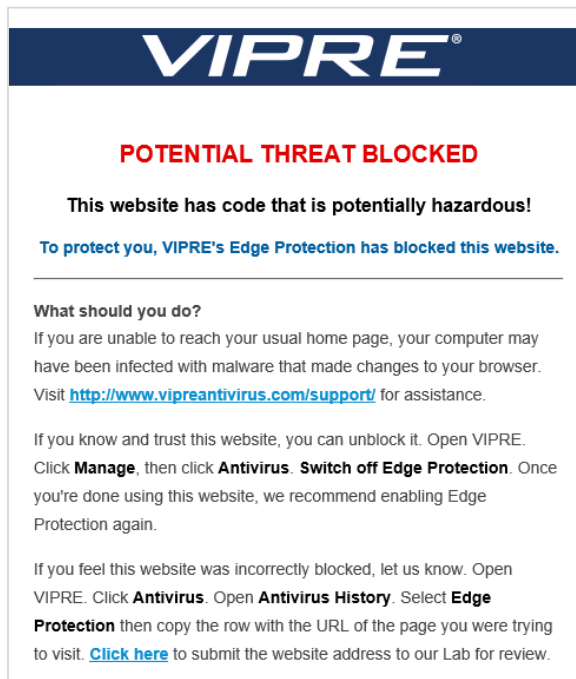
We note that *Edge Protection* refers to the program's own protection component, and is not related to the default Windows 10 browser *Microsoft Edge*.

USB on-access

If malware is detected on a flash drive by VIPRE's real-time protection, the malware is automatically quarantined, and the following alert is displayed:
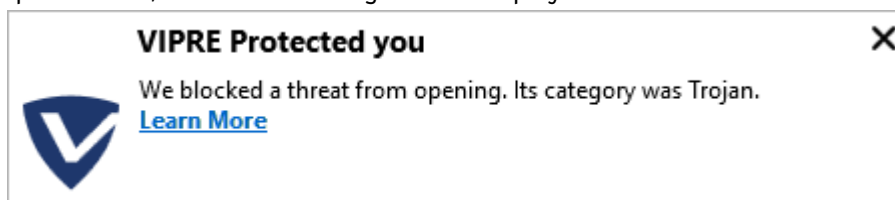
No user action is required.

USB on-demand

If an on-demand scan is run of a flash drive containing malware, the malware is quarantined automatically, and the results shown in the main program window:

No user action is required.

Additional comments

After installation, VIPRE prompts the user to define the current network as trusted or public:
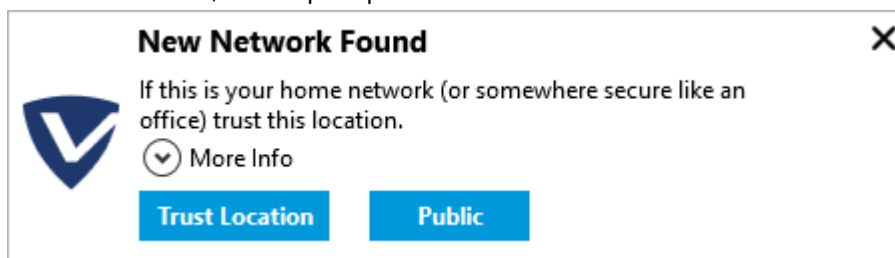
Trend Micro Internet Security 10.0

Supported operating systems
Windows XP (32-bit only); Windows Vista, 7, 8, 8.1, 10

Firewall
Trend Micro Internet Security uses Windows Firewall.

Product page on vendor's website
http://www.trendmicro.com/us/home/products/software/internet-security/index.html

Help
The *Get Help* item in the program's menu opens the program's support page on Trend Micro's website[34].

---

[34] http://esupport.trendmicro.com/en-us/home/pages/technical-support/internet-security-10/support-topics/features-and-settings.aspx?cm_mmc=0LH-_-TI90-_-001001-_-EN-US

Good points

The program interface is clean and easy to navigate, with a good status display and malware alerts. We liked the caption *Feel free to close this window* shown in the scan-results window, to emphasize that the user does not need to take any further action.

Suggestions for improvement

We feel it would be ideal if the setup process were to prompt the user to password protect the settings, in order to prevent users with non-administrator accounts from disabling the protection. We also wonder whether it is necessary to restart the computer after malware is recognised and deleted in a download.

Installation, deinstallation, deactivation

Installation options

The user can choose the interface language, and the location of the installation folder.

Deinstallation options

There are none.

Deinstallation/deactivation from a standard user account

A standard user cannot uninstall the program without administrator credentials, but can deactivate real-time protection. It is possible to password protect the settings to prevent this.

Windows Security Center, Windows Defender

If real-time protection is disabled, Windows Defender is not automatically reactivated. However, Trend Micro displays an alert, which notes that protection will be resumed automatically after 30 minutes, or after a restart if the user so chooses:

User Interface

Main program window

This includes a status display, scan button, licence information, and buttons for help, settings and logs/quarantine. We note that updates can be run from the System Tray menu, shown below.

System Tray menu
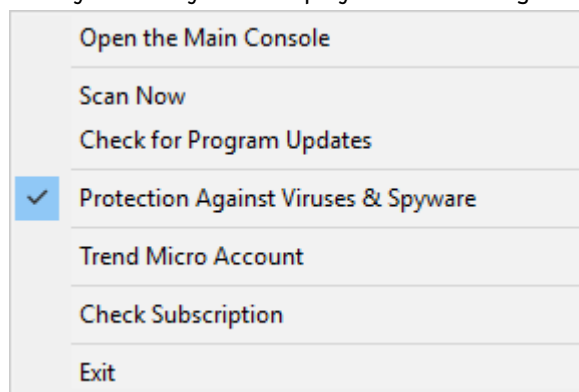
The System Tray icon displays the following menu:

Windows Explorer context menu

The following entry is added to the menu shown when a file is right-clicked in Windows Explorer:
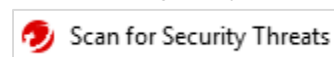
Internet Explorer

Toolbar

A toolbar is added, which displays the following menu:
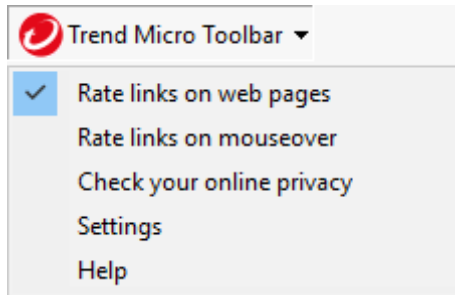
Search service

The default search service in Internet Explorer is not changed.

Search ratings

Search results are rated by means of a symbol before each result's headline:
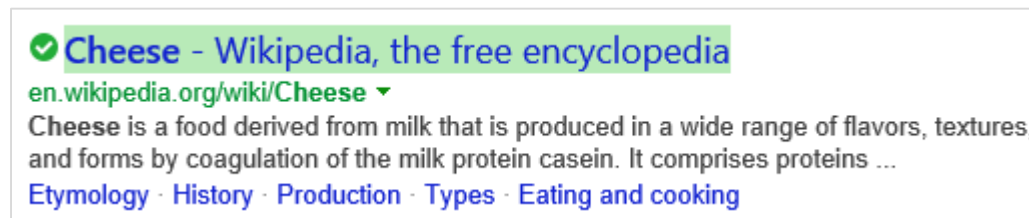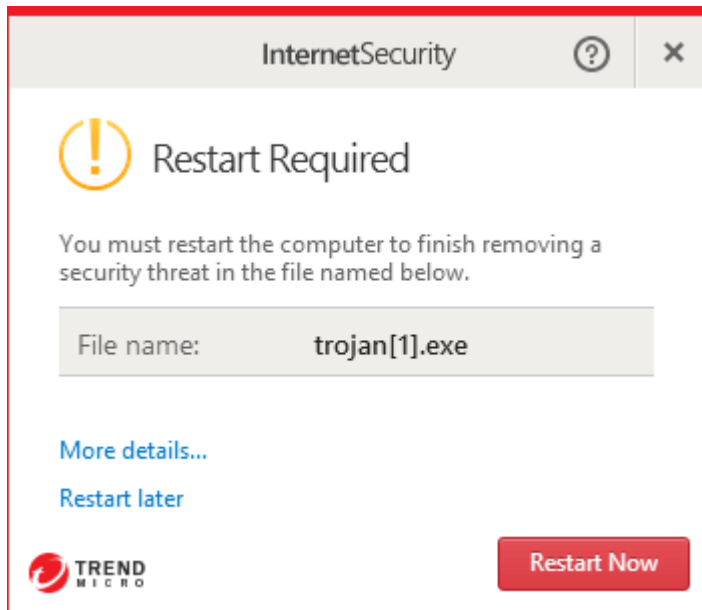

Status alerts

Real-time protection

If real-time protection is disabled, the following alert is shown in the status section of the main window:

Clicking *Enable Now* immediately reactivates the protection.

Malware alerts

Web

Although Trend Micro prompts the user to restart the computer, a glance at the Downloads folder shows that it contains only a harmless 0 KB file.

USB on-access

When Trend Micro's real-time protection detects malware on a flash drive, it is automatically cleaned, and the following alert displayed:

No user action is required. We note that the real-time protection is very sensitive, and detects the malware as soon as the drive is opened in Windows Explorer.

USB on-demand

When an on-demand scan is run on a USB flash drive containing malware, the following alert is shown:
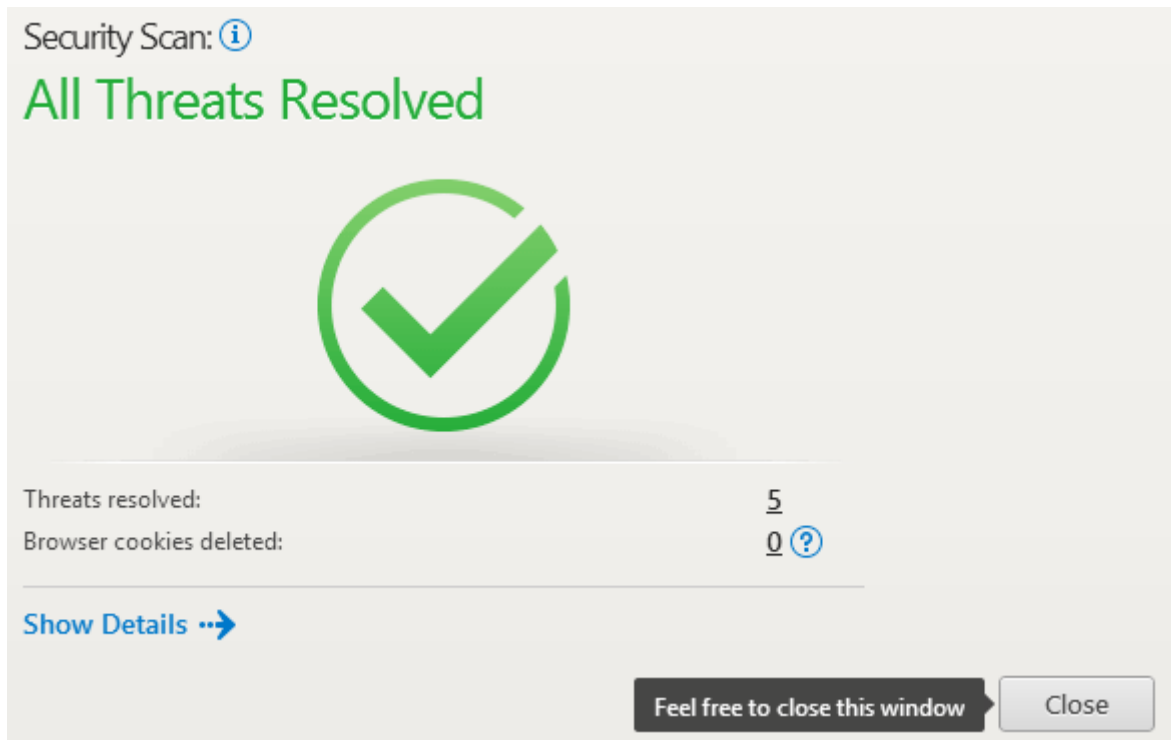
No user action is required.

Copyright and Disclaimer

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

AV-Comparatives (January 2016)