

Mac Security Test & Review



Mac Security Test & Review

Language: English

July 2015

Last revision: 21st July 2015

www.av-comparatives.org

Contents

Introduction: Macs and Security Software	3
Review of Security Software for Mac OS X.....	4
Malware Protection Test.....	6
Summary.....	8
Avast Free Mac Security	10
AVG AntiVirus for Mac.....	15
Avira Free Antivirus for Mac	19
Bitdefender Antivirus for Mac.....	24
ESET Cyber Security Pro	28
F-Secure SAFE.....	34
Intego Mac Premium Bundle X8	39
Kaspersky Internet Security for Mac.....	45
Kromtech MacKeeper.....	50
Sophos Anti-Virus for Mac	60
Appendix: Feature List.....	63
Copyright and Disclaimer.....	64

Introduction: Macs and Security Software

In October 2014, the existence of Mac malware called iWorm was widely reported¹. This is believed to have infected about 18,000 Mac OS X systems, which were harnessed into a botnet. Although Apple is reported to have updated OS X protection to prevent the iWorm from installing, it once again illustrates that Mac systems are not immune to infection by malware, and that it is necessary to take precautions to protect them.

For a sensible discussion of the subject, it is necessary to understand that a *computer virus* is only one of a number of different types of *malware* (malicious software). These days, viruses make up a small percentage of all known malware; *Trojans* (malicious programs disguised as e.g. games or music files) are much more common. Whilst the number of actual *viruses* affecting Mac OS X may be negligible or even zero, Mac systems clearly can be infected by Trojans, if users are fooled into installing them. Please note that nearly all manufacturers still call their products "antivirus", although in reality they protect against all types of malware, including Trojans.

Experienced and responsible Mac users who are careful about which programs they install, and which sources they obtain them from, may well argue – very reasonably – that they are not at risk from Mac malware. However, we feel that non-expert users, children, and users who frequently like to experiment with new software, could definitely benefit from having security software on their Mac systems.

As with Windows computers, Macs can be made safer by employing good security practices. We recommend the following:

1. Do not use an administrator account for day-to-day computing
2. Use a sandboxed browser such as Google Chrome
3. Uninstall/disable the standalone Flash Player
4. Uninstall/disable Java unless it is essential for you
5. Keep your Mac operating system and third-party software up-to-date with the latest patches
6. Use secure passwords (the Mac includes the KeyChain password manager)
7. Deactivate any services such as Airport, Bluetooth or IPv6 that you don't use
8. Be careful about which programs you install and where you download them from

¹ E.g. <https://grahamcluley.com/2014/10/mac-malware-botnet-reddit/>

Review of Security Software for OS X 10.10.3 Yosemite

We have reviewed and tested the following products for this report, using the newest version available in July 2015:

- **Avast Free Mac Security 10.14**
<https://www.avast.com/free-mac-security>
- **AVG AntiVirus for Mac 2015.0.4801**
<http://www.avg.com/eu-en/avg-antivirus-for-mac>
- **AVIRA Free Antivirus for Mac 3.1.0**
<http://www.avira.com/en/free-antivirus-mac>
- **Bitdefender Antivirus for Mac 3.3.9151**
<http://www.bitdefender.com/solutions/antivirus-for-mac.html>
- **ESET Cyber Security Pro 6.0.14**
<http://www.eset.com/int/home/products/cyber-security-pro/>
- **F-Secure SAFE for Mac 1.0.1084 1.0.1102**
https://www.f-secure.com/en/web/home_global/anti-virus
- **Intego Mac Premium Bundle X8 10.8.4**
<http://www.intego.com/mac-protection-bundle-x8>
- **Kaspersky Internet Security for Mac 15.0.1**
<http://www.kaspersky.com/security-mac>
- **KromTech MacKeeper 3.4.15**
<http://mackeeper.com/>
- **Sophos Anti-Virus for Mac 9.2.7**
<https://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-mac-home-edition.aspx>



Review format

Here we have outlined the features and functionality that we have looked at for each program in this review:

Product version reviewed

The specific version used in the test/review.

Operating systems supported

Which versions of OS X are supported by the manufacturer (according to manufacturer's website).

Additional features

Any of the program's features other than malware protection, such as a firewall or phishing protection, are listed.

Installation

We note any options or points of particular interest encountered during the setup process. The deinstallation process is also stated, and whether this is described in the help or user guide.

Main window

We check to see which commands can be accessed from the main window.

Operating system integration

We look for a System Tray icon and menus in the Mac menu bar, to see what additional commands are available there. We note whether a scan can be started by right-clicking a file, folder or drive.

Maintenance

We check whether signatures can be easily updated (where applicable), if the status display shows an alert if real-time protection is disabled, and if so, whether there is a Fix-All button to rectify the problem when it occurs.

Non-administrator access

We find out if a user with a standard user account can disable the protection.

Scanning

We check whether a quick scan, full scan, custom scan and scheduled scan all can be run, and if so, how this is done.

Settings, quarantine and logs

We find out how the program's settings, quarantine and log features are accessed.

Malware and phishing alerts

We check what sort of alert is shown when the EICAR test file and AMTSO Potentially Unwanted test file are downloaded, and the AMTSO Phishing Test page is accessed.

Help

We look to see what help facilities, such as local help, manual or knowledge base, are available, and how clear and comprehensive they are.

Malware Protection Test

In addition to the interface review described above, we have also conducted malware protection tests to see how effectively the Mac security products protect the system against malware. For this test, we used 105 recent and prevalent samples of Mac malware that are not blocked by Mac OS X Yosemite itself. All are distinctly malicious, functioning programs and were seen in-the-field in 2015. As usual, we did not include any potentially unwanted or grey samples (adware, hacking tools, etc.) in the set. We also excluded component files (which could be in the thousands) as these cannot run and do not pose a risk by themselves; certain magazine tests tend to use such files just because they are detected by various products, but we consider inactive components to be irrelevant. We ended up with a test set consisting of 105 malicious Mac apps found in-the-field that pose a risk to users, and should be covered by Mac Security products. In our opinion, these 105 malicious Mac apps represent a substantial part of all in-the-field Mac malware from the first half of 2015.

The number of malicious programs that can currently attack Mac OS X Yosemite is limited. However, as most Mac systems do not run any third-party security software, even these few threats could cause widespread damage. Precisely because a Mac security product only has to identify a small number of samples, we would expect it to protect the system against all threats that have not yet been blocked by OS X itself.

Before the test, the Mac OS X was updated and an image created; no further OS X updates were then applied. Each program was installed on the freshly imaged machine and the definitions updated to the 1st July 2015. The Mac remained connected to the Internet during the tests, so that cloud services could be used. A USB flash drive containing the malware samples was then plugged in to the test computer. At this stage, some antivirus programs recognised some of the samples. We then ran an-on demand scan of the flash drive, either from the context menu if available, or from the main program window if not. Samples found were quarantined or deleted. After this, we copied the remaining samples to the Mac's hard disk. Any samples not detected or deactivated by the scan or real-time protection were then installed and executed, providing the security product with a final chance to detect the malware.

Most of the Mac security products in our review claim to detect Windows malware as well as Mac malware, thus ensuring that the user's computer does not inadvertently act as a conduit for programs that could attack Windows PCs. For this reason, we also checked if the Mac antivirus products in our review detect Windows malware. We used 1,000 very prevalent Windows malware samples; the procedure was identical to that for Mac malware, except that we did not make any attempt to run any of the samples that were not detected in the scan, as Windows programs cannot be executed under Mac OS.

Product	Mac Malware Protection (105 recent samples)	Windows Malware Detection (1,000 most-prevalent samples)
Avast Free Mac Security	100%	100%
AVG AntiVirus for Mac	100%	100%
AVIRA Free Antivirus for Mac	99%	100%
Bitdefender Antivirus for Mac	99%	100%
ESET Cyber Security Pro	100%	100%
F-Secure SAFE for Mac	100%	28%
Intego Mac Premium Bundle X8	100%	50%
Kaspersky Internet Security for Mac	100%	100%
Kromtech MacKeeper	98%	97%
Sophos Anti-Virus for Mac	100%	100%

The test was conducted on the 1st July 2015. After the test, the participating vendors received the malicious files they missed. By now (18th July 2015), they have updated their definitions so that they recognise all the malware samples used in our test. We congratulate those manufacturers who took part in the public test, as we feel their commitment is a valuable contribution to improving their products and thus preventing the spread of cybercrime.

A more complete list of available antivirus programs for the Mac can be seen here:
<http://www.av-comparatives.org/av-vendors-mac>

Summary

Nine of the products we have reviewed receive our Approved Security Product award. Unfortunately, we were unable to give Kromtech Mackeeper an award, due to a number of issues relating to the initial system analysis².

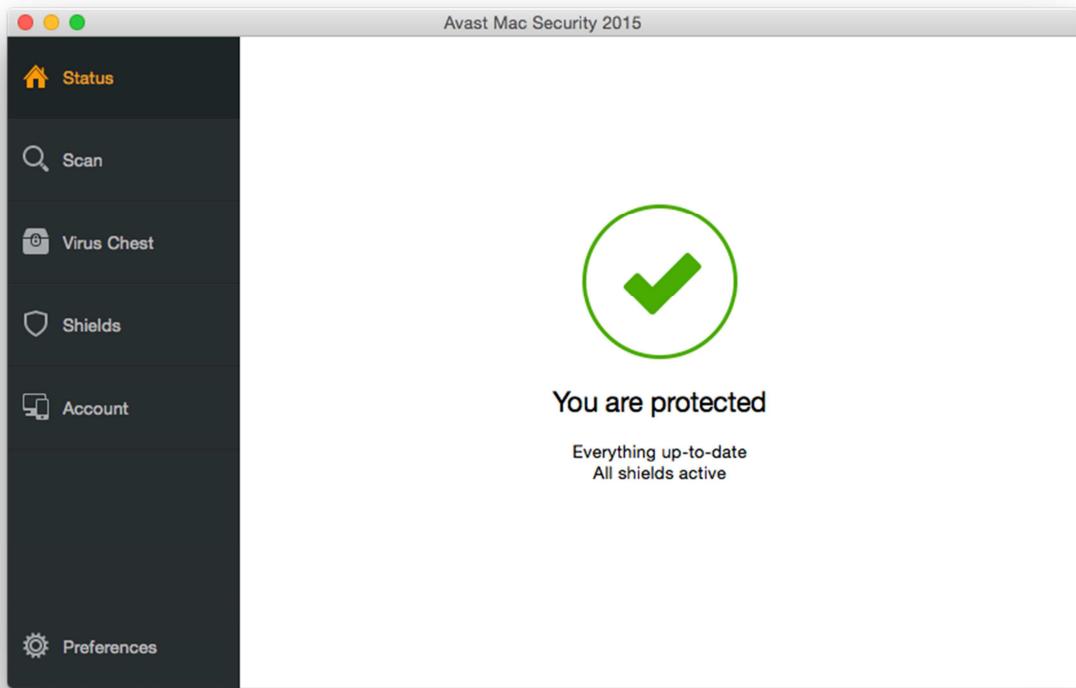
The test covers protection against Mac malware and detection of Windows malware, while the review looks at ease of use and help functions. Potential users should also consider additional features and price before choosing a product. We always recommend installing a trial version of any paid-for product before making a purchase.

	<p>Avast Free Antivirus for Mac identified 100% of samples in our Mac malware test. The user interface is modern and largely very straightforward to use.</p>
	<p>AVG AntiVirus for Mac is a simple, easy-to-use antivirus program for Mac, with all essential features. Its detection of Mac malware was perfect.</p>
	<p>Avira Free Antivirus for Mac combines excellent protection against Mac malware (99% detected) with a new, well-designed interface.</p>
	<p>Bitdefender Antivirus for Mac provides very good Mac malware detection (99%), but may have difficulty removing some of the malware detected. The program is mostly very easy to use.</p>
	<p>ESET Cyber Security Pro is a fully featured security program with a very clearly laid-out user interface. It identified 100% of our Mac malware samples.</p>
	<p>F-Secure SAFE for Mac is a very simple, easy-to-use antivirus program, albeit with minimal features. It detected 100% of Mac malware in our test, but provides very little detection of Windows malware.</p>
	<p>Intego Mac Premium Bundle X8 identified 100% of our Mac malware samples, and the interface would be fine for experienced Mac users. Detection of Windows malware was limited, however.</p>
	<p>Kaspersky Internet Security for Mac combines perfect protection against Mac malware (100% detected) with a very usable interface.</p>
	<p>Sophos Antivirus for Mac is a free program that is extremely effective at protecting against Mac malware (100% detected). It also detected 100% of Windows malware, but could not remove all of it. Its minimalist interface would be fine for experienced Mac users.</p>

² Please see detailed report starting on page 50.

X	Kromtech MacKeeper has a usable interface and good detection of Mac malware (98%). However, we feel that some users may find the program's initial analysis of the Mac to be misleading.
----------	---

Avast Free Mac Security 2015



Product version reviewed

10.14

Operating systems supported

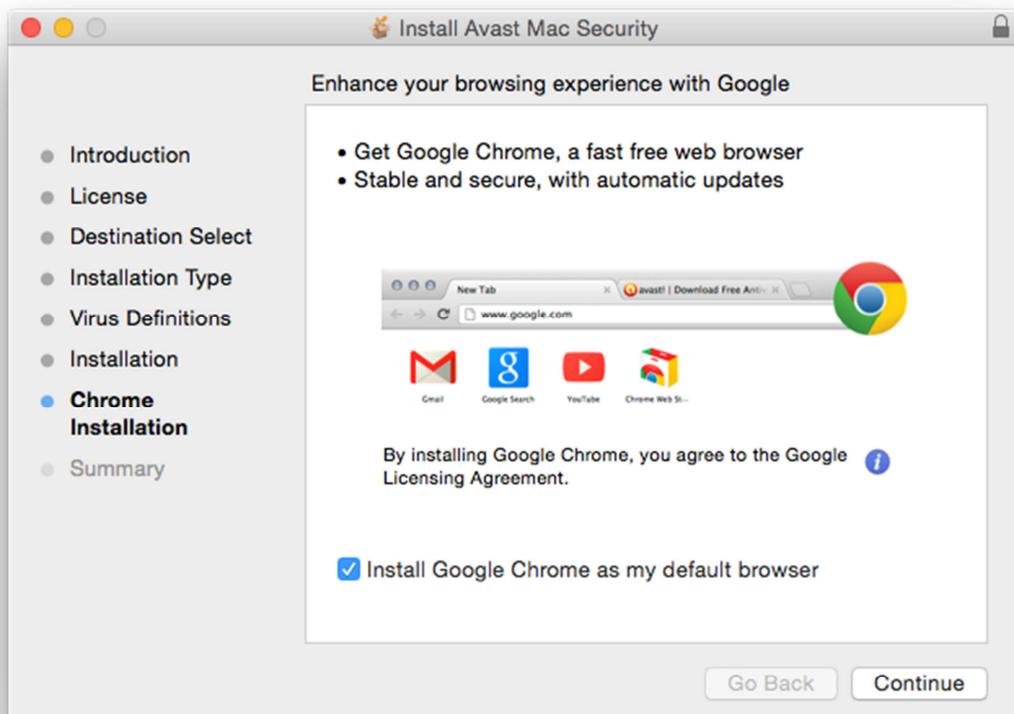
OS X 10.6.8 and later

Additional features

Avast Free Mac Security is a straightforward antivirus program.

Installation

A 9 MB .DMG installer is downloaded from the Avast website (a 180 MB offline installer is also available). We note that the OS is recognised and the user is automatically taken to the appropriate page for the Mac product. The setup wizard involves accepting a licence agreement, and there is the option to change the installation folder location. The installer also offers to install Google Chrome (we declined):



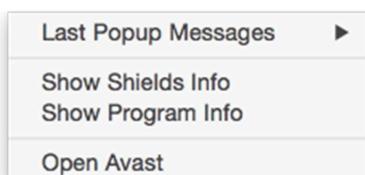
The program can be uninstalled by re-running the installer file, or from the *Avast Mac Security* menu (described in the online FAQ page).

Main window

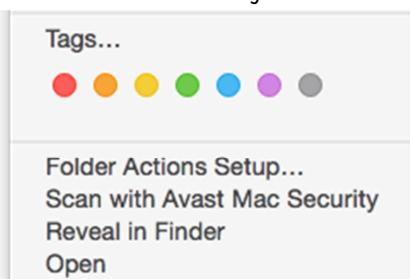
The home page of the main program window shows protection status, and provides buttons for scans, quarantine and settings (amongst other things).

Operating system integration

Avast Free Mac Security adds the following menus to the Mac menu bar: *Avast Mac Security*, *Edit*, *Tools*, *Window*, *Help*. There is also a System Tray icon, which displays the following menu:



Avast adds a scan entry in the Finder context menu:



Maintenance

If real-time protection is turned off, an alert is shown in the status display:



There is however no obvious way of reactivating the protection, the user has to go into *Preferences* to find the appropriate switch. The promising-looking *Shields* link in the menu panel does not have an on/off switch.

Malware signatures can be updated by going into *Preferences*, *Updates*, and clicking *Update now*.

Non-administrator access

Disabling the protection requires administrator credentials to be entered, even if the current user has administrator status.

Scanning

The *Scan* page, accessible from the link of the same name, provides options for full and custom scans, and removable-drive scans:

The interface shows a list of scan types with icons, descriptions, and action buttons:

- Full System Scan** (Icon: Computer monitor):
 - Description: Performs an in-depth scan of the whole system.
 - Action Buttons: **Start** (gray button), **Settings** (orange link).
- Removable Volumes Scan** (Icon: Camera):
 - Description: Performs a scan of any mounted removable volumes.
 - Action Buttons: **Start** (gray button), **Settings** (orange link).
- Custom Scan** (Icon: Folder):
 - Description: Performs a scan of any selected folders and/or files.
 - Action Buttons: **Start** (gray button), **Settings** (orange link).

We could not find a means of setting a scheduled scan.

Settings, quarantine and logs

Settings can be accessed from the *Preferences* link in the menu panel. Quarantine is opened by clicking *Virus Chest*, also in the menu panel. Logs can be found under *Shields | History*, with a separate log for each protection component:

The screenshot shows the Avast Shields interface. At the top, there are tabs for 'Activity' and 'History'. Below this, three sections are listed: 'File System Shield', 'Mail Shield', and 'Web Shield'. Under 'Web Shield', a table displays the following log entries:

URL	VIRUS NAME	TIME
http://www.amtso.org/check-desktop-phishing-page	URL:Mal	Today 11:52
http://www.amtso.org/amtso/uploads/PotentiallyUnwanted.exe	Win32:AmtsoTest-A [PUP]	Today 11:52
http://www.eicar.org/download/eicar.com	EICAR Test-NOT...	Today 11:51
http://www.amtso.org/check-desktop-phishing-page	URL:Mal	Yesterday 15:02
http://www.eicar.org/download/eicar.com	EICAR Test-NOT...	Yesterday 14:59

Malware and phishing alerts

When the EICAR test file is downloaded, the following alert is shown – it persists until the user clicks it:



In the case of the AMTSO Potentially Unwanted test file, a similar alert is shown, along with a block page in the browser window:

Infection detected!

<http://www.amtso.org/amtso/uploads/PotentiallyUnwanted.exe>

The requested URL contains malicious code that can damage your computer. If you want to access the URL anyway, turn off the Avast web shield and try it again.

Infection type: Win32:AmtsoTest-A [PUP]

The AMTSO phishing test page is also blocked with a similar browser alert and pop-up warning.

Malware protection test

Avast Free Mac Security identified and disabled 100% of both Mac and Windows malware in our test.

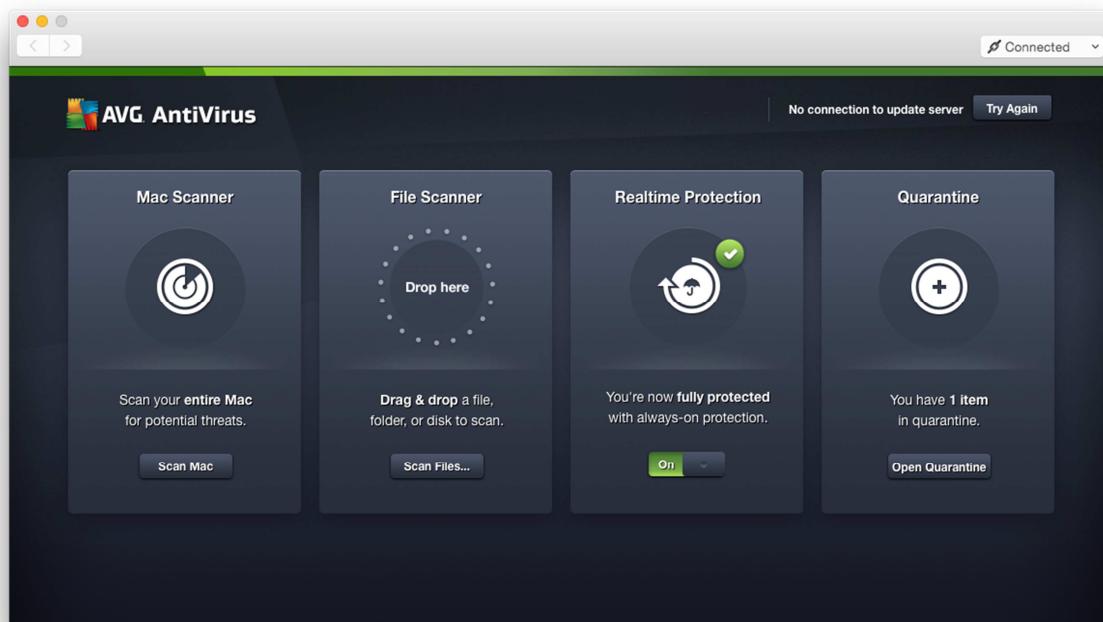
Help

The product's help feature is an online FAQ section, accessible from the *Help* menu. We found that of the *Hot Topics* links at the top of the page, four out of five articles specifically relate to previous versions of the program, 8.x or 9.x.

Verdict

We feel Avast Free Mac Security has all the important features of an antivirus program and is largely very simple to use. We particularly liked the informative and persistent malware alerts. A suggestion for improvement would be to add a "Fix-All" button to make it easier to reactivate the protection if it is disabled. Protection against both Mac and Windows malware in our test was flawless.

AVG AntiVirus for Mac



Product version reviewed

2015.0.4801

Operating systems supported

OS X 10.8 or later

Additional features

AVG AntiVirus for Mac is a straightforward antimalware program. The latest version includes quarantine and a whitelisting feature.

Installation

A 211 MB .DMG installer file is downloaded from the AVG website. The installation wizard involves accepting the licence agreement, and allows the user to change the installation folder. When installation is complete, the program window opens and invites the user to register an AVG account or log in with an existing one. There is a *Skip for Now* option; it appears that the program functions fully if the user clicks on it.

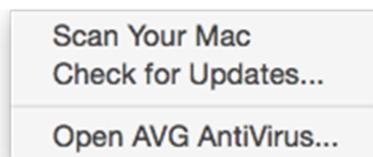
The software can be uninstalled from the *AVG AntiVirus* menu in the Mac menu bar.

Main window

The main program window displays the status of real-time protection (in the right-hand panel) and signature updates. There are also two scan options: the *Mac Scanner* in the left-hand panel runs, and displays the progress of, a full scan, while the central panel can be used to drop files, folders or disks, or browse for items to scan. A quarantine tile completes the functionality.

Operating system integration

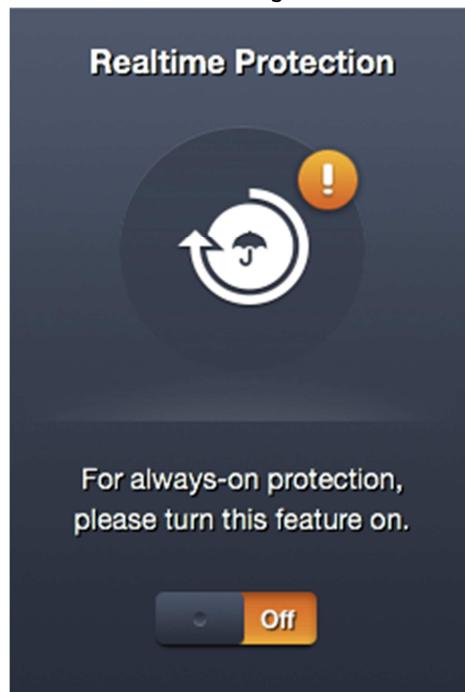
AVG AntiVirus for Mac adds four menus to the Mac menu bar: *AVG AntiVirus*, *Edit*, *Window*, *Help*. There is also a System tray icon, clicking which shows a short menu:



A Finder context menu is not shown.

Maintenance

If real-time protection is turned off, a warning is shown in the status panel, which also includes the button to turn it on again:



Malware signatures can be updated from the System Tray menu or *AVG AntiVirus* menu.

Non-administrator access

Disabling the protection always requires administrator credentials to be entered, regardless of whether the current user is an admin or standard user, thus preventing unauthorised access.

Scanning

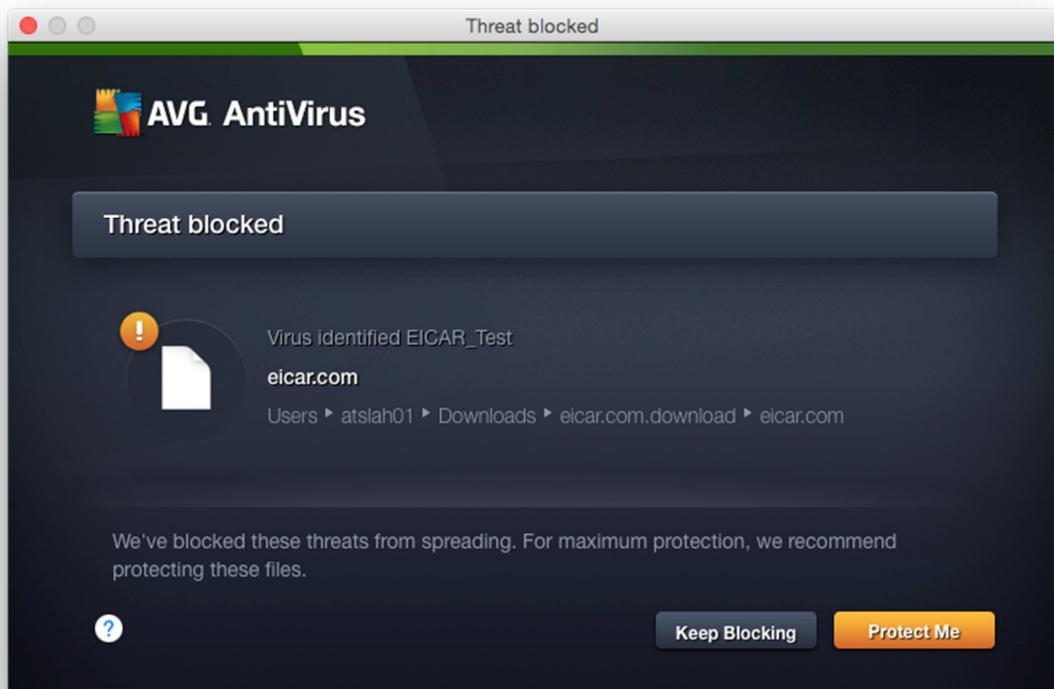
Full or custom scans can be run from the relevant panels on the home page. We could not find a means of scheduling a scan.

Settings, quarantine and logs

Settings (*Preferences*) can be accessed from the *AVG AntiVirus* menu in the Mac Menu bar. Quarantine has its own tile in the main program windows; we could not find a separate log feature.

Malware and phishing alerts

If the EICAR test file is downloaded, the following alert is shown:



The alert for the AMTSO Potentially Unwanted test file is the same. Clicking the highlighted *Protect Me* button quarantines the detected file. The AMTSO phishing test page was not recognised in our test.

Malware protection test

In our test, AVG AntiVirus for Mac identified and disabled 100% of both Mac and Windows malware samples.

Help

The local help file, accessed from the *Help* menu in the Mac menu bar, provides simple text instructions for the program's features:

The screenshot shows a Mac OS X style window titled "AVG AntiVirus Help". The main content area has a blue header "Update". Below it, a text block says: "Keeping **AVG AntiVirus** up-to-date is essential for its correct functioning. To update immediately:" followed by a numbered list. A callout box contains a note about automatic updates. Another text block at the bottom explains how to find the last successful update.

Keeping **AVG AntiVirus** up-to-date is essential for its correct functioning.
To update immediately:

1. In the menu bar, click on the **AVG AntiVirus** menu, or on the **AVG AntiVirus** status icon:
2. Select **Check for updates**.

💡 Usually, you will not need to worry about updating because **AVG AntiVirus** updates automatically every day for you.
The manual update is advisable if 1) you are about to run a scan, 2) your Mac has been offline for some time and could not have been updated automatically.

The current update status (updated/outdated) is displayed in the top right corner of the main page of **AVG AntiVirus**.
To find out the date of the last successful update:

1. In the menu bar, click on the **AVG AntiVirus** menu.
2. Select **About AVG AntiVirus**.
3. Look for the line **Last update**.

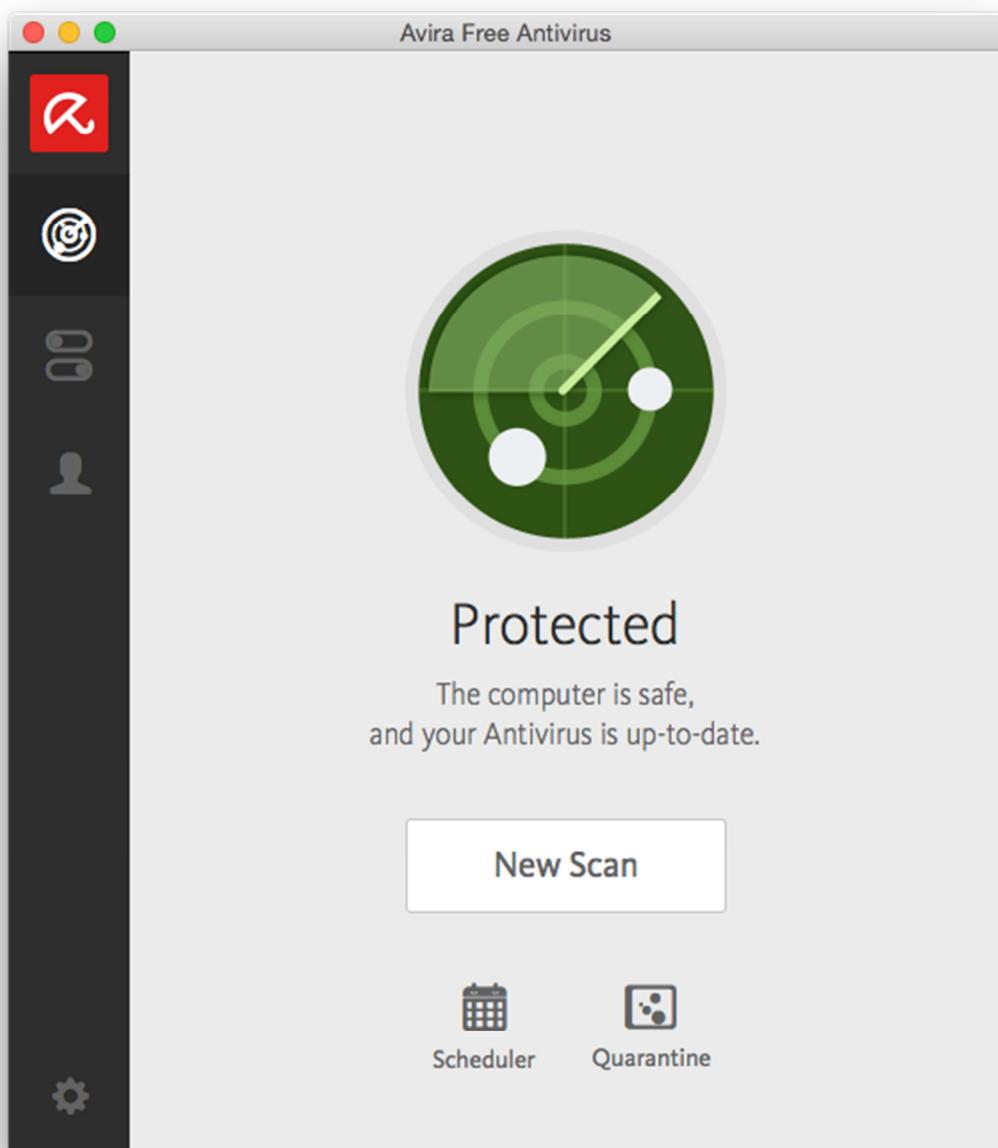
What is actually an update, why is it so important?
The main purpose of an update is to add definitions of new threats to the internal database stored locally on your Mac. This is very important because new threats emerge every day, and fully updated antivirus program is the most reliable protection from them.

In the example above, we liked the explanation of what an update is and why it's important, and the note about automatic updates and when a manual update is advisable.

Verdict

AVG AntiVirus for Mac is a free antivirus program with real-time protection, on-demand scanning and quarantine. Whilst we slightly miss a separate log feature, the program's simplicity makes it very easy to find and use the available functions. Its protection against Mac and Windows malware in our test was flawless.

Avira Free Antivirus for Mac



Product version reviewed

3.1.0

Operating systems supported

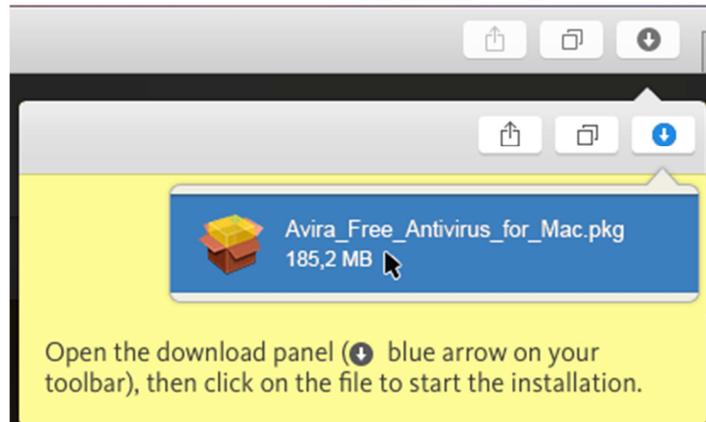
Mac OSX 10.9 (Mavericks) or higher

Additional features

Avira Free Antivirus for Mac is a straightforward antimalware program.

Installation

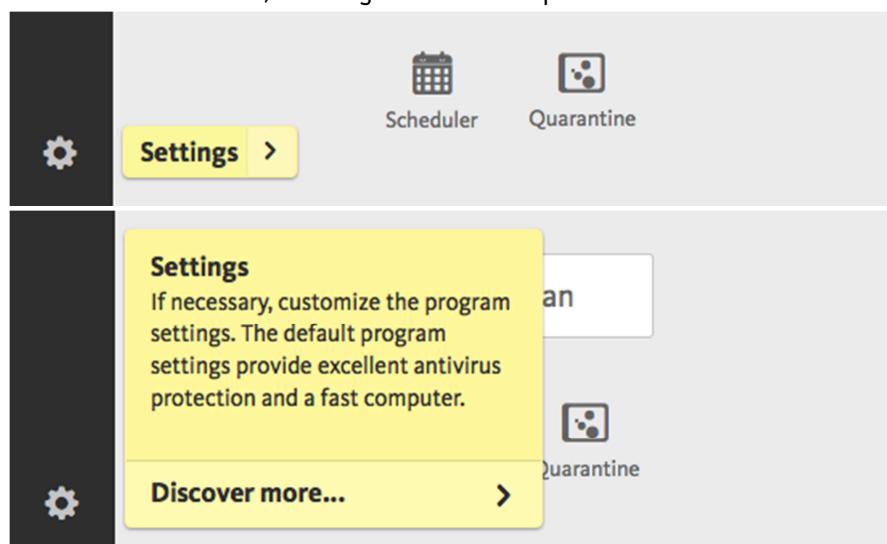
A 187 MB .PKG installer file is downloaded from the Avira website. We notice that the site automatically detects the operating system and takes the user to the appropriate download. The page shows how to run the installer when it has been downloaded:



The setup wizard requires the user to accept a licence agreement, and there is the option of changing the installation folder location. Otherwise, there are no decisions to make. The program can be uninstalled with its own removal tool, which is located in the Applications | Utilities folder. Instructions for using this are provided in Avira's online knowledge base.

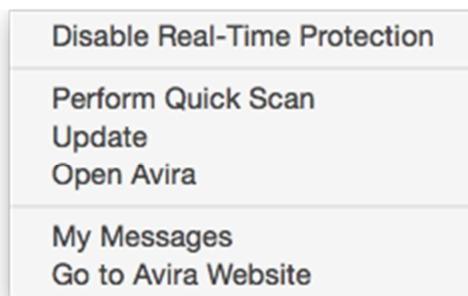
Main window

The home page of the program window has a status display, scan button, and links to the scheduler and quarantine. On the left-hand side of the window is a menu bar with buttons for settings, accessing the Avira account, enabling or disabling real-time protection, and returning to the home page. There is an Avira umbrella symbol at the top of the menu bar, but this is just a graphic and has no function. We note that hovering with the mouse over a button displays a big tool tip with the button's function; clicking on the arrow provides more details:



Operating system integration

Avira adds two menus to the Mac menu bar: *Avira* and *Help*. It also displays a System Tray icon, clicking which shows the following menu:

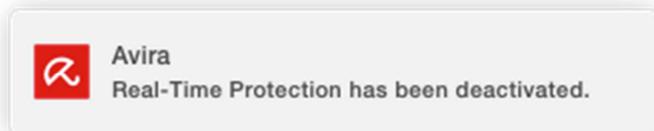


The System Tray icon indicates whether protection is enabled or not, by showing an open umbrella for protection active, closed umbrella for protection inactive.

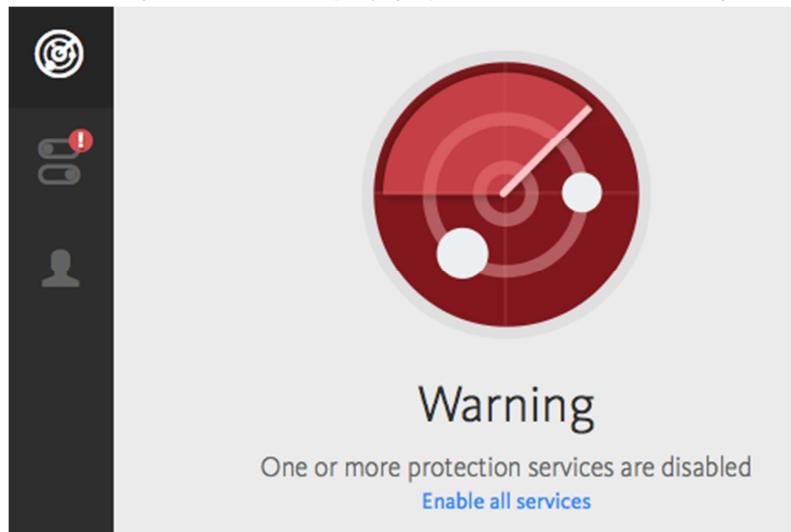
The Mac Finder context menu is not altered.

Maintenance

If real-time protection or firewall is turned off, a warning message pops up in the top right-hand corner of the screen:



Additionally, the status display graphic and text both change to show an alert:



Clicking *Enable all services* immediately reactivates the protection.

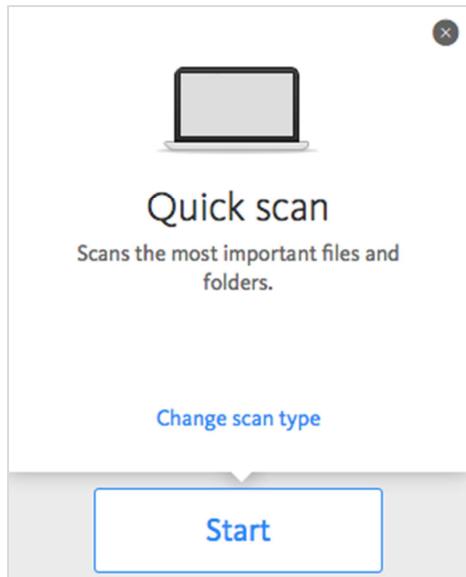
Malware signatures can be updated by clicking *Update* in the program's System Tray menu.

Non-administrator access

Disabling real-time protection always requires administrator credentials to be entered, regardless of whether the current user is an administrator or standard user, thus preventing unauthorised access.

Scanning

Clicking the *New Scan* button on the home page runs a quick scan by default, but allows the user to change to a full scan by clicking *Change scan type*:



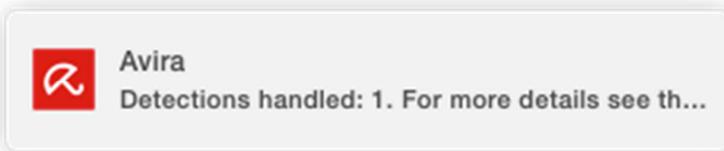
The *Scheduler* button, just below the scan button, allows a scheduled scan to be configured.

Settings, quarantine and logs

Settings (*Preference*) can be accessed from the cog-wheel icon in the bottom left-hand corner of the program window, or the *Avira* menu in the Mac menu bar. Quarantine is easily accessible from the button of the same name on the home page. Despite much searching, we were unable to find a log of malware detection (only the settings for configuring the database size). The System Tray menu includes the entry *My messages*, but we did not find any messages displayed in this.

Malware and phishing alerts

When the EICAR test file or AMTSO Potentially Unwanted test file is downloaded, the respective file is quarantined and the following alert is shown:



Unfortunately, the message box is not big enough to display the full message, so the user cannot see where to find more details. Clicking or double-clicking the message itself has no effect.

The AMTSO phishing test page was not recognised in our test.

Malware protection test

In our test, Avira Free Antivirus for Mac identified and disabled 99% of Mac malware, and 100% of Windows malware samples.

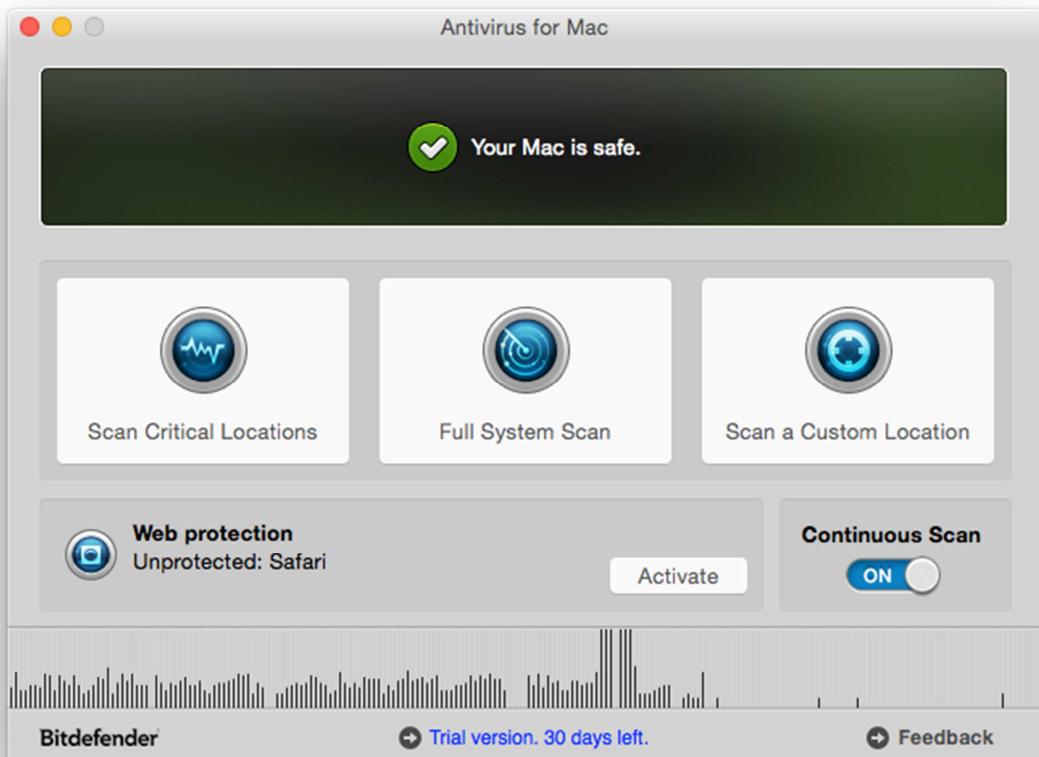
Help

Clicking the program's *Help* menu in the Mac menu bar, then *Avira Help*, opens the product's knowledge base on the Avira website. This has a very prominent search box for entering queries. We were able to find detailed and illustrated instructions for uninstalling Avira Free Antivirus for Mac, but a query on running an update only produced answers on how to update the product version rather than the signatures.

Verdict

The latest version of Avira's Free Antivirus for Mac is something of a departure from the previous design, but we found that it is still very simple to use and makes most important functions easy to find. We particularly liked the instructions on the download page for starting the installer, and the expandable tool tips in the main program window. We were however unable to find a log of malware detections. Protection against Mac malware in our test was all but flawless, and neutralisation of Windows malware perfect.

Bitdefender Antivirus for Mac



Product version reviewed

3.3.9151

Operating systems supported

Mac OS X 10.7, 10.8, 10.9, 10.10

Additional features

We would describe Bitdefender Antivirus for Mac as a fully-featured antivirus program.

Installation

A 184 MB .DMG installer is downloaded from the Bitdefender website. When opened, this provides not only install and uninstall options, but a link to the product's manual too:



The setup wizard requires the user to accept a licence agreement. There is the opportunity to change the installation folder location, but otherwise no choices to be made. At the end of the process, an activation dialog lets the user try the program for free, enter an existing licence key, or buy one online.

The program can be uninstalled using its own uninstaller, located in the Applications folder. This is described in the manual.

Main window

The main window features an overall status display, buttons for a quick, full or custom scan, a button to enabling/disabling real-time protection (*Continuous Scan*), a panel showing the status of the *Web protection* feature, and subscription information.

Operating system integration

Bitdefender adds the following menus to the Mac menu bar: *Antivirus for Mac*, *File*, *Edit*, *Window*, *Actions*, *Help*. There is a System tray icon, which displays the following menu:

- No new files to scan
- Turn OFF Continuous Scan
- Preferences...
- Open Main Window

The Finder context menu is not altered.

Maintenance

If the real-time protection is turned off, the status display warns of this:



Clicking the arrow to the right of the text immediately reactivates the protection. Malware signatures can be updated by clicking *Update Virus Database* in the *Actions* menu.

Non-administrator access

Deactivating the protection requires administrator credentials to be entered, regardless of whether the current user has administrator privileges, thus preventing unauthorised access.

Scanning

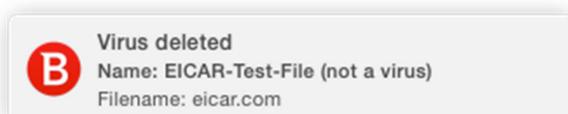
Full, quick and custom scans can be run from their respective buttons on the home page. We could not find a means of scheduling a scan.

Settings, quarantine and logs

Settings (*Preferences*) and logs (*Show History*) are located in the *Antivirus for Mac* menu. Quarantine can be opened by clicking *View Quarantine* in the *Actions* menu.

Malware and phishing alerts

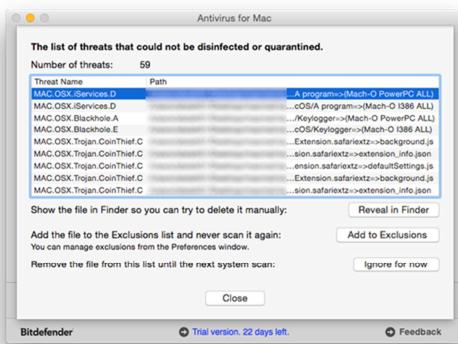
If the EICAR test file is downloaded, the following alert is shown:



A similar alert is shown for the AMTSO PUA file. The AMTSO phishing test page was not recognised in our test.

Malware protection test

In our test, Bitdefender identified and disabled 100% of Windows malware samples. It also detected 99% of our Mac malware samples. However, in a number of cases, the program stated that it was unable to disinfect or quarantine the Mac malware; the only option offered was to show the relevant files one by one in the Finder, and delete them manually:



Using this method we were able to manually delete all but 3% of the detected samples.

Help

The *User Guide*, accessible from the installer file, is very comprehensive at 45 pages. It has been very clearly laid out and well-illustrated with screenshots. A clickable contents page and bookmarks make it easy to find the right page.

Verdict

Bitdefender Antivirus for Mac strikes us a fully featured antivirus program with a very straightforward and easy-to-use interface. The manual is produced to a very high standard and is very easy to access from the installer. Windows malware detection and removal was perfect. All but one of the Mac samples was detected, although the program was unable to remove three of these inactive threats. We feel this last point is something that Bitdefender could improve.

ESET Cyber Security Pro



Product version reviewed

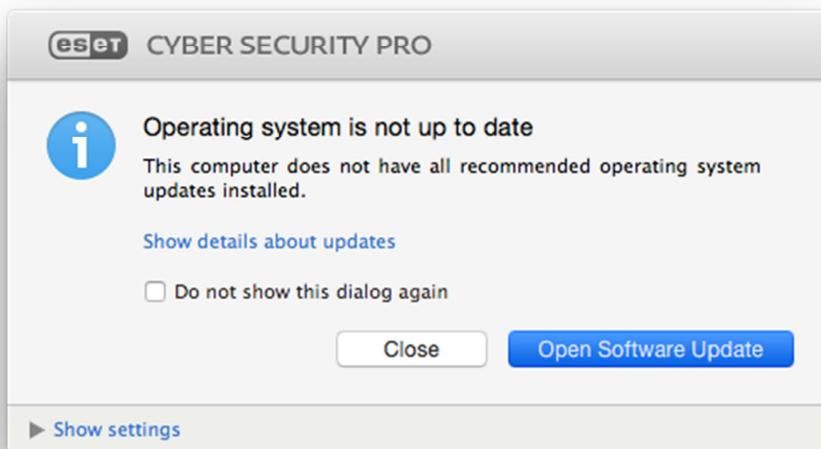
6.0.14 (2014)

Operating systems supported

Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10

Additional features

As well as malware protection, ESET Cyber Security Pro includes a firewall and parental controls. We note that the program also warns the user as soon as an operating system update becomes available:



Installation

A 59 MB .DMG file is downloaded from the ESET website. Double-clicking it starts the setup wizard, which displays the system requirements at the beginning. The user has to accept a licence agreement, decide whether to join ESET's *Live Grid* data-sharing scheme, and whether to enable protection of potentially unwanted programs. A custom option is available, which allows advanced options such as specifying a proxy server. The user is also asked to activate the product, whereby a 30-day trial version can be selected. At the end of the setup process, a dialog asks the user whether the current network should be regarded as home, work or public (on account of the integrated firewall in the product).

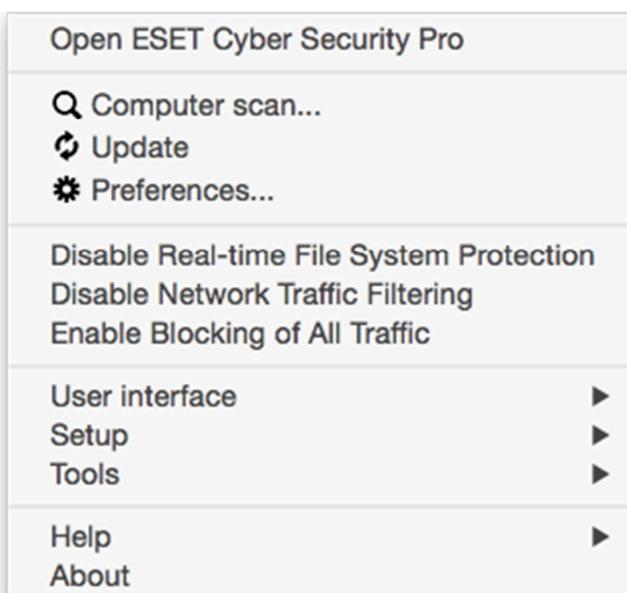
There are two possible methods of uninstalling the software, both described in the *User Guide*: re-running the installation CD or downloaded installer file and clicking *Uninstall*; using the Mac Finder to locate the local uninstaller program.

Main window

The home page of the main program window includes a very prominent status display, with the text *Maximum Protection* when all the protection features are enabled and working. Four icons show the status of individual components: *Computer* (real-time protection), *Firewall*, *Web & Email*, *Parental Control*. The latter icon is initially shown as inactive, to alert parents to the fact that the feature has to be enabled and configured. Also shown on the home page are *Update* and *Smart Scan* (quick scan of the most important areas) and subscription information. A menu panel on the left-hand side enables easy access to further scan options, settings (*Setup*), *Tools*, and the help features.

Operating system integration

By default, ESET Cyber Security Pro does not make use of the Mac OS Menu Bar, nor does it display an icon in the Dock when the program window is opened. However, both of these can be activated together by checking *Present application in Dock* in the settings. In any event, the program can be accessed via its icon in the System Tray – clicking this shows a menu of common tasks, including opening the main program window:



An entry in Finder's context menu is not displayed by default but can easily be activated from the settings, which adds the following sub-menu:

- Folder Actions Setup...
- ESET Cyber Security Pro - Submit files to ESET
- ESET Cyber Security Pro - Scan
- ESET Cyber Security Pro - Clean
- ESET Cyber Security Pro - Add files to Quarantine
- Reveal in Finder
- Open

Maintenance

If real-time protection or the firewall is turned off, an obvious warning is shown in the status display. This includes a text link to reactivate the inactive component:

Maximum protection is not ensured



Computer



Firewall



Web and Mail



Parental Control

Disabled Protection

Real-time file system protection was disabled by the user. The computer is not currently protected against threats. [Enable Real-time file system protection](#).

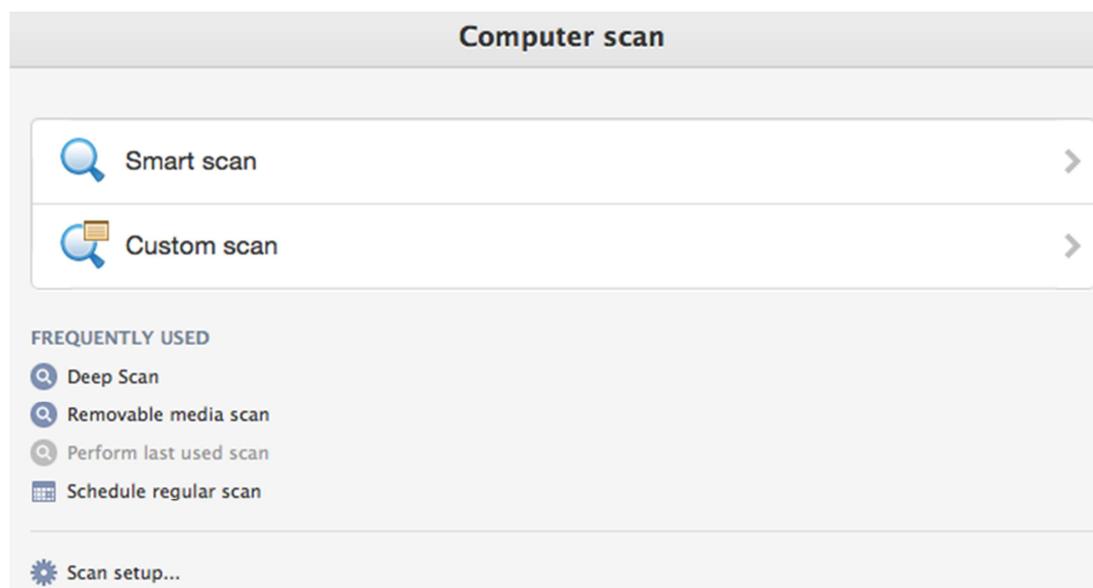
Signatures can be updated from the link on the home page, or the *Update* button in the menu panel.

Non-administrator access

When used under a non-administrator account, the entry for disabling real-time protection is removed from the System Tray menu, and in the main program window, all relevant controls are greyed out. This prevents unauthorised users from disabling the protection.

Scanning

The *Computer Scan* page provides a variety of scan options: *Deep Scan* (full), *Smart Scan* (quick scan of most important areas), *Custom Scan*, and *Removable Media Scan*. A scheduled scan can also be set up:



Settings, quarantine and logs

Quarantine and logs can be found by clicking *Tools* in the menu panel:

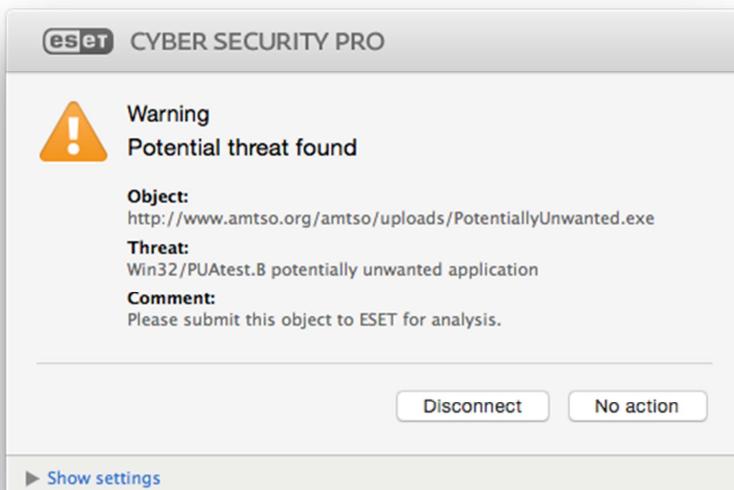
	Log files	Show log files	>
	Protection Statistics	Display graph with statistics data	>
	Scheduler	Show scheduler	>
	Quarantine	Add, restore and delete quarantined objects	>
	Running processes	Reputation information powered by ESET Live Grid	>
	Submit file for analysis	Submission of a suspicious file to ESET's lab for...	>
	ESET Social Media Scanner	Open ESET Social Media Scanner web page	>

Malware and phishing alerts

The alert below is shown when the EICAR test file is downloaded:



In the case of the AMTSO Potentially Unwanted test file, the following dialog is shown (assuming that detection of PUAs was enabled during setup or later on):



If the user attempts to open the AMTSO phishing test page, ESET Cyber Security Pro shows the following block page:

The screenshot shows a red header bar with 'ESET Cyber Security Pro'. Below it is a warning message:

Potential phishing threat

This page is identified as a phishing page. [Show URL](#)

Phishing pages often look similar to pages of known banks or other trusted institutions in order to acquire personal information such as usernames, passwords or credit card details. You are not advised to proceed to this page.

- [Learn more about phishing](#)
- [This page is not a phishing page](#)

Buttons at the bottom include '← Go Back' and 'Proceed to the site'.

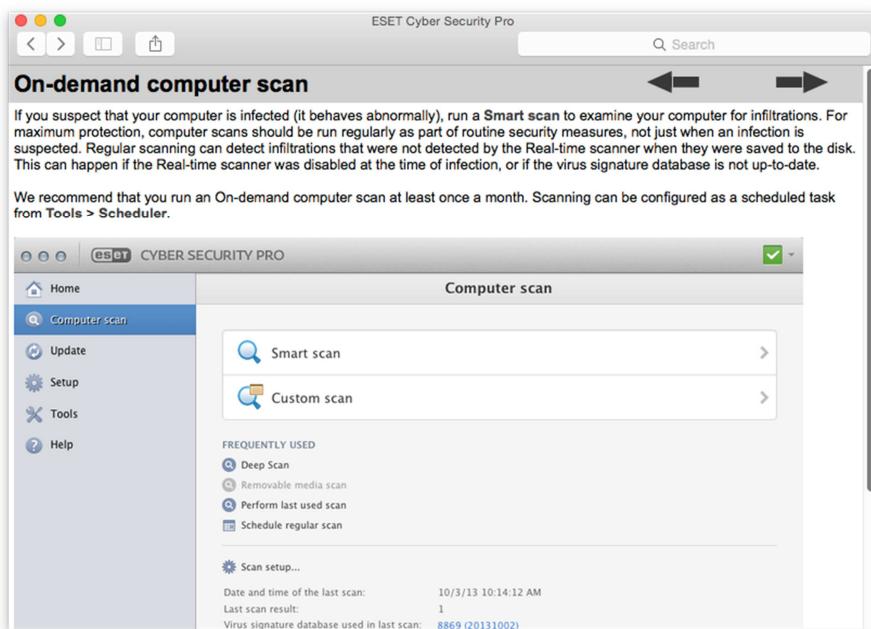
At the bottom right: Open ESET Knowledgebase | [www.eset.com](#)

Malware protection test

ESET Cyber Security Pro identified and disabled 100% of both Mac malware and Windows malware in our test.

Help

The local help feature, accessible from the System Tray menu or *Help* page in the main program window, displays an overview of tasks functions; clicking on one of these opens a page of text instructions, frequently illustrated with screenshots:



The online Knowledgebase, also accessed from the System Tray menu or *Help* page, provides very detailed instructions illustrated with annotated screenshots, and even video tutorials:

How do I download, install and activate ESET Cyber Security?
KB Solution ID: SOLN3237 | Last Revised: May 05, 2014
[Details](#)

Solution

- I. Install ESET Cyber Security
- II. Activate ESET Cyber Security

KB video tutorial

I. Install ESET Cyber Security

1. Download the latest install package from the ESET download page (or insert the ESET Cyber Security CD into your CD drive):
[Download ESET Cyber Security](#)
2. The install package will appear in your **Downloads** folder or the default folder set by your browser. Click the file to open it (if you inserted a CD in step 1, the **ESET Cyber Security CD** window will open automatically. Double-click **English**).
3. Double-click the **Install** icon. When prompted, click **Continue** to launch the Installation Wizard.

Tools

- [Printer Friendly](#)
- [Rate this Page](#)

Additional Assistance

- [Malware Descriptions](#)
- [Submit a Case Online](#)

Community

- [ESET User Forums](#)
- [Visit us on Facebook](#)
- [Follow us on Twitter](#)
- [ESET KB on YouTube](#)

ESET produce two manuals for Cyber Security Pro. There is Quick Start Guide, which is 12 pages long, and covers installation and using the most essential features. Also available is the *User Guide*, which at 25 pages is more comprehensive, and includes an index. Both have been produced to a very high standard, are well illustrated with screenshots, and can be downloaded very conveniently from the same page as the program's installer.

Verdict

We feel that ESET Cyber Security Pro retains all the plus points of previous versions, namely a clear and well-laid out interface, easily accessible features, along with good alerts and outstanding help facilities. Protection against both Mac and Windows malware in our test was perfect.

F-Secure SAFE



Product version reviewed

15524

Operating systems supported

Mac OS X 10.6.8 and later³

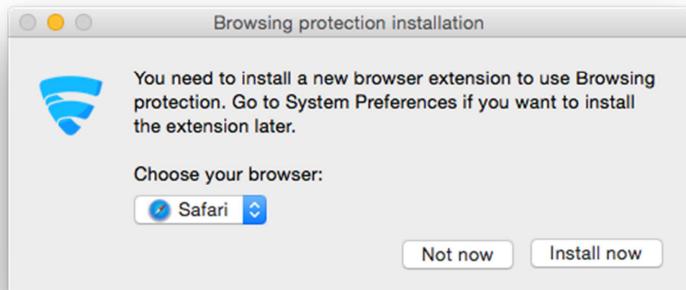
Additional features

F-Secure SAFE for Mac is an antimalware program with web protection (includes “traffic light” colour rating of search-engine links); there is also a feature called *Banking Protection*, which “notifies you whenever you access verified, secure banking sites”, according to the feature’s settings page.

Installation

The program is installed from a 33.4 MB .MPKG installer file. The installation wizard requires the user to accept the licence agreement, and there is the option of changing the installation folder. When installation is complete, the user is asked whether to install the browser protection; we chose to install it.

³ On OS X 10.7 or lower, there is a different GUI, and Browsing Protection/Banking Notification/Security Cloud are not included.



The help file provides instructions for uninstalling the product via its uninstaller program in the Applications folder.

Main window

A status display is provided in the form of a graphic of a Mac, and a text display that also shows subscription status and the time & date of the last update. There are buttons marked *Scan* (which immediately starts a default scan), and *Preferences*, as well as a button for the help feature. A tab marked *Tools* provides access to other functions, such as update, custom scan, and logs.

Operating system integration

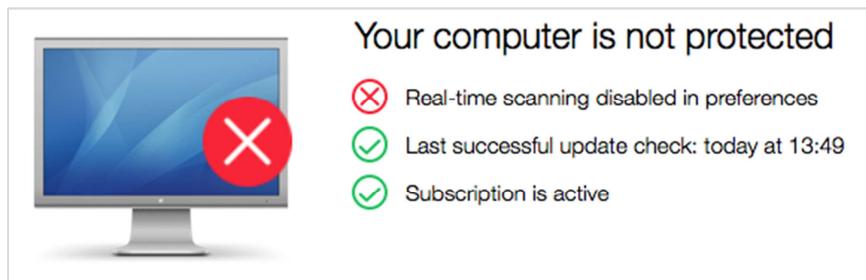
F-Secure SAFE for Mac uses the Mac menu bar, with the menus *F-Secure SAFE*, *Edit*, *Window*, *Help*. There is also a System Tray icon, which displays the following menu:



The Mac Finder context menu is not altered.

Maintenance

If real-time protection is switched off, the status display changes to show this:



Switching the Mac firewall off from the Mac System Preferences displays a similar warning. Malware signatures can be updated by clicking the *Tools* tab, then *Check for updates*.

Non-administrator access

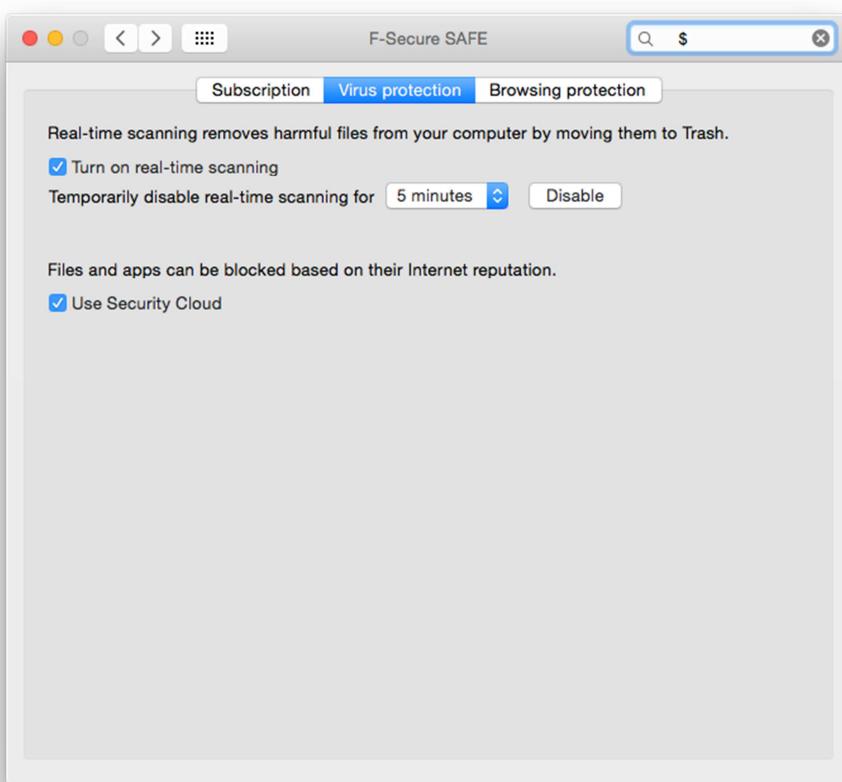
Disabling the real-time protection requires administrator credentials to be entered, regardless of whether the current user has administrator rights or not.

Scanning

A full scan can be run by clicking the *Scan* button on the home page, while the *Choose what to scan* button on the *Tools* tab lets the user browse for a particular folder to scan. We could not find a means of scheduling a scan.

Settings, quarantine and logs

Settings can be accessed from the *Preferences* button on the home page of the program. We note that the available options are very limited:



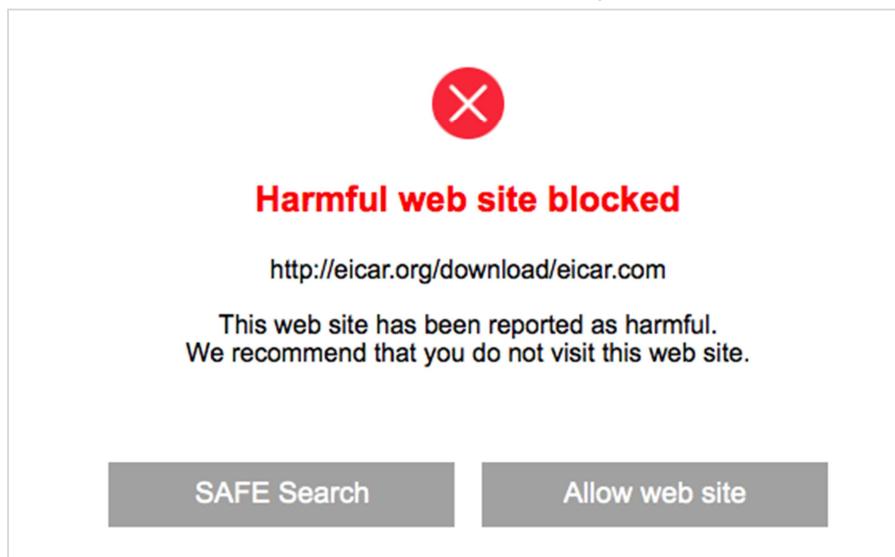
The *Infection report...* button on the *Tools* tab shows the malware detection log:

Infections					
File name	Malware name	Action	File modification time	Detection time	
/Downloads/eicar.com	EICAR_Test_File	Trashed	14 Jun 2015 12:50:03	14 Jun 2015 12:5	
/Downloads/Potentially...	Application:W32/...	Access reported	23 Jun 2014 23:12:42	14 Jun 2015 12:5	
/Downloads/eicar.com	EICAR_Test_File	Access reported	23 Jun 2014 23:12:42	14 Jun 2015 12:5	
/Downloads/eicar.com	EICAR_Test_File	Trashed	14 Jun 2015 12:52:02	14 Jun 2015 12:5	
/Downloads/eicar.com	EICAR_Test_File	Trashed	14 Jun 2015 13:06:56	14 Jun 2015 13:0	

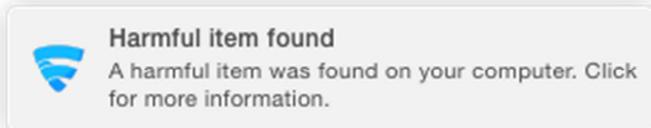
There is no quarantine function as such. The EICAR test file, which is detected as malware, is put into the Mac Trash folder, which then effectively functions as quarantine. However, as we could not find a means of whitelisting files, moving the file out of the Trash folder merely leads to it immediately being re-detected and thus sent straight back to the Trash.

Malware and phishing alerts

If the EICAR test file is downloaded, the following alert is shown:



Similar alerts are shown for the AMTSO PUA test file and phishing test page. In the case of the AMTSO cloud protection test file (Cloudcar), the following alert is shown:



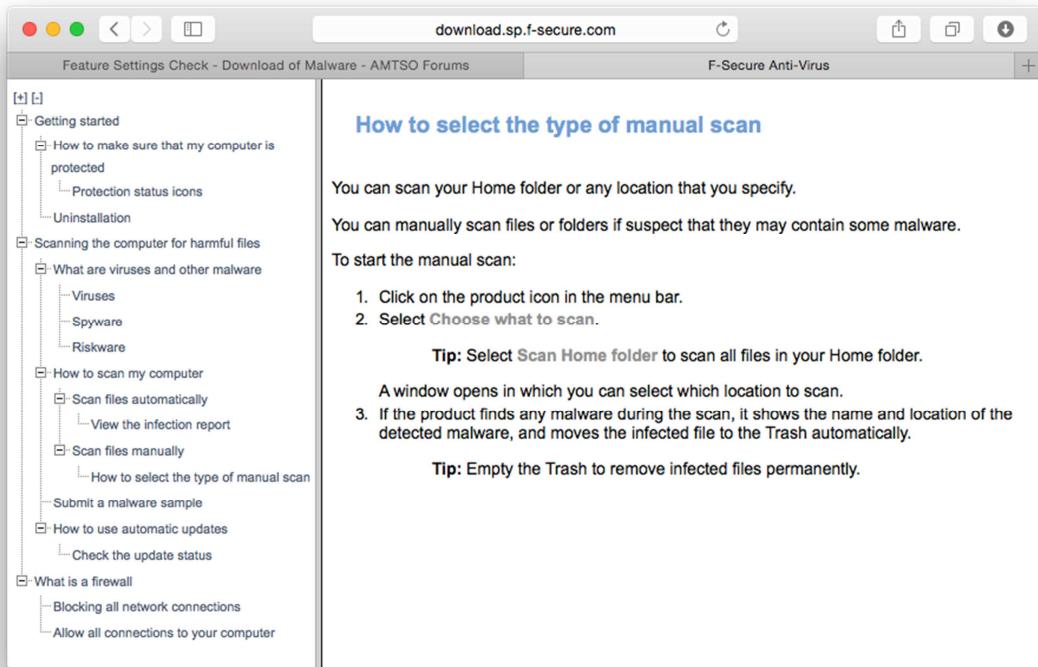
Clicking on the alert opens the *Infections* window (see screenshot in the previous section).

Malware detection test

In our test, F-Secure SAFE for Mac identified and disabled 100% of our Mac malware samples, but only 28% of Windows malware samples. F-Secure tell us that their focus "is on detecting Mac malware and protecting the computer against relevant threats as well as possible".

Help

Clicking the ? symbol in the main program window, or the *Help* menu and then *Help* will open the program's local help feature. This provides very simple text instructions for using the program:



How to select the type of manual scan

You can scan your Home folder or any location that you specify.

You can manually scan files or folders if suspect that they may contain some malware.

To start the manual scan:

1. Click on the product icon in the menu bar.
2. Select Choose what to scan.

Tip: Select Scan Home folder to scan all files in your Home folder.

A window opens in which you can select which location to scan.

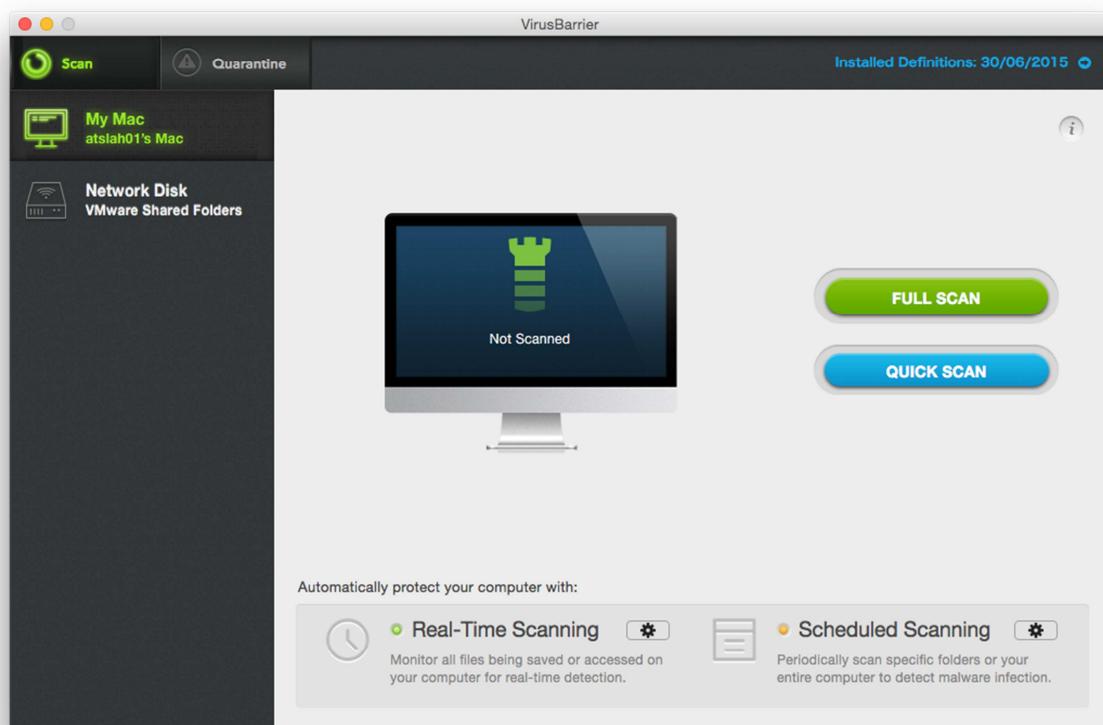
3. If the product finds any malware during the scan, it shows the name and location of the detected malware, and moves the infected file to the Trash automatically.

Tip: Empty the Trash to remove infected files permanently.

Verdict

F-Secure SAFE for Mac could be described as a simple antivirus program that is largely easy to use. Suggestions for improvement include a useable quarantine function, a Fix-All button to reactivate protection when necessary, and an extension of the minimalist program settings. Whilst its protection against Mac malware is exemplary, it missed the great majority of our Windows malware samples.

Intego Mac Premium Bundle X8



Product version reviewed

10.8.4

Operating systems supported

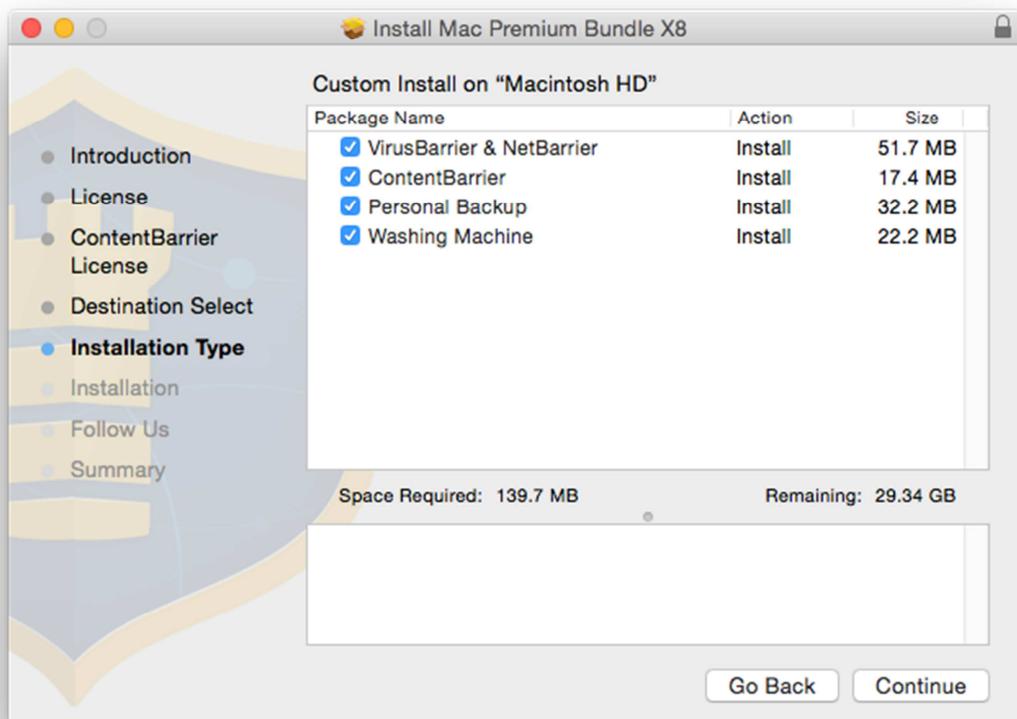
Mac OS X 10.7 or later

Additional features

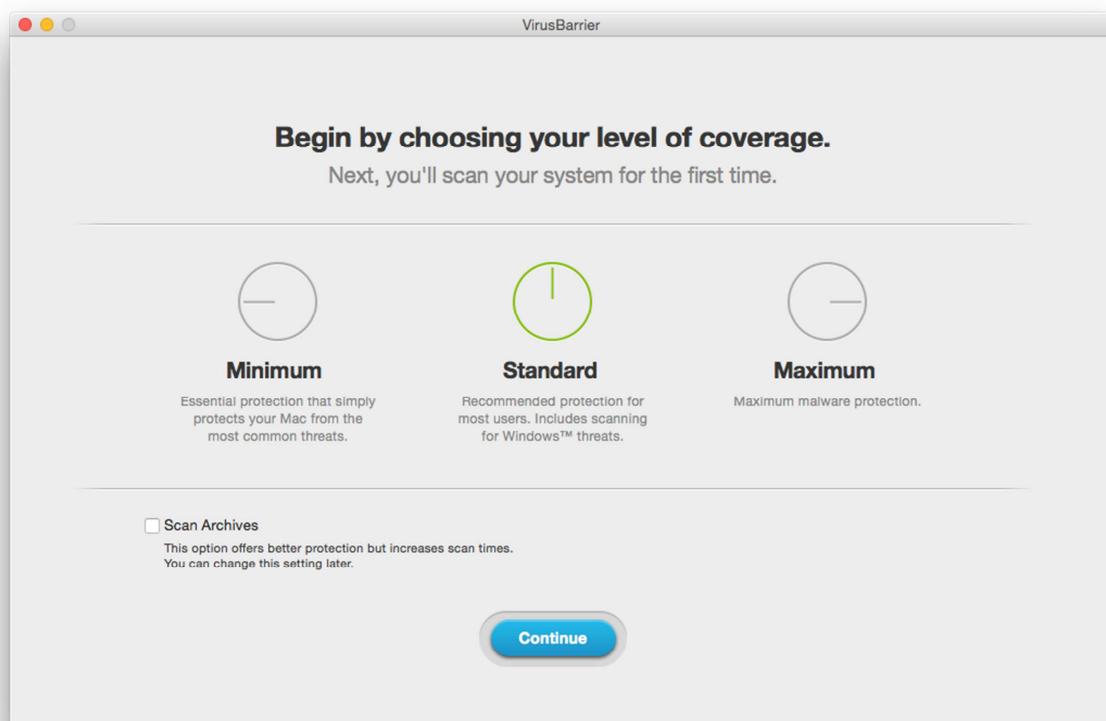
In addition to malware protection, the Mac Premium Bundle X8 includes a firewall, backup, parental controls and a cleaning tool.

Installation

A 92 MB .DMG installer file is downloaded from the vendor's website. The setup wizard requires the user to accept a licence agreement, and provides a choice of components to install:



A restart is required after installation. After this, the product has to be activated or the trial version selected. The program asks the user to define a protection level (we used the default *Standard*):



When the main program window is first opened, an overlay with a quick-start guide is shown:



The software can be uninstalled by re-running the setup program and selecting *Uninstall Software*. This is described in the program's knowledge base.

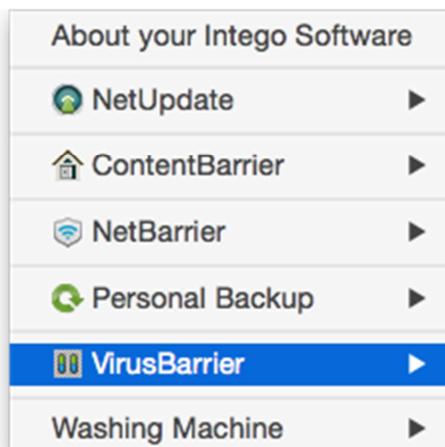
Main window

The main program window provides buttons for full and quick scans, links to drives, definitions display/update button, and links/status display for real-time scanning and scheduled scanning.

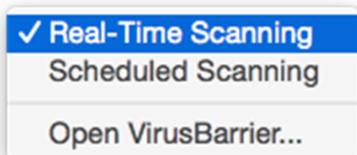
Operating system integration

The Mac menu bar shows menus for *VirusBarrier*, *File*, *Edit*, *View*, *Window* and *Help*.

There is a System Tray icon, which displays sub-menus for the different components:



The VirusBarrier sub-menu looks like this:



A *Scan with VirusBarrier* entry is added to the Finder context menu.

Maintenance

There is a subtle status display for real-time scanning and scheduled scanning: a “light” next to each function is shown in green for active, yellow for inactive.

Malware signatures (which are updated automatically) can be manually updated by clicking the Installed Definitions link in the top right-hand corner of the window.

Non-administrator access

If the user is logged on with a non-administrator account, administrator credentials have to be entered to disable the protection.

Scanning

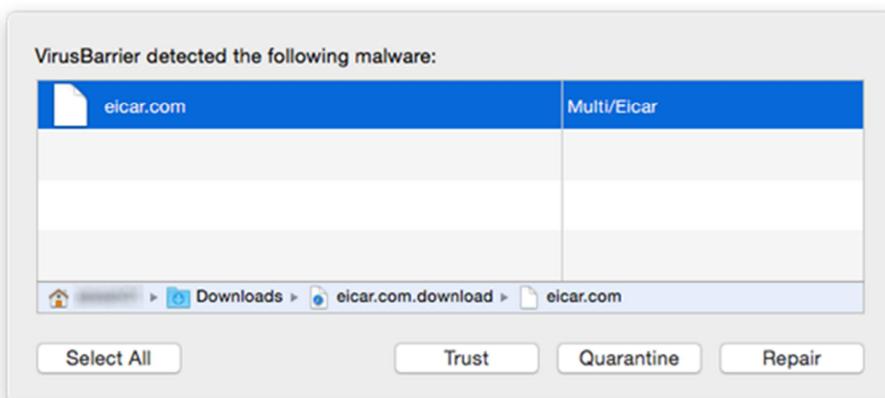
Quick, full and scheduled scans can be run from their respective buttons on the program’s home page. A custom scan can be started by dragging a drive, folder or file from Finder to the iMac graphic in the program window.

Settings, quarantine and logs

Settings (*Preferences*) can be found in the *VirusBarrier* menu. Quarantine has its own button in the top left-hand corner of the window. Logs can be found in the *Window* menu.

Malware and phishing alerts

If the EICAR test file is downloaded, the following alert is shown:



If the user enables detection of *Hacking tools* and *Keyloggers* in the settings (or selects *Maximum protection* at the end of the installation process), Virus Barrier detects the AMTSO PUA test file, with a similar alert to the one above being shown.

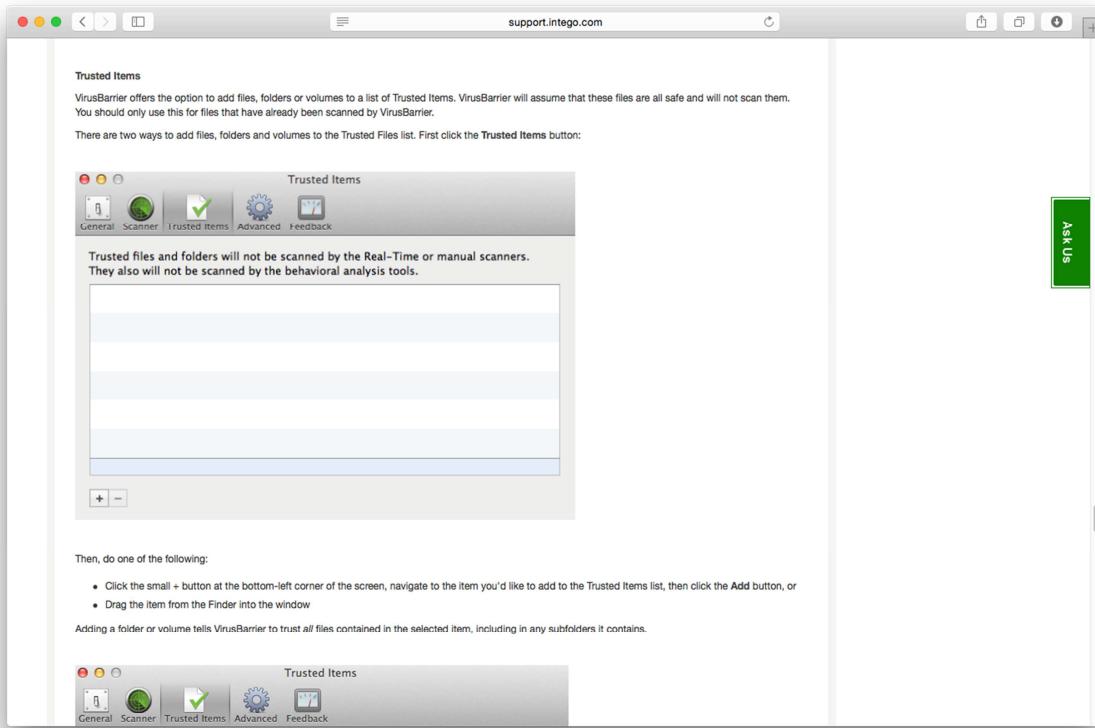
Intego does not support the AMTSO phishing test page.

Malware protection test

Intego VirusBarrier identified and disabled 100% of the Mac malware in our test. However, it was much less successful with Windows malware, detecting only half of the samples.

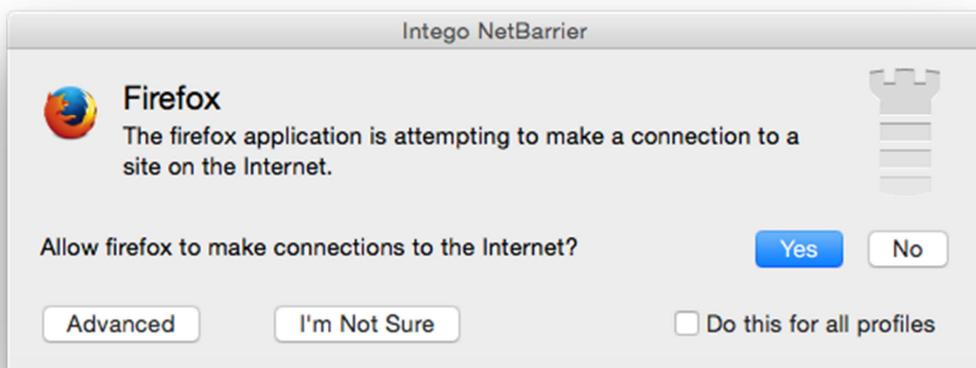
Help

Clicking the *Help* menu, *VirusBarrier Help* opens the program's online manual. This provides clear, very well-illustrated instructions for installing, configuring and using the product:

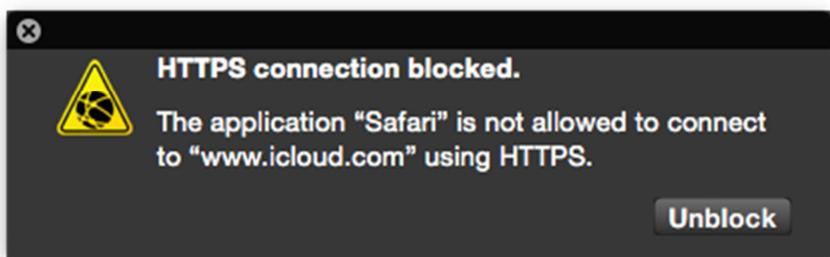


Other points of interest

We found that NetBarrier – the firewall component included in the Premium Bundle suite – frequently asked whether to allow common applications such as Firefox and Dropbox to access the Internet:



We note that when we logged in with a standard-user account, a number of alerts were shown, showing connections that had been blocked:



Verdict

We found Intego Mac Premium Bundle X8 to be straightforward to install, with a good help feature. The antivirus component is largely straightforward to use. We did however find the firewall component, NetBarrier, to be very intrusive sometimes, with potential for confusing non-expert users. Whilst VirusBarrier protected against 100% of the Mac malware in our test, it only identified half of our Windows malware samples.

Kaspersky Internet Security for Mac



Product version reviewed

15.0.1

Operating systems supported

Mac OS X 10.7, 10.8, 10.9, 10.10

Additional features

As well as anti-malware features, Kaspersky Internet Security for Mac includes *Parental Control*. Amongst other things, this allows parents to filter the websites their children can see, and to limit the time they spend surfing the Internet. It also includes *Safe Money*, which runs specified websites for financial transactions (such as online banking) in a protected mode in the browser. Another feature, *Network Attack Blocker*, is intended to provide protection against network attacks such as the Darwin Nuke⁴.

Installation

A 197 MB .DMG installer file is downloaded and run. This is a very simple process, the only option is whether to join the Kaspersky Security Network data-sharing scheme. When the installer has finished, the options *Try*, *Activate* and *Buy* are provided, allowing the user to test the trial version, enter a licence key, or buy a key online.

The program can be uninstalled by downloading a removal tool from the manufacturer's website. This process is described in detail in a knowledge-base article.

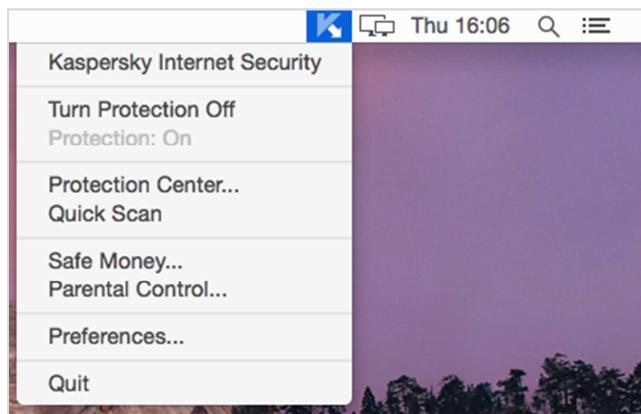
⁴ <http://www.itpro.co.uk/security/24379/your-iphone-and-ipad-are-at-risk-from-darwin-nuke>

Main window

This features a very prominent status display, with the essential functions scan, update, help, settings (*Preferences*) and licence information all easily accessible from the home page.

Operating system integration

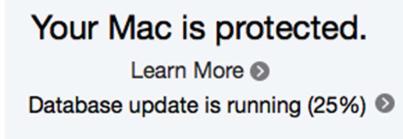
KIS for Mac uses the Mac OS Menu Bar, with the menus Kaspersky Internet Security, Edit, Protection and Window. It also displays an icon in the OS X System Tray, which shows a menu of common tasks:



The Mac Finder context menu is not altered.

Maintenance

Malware signatures can be updated using the big *Updates* button on the program's home page. The status display shows the progress of updates:



It also shows a warning if protection is disabled, and displays a button with which it can instantly be re-enabled:



Non-administrator access

The protection cannot be disabled from a standard-user account without entering administrator credentials.

Scanning

Clicking the *Scan* button on the home page opens the dialog box shown below:



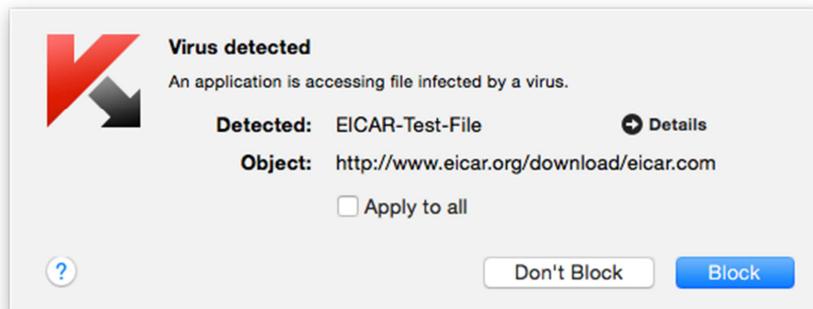
The user can run quick, full or custom scans from the buttons at the bottom, or drag individual files and folders into the main panel. There is no means of setting a scheduled scan. Whilst we would normally regard the latter as a useful feature, Kaspersky Lab say that they have not included it as they feel that other features in the program, such as a background scan and real-time protection, make it unnecessary.

Settings, quarantine and logs

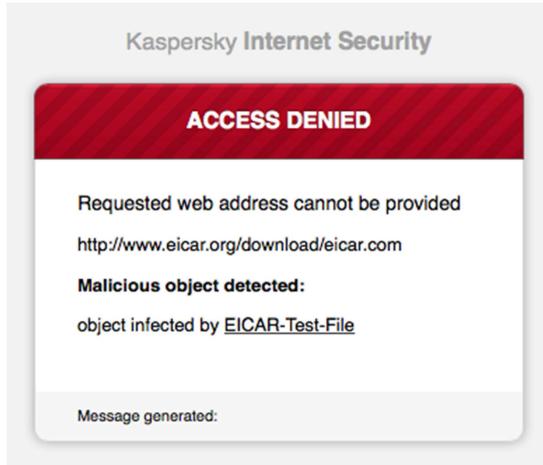
Settings can be accessed from the *Preferences* button in the menu panel at the top of the home page. Quarantine and logs can be accessed by clicking *Reports* in the same place.

Malware and phishing alerts

If the EICAR test file is downloaded, KIS for Mac shows the following alert:



Additionally, a block page is shown in the browser window:



Similar alerts (pop-up and browser window) are shown as for the AMTSO Potentially Unwanted test file and Phishing Test Page. Please note that the AMTSO Potentially Unwanted file is only recognised if the user selects detection of *Other programs* under *Preferences | Threats*.

Malware protection test

Kaspersky Internet Security for Mac identified and disabled 100% of Mac malware, and 100% of Windows malware in our test.

Help

Clicking the Help button on the menu bar at the top of the program window opens the local help service, which provides simple text instructions for all the features of the product. There are no screenshots as such, but as illustrated below, icons are shown when applicable:

The full scan task created by default is included in Kaspersky Internet Security. While running this task, the application scans all the internal drives of the computer for viruses and other threats.

To launch a full computer scan:

1. Open the [main application window](#).
2. Click the  button.
3. In the [Scan](#) window that opens, select the  [Full Scan](#) task.

A full scan of the computer starts automatically.

You can view the results of the task in the [reports window](#).

There is a 66-page manual with text instructions for Kaspersky Internet Security for Mac, which can be downloaded from the same page of the manufacturer's website as the software itself. It has comprehensive text instructions, although no screenshots aside from a few icons. Clicking the Help | Kaspersky Internet Security Support | Technical Support in the Mac Menu Bar opens the program's knowledge-base section on the Kaspersky Lab Website. This has step-by-step instructions for common tasks, well-illustrated with annotated screenshots:

The screenshot shows a web browser displaying a knowledge base article. The URL in the address bar is "Home → Support → Kaspersky Internet Security 15 for Mac". The main title is "Kaspersky Internet Security 15 for Mac" with version numbers "15.0" and "14.0" in a green box. Below the title, it says "How to run a scan task in Kaspersky Internet Security 15 for Mac". A button "◀ Back to 'Popular Tasks'" is visible. To the right, the date "2014 Nov 14" and ID "ID: 11535" are shown. The article starts with "1. How to start a scan task" and provides two steps: "1. Open Kaspersky Internet Security 15 for Mac." and "2. In the lower part of the window, click Scan.". Below this, there is a screenshot of the Kaspersky Internet Security application window. The window title is "Kaspersky Internet Security". The menu bar includes "Reports", "Preferences", "Support", and "Help". The main interface shows a large green checkmark icon with the text "Your Mac is protected." and a "Learn More" link. At the bottom, there is a navigation bar with four items: "Scan" (highlighted with a red arrow pointing to it), "Update", "Safe Money", and "Parental Control".

Verdict

We found the interface of Kaspersky Internet Security for Mac to be very well designed, with a clear layout that makes important features easy to find. We were also impressed with the illustrated instructions in the knowledge base. Protection against both Mac and Windows malware in our test was perfect.

Kromtech MacKeeper



Product version reviewed

3.4.15

Operating systems supported

Mac OS X 10.6 or later

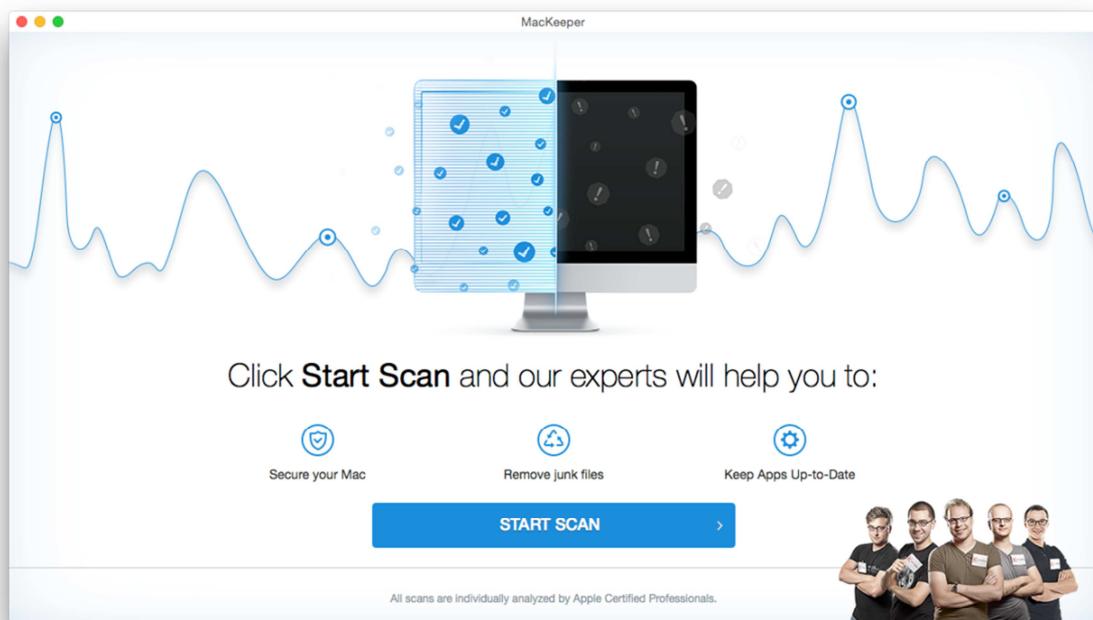
Additional features

In addition to antimalware features, MacKeeper includes a number of other functions. Aside from *Find & Fix*, which has to be run after installation, we did not test any of these. The list includes the following: *Anti-Theft*, *Duplicates Finder*, *Smart Uninstaller*, *Files Recovery*, *Data Encryptor*, *Files Finder*, *Disk Usage*, *Update Tracker*, *Backup*, and *Shredder*. There is also a support service called *Geek on Demand*.

Installation

A 173 KB .PKG downloader is downloaded from the manufacturer's website. The actual installation process is very simple, without any user decisions, and can be completed in a couple of clicks.

Once the program has been installed, the program window opens, and the user has to click *Start Scan* before anything else can be done with the program:



The window then shows a progress bar, along with a link entitled *Show what MacKeeper is scanning*. Clicking this does not actually provide any information about the scan, but rather gives some basic information about the hardware. Kromtech tell us that they intend to change the descriptive text of the link to make it more appropriate. Once the scan has been shown to have finished, the window displays some messages which it says are being provided by a "Senior Support Engineer" called Andrew, who is said to be analysing the scan results:

The picture of Andrew is identical to the one shown in the version we reviewed last year, who was named Michael Medvediev – see screenshot from last year's test below:

MacKeeper



Hello! My name is Michael and I am an Apple Certified specialist.

I have received your system scan report and I will start analyzing it right now.

MICHAEL MEDVEDIEV
Senior Support Engineer

In spite of his apparent change of name, Andrew assures us that he is a real person, and tells us "At the moment your Mac is in wonderful shape, but there is a number of threats that might affect its performance". He then goes on to list a variety of problems that might befall a Mac:

By the way, thanks for using our software.

At the moment your Mac is in wonderful shape, but there is a number of threats that might affect its performance.

Junk files is one of them.

Sometimes they can load when your system starts up, take up memory and slow your Mac down.

Junk files are unused parts of apps (binaries), localizations of the apps and caches (temporary system and internet files), and logs.

Unfortunately, even a short period of time is enough for a substantial amount of junk to accumulate.

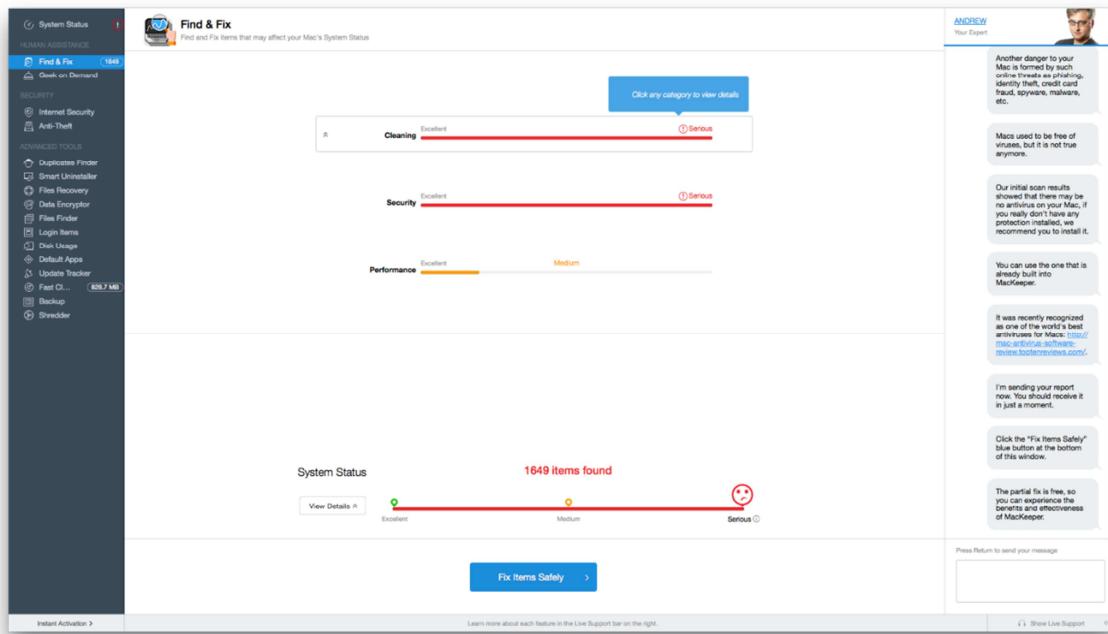
Additionally, some applications come with unneeded language packs and localizations by default.

But with MacKeeper you can remove current junk and make sure it doesn't accumulate in the future.

Another danger to your Mac is formed by such online threats as phishing, identity theft, credit card fraud, spyware, malware, etc.

Macs used to be free of viruses, but it is not true anymore.

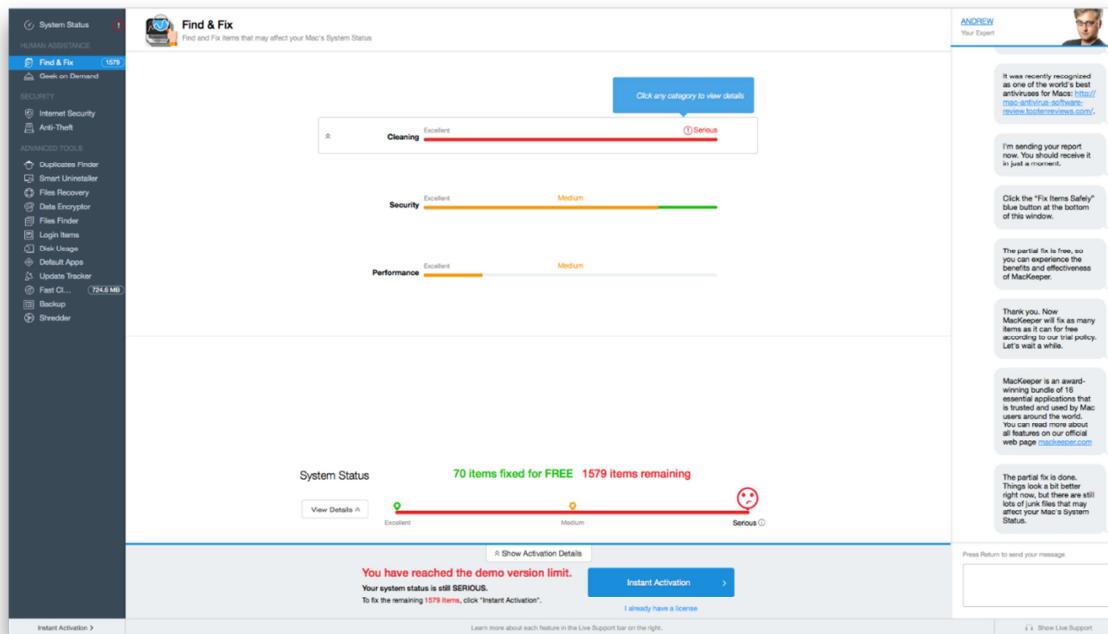
After this, a results page is shown. According to this, our freshly installed, up-to-date Mac, on which the only additional installed program is Dropbox (latest version at the time of testing), is in a *Serious* state (worst possible rating) with regard to *Cleaning* and *Security*, and overall. The status as regards *Performance* is unclear, as the status bar suggests *Excellent* whilst the colour suggests *Medium*. Kromtech tell us this is a flaw in the user interface, which will be corrected in the next version.



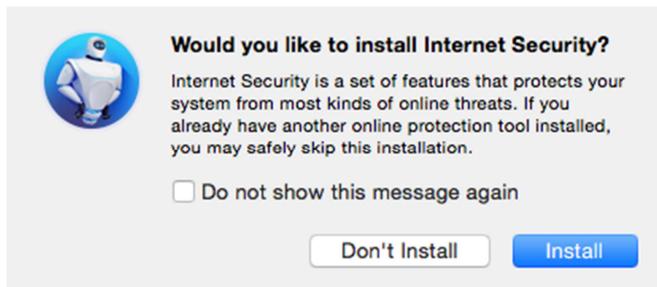
There is no explanation as to the difference between *Cleaning* and *Performance*. We note that Andrew's comments, now shown on the left, include a link to a website with a review of MacKeeper. The review correctly notes that AV-Comparatives tested the product last year (2014), and that its malware detection rate was poor compared to other programs in the test.

Shortly before publication of this report, Kromtech released version 3.4.17 of MacKeeper, which we installed on our test system. This found almost the same number of *issues* with the system – 1,627 – but this time classified all three areas (Cleaning, Security and Performance) as *Excellent*.

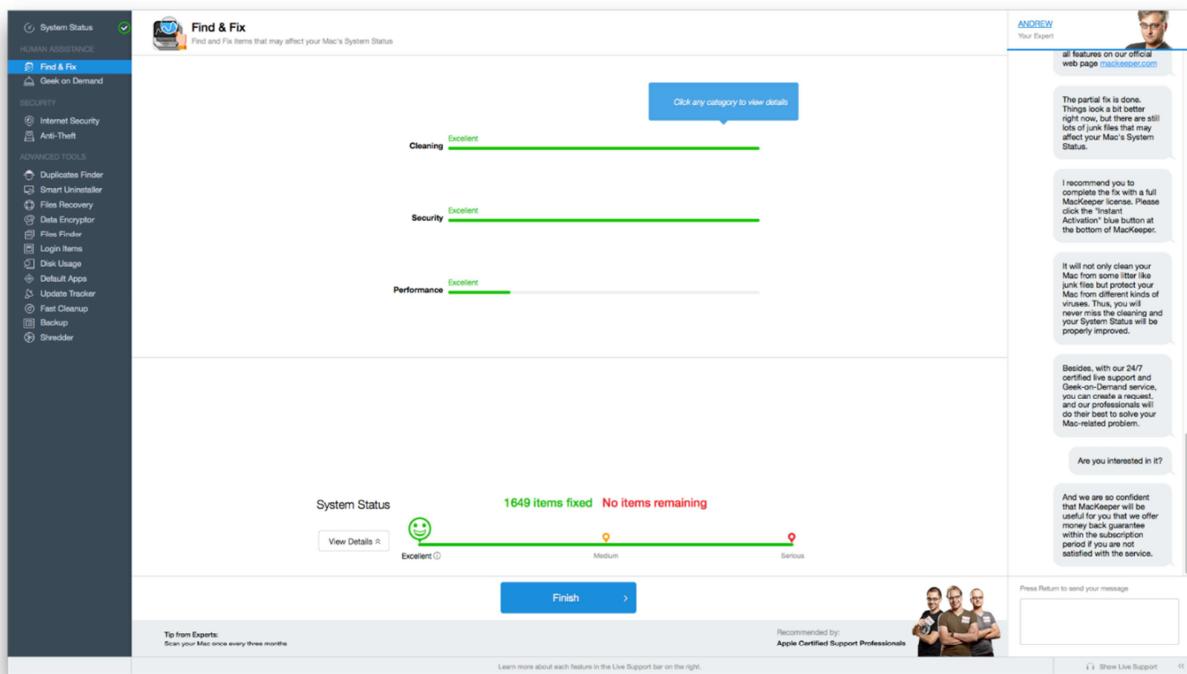
At the bottom of the page is a prominent button, marked *Fix Items Safely*. Clicking this then changes the display, as shown below:



The program now claims that 70 of 1579 *items* have been fixed. As a result of this, the *Security* status has changed from *Serious* to *Medium*, whilst all other ratings remain the same as before. We are then informed that the demo version limit has been reached, and that to fix the remaining *items*, we have to activate the program. No information is provided as to what any of the *items* are. Once a licence key has been entered, the program offers to install the *Internet Security* component:



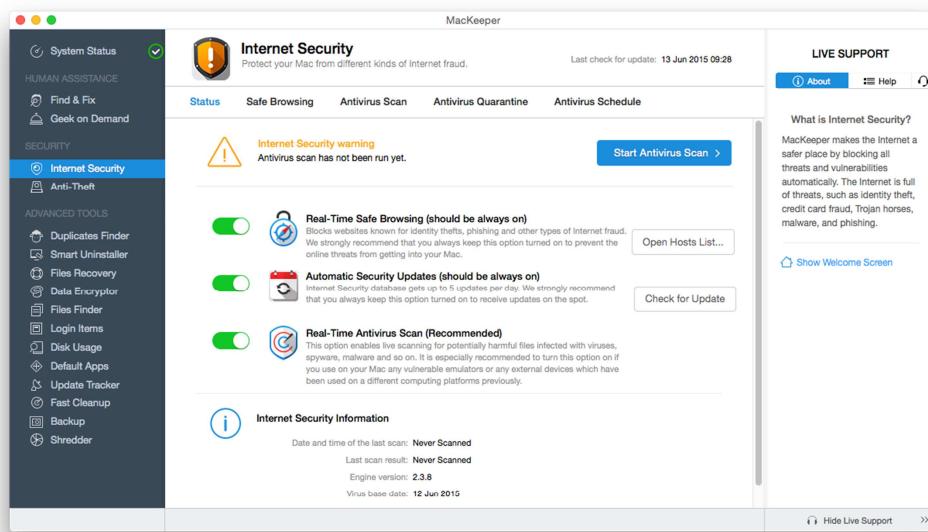
Clicking *Install* quickly sets up the component, after which the results page shows all *items* have been fixed:



According to the program's help feature, MacKeeper can be uninstalled by dragging its icon from the Applications folder to the Mac Trash bin.

Main window

When the program is first opened, a warning is shown to indicate that an antivirus scan has not yet been run. This persists until a full scan has been completed. The same alert also shows an alert if malware has been detected but not quarantined. However, no warning is shown if any or all of the protection components are switched off; Kromtech tell us that they intend to address this issue.



Scans can be run by clicking the *Antivirus Scan* link at the top of the window. This provides a choice of full or custom scans. Malware signatures can be updated from the *check for Update* button in the main pane of the window. The help function is opened by clicking *Help* in the *Live Support* panel on the right-hand side of the window. The *System Status* page of the application window states "Your license is activated", but does not give any further information.

Operating system integration

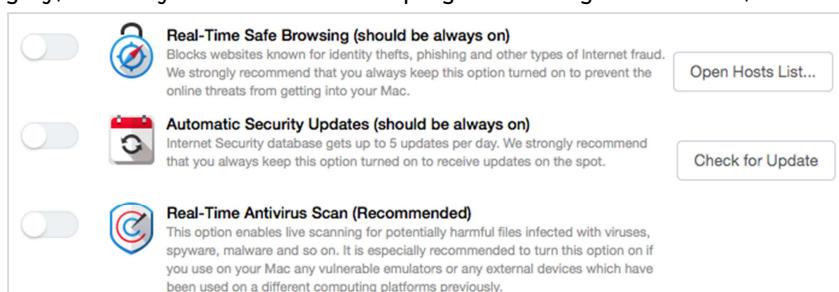
Four menus are added to the Mac menu bar: MacKeeper, Edit, Window and Help. There is also a System Tray icon, which displays the following menu:



The Mac Finder context menu is not altered.

Maintenance

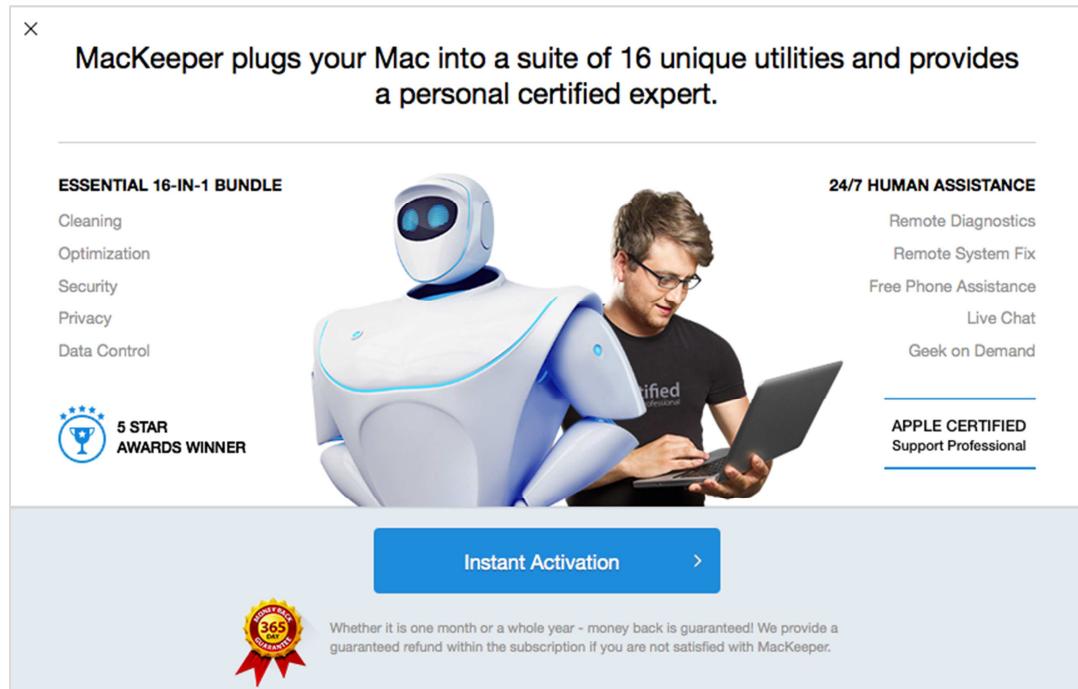
No warnings are shown if real-time protection or other protection components are turned off. The slider controls for the protection components are shown in green when active, but in a very soft grey, not very different from the program's background colour, when disabled:



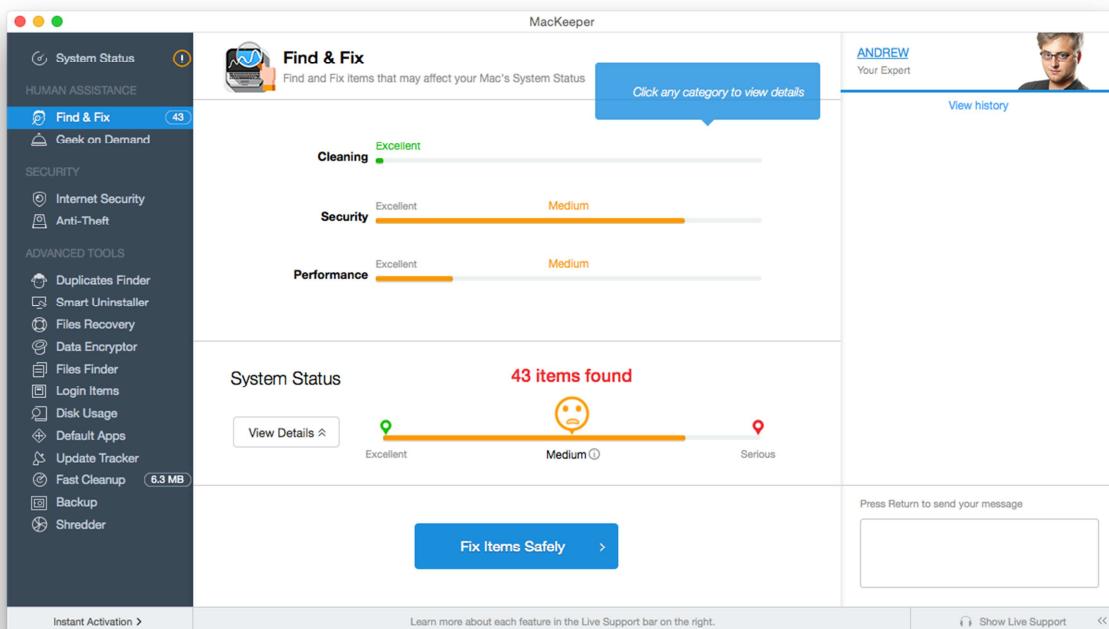
Signatures can be updated by clicking *Check for Update* in the main panel of the Internet Security page (see above).

Non-administrator access

When we attempted to check non-administrator access by logging on with a standard user account, we found that the program was shown in its initial pre-activation state, with *Start Scan* being the only available option. If the system tray menu is used to activate or de-activate real-time protection (both are possible), a dialog is shown with *Instant Activation* being the only option:



Clicking *Instant Activation* opens the MacKeeper online store, where a licence can be purchased. We closed the activation dialog, and then ran the scan option from the main window. We were intrigued to see that the scan had found 43 items, apparently putting it somewhere between *Medium* and *Serious* – despite the fact that it had only just declared the system status to be *Excellent* when run under the administrator's account:



We logged out of the standard user account, logged on again with the administrator account, and re-ran the scan. The results page is shown below:

The screenshot shows the MacKeeper interface. On the left, a sidebar lists various tools: System Status, HUMAN ASSISTANCE (Find & Fix, Geek on Demand), SECURITY (Internet Security, Anti-Theft), ADVANCED TOOLS (Duplicates Finder, Smart Uninstaller, Files Recovery, Data Encryptor, Files Finder, Login Items, Disk Usage, Default Apps, Update Tracker, Fast Cl... (102.5 MB), Backup, Shredder). The main area is titled 'Find & Fix' with the sub-section 'Find and Fix items that may affect your Mac's System Status'. It displays three categories: Cleaning (Excellent), Security (Excellent), and Performance (Excellent). Below this, the 'System Status' section shows '48 items found'. A summary bar indicates the status is 'Excellent' (smiley face icon), the risk level is 'Medium', and there are 'Serious' items. A large blue button at the bottom right says 'Fix Items Safely >'. To the right, there is a portrait of a support expert, contact information (24/7 MacKeeper Expert, Start Live Chat, Get answer in 24 hours, Send Message), and international support options (USA, UK, Australia, Skype) with the phone number 1 (888) 572-5876.

We had created the standard user account immediately before logging on with it, and that other than MacKeeper itself, we had not opened a single application before running the scan. We invite readers to compare the results pages for the scans run before and after activation with an admin account, the scan run as a standard user, and the subsequent repeat scan as the admin, and decide for themselves whether any sense can be made of them.

Scanning

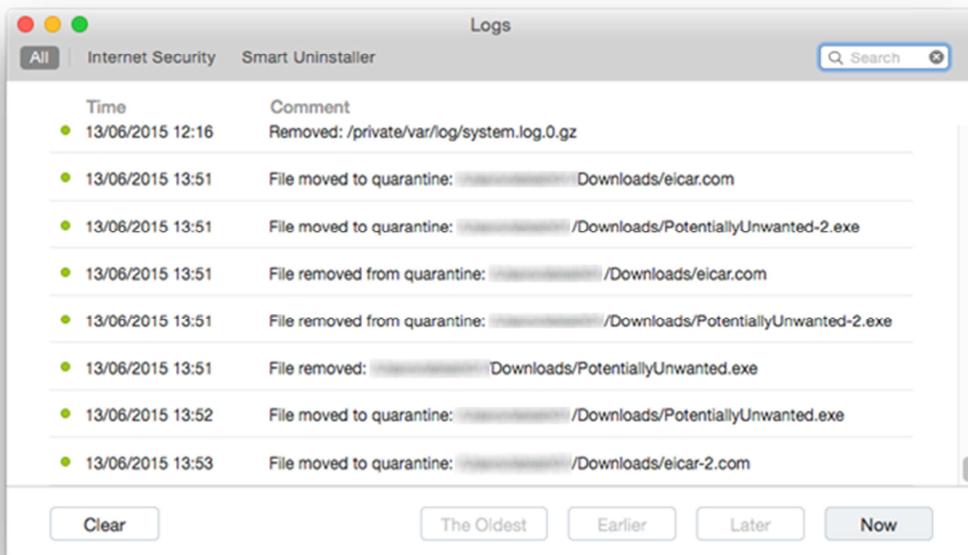
Clicking the *Antivirus Scan* link in the menu bar at the top of the window provides buttons to start a full scan or custom scan:

The screenshot shows the Internet Security settings window. At the top, there is a shield icon with a warning sign, the title 'Internet Security', a subtitle 'Protect your Mac from different kinds of Internet fraud.', and a note 'Last check for update: 13 Jun 2015 09:28'. Below this, there are tabs: Status, Safe Browsing, **Antivirus Scan**, Antivirus Quarantine, and Antivirus Schedule. The 'Antivirus Scan' tab is selected. A note says 'Use the manual virus scan to check your files, folders, drives and network devices for viruses.' Below this are buttons for 'All', 'Whitelist', and 'Blacklist'. A table follows with columns 'Title' and 'Description'. At the bottom are buttons for 'Move to Quarantine' (with a biohazard icon), 'Delete' (with a trash bin icon), 'Check All/Uncheck All' (with checkboxes), 'Start Antivirus Scan' (with a magnifying glass icon), and 'Start Custom Scan...' (with a folder icon).

The *Antivirus Schedule* link, also in the menu bar, enables a scheduled scan to be set up.

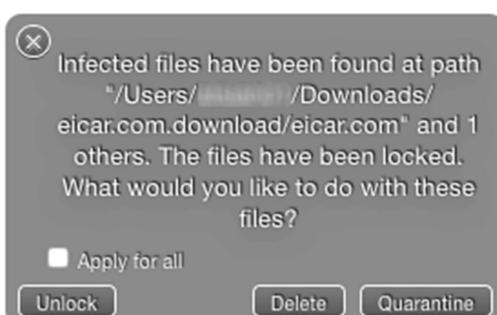
Settings, quarantine and logs

Clicking *MacKeeper* in the Mac Menu bar, then *Preferences...* opens the program's settings. A link to *Antivirus Quarantine* can be found in the menu bar at the top of the window. Logs can be found in the *Window* menu in the Mac menu bar:



Malware and phishing alerts

If the EICAR test file is downloaded, the following warning is displayed:



The *Unlock* button essentially causes the file to be whitelisted. A very similar warning is displayed for the AMTSO Potentially Unwanted test file. MacKeeper does not block the AMTSO phishing test page.

Malware protection test

In our test, Kromtech MacKeeper identified and disabled 98% of Mac malware samples, and about 97% of the used prevalent Windows malware samples. The Internet Security component in Kromtech MacKeeper is based on the Avira antimalware engine, meaning that results are similar to Avira Free Antivirus for Mac.

Help

At the top of the *Live Support* panel on the left-hand side of the window is a *Help* button. Clicking this displays a list of questions/problems, answers for which are shown in the main panel of the window:

The screenshot shows the 'Quick Help' feature within the 'Customer Support Feature'. On the left, under 'Is it safe to use the MacKeeper features?', there is a 'Solution' section stating: 'Most MacKeeper tools are absolutely safe, however, you should be careful while using the Disk Usage and Smart Uninstaller tools. These features do not suggest removing anything by default, it is up to you to decide which files or applications you want to remove. Be careful when removing something with these tools.' Below this is a list of frequently asked questions (FAQ) under 'LIVE SUPPORT'.

- Choose the nature of problem:
 - ▶ Questions about Price/License Types/Subscription
 - ▶ MacKeeper Installation/Reinstallation and Removal
 - ▶ MacKeeper Activation
 - ▶ MacKeeper (Kromtech) Account Issues
 - ▶ Billing Questions
 - ▶ MacKeeper Usage Problems
 - Is it safe to use the MacKeeper features?
 - How long should MacKeeper scans take?
 - MacKeeper cannot delete the found junk files or duplicate files.
 - Infected files cannot be deleted.
 - Internet Security Issues

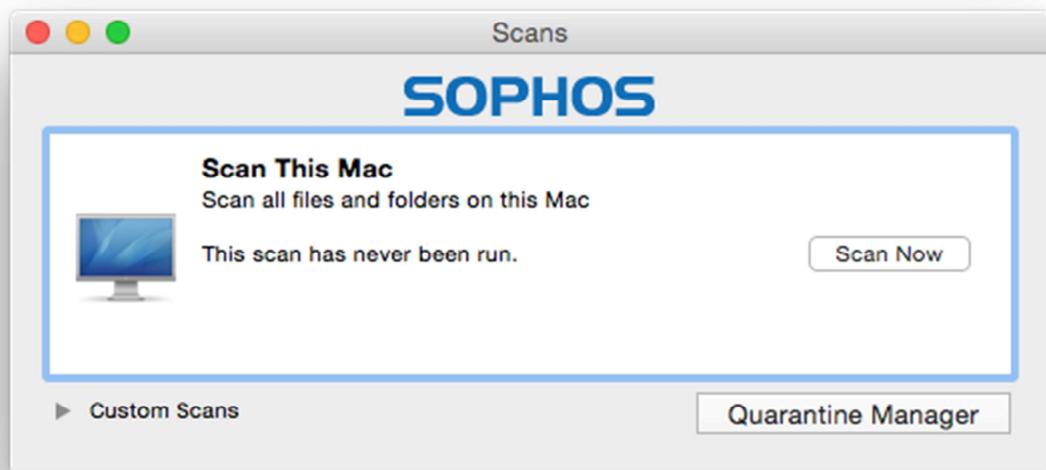
At the bottom of the help section are two buttons: 'It Doesn't Help Me' and 'Okay! I Got It!' with a dropdown arrow.

Verdict

We would say that the Internet Security component of Kromtech MacKeeper provides all the essential features of an antivirus program in a simple and straightforward interface. Protection against both Mac and Windows malware is very good but not perfect. With regard to the installation and initial configuration of the suite, we are left with a number of concerns that we feel have not been answered. Kromtech are keen to stress that the agent at the other end of the chat line is a real human being. The apparent name change of the person shown in the picture does not reassure us in this respect. Neither did the fact that the agent started off by telling us that our Mac was in "wonderful shape" before presenting the results of the "scan", which showed us that it was in the worst possible state in two areas. We wonder how it is possible for a freshly installed, up-to-date Mac to get the lowest possible rating in terms of security and "cleaning"⁵. We also wonder how the system can get an "excellent" rating when run from the administrator account, but be between "medium" and "serious" when run from a newly created, unused standard user account. Finally, there is the question of why a program that has been properly activated by one user should prompt a different user of the same computer to activate it, whilst providing obvious encouragement to the second user to buy a new licence. We suggest that readers should carefully consider the points we have raised in this review, and decide for themselves what to make of MacKeeper.

⁵ We note that it is entirely possible for the security of a Mac to be reduced, if the OS is not kept updated, and a number of unpatched older programs with known security vulnerabilities are installed. As MacKeeper awards a clean, fully patched system the lowest possible security rating, we conclude that it has no means of showing the difference between this and a system that is very out-of-date and does indeed have significant security flaws. Similar remarks could be made about the performance.

Sophos Anti-Virus for Mac



Product version reviewed

9.2.7

Operating systems supported

Mac OS X 10.6 or later

Additional features

Sophos Anti-Virus for Mac is a straightforward antivirus program.

Installation

A 125 MB installer is downloaded from the Sophos website. The first page of the setup wizard provides some information about the program, including how to get help and how to uninstall it. A licence agreement has to be accepted, otherwise there are no other choices to make.

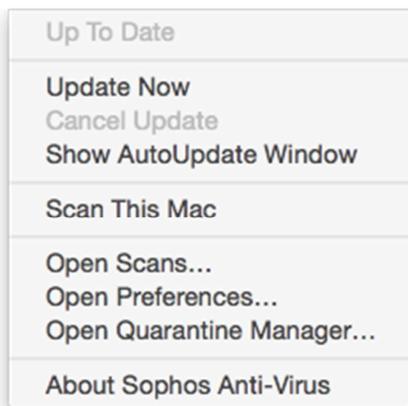
The program can be uninstalled using the *Remove Sophos Anti-Virus* icon in the Applications folder, as described in the setup wizard.

Main window

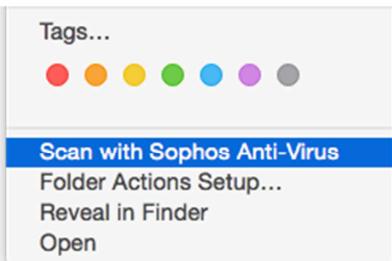
Sophos Anti-Virus for Mac does not have a main program window in the traditional sense. The *Scans* window (main screenshot at the start of this report) allows default and custom scans to be run, and the quarantine feature to be opened.

Operating system integration

The menus *Sophos Anti-Virus*, *File*, *Edit*, *Scan*, *Window* and *Help* are added to the Mac menu bar. There is also a System Tray icon, which displays the following menu:

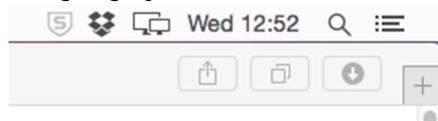


The Finder context menu is extended to include a *Scan with Sophos Anti-Virus* entry:



Maintenance

If the real-time protection is turned off, the Sophos icon in the System Tray changes from dark grey to light grey:



This change is very subtle, and we would not describe it as a warning or alert. Malware signatures can be updated from the System Tray menu or *Sophos Anti-Virus* menu.

Non-administrator access

Disabling the real-time protection always requires administrator credentials to be entered, regardless of whether the current user is an administrator or standard user.

Scanning

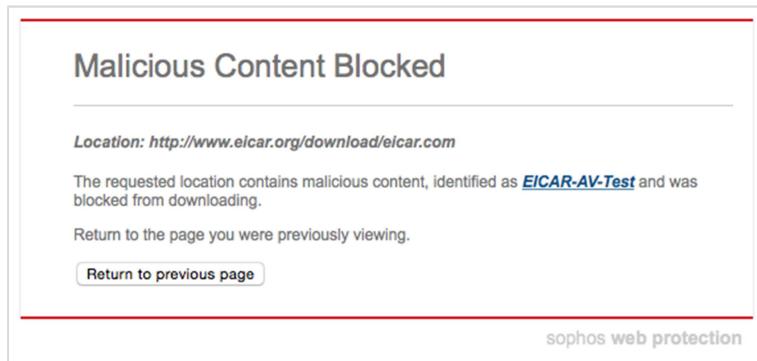
The *Scans* window lets the user run a full or custom scan. We could not find a means of setting a scheduled scan.

Settings, quarantine and logs

Settings (*Preferences*) can be opened from the *Sophos Anti-Virus* menu or System Tray menu. Quarantine is accessible from the *Window* menu, System Tray menu, or the *Scans* window. Logs can be seen by clicking the *Scan* menu, *View Scan Log*.

Malware and phishing alerts

If the EICAR test file is downloaded, the following alert is displayed in the browser window:



A similar page is displayed if the user tries to open the AMTSO phishing test page. The product does not detect PUAs, so the AMTSO Potentially Unwanted test file was not recognised.

Malware protection test

In our test, Sophos Anti-Virus for Mac identified and disabled 100% of our Mac malware samples. It also detected 100% of Windows malware samples; however, it was not able to neutralise some of these.

Help

Clicking *Help*, *Sophos Anti-Virus Help* opens the local help feature, which has simple text instructions for all the program's features:



Verdict

Sophos Anti-Virus for Mac is free software with all the essential features of an antimalware program. Whilst we did not find it in any way difficult to use, we would suggest that the nature of its interface makes it more suited to Mac enthusiasts than non-expert users. Whilst its Mac malware protection was exemplary, it was not able to neutralise some of the Windows malware samples in our test.

Featurelist Mac (as of July 2015)	FREE	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE
Product name:	Avast Free Mac Security	AVG AntiVirus for Mac	AVIRA Free Antivirus for Mac	Bitdefender Antivirus for Mac	ESET Cyber Security Pro	F-Secure SAFE	Intego Mac Premium Bundle	Kaspersky Internet Security for Mac	Kromtech MacKeeper Premium	Sophos Anti-Virus for Mac	
Supported OS X versions:	10.6.8 and up	10.8 and up	10.9 and up	10.7 and up	10.6 and up	10.6.8 and up	10.7 and up	10.6 and up	10.6 and up	10.6 and up	
Supported Program languages:											
	English, German, Czech, Spanish, Finnish, French, Italian, Dutch, Polish, Korean, Portuguese, Russian, Swedish, Norwegian	English	English, German	English, German, French, Italian, Spanish	English, Czech, Danish, Dutch, Finnish, French, German, Hungarian, Chinese, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Slovak, Spanish, Swedish, Thai, Turkish	English, Chinese, Bulgarian, Czech, Danish, German, Greek, Spanish, Estonian, Finnish, French, Hungarian, Italian, Japanese, Dutch, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Swedish, Turkish, Vietnamese	English, French, German, Japanese, Spanish	English, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English, French, German, Japanese, Spanish, Italian, Dutch, Russian, Portuguese, Danish, Swedish, Korean, Finnish, Czech, Norwegian, Polish, Chinese, Turkish	English, French, German, Japanese, Spanish, Italian, Dutch, Russian, Portuguese, Danish, Swedish, Korean, Finnish, Czech, Norwegian, Polish, Chinese, Turkish	English, French, German, Japanese, Spanish
Protection											
Real-Time protection	•	•	•	•	•	•	•	•	•	•	•
On-demand scanner	•	•	•	•	•	•	•	•	•	•	•
Detects also threats for other platforms (e.g. Windows malware)	•	•	•	•	•	•	limited detection of windows threats	limited detection of windows threats	•	•	•
Prevents access to malicious and phishing web sites	•	•	•	•	•	•	•	•	•	•	•
Quarantine	•	•	•	•	•	•	•	•	•	•	•
Whitelisting for specific files/folders	•	•	•	•	•	•	•	•	•	•	•
Cloud Scanning (requires internet connection)				•	•	•	•	•	•		•
Scheduled Update	•	•	•	•	•	•	•	•	•	•	•
Scheduled On Demand Scan						•	•	•	•	•	•
Statistics	•		•	•	•	•	•	•	•	•	
Additional features											
Parental Control					•		•	•	•		•
Mail Protection	•				•	•	•	•			
Removable media blocking					•		•				•
Firewall					•		•				
Network attack protection									•		
Secured browser for online banking						•		•			
Game/Presentation mode					•						
Support											
Online Help and User Forum	•	•	•	•	•	•	•	•	•	•	•
Email and Phone Support	•	•	•	•	•	•	•	•	•		
User manual		•		•	•	•	•	•	•		•
Online Chat			•	•			•	•	•	•	
Supported languages (of support)	English, German, Chinese, Spanish, French, Italian, Korean, Portuguese	English, Czech	English, German, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malay	English, German, French, Italian, Spanish, Portuguese, Romanian, Turkish	All	English, Finnish, French, Dutch, Danish, German, Chinese, Italian, Norwegian, Polish, Swedish	English, French, Japanese	English, Arabic, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English	English, French, German, Spanish, Japanese, Italian, Chinese	
Price (may vary)											
Price 1 Mac / 1 year (USD/EUR)	FREE	FREE	FREE	USD 40 / 40 EUR	USD 45 / 35 EUR	USD 50 / 50 EUR	USD 90 / 75 EUR	USD 40 / 40 EUR	USD 90 / 90 EUR	USD 90 / 90 EUR	FREE

Copyright and Disclaimer

This publication is Copyright © 2015 by AV-Comparatives ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives (July 2015)