Mac Security Test & Review

AV comparatives

Mac Security Test & Review

Language: English

July 2016
Last revision: 22nd July 2016

www.av-comparatives.org

Contents

Introduction: Macs and Security Software

In March 2016, a ransomware program called KeRanger was discovered by Palo Alto Networks.[1] It is believed to have affected over 7,000 Mac users, whose personal data was rendered unusable by encryption. This once again illustrates that Mac systems are not immune to infection by malware, and that it is advisable 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, in addition to the security features provided by the Mac OS itself. Readers who are concerned that third-party security software will slow their Mac down can be reassured that we considered this in our test; we did not observe any significant performance reduction during daily operations with any of the programs reviewed.

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] https://en.wikipedia.org/wiki/KeRanger

Review of Security Software for OS X 10.11.5 El Capitan

We have reviewed and tested the following products for this report, using the newest version available in July 2016:

- **Avast Free Mac Security 11.13.46580**
  https://www.avast.com/free-mac-security
- **AVG AntiVirus for Mac 2015.0.4818**
  http://www.avg.com/ww-en/avg-antivirus-for-mac
- **AVIRA Free Antivirus for Mac 3.2.5.5**
  http://www.avira.com/en/free-antivirus-mac
- **Bitdefender Antivirus for Mac 4.1.1.7**
  http://www.bitdefender.com/solutions/antivirus-for-mac.html
- **ESET Cyber Security Pro 6.1.12**
  https://www.eset.com/int/home/cyber-security-pro
- **Intego Mac Premium Bundle X9 10.9.1**
  https://www.intego.com/mac-protection-bundle
- **Kaspersky Internet Security for Mac 16.0.0.245a**
  http://www.kaspersky.com/security-mac
- **McAfee Live Safe for Mac 3.8.1.0**
  https://www.mcafee.com/consumer/en-us/store/m0/catalog/mls_430/mcafee-livesafe.html?pkgid=430
- **Sophos Home for Mac 1.1.4**
  https://www.sophos.com/en-us/lp/sophos-home.aspx
- **Webroot SecureAnywhere Internet Security Complete for Mac 9.0.2.22**
  http://www.webroot.com/us/en/home/products/complete

We congratulate these manufacturers, who elected to have their products reviewed and tested, as we feel their commitment is a valuable contribution to improving security for Mac systems.

Review format

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

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

Installing and uninstalling
Installation
We note any options or points of particular interest encountered during the setup process.

Integration with operating system and browser
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 be started by right-clicking a file, folder or drive. Finally, we check whether any extensions are available for the built-in Safari browser.

Deinstallation
The deinstallation process is also stated, and whether this is described in the help or user guide.

Deinstallation/deactivation from a standard user account
We find out if a user with a non-administrator user account can disable the protection or uninstall the program.

Using the program
Status
We check to see if there is a status display that 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.

Updates
We look for a means of manually updating malware signatures.

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

Preferences, quarantine, logs and subscription information
We find out how the program's settings, quarantine and log features are accessed, and where to find licence information (where applicable).

Help
We look to see what help facilities are available and how clear and comprehensive they are.

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. If the program displays search ratings for Google searches with Safari, we point this out.

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 the 50 most recent and prevalent Mac malware samples (such as KeRanger and OceanLotus) that are not blocked by Mac OS X itself. All are distinctly malicious, functioning, self-contained programs and were seen in-the-field in 2016. We did not include any potentially unwanted or "grey" samples (adware, hacking tools, etc.) in the test set. We also excluded corrupted files, and component files (which cannot run independently), as these do not pose a risk by themselves. We ended up with a sample set consisting of 50 malicious Mac apps (made up of variants of seven Mac malware families), found in-the-field, that pose a risk to users, and should thus be covered by Mac Security products. The test set may be smaller than those used in some other tests by magazines etc., but any magazine claiming to use more samples most probably includes PUAs, corrupted files or outdated samples. In fact, the number of new Mac malware families appearing per year is usually less than a dozen.

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 system 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 4th July 2016. 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 executed, providing the security product with a final chance to detect the malware. After each active infection, a full-scan was performed, in order to give the products a chance to check for active malware.

In addition to the Mac malware samples, we also scanned and executed a set of clean Mac programs to check for false positives. **None of the programs we tested produced any false alarms.**

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 detect Windows malware. We used 250 prevalent and current Windows malware samples (according to the AMTSO Real-Time Threat List – RTTL); 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.

The table below shows protection results for the products in the review. The figures for Mac malware protection indicate the number of samples blocked at any stage of the testing procedure, i.e. regardless of whether the malware was detected/blocked in one of the on-demand scans, by real-time protection, or on-execution.

Product	Mac Malware Protection 50 most-recent Mac samples	Windows Malware Detection[2] 250 most-prevalent Windows samples
Avast Free Mac Security	100%	100%
AVG AntiVirus for Mac	100%	97%
Avira Free Antivirus for Mac	100%	100%
Bitdefender Antivirus for Mac	100%	100%
ESET Cyber Security Pro	100%	100%
Intego Mac Premium Bundle X9	100%	28%
Kaspersky Internet Security for Mac	100%	100%
McAfee LiveSafe Internet Security for Mac	100%	94%
Sophos Home for Mac	100%	98%
Webroot SecureAnywhere for Mac	100%	92%
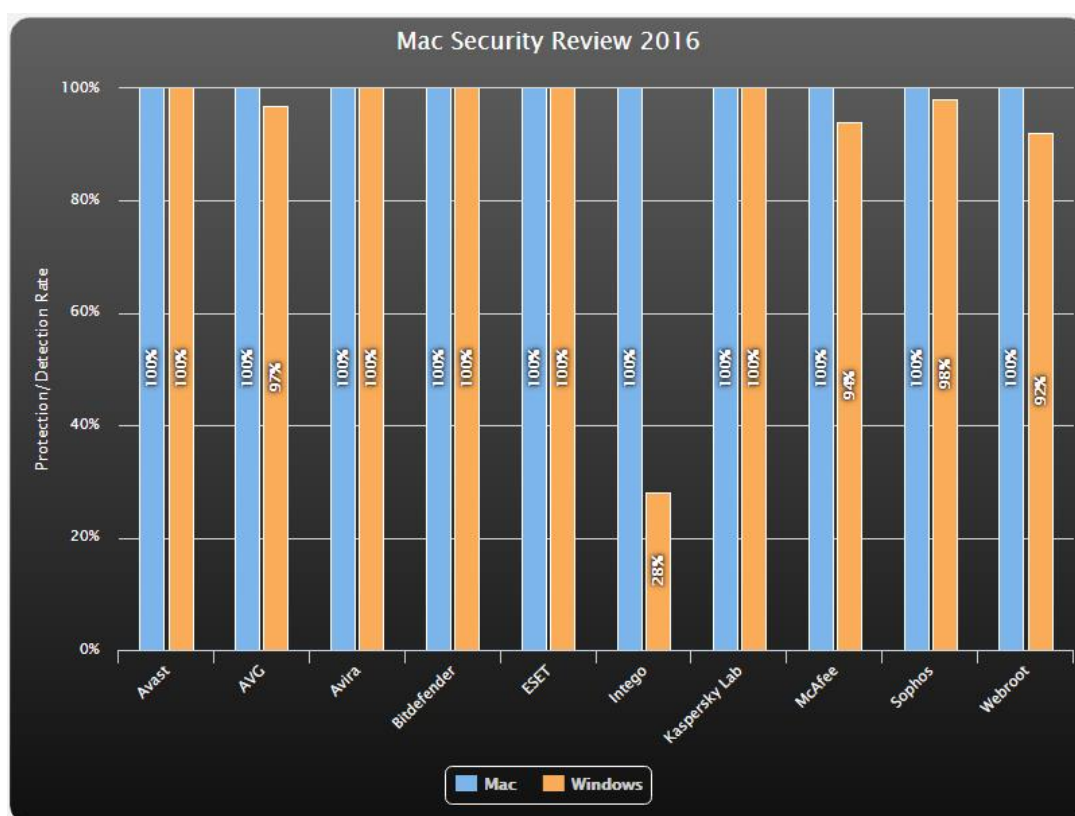
A more complete list of available antivirus programs for the Mac can be seen here:
http://www.av-comparatives.org/av-vendors-mac

___

[2] Detection of Windows threats on Macs can be seen as discretionary. Some products do not include detection for non-Mac threats or have limited detection capabilities due to technical constraints.

Summary

All of the products we have reviewed protected the Mac test system against 100% of the recent Mac malware samples used, performed everyday functions satisfactorily and without noticeably affecting system performance, and so receive our Approved Security Product Award.

Please note that 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.
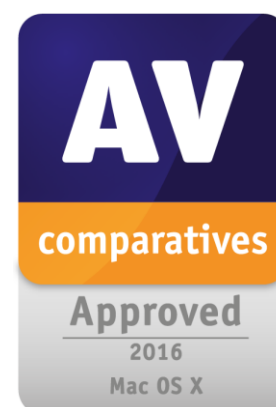
Avast Free Mac Security has all the important features of an antivirus program and is largely very simple to use. We particularly liked the informative and persistent malware alerts.

AVG AntiVirus for Mac is a free program with a very clear and straightforward interface, making it suitable for experts and non-experts alike. The help feature is simple but useful.

Avira Free Antivirus for Mac is very simple to install and use, and makes all important functions easy to find. We particularly liked the expandable tool tips in the main program window.

Bitdefender Antivirus for Mac has a new design for the program window, similar to its Windows counterpart, and we had no difficulty finding any important features. There is a well-produced and comprehensive user's manual.

ESET Cyber Security Pro retains its clear, well-designed interface and exemplary help facilities in version 6, making it easy to use for both experts and non-experts.

Intego Mac Premium Bundle X9 has a very clear status display in the new version, showing a warning if protection is disabled. The overlay showing the functions available in the window is a clever means of introducing the program quickly to new users.

Kaspersky Internet Security for Mac has a clear, modern design that makes important features and information easy to find. Users of its Windows counterpart will easily find their way around the program, and help features are good.


McAfee LiveSafe for Mac is very easy to install and use. Important features and information are largely easy to find.

Sophos Home for Mac is an easy-to-use free program, managed by cloud console. The consistency of design between the Mac and Windows versions will be appreciated by anyone who uses or manages both platforms.

Webroot SecureAnywhere Internet Security for Mac The program's interface is easy to navigate and makes important functions easy to find. Anyone who uses or manages both Windows and Mac platforms will find the consistency of design between the two versions helpful.

Avast Free Mac Security
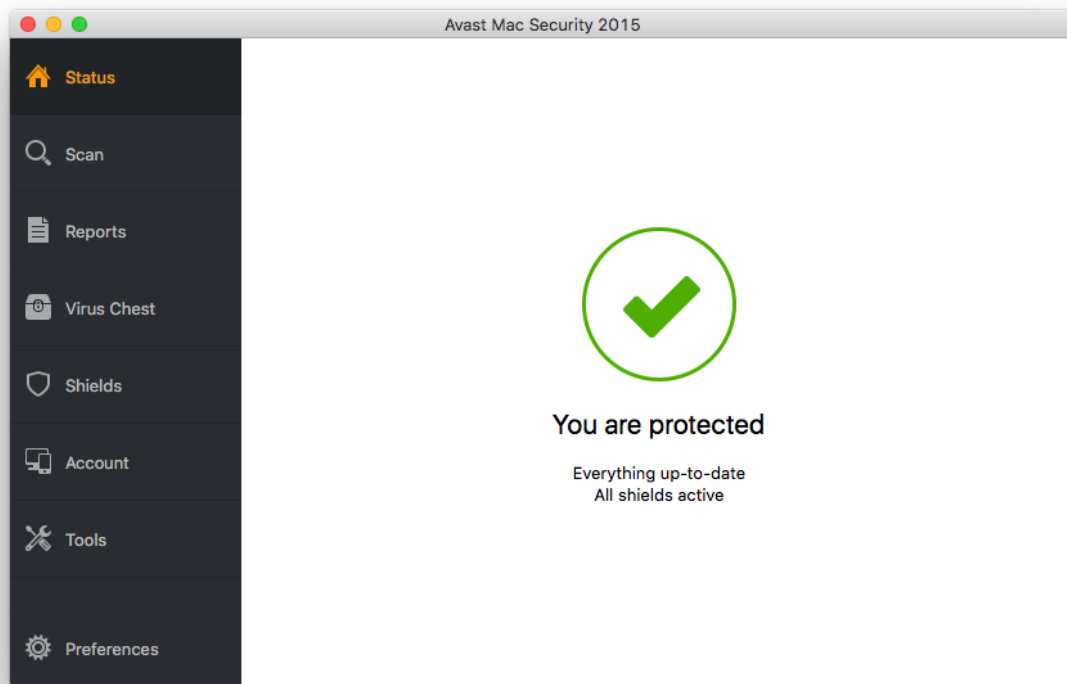
Overview

Features

Avast Free Mac Security is an antimalware program with phishing protection.

Good points

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. Protection against Mac malware in our test was flawless.

Suggestions for improvement

A suggestion for improvement would be to add a "Fix-All" button to make it easier to reactivate the protection if it is disabled.

Installing and uninstalling

Installation

A 10 MB .DMG installer is downloaded from the Avast website. The setup wizard provides the option to change the installation folder location, and also offers to install Avast Online Security and Avast SecureLine VPN (we accepted):
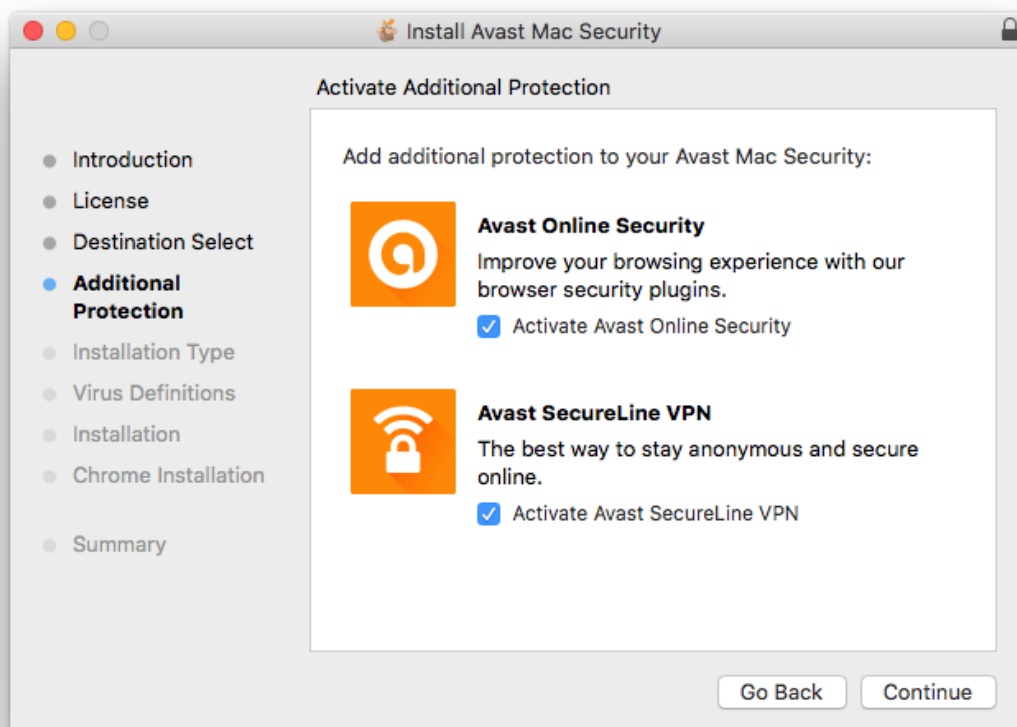
Finally, there is an option to install Google Chrome (we declined).

Integration with operating system and browser

Avast Free Mac Security adds menus to the Mac menu bar. There is also a System Tray icon, which displays the following menu:
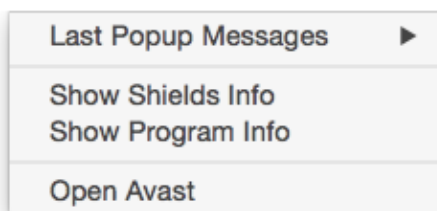
Avast adds a scan entry in the Finder context menu:
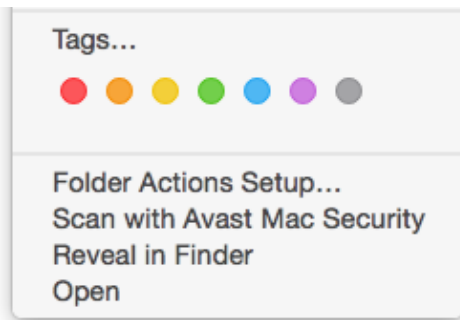
No extensions or other modifications are added to Safari.

Deinstallation

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

Deinstallation/deactivation from a standard user account

Uninstalling the program or disabling the protection requires administrator credentials to be entered, even if the current user has administrator status.

Using the program

Status

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.

Updates

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

Scanning

The *Scan* page, accessible from the link of the same name, provides options for full and custom scans, and removable-drive scans, as well as a scan of other devices on the network:
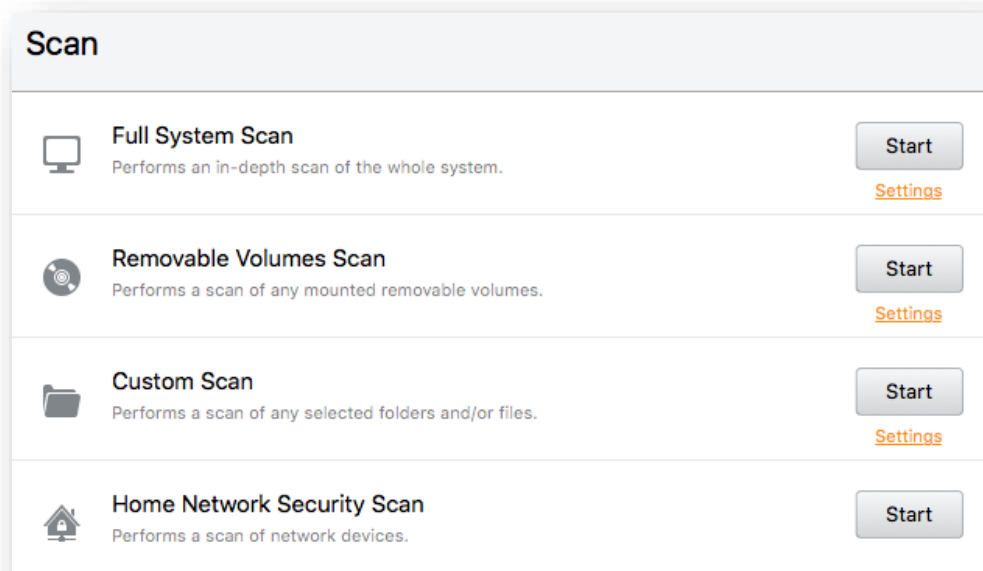
A custom scan can also be run by right-clicking a drive, folder or file. We could not find a means of setting a scheduled scan.

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:
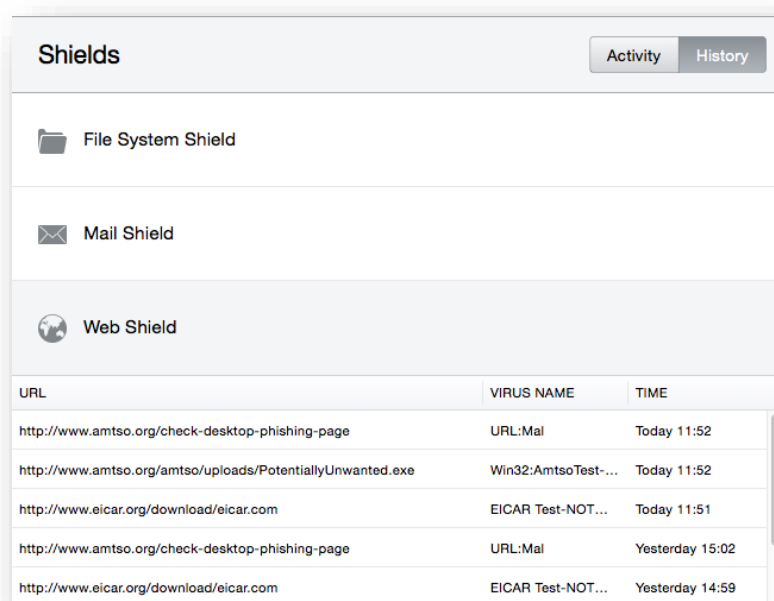
Help

The product has a local help feature, found by clicking the *Help* menu, then *Avast help*. This provides a brief overview of the main features of the program. There is also an online FAQ section, also accessible from the *Help* menu.

Malware and phishing alerts

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

Additionally, a block page is shown in the browser window:
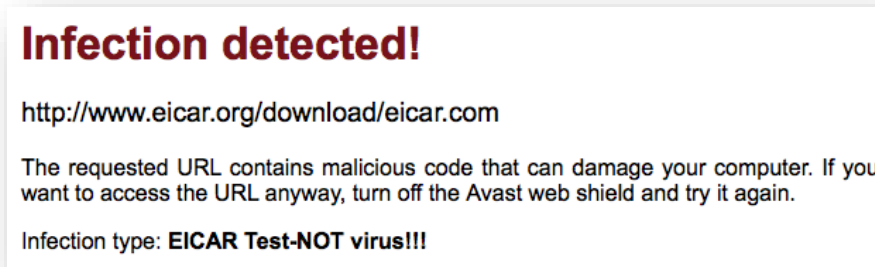
The AMTSO Potentially Unwanted Application test file and phishing test page are also blocked, with similar browser alerts and pop-up warnings shown.

AVG AntiVirus for Mac
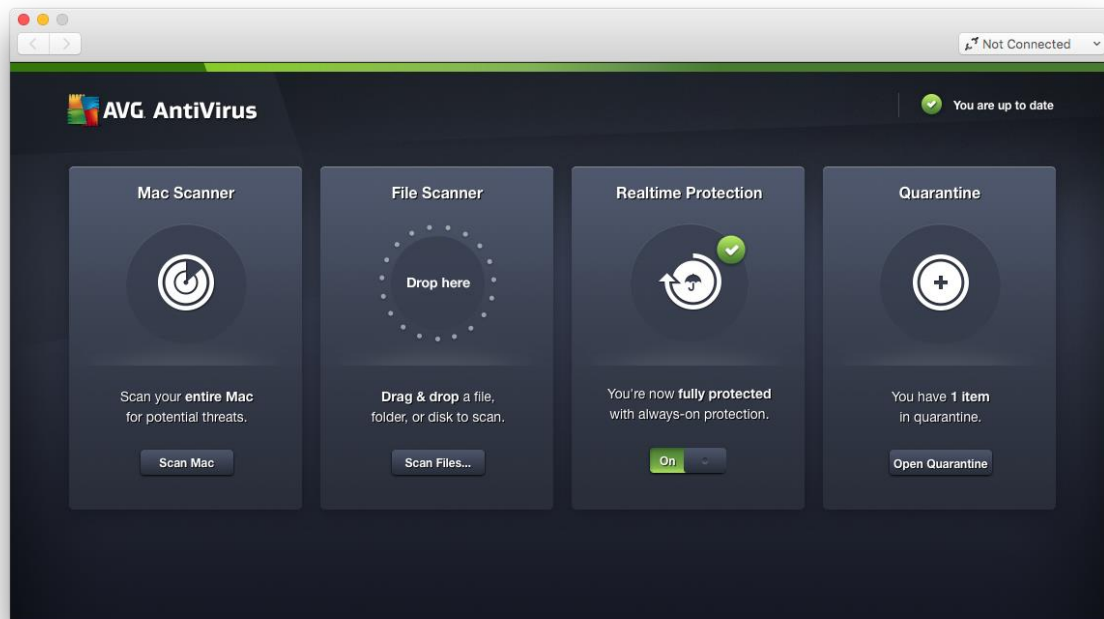
Overview

Features

AVG AntiVirus for Mac is a fully featured antimalware program.

Good points

We found the interface of AVG AntiVirus for Mac to be very clear and straightforward, making it suitable for experts and non-experts alike. The help feature is simple but useful. Protection against Mac malware in our test was flawless.

Suggestions for improvement

We feel that a separate log feature would be a useful addition.

Installing and uninstalling

Installation

A 220 MB .DMG installer file is downloaded from the AVG website. The installation wizard allows the user to change the installation folder. The user is invited 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 this.

Integration with operating system and browser

AVG AntiVirus for Mac adds menus and a System Tray icon to the Mac menu bar, but does not alter Safari or the Finder context menu.

Deinstallation

The software can be uninstalled from the *AVG AntiVirus* menu in the Mac menu bar; this is described in the product's FAQ page on the AVG website.

Deinstallation/deactivation from a standard user account

Uninstalling the program or 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.

Using the program

Status

Real-time protection has its own tile in the main program window, complete with button to switch it on and off. If the protection is turned off, the tile shows the following warning:
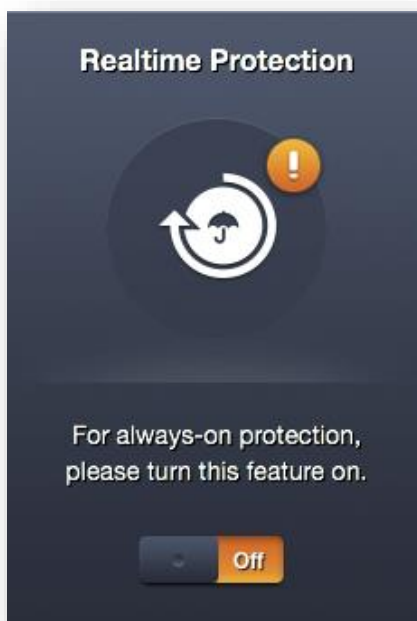
Updates

Malware signatures can be updated from the *AVG AntiVirus* menu or the System Tray menu, shown below:
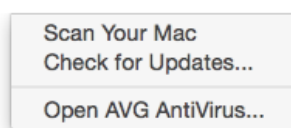

Scanning

Full scans can be run from the Mac scanner panel in the main program window, or the System Tray menu. The *File Scanner* panel in the main window lets users drag and drop a file, folder or disk to scan, or browse for an item by clicking *Scan Files*. We could not find a means of scheduling a scan.

Settings, quarantine, 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 window; we could not find a separate log feature.

Help

The local help file, accessed from the *Help* menu in the Mac menu bar, provides simple text instructions for the program's features:
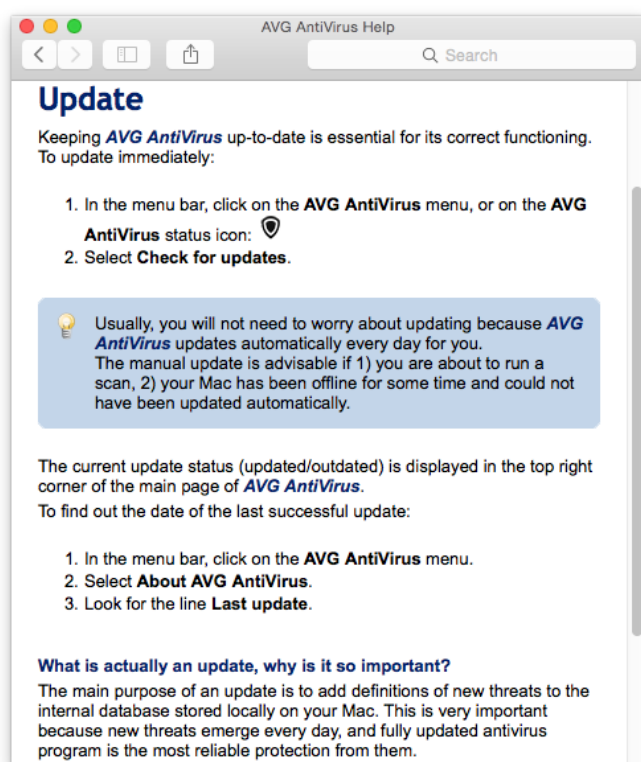
In the example above, we liked the explanation of what an update is and why it's important, and the note about automatic updates and when a manual update is advisable. Whilst the local help file is quite limited in scope, it does include a link to the program's FAQ page on the AVG website.

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.

Additional comments

When installation is complete, the program window opens and displays a short explanation for each of the tiles on the home page:
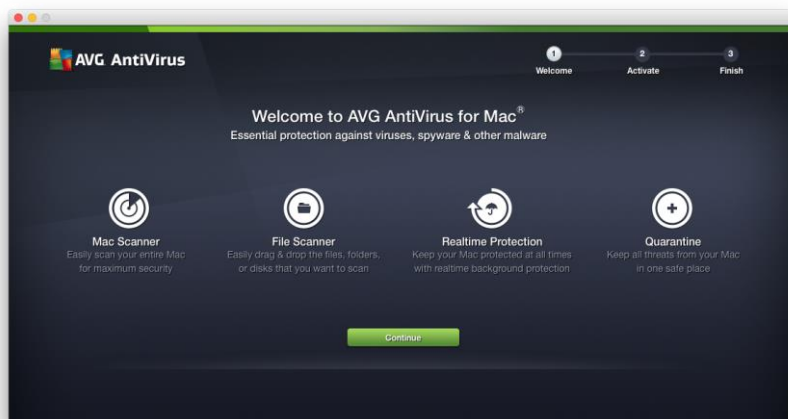
Avira Free Antivirus for Mac
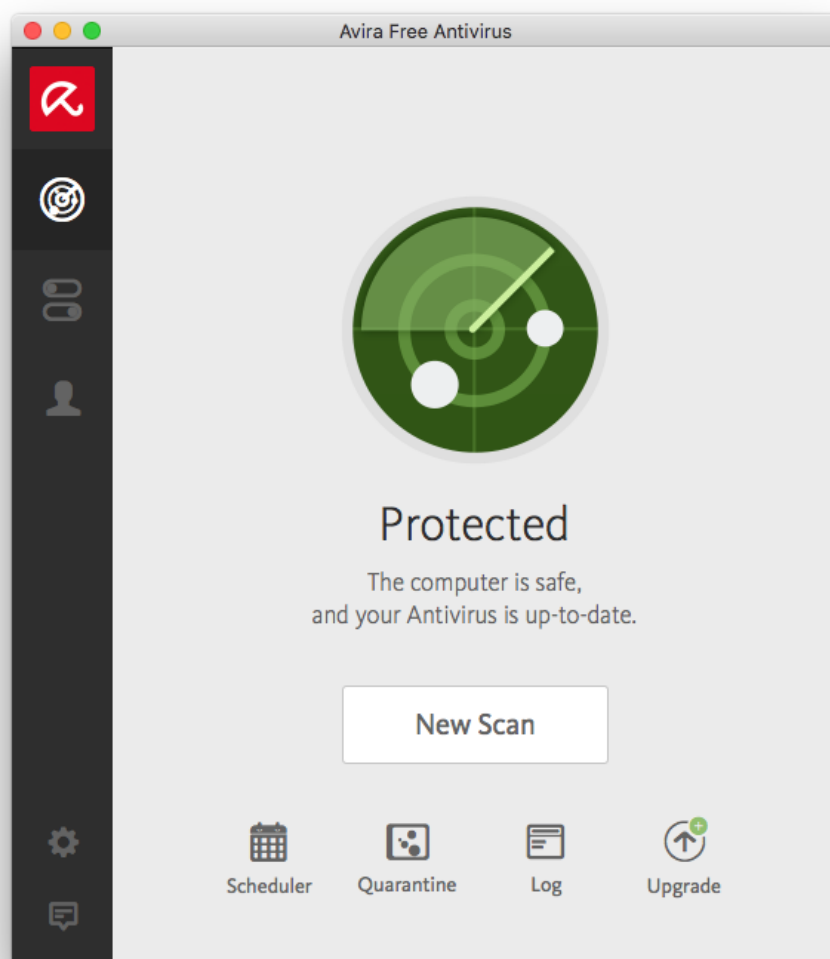
Overview

Features

Avira Free Antivirus for Mac is a straightforward antimalware program.

Good points

Avira's Free Antivirus for Mac is very simple to install and use, and makes all important functions easy to find. We particularly liked the instructions on the download page for starting the installer, the expandable tool tips in the main program window, and the system tray icon showing protection status with an open or closed umbrella. Protection against Mac malware in our test was flawless.

Suggestions for improvement

We initially tested Avira Free Antivirus for Mac at the beginning of July 2016, and suggested to the vendor that a log function and Finder context menu would be useful additions. We are pleased to report that Avira responded very rapidly to this, and released a newer version that includes both of these features; we have updated this review accordingly.

Installing and uninstalling

Installation

A 219 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:
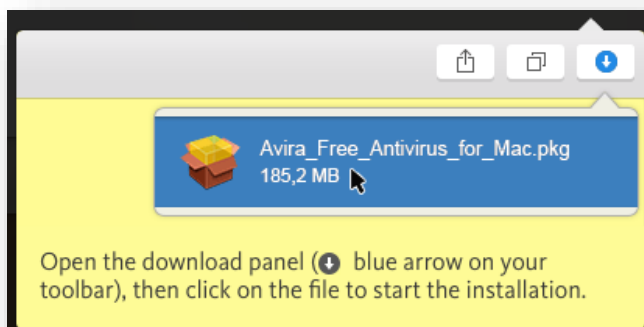
The setup wizard requires the user to accept a licence agreement, and there is the option of changing the installation drive. Otherwise, there are no decisions to make.

Integration with operating system and browser

No extension is added to Safari. Avira does add two menus to the Mac menu bar: *Avira* and *Help*. It also displays a System Tray icon, clicking which shows the following menu:
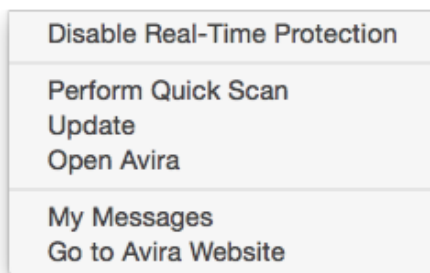
The System Tray icon indicates whether protection is enabled or not, by showing an open umbrella for protection active, closed umbrella for protection inactive.

A *Scan with Avira* entry is added to the Finder context menu:
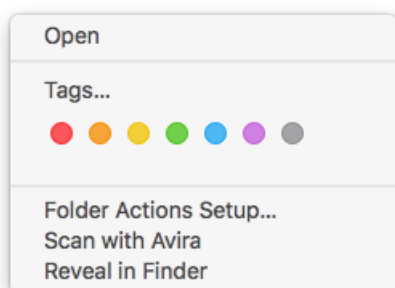
Deinstallation

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.

Deinstallation/deactivation from a standard user account

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. Administrator credentials are also required to uninstall the progam.

Using the program

Status

The home page of the program window has a status display with a graphic and text. If real-time protection is turned off, a warning message pops up in the top right-hand corner of the screen:
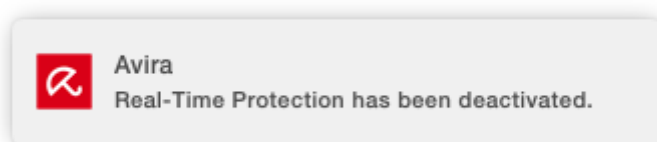
Additionally, the status-display graphic and text both change to show an alert:
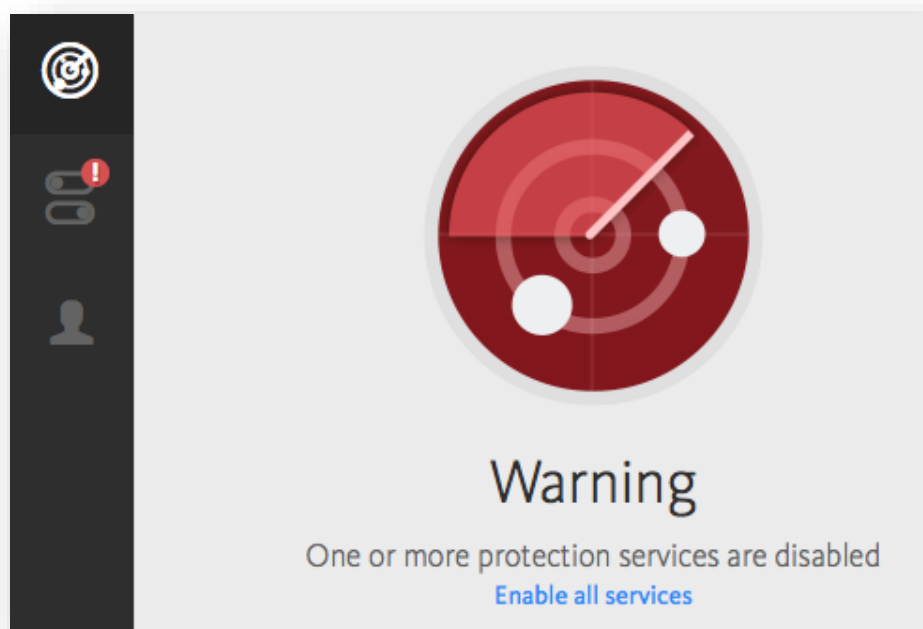
Clicking *Enable all services* immediately reactivates the protection.

Updates

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

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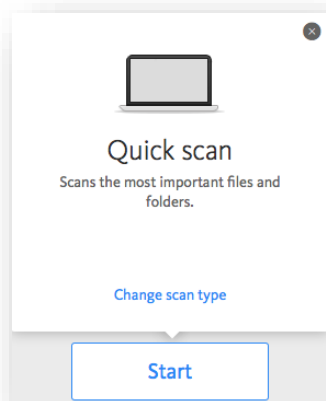
The *Scheduler* button, just below the scan button, allows a scheduled scan to be configured.

Preferences, 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. Logs can be displayed by clicking the *Log* button on the program's home page.

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.

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:
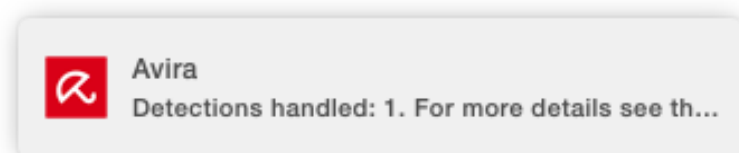

Unfortunately, the message box is not big enough to display the full message, so the user cannot see where to find more details. Clicking or double-clicking the message itself has no effect.

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

Additional comments

We note that hovering with the mouse over a button in the left-hand menu panel displays a big tool tip with the button's function; clicking on the arrow provides more details:
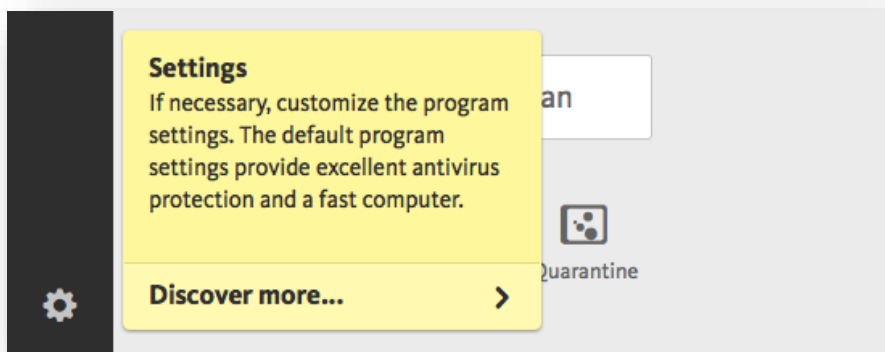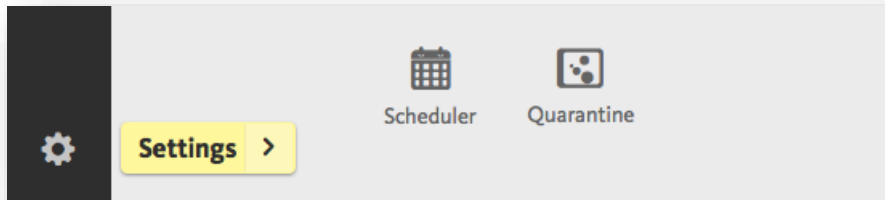
Bitdefender Antivirus for Mac
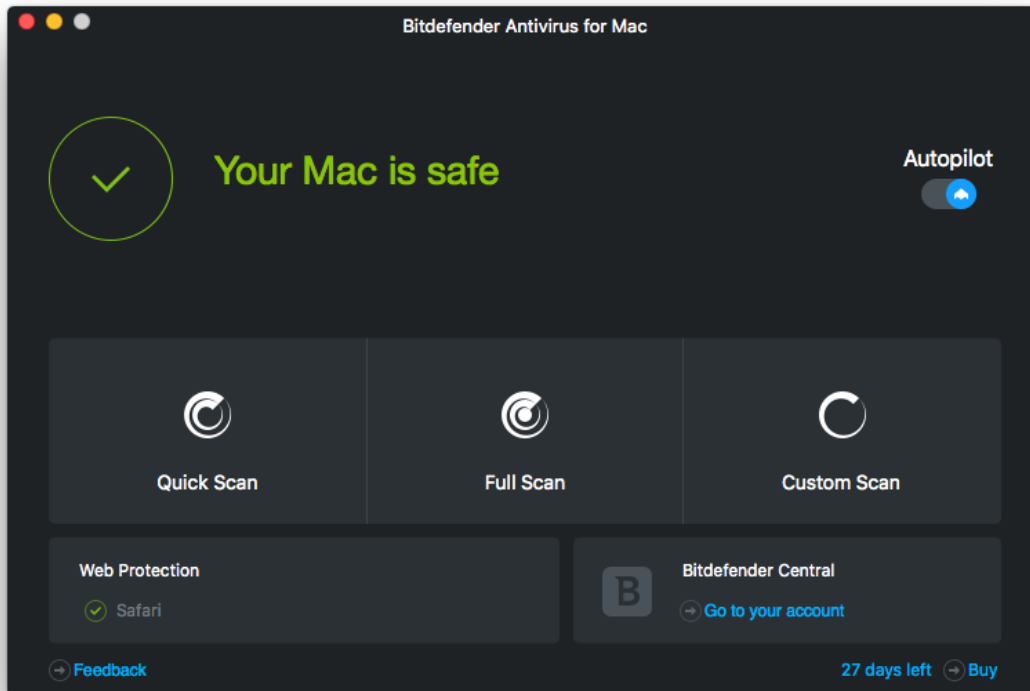
Overview

Features

In addition to providing malware protection, Bitdefender Antivirus for Mac also blocks phishing websites.

Good points

The new design of the program window is similar to the program's Windows counterpart, and we had no difficulty finding any important features in the program's interface. There is a well-produced, clearly written, neatly laid-out and comprehensive user's manual, easily accessible from the Help menu. Protection against Mac malware in our test was flawless.

Suggestions for improvement

We found that the AMTSO Phishing Test Page was only blocked rather sporadically by Bitdefender's *TrafficLight* extension for Safari. Likewise, the ratings for search results did not always appear for Google search results.

Installing and uninstalling

Installation

The user has to create a Bitdefender account and log in. A 2.7 MB .PKG installer file is provided. The user can choose to install which disk to install the application on.

Integration with operating system and browser

Bitdefender Antivirus for Mac adds its own menus and a System Tray icon to the Mac Menu bar, as well as a scan entry in the context menu. It also installs a Safari (and Chrome and Firefox) extension called *TrafficLight*, which can be enabled after setup. This is a safe browsing feature.

Deinstallation

The program can be removed from the computer using its own uninstaller found under Apps/Utilities. This is described in the user guide.

Deinstallation/deactivation from a standard user account

Attempting to disable *Autopilot* (real-time protection) or uninstall the program produces an OS X prompt for administrator credentials, regardless of who is logged on at the time; this prevents non-administrators from deactivating or removing the protection.

Using the program

Status

The main window has a prominent status display with a symbol and text. If real-time protection is turned off, the graphic and text of the status display change to show this:
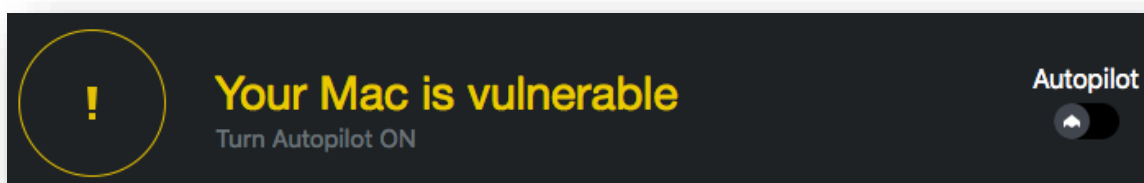
The warning instructs the user how to remedy this: *Turn Autopilot ON*, and the button for this is conveniently situated just to the right of the status text.

Updates

A manual update of malware signatures can be run by clicking the *Actions* menu, *Update Virus Database*.

Scanning

Quick, full and custom scans can be run from the respective buttons in the main program window, or the respective entries in the *Actions* menu. The custom scan option opens a dialog box, from which the user can browse to the folder or drive to be scanned. A custom scan can also be run by right-clicking a drive, folder or file, and then clicking *Scan with* Bitdefender in the context menu:
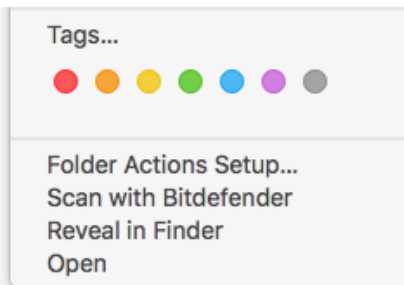
We could not find a means of setting a scheduled scan.

Settings, quarantine, logs and subscription information

Settings (*Preferences*) can be found in the *Antivirus for Mac* menu and the System Tray menu:
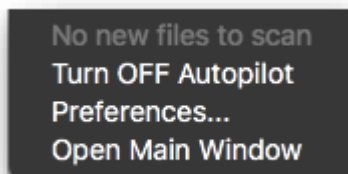
Quarantine and logs (*History*) can both be found in the *Preferences* dialog box:
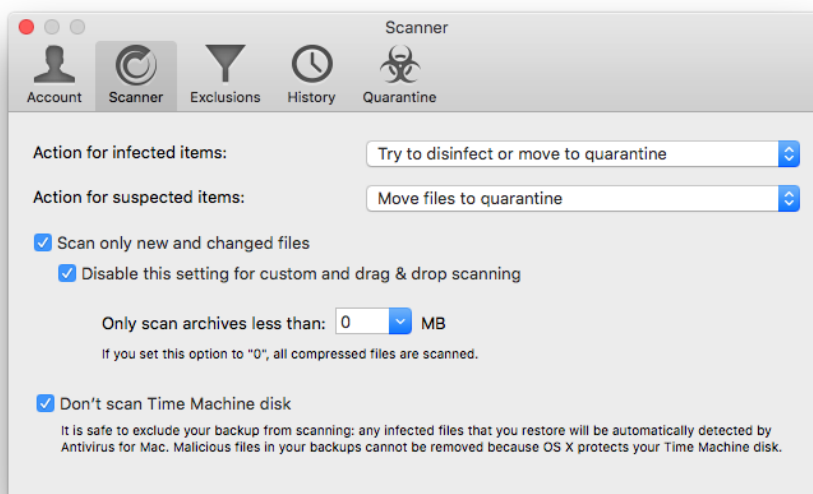
Subscription information is shown in the bottom right-hand corner of the program window.

Help

Clicking the *Help* menu, then *Antivirus for Mac Help* opens the product's user guide in .PDF format. This is a comprehensive, 48-page document covering all aspects of installing, configuring and using the program, with a clickable contents page and numerous screenshots.

Malware and phishing alerts

If the user attempts to download the EICAR test file, Bitdefender Antivirus for Mac deletes the file and displays the following alert:

Virus deleted
Name: EICAR-Test-File (not a virus)
Filename: eicar.com
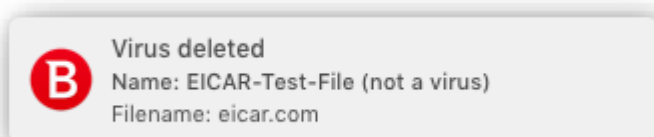
The AMTSO Potentially Unwanted test file is also deleted, and a similar message displayed. The AMTSO phishing test page is blocked with the following warning page:

Phishing attempt!

This page is part of a phishing attempt.

Web page:
http://www.amtso.org/check-desktop-phishing-page/

Take me back to safety

I understand the risks, take me there anyway

Search ratings are provided for Google searches in Safari:

Cheese - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/**Cheese** ▾
Cheese is a food derived from milk that is produced in a wide range of flavors, textures, and forms by coagulation of the milk protein casein. It comprises proteins ...
List of cheeses · Types of cheese · Coulommiers · Emmental

ESET Cyber Security Pro

Overview

Features

Cyber Security Pro includes malware protection, phishing protection, parental controls and a firewall.

Good points

As with previous incarnations of ESET Cyber Security Pro, version 6 has an extremely clear and well-designed interface, making it easy to use for both experts and non-experts. Help facilities are exemplary. Protection against Mac malware in our test was flawless.

Installing and uninstalling

Installation

An 87 MB .DMG installer file is provided. The two manuals for the product can be downloaded from the same page as the installer. The installer offers standard and custom installation types. The standard installation asks the user whether they want to join LiveGrid (ESET's data-sharing scheme), and whether to enable detection of potentially unwanted applications (we chose to do so).

Integration with operating system and browser

Cyber Security Pro adds menus and a System Tray icon to the Mac menu bar. No changes are made to Safari. By default, no changes are made to the Finder context menu, although ESET entries can be added to this in the program's preferences:
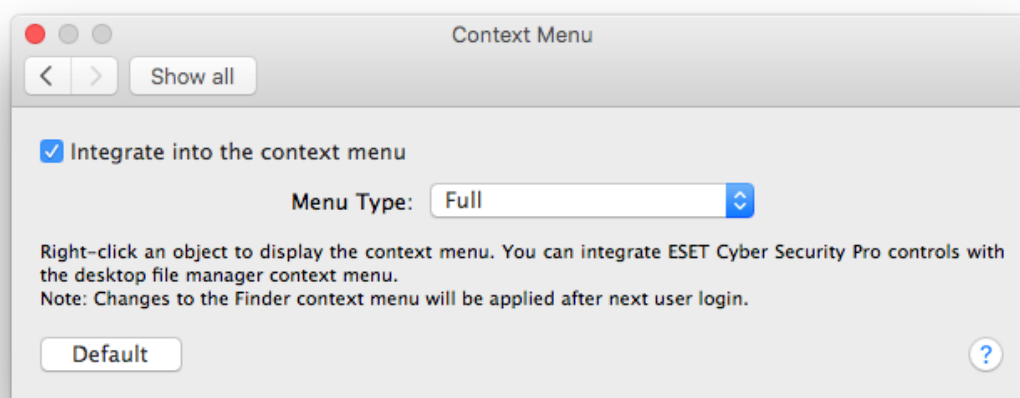
The options provided under *Menu Type* are *Full, Only Scan* and *Only clean*; it is not clear to us what the differences between these are. If the *Full* option is selected, the ESET options are shown in a sub-menu called *Services*; it was not immediately apparent to us that this was related to ESET, and so we did not initially look here to find scan options.

Deinstallation

The program can be uninstalled by re-running the installer, and clicking *Uninstall*.

Deinstallation/deactivation from a standard user account

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

Using the program

Status

If real-time protection is disabled, the status display in the main program window changes to show this:
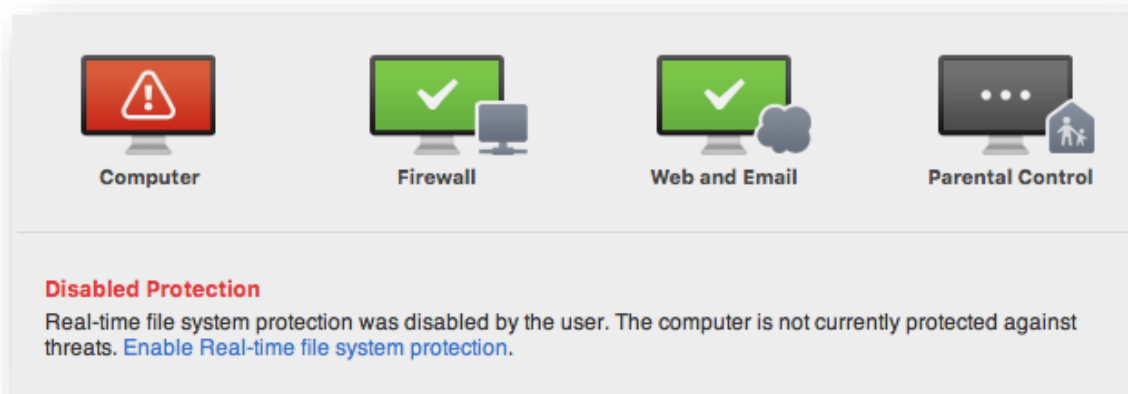

Protection can be reactivated by clicking *Enable real-time file system protection*.

Updates

Cyber Security Pro provides the standard automatic and manual signature update features; the latter can be run from the links in the main program window, or the System Tray menu.

Scanning

The *Computer scan* page of the program window allows the user to run full, custom or scheduled scans:
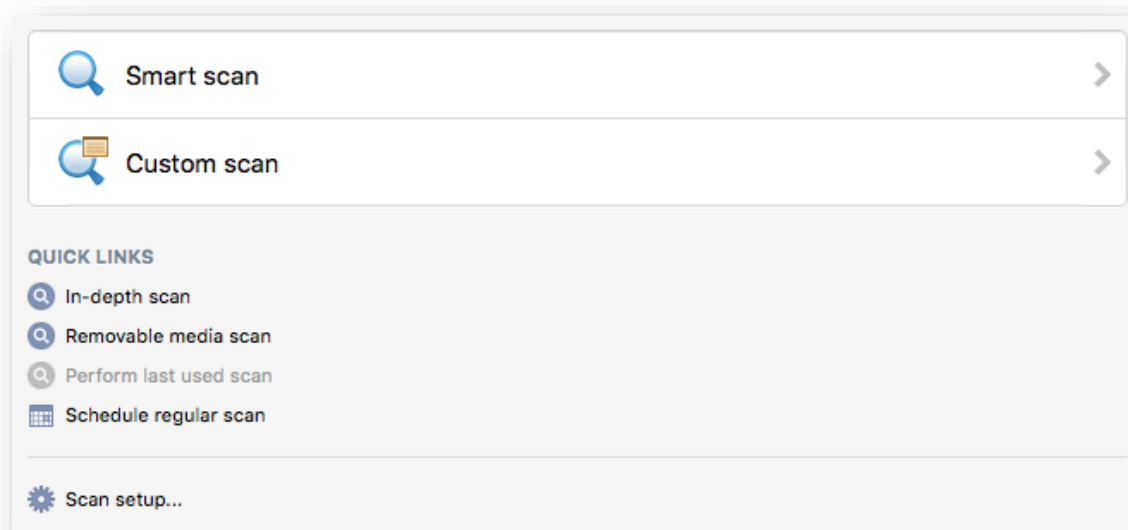
Settings, quarantine, logs and subscription information

Settings (*Preferences*) can be accessed via the *ESET Cyber Security Pro* menu, System Tray menu, or *Setup* page of the program window. Quarantine and logs can both be found on the program's *Tools* page, while subscription information is displayed on the *Home* page.

Help

Both the local help feature and the ESET online Knowledgebase can be accessed from the program's *Help* page or the *Help* menu. The local help window provides comprehensive text instructions, with some screenshots, for installing, configuring and using the program. The ESET Knowledgebase is a searchable FAQ page, and provides very detailed instructions with annotated screenshots for a wide range of common tasks. A quick-start guide and comprehensive manual, both well illustrated and produced to an excellent standard, are also available from the vendor's website.

Malware and phishing alerts

If the user attempts to download the EICAR test file, the following alert is displayed:
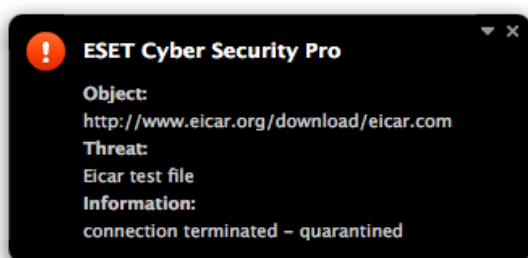
If detection of potentially unwanted programs has been enabled in the settings, Cyber Security Pro shows the following alert in the browser window if the AMTSO PUA test file is downloaded:
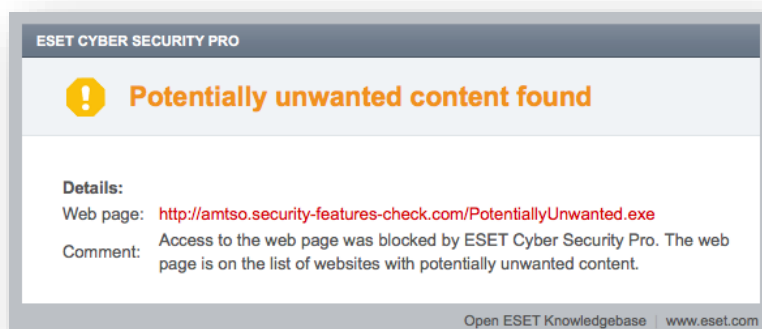
The AMTSO phishing test page is blocked with a similar warning:
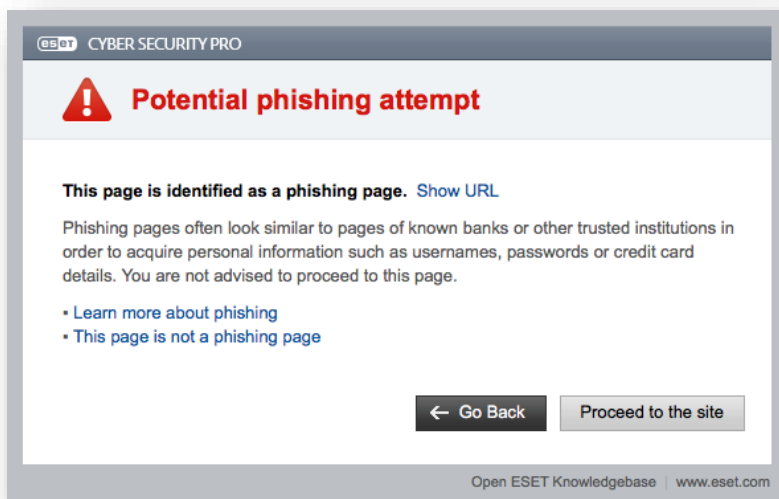
Additional comments

After installation, an ESET prompt asks the user whether the current network is to be regarded as public or private, so as to configure the ESET firewall appropriately:
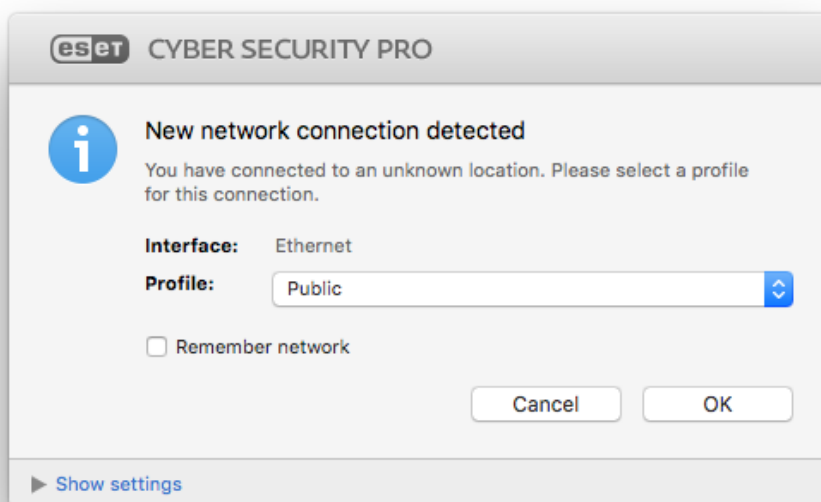
Intego Mac Premium Bundle X9
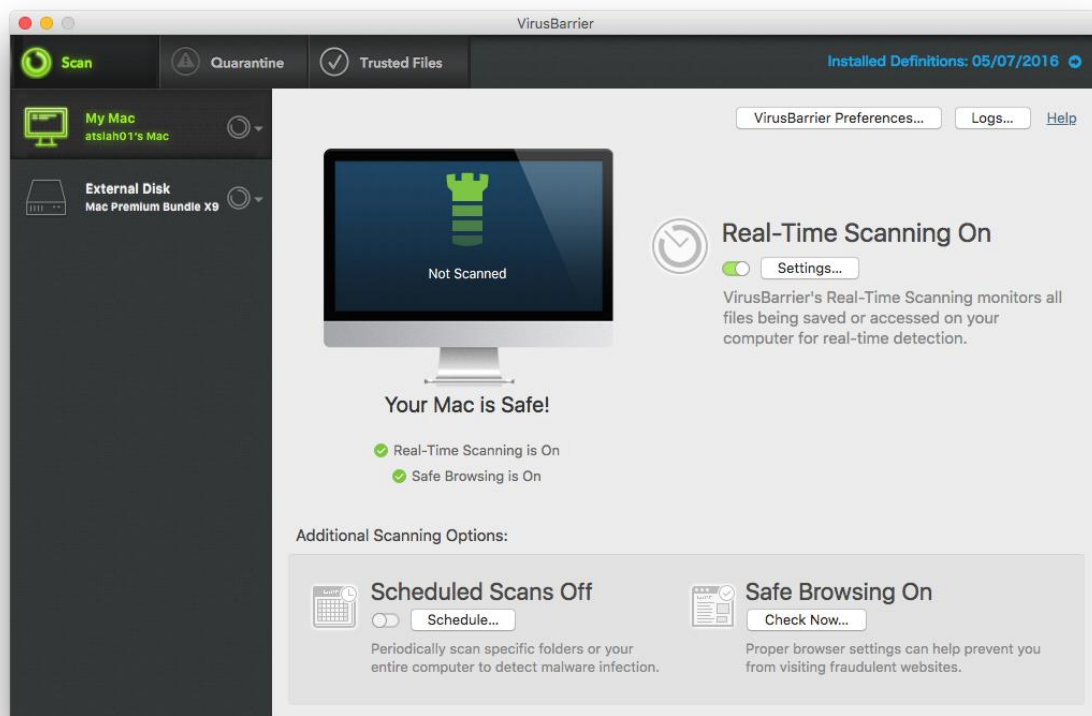
Overview

Features

In addition to malware protection, the Mac Premium Bundle X9 includes a firewall, backup, parental controls and a cleaning tool.

Good points

We are pleased to see the very clear status display, showing a warning if protection is disabled, in the new version. The overlay showing the functions available in the window is a clever means of introducing the program quickly to new users. Protection against Mac malware in our test was flawless.

Installing and uninstalling

Installation

A 93 MB .DMG installer file is provided. The wizard allows the user to choose which components to install:
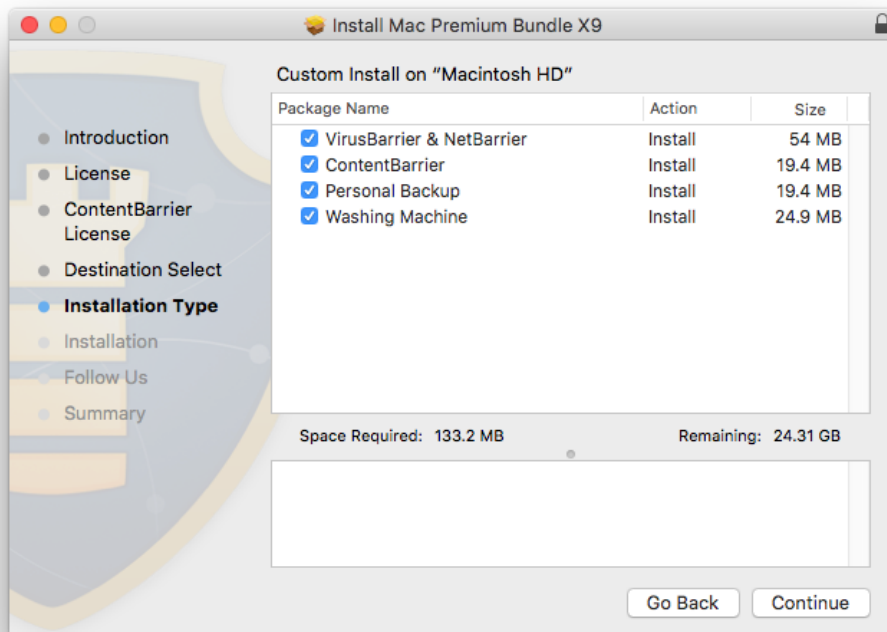
A restart is required when the installation is complete. After this, the product has to be activated or the trial version selected. The program asks the user to define a protection level (we used the default *Standard*):
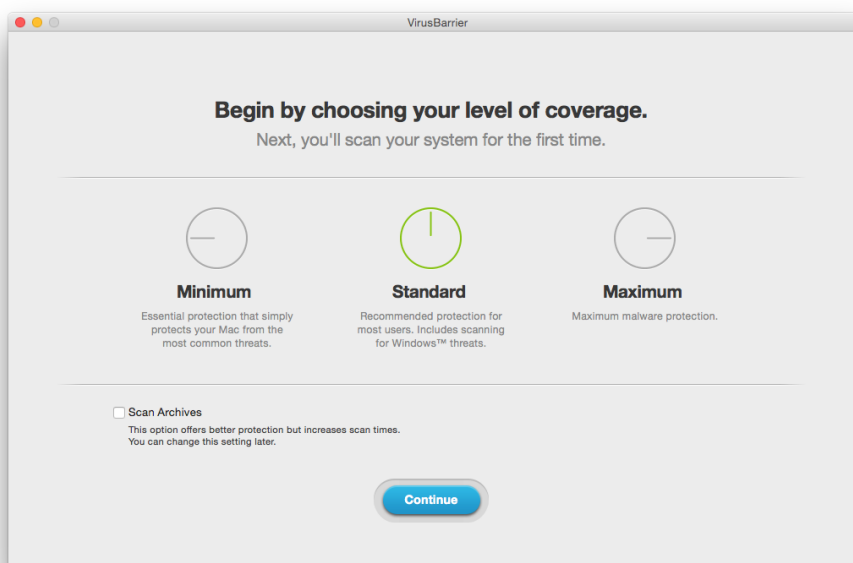
Next, the main program window is shown with an overlay that points out its main features:
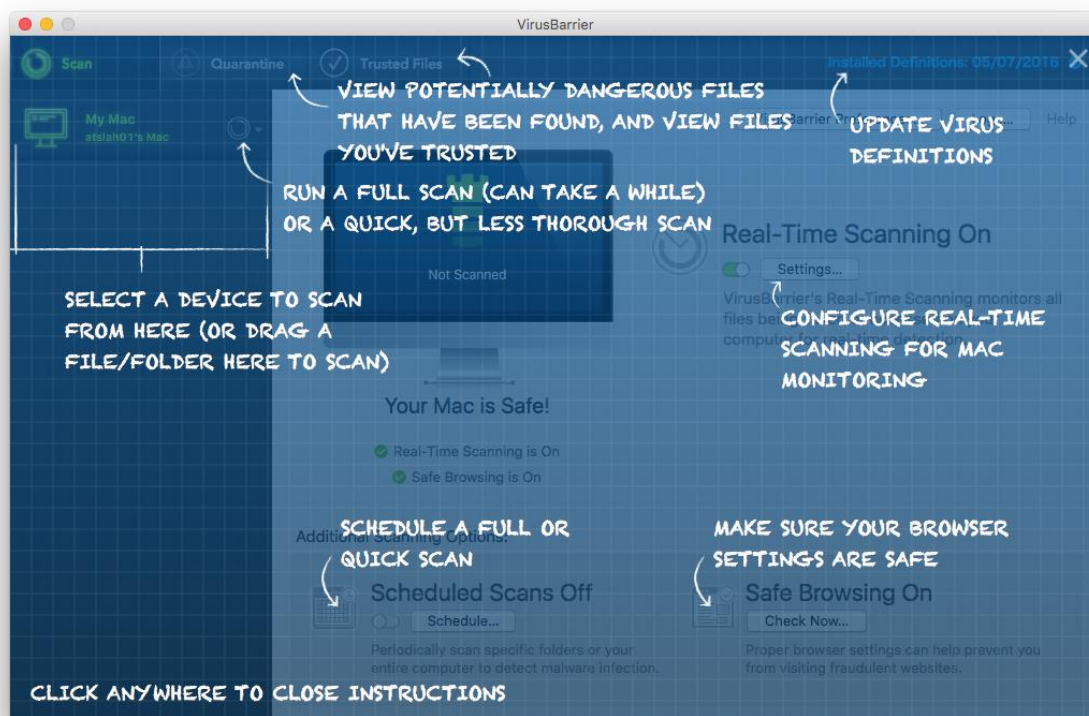

Integration with operating system and browser

The Mac menu bar shows menus and a System Tray icon, which displays sub-menus for the different components:
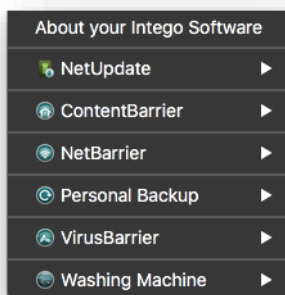
The VirusBarrier sub-menu looks like this:
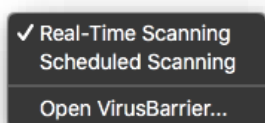
A *Scan with VirusBarrier* entry is added to the Finder context menu. Safari is not altered.

Deinstallation

The program can be uninstalled by re-running the installer program. This is described in the program's knowledge base.

Deinstallation/deactivation from a standard user account

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

Using the program

Status

There is a status display for real-time protection, which displays the text *Real-Time Scanning On* when all is well. If protection is disabled, the text changes to *Real-Time Scanning Off*, with additional warning text and graphic, plus a link to turn the protection on again:
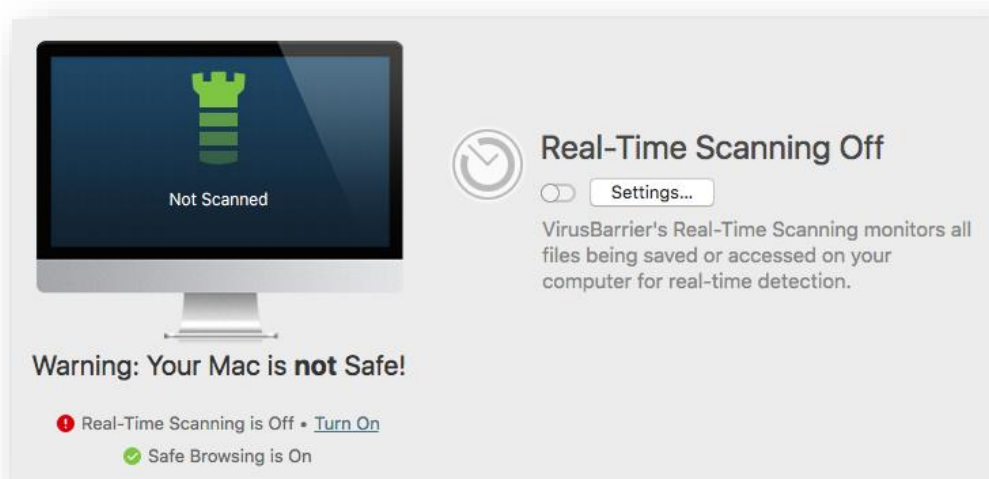
Updates

Malware signatures (which are updated automatically) can be manually updated from the VirusBarrier menu in the Mac menu bar, or by clicking the Installed Definitions link in the top right-hand corner of the window.

Scanning

Scheduled scans can be setup from the *Schedule…* button 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. Custom scans can be run from the *File* menu in the Mac menu bar.

Preferences, quarantine, logs and subscription information

Preferences can be found in the *VirusBarrier* menu. Quarantine has its own button in the top left-hand corner of the window, and logs can be found in the *Window* menu. Clicking the *VirusBarrier* menu, then *About VirusBarrier*, shows the licence key used, but we could not find a means of showing the expiry date.

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:
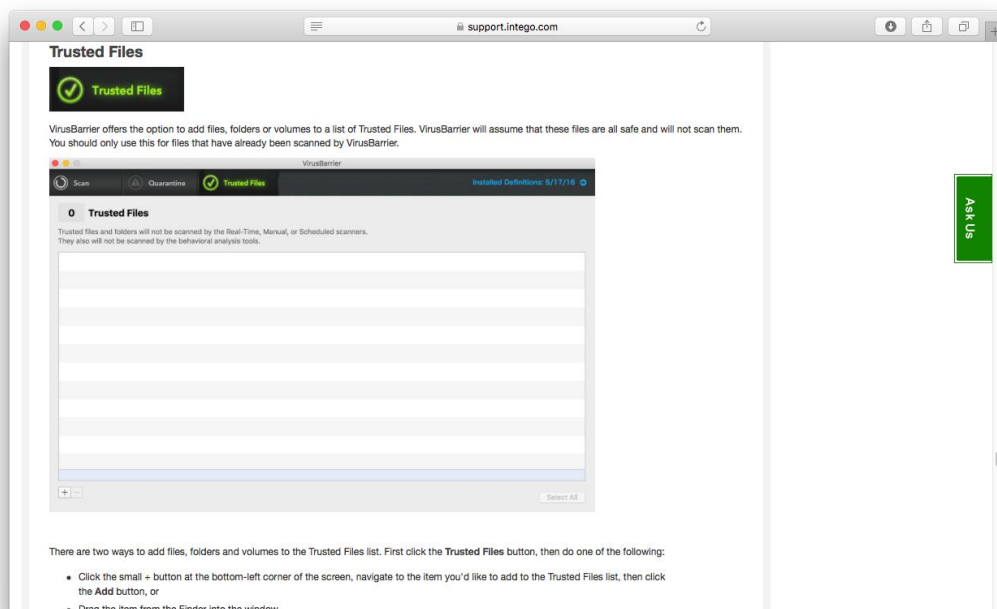
The *Show Basic Help* entry in the same menu displays the overlay shown after installation.

Malware and phishing alerts

If the EICAR test file is downloaded, the following alert is shown:
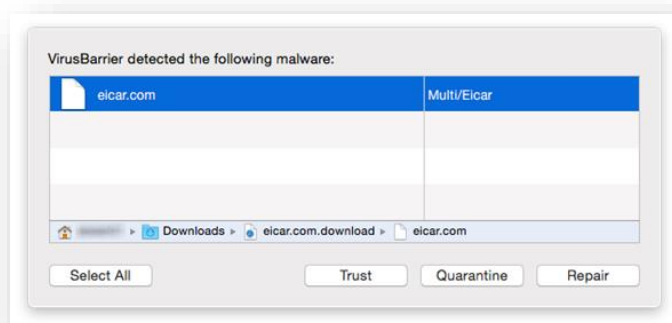
If the user enables detection of *Hacking tools* and *Keyloggers* in the settings (or selects *Maximum protection* at the end of the installation process), Virus Barrier detects the AMTSO PUA test file, with a similar alert to the one above being shown. Intego does not support the AMTSO phishing test page.

Additional comments

In last year's report, we noted a number of firewall prompts, some relating to other components of the Intego suite. We are pleased to report that we did not see any such prompts during testing for this year's report.

Kaspersky Internet Security for Mac

Overview

Features

Kaspersky Internet Security for Mac includes malware protection, phishing protection, parental controls, plus Safe Money (protects online banking) and Privacy Protection (allows blocking the webcam, and prevents tracking by ad services).

Good points

Kaspersky Internet Security for Mac has a clear, modern design that makes important features and information easy to find. Users of its Windows counterpart will easily find their way around the program, and help features are good. Protection against Mac malware in our test was flawless.

Suggestions for improvement

The setup wizard could inform the user to the fact that Safari extensions are available (the *Browsers* tab in the program's Preferences links to these). Additionally, the user manual would benefit the addition of appropriate screenshots.

Installing and uninstalling

Installation

A 182 MB .DMG installer file is provided. The download page also includes a link to the product manual. The only option in the setup wizard is whether to join the Kaspersky Security Network (data sharing scheme).

Integration with operating system and browser

Kaspersky Internet Security for Mac adds menus and a system tray icon to the Mac menu bar, and a *Scan for Viruses* entry to the Finder context menu. By default, no Safari extensions are installed, although two are available to install from the *Preferences* dialog:
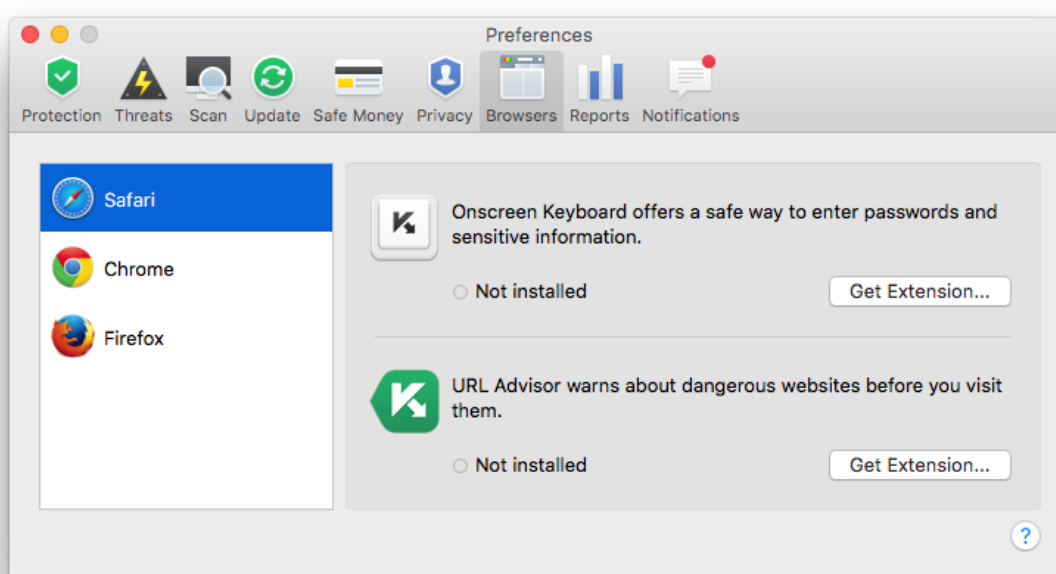
Deinstallation

The program can be uninstalled by re-running the installer program and selecting *Uninstall Kaspersky Internet Security*.

Deinstallation/deactivation from a standard user account

The program cannot be uninstalled, or the protection deactivated, using non-administrator credentials.

Using the program

Status

The status display in the main window displays the text *Your Mac is protected* if all is well. If real-time protection is disabled, this changes to a warning, as shown below:
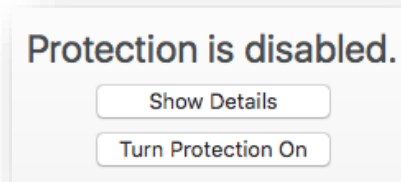
Protection can be easily reactivated by clicking *Turn Protection On*.

Updates

Malware signatures can be updated from the System Tray menu, *Protection* and *Kaspersky Internet Security* menus, or the button on the main window.

Scanning

Quick, full, and custom scans can be run from the Protection menu, or by clicking the *Scan* button on the program's home page:

### Settings, quarantine, logs and subscription information

Logs and quarantined are combined, and can be accessed by clicking *Detected objects*:
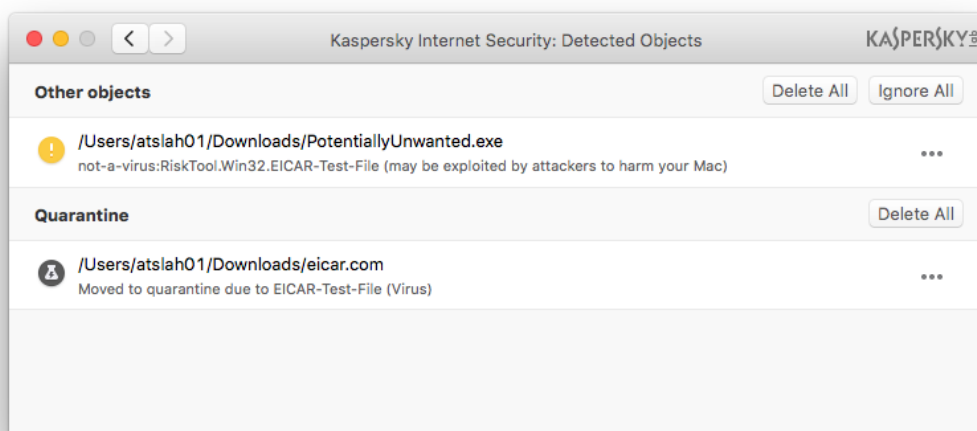
Settings (*Preferences*) are found in the *Kaspersky Internet Security* menu, and subscription information is shown in the bottom right-hand corner of the main window.

Help

There is a local help feature, which can be opened from the *Help* menu. It provides comprehensive text instructions for installing, configuring and using the program:
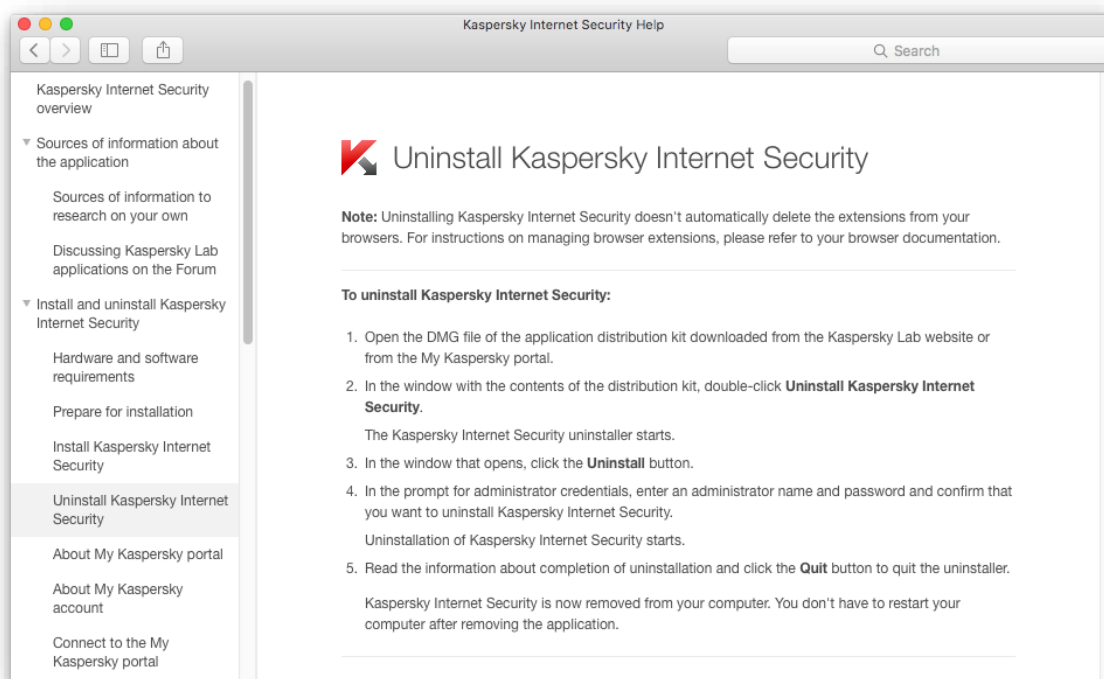
A comprehensive manual is available for download from the Kaspersky Lab website. This is well written and clearly laid out, but with the exception of a few icons, does not include any screenshots.

Malware and phishing alerts

If the EICAR test file is downloaded, the following alert is shown in the browser window:
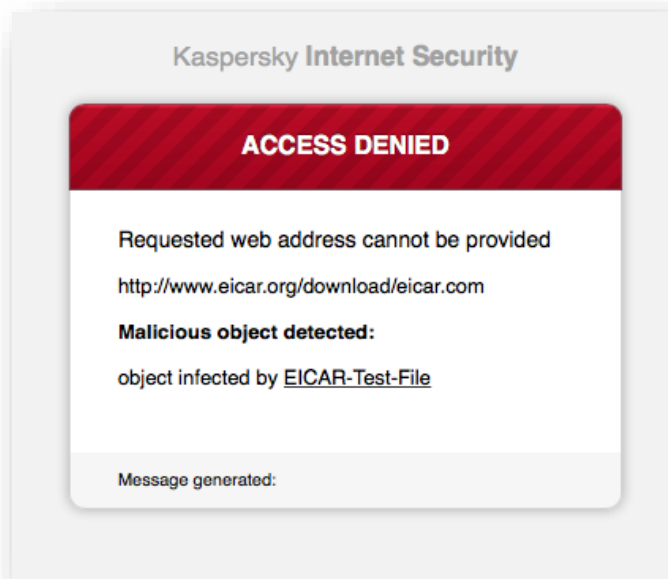
A similar alert is shown for the AMTSO phishing test page, and (if *Other applications* is selected in *Preferences/Threats*) for the AMTSO PUA test file. In the default configuration (without Safari extensions installed), search ratings are not shown for Google searches in Safari.

McAfee LiveSafe for Mac
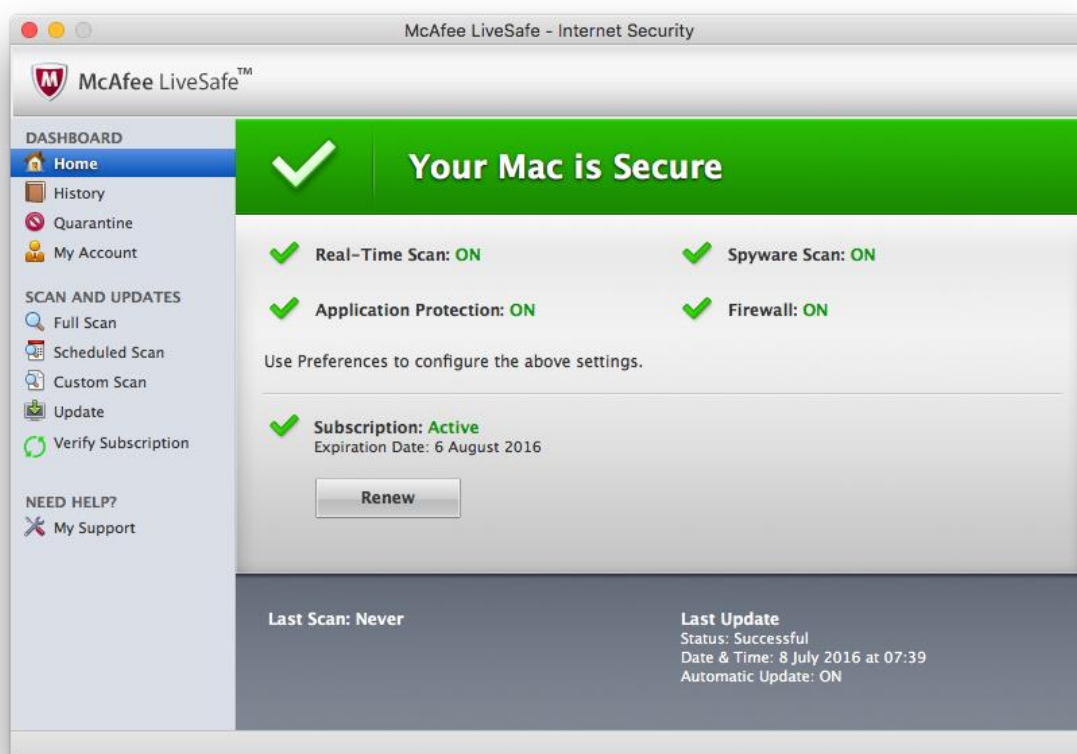
Overview

Features

McAfee LiveSafe for Mac is an antimalware program with firewall.

Good points

We found McAfee LiveSafe for Mac very easy to install and use. Important features and information are largely easy to find. Protection against Mac malware in our test was flawless.

Suggestions for improvement

A "Fix-All" button, to rectify problems such as disabled protection or outdated signatures, would be useful.

Installing and uninstalling

Installation

A 6 MB .DMG installer file is provided. The user has to confirm the installation of, and options for, the *SiteAdvisor* extension for Safari (shown below), and state whether the current network should be regarded as private or public (for the McAfee firewall).
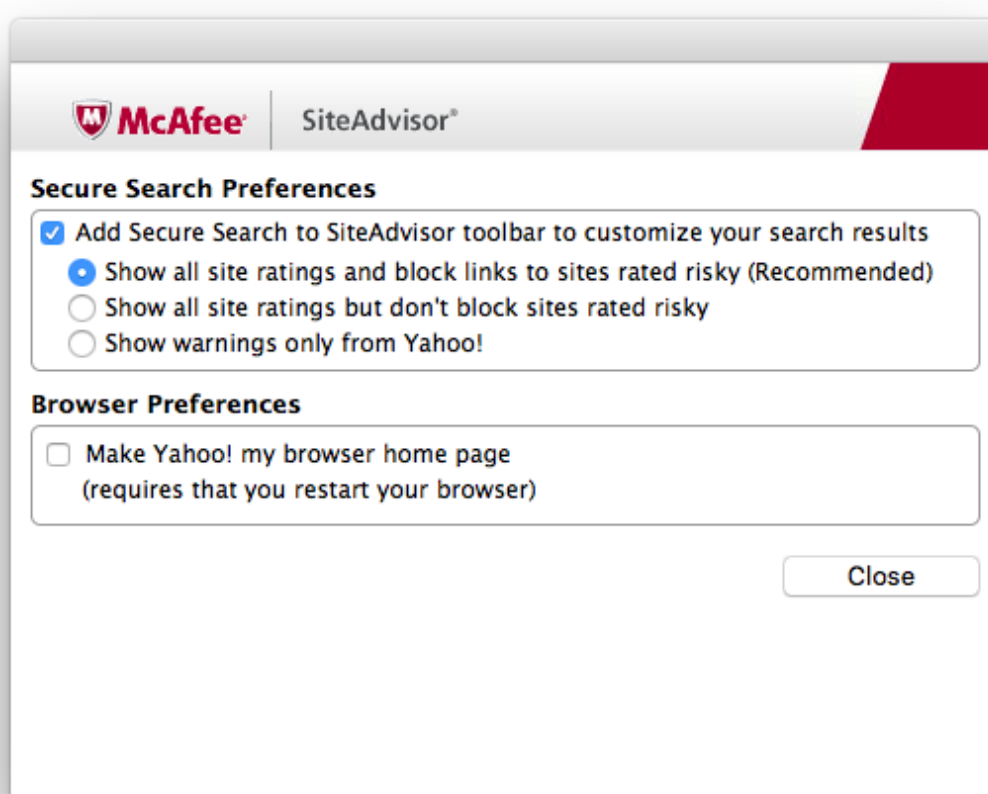
Integration with operating system and browser

LiveSafe for Mac adds menus and a system tray icon to the Mac menu bar, and a *SiteAdvisor* extension to Safari.

Deinstallation

An uninstaller program is provided, and can be found in the Applications folder.

Deinstallation/deactivation from a standard user account

The protection cannot be disabled, or the program uninstalled, without entering administrator credentials.

Using the program

Status

There is a prominent green strip on the home page of the program with a status display as text and a graphic. If real-time protection is disabled, the following warning is shown:

There is no "Fix-All" button to reactivate the protection, but a message to use Preferences to turn on disabled features is displayed.

Updates

Malware signatures can be updated by clicking the *Update* link in the menu panel on the left-hand side of the window.

Scanning

Full, custom and scheduled scans can be run from the respective links in the left-hand menu panel.

Settings, quarantine, logs and subscription information

Settings (*Preferences*) can be found in the *McAfee LiveSafe…* menu in the Mac menu bar. Quarantine and logs (*History*) have their own links in the menu panel on the left. Subscription information is displaye in the main panel of the program window.

Help

There is a local help feature, accessible from the *Help* menu in the Mac menu bar. It provides concise text explanations of features and instructions for everyday tasks:
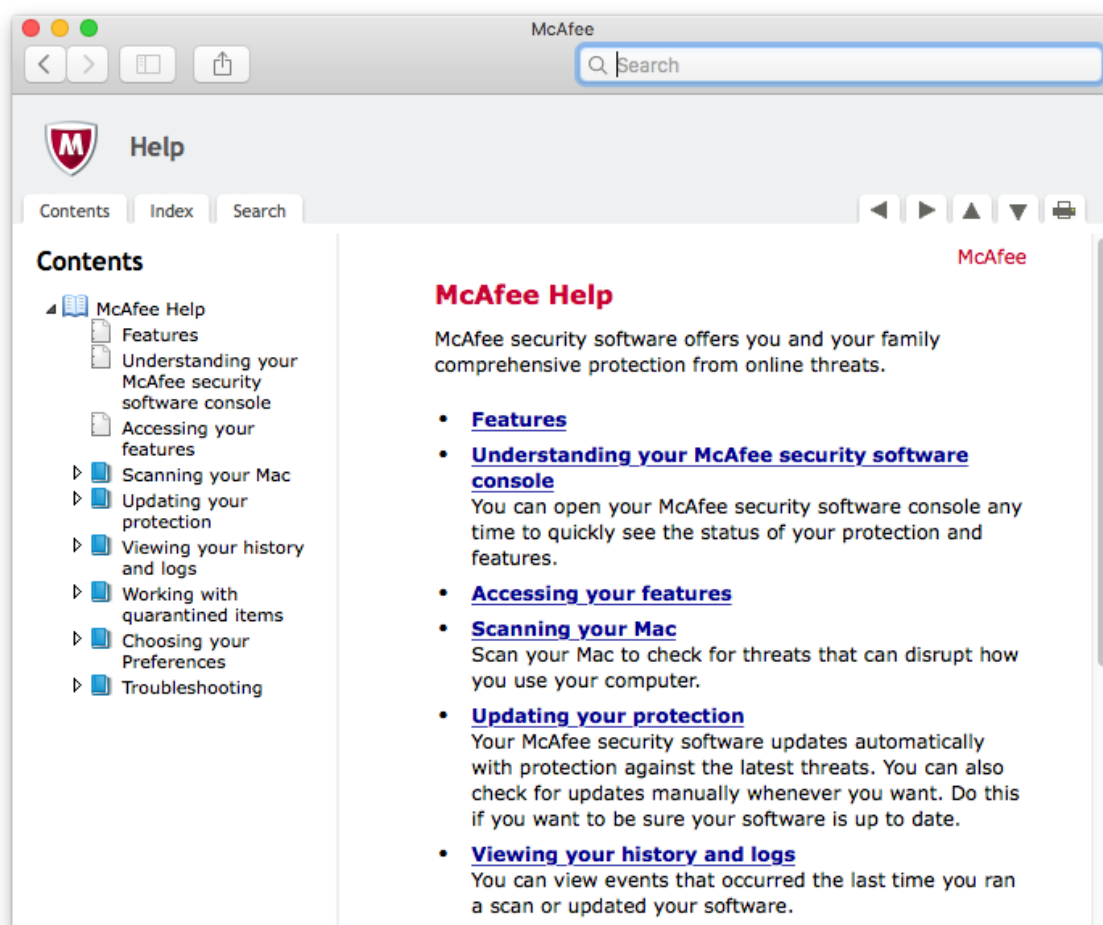
Malware and phishing alerts

If the EICAR test file is downloaded, McAfee blocks the download and displays the notification shown below:

When the user tries to download the AMTSO PUA file, the download is again blocked, and the following alert shown in the browser window:
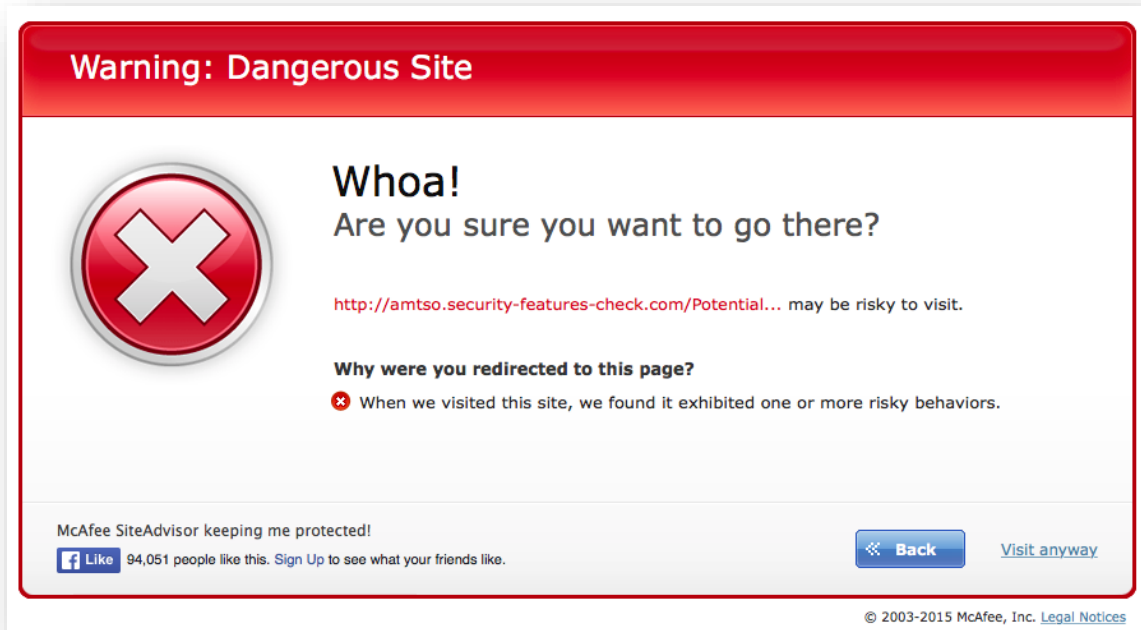

A very similar browser warning is shown for the AMTSO Phishing Test Page. Search ratings are provided for Google searches with Safari:
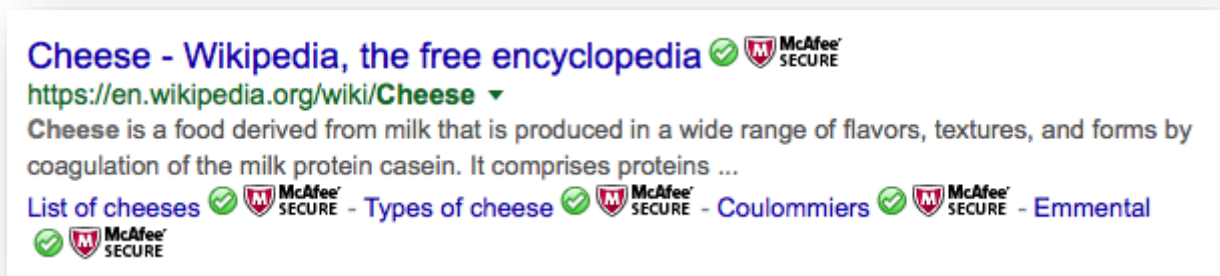
Sophos Home for Mac

Overview

Features

Sophos Home for Mac provides malware and phishing protection with parental controls. It is installed and managed using the Sophos Home cloud management console. Protection against Mac malware in our test was flawless.

Good points

The very clean and simple design of the program interface, both in the program window and the management console, makes it very easy to use. The consistency of design between the Mac and Windows versions will be appreciated by anyone who uses or manages both platforms. Protection against Mac malware in our test was flawless.

Installing and uninstalling

Installation

To install the product, the user has to create a Sophos Home account and log in to the cloud management console, then click *Add Device* to download the installer:
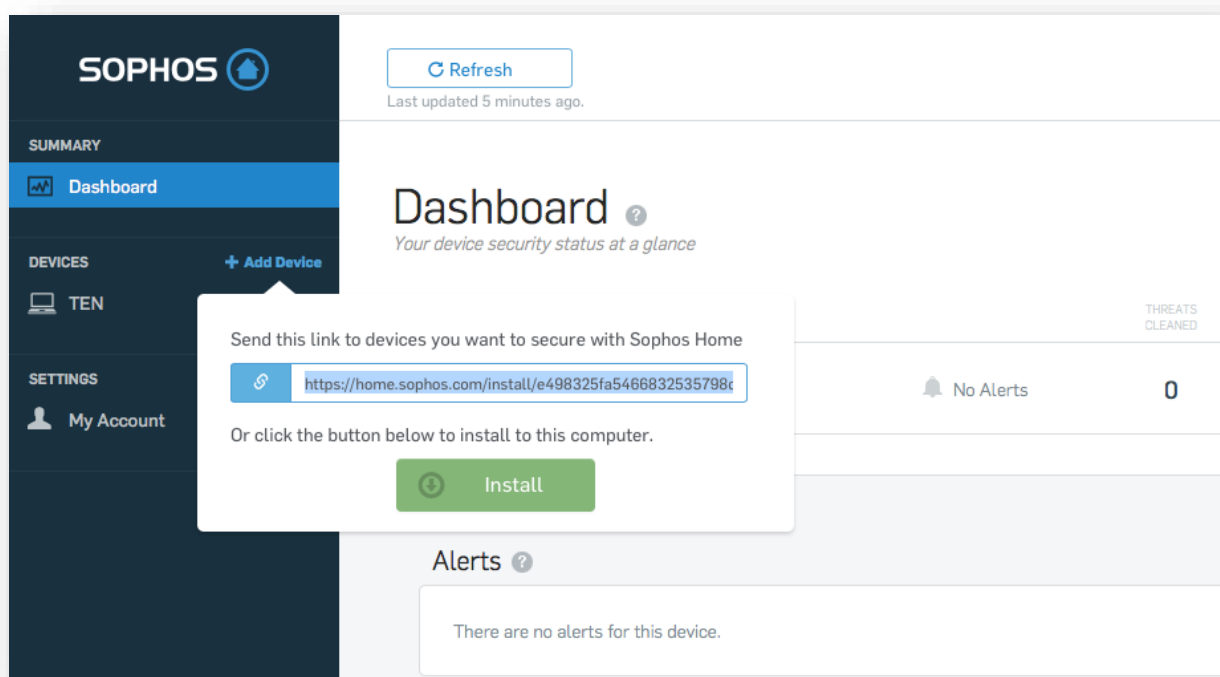
The setup wizard has no options and can be completed with a single click.

Integration with operating system and browser

Sophos Home adds a menu and System Tray icon to the Mac menu bar, and a *Scan with Sophos Home* entry to the Finder context menu:
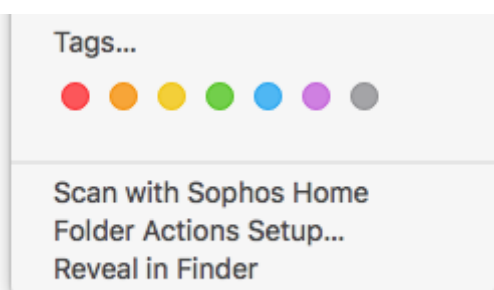
No changes are made to Safari; Sophos inform us that they provide web security for Safari and other browsers, but by other means than plug-ins.

Deinstallation

Sophos Home has its own uninstaller program. The help feature describes how to run this by using the Mac's Spotlight search function.

Deinstallation/deactivation from a standard user account

Protection can only be deactivated from the cloud console, so only users who have the console credentials are able to do this. Removing the software requires administrator credentials to be entered, regardless of who is logged in.

Using the program

Status

If real-time protection is disabled, the status display shows a warning:
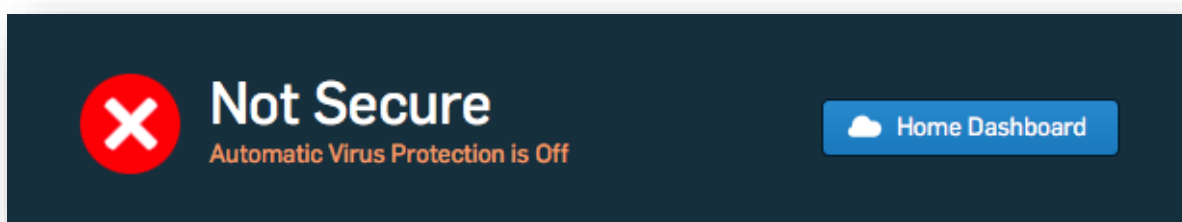
To reactivate protection, the user has to use the Sophos Home cloud management console.

Updates

Malware signatures can be updated from the System Tray menu:
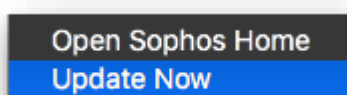
Scanning

Full scans can be run from the program's home page, or the device's page in the console. Custom scans can be run by right-clicking a drive, folder or file, and right-clicking *Scan with Sophos Home*. We could not find a means of running a scheduled scan.

Preferences, quarantine, and logs

Preferences are limited to enabling and disabling the three main protection components, and settings scan exceptions, both of which can be done from the cloud management console. The console also displays malware detection logs (*Device Events*). There is no quarantine as such.

Help

Clicking the *?* symbol in the program window opens the Sophos Home help page on the Sophos website. This could be described as an online manual, with straightforward explanations and instructions for installing and using the product. It is very well illustrated with screenshots:
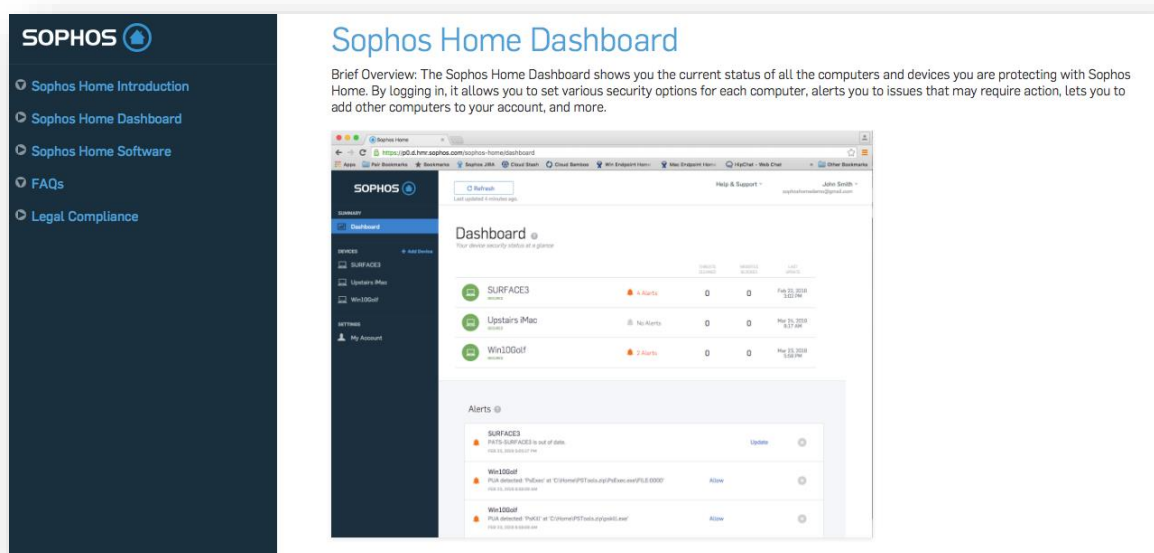
Malware and phishing alerts

If the EICAR test file is downloaded, Sophos Home blocks the download and displays an alert in the browser window:
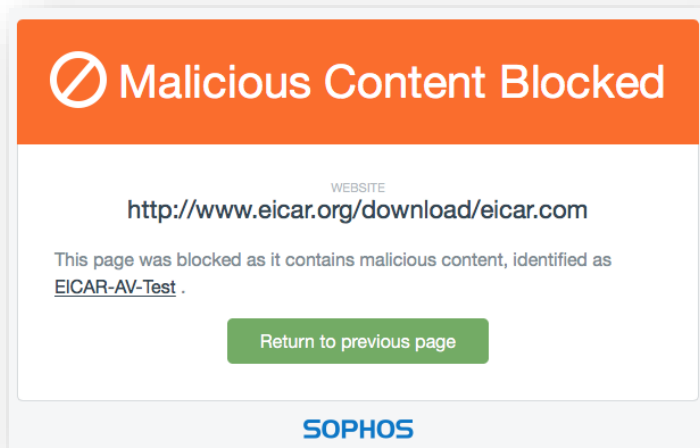
A similar alert is shown if the AMTSO phishing test page is accessed. If the AMTSO PUA test file is downloaded, Sophos displays an alert message box, and also shows an alert in the status area of the program window:
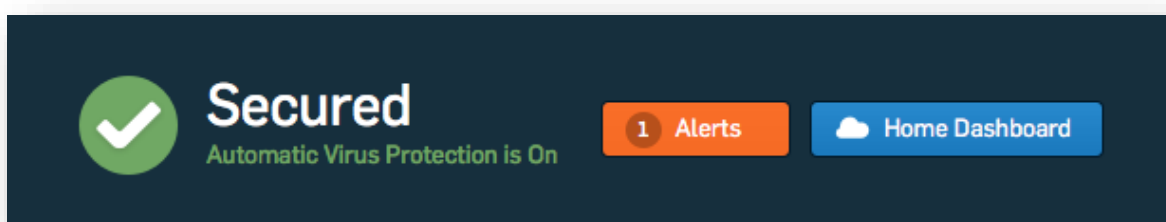
Clicking the *Alerts* button allows the user to delete the file if desired:
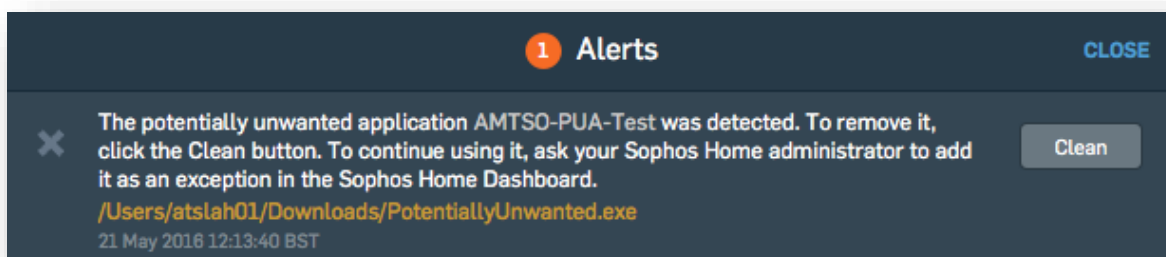
Additional comments

There is a Sophos Home antivirus for Windows, which has an identical window layout to the Mac version. Management of Mac and Windows devices from the console is identical.

Webroot SecureAnywhere Internet Security Complete
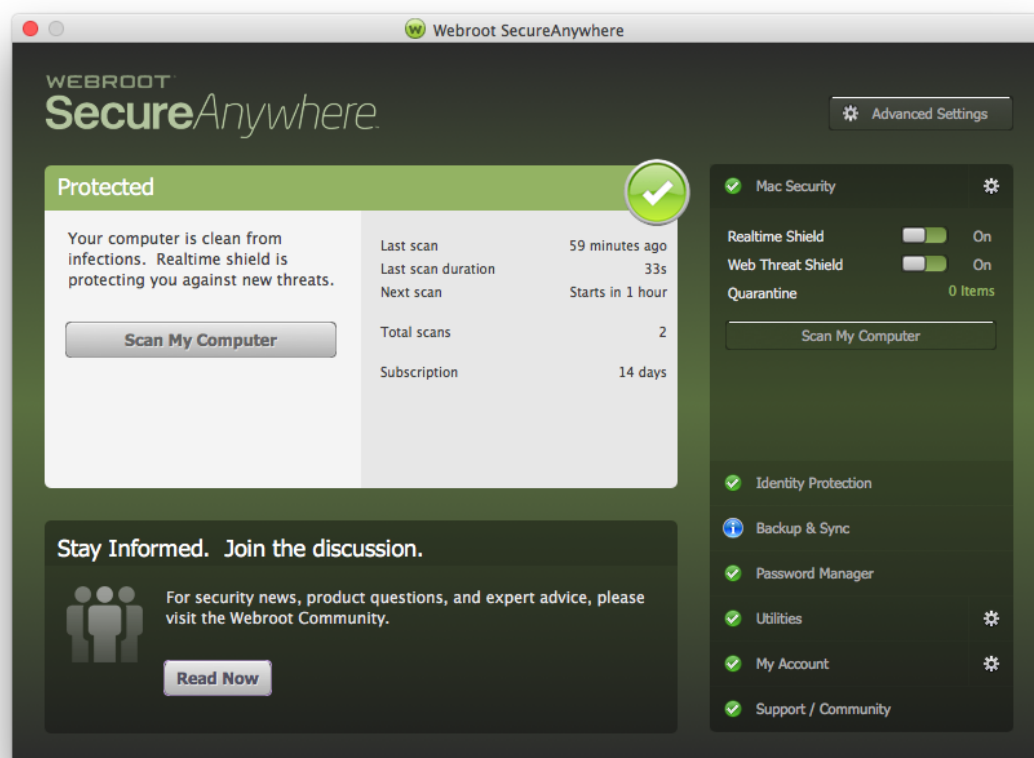
Overview

Features

Webroot Internet Security Complete for Mac is an antimalware solution with a password manager, backup feature, system optimiser and identity protection.

Good points

The program's interface is easy to navigate and makes important functions easy to find. Anyone who uses or manages both Windows and Mac platforms will find the consistency of design between the two versions helpful. Protection against Mac malware in our test was flawless.

Suggestions for improvement

The ability to password-protect the settings, in order to prevent unauthorised users disabling the protection, would be useful.

Installing and uninstalling

Installation

A 1 MB .DMG installer file is downloaded. There is a choice of UI languages. The setup wizard encourages the user to create a Webroot account, although this is optional.

Integration with operating system and browser

Webroot SecureAnywhere adds four menus to the Mac menu bar, along with a system tray icon that displays the following menu:
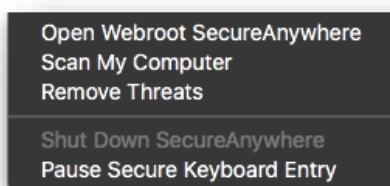
A Safari extension by the name of "webfilter" is added. The Finder context menu is not altered.

Deinstallation

The program can be uninstalled by shutting it down and dragging the program's icon in the Applications folder to the Trash.

Deinstallation/deactivation from a standard user account

It is possible to deactivate protection using a non-administrator account. We could not find a means of preventing this in the program settings. Uninstalling the software requires administrator credentials to be entered, however.

Using the program

Status

The main program window includes a status display with text and a graphic in green. If real-time protection is disabled, this changes to show a warning in red:
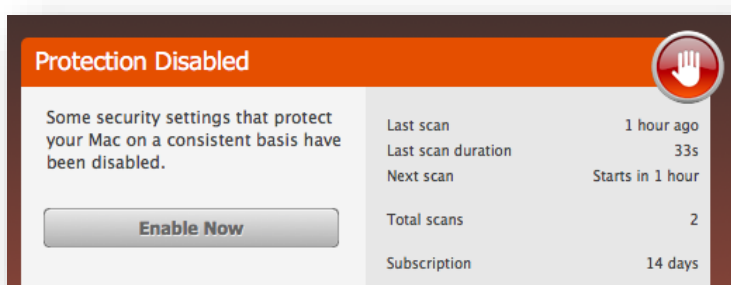
Clicking *Enable Now* immediately reactivates protection.

Updates

Webroot SecureAnywhere does not use local malware signatures and so there is no need for an update feature.

Scanning

A default scan can be run from the *Scan My Computer* button on the home page of the main program window. By default, this runs a full scan, although this can be changed to a quick scan in *Advanced Settings*:
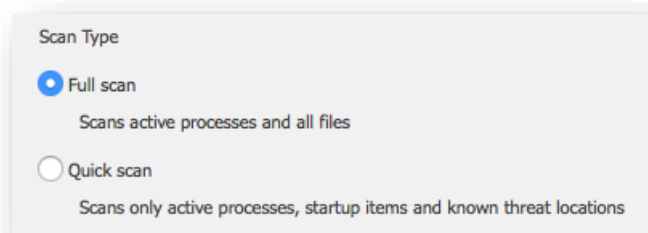
A scheduled scan can also be set by clicking *Schedule* in the *Advanced Settings* dialog box.

Preferences, quarantine, logs and subscription informatio

Preferences can be set by clicking *Advanced Settings* in the top right-hand corner of the program window. There is a *Quarantine* button in the settings panel on the left-hand side of the program window.

Help

Clicking *SecureAnywhere Help* in the *Help* menu opens the program's online help page on the Webroot website. This is very simply and clearly laid out, and provides straightforward instructions for using the program's features, well illustrated with screenshots:
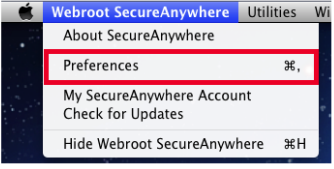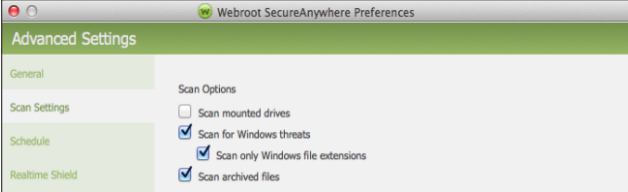
Malware and phishing alerts

If the EICAR test file or AMTSO PUA test file is downloaded, Webroot displays the scan window, showing the threat discovered:

To quarantine the threat, the user needs to click *Next*, and then *Begin Threat Removal* on the next page of the wizard. The AMTSO phishing test page is not recognised. Search ratings for Google searches are displayed:

Featurelist Mac (as of July 2016)	FREE	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL
Product name:	Avast Free Mac Security	AVG AntiVirus for Mac	AVIRA Free Antivirus for Mac	Bitdefender Antivirus for Mac	ESET Cyber Security Pro	Intego Mac Premium Bundle	Kaspersky Internet Security for Mac	McAfee LiveSafe for Mac	Sophos Anti-Virus for Mac	Webroot SecureAnywhere Internet Security Complete for Mac
Supported OS X versions:	10.6.8 and up	10.8 and up	10.10 and up	10.8.5 and up	10.6 and up	10.8 and up	10.9 and up	10.8 and up	10.8 and up	10.7.3 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, French, German, Japanese, Spanish	English, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	Chinese, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish	English, French, German, Japanese, Spanish	English, Chinese, Dutch, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish
Protection										
Real-Time protection	•	•	•	•	•	•	•	•	•	•
On-demand scanner	•	•	•	•	•	•	•	•	•	•
Detects also threats for other platforms (e.g. Windows malware)	•	•	•	•	•	limited detection of windows threats	•	•	•	•
Detects also PUA on Mac	•	•	•	•	•		•	•	•	•
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	•				•	•				
Firewall					•	•		•		•
Removable media blocking					•	•			•	
Other features	Home network security, VPN				Game/Presentation mode		Webcam protection, Private browsing, Network attack protection, Secured browser for online banking	Backup		Backup, System optimizer, Identity protection, Password manager
Support										
Online Help and/or User Forum	•	•	•	•	•	•	•	•	•	•
Email and/or 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, French, Japanese	English, Arabic, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	Chinese, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish	English, French, German, Spanish, Japanese, Italian, Chinese	All
Price (may vary)										
Price 1 Mac / 1 year (USD/EUR)	FREE	FREE	FREE	USD 40 / 40 EUR	USD 45 / 35 EUR	USD 90 / 75 EUR	USD 40 / 40 EUR	USD 90 / 90 EUR	FREE	USD 60 / 75 EUR

Copyright and Disclaimer

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

AV-Comparatives (July 2016)