

# Mac Security Test & Review



## Mac Security Test & Review

Language: English

July/August 2014

Last revision: 29<sup>th</sup> August 2014

[www.av-comparatives.org](http://www.av-comparatives.org)

# Contents

Introduction: Macs and Security Software .....	3
Review of Security Software for OS X 10.9 Mavericks .....	4
Malware Protection Test.....	6
avast! Free Antivirus for Mac .....	8
Avira Free Antivirus for Mac.....	11
Bitdefender Antivirus for Mac .....	14
ESET Cyber Security Pro.....	18
Intego Mac Premium Bundle X8.....	21
Kaspersky Internet Security for Mac .....	26
Kromtech MacKeeper .....	29
Sophos Antivirus for Mac.....	33
Summary .....	36
Copyright and Disclaimer .....	38

## Introduction: Macs and Security Software

In January 2014, ZDNet<sup>1</sup> and other sources reported the existence of cross-platform botnet software that installs by exploiting a vulnerability in Java SE 7 Update 21 and earlier. It can infect Windows, Linux and Mac OS X computers running the affected Java versions. At about the same time, ZDNet also reported that the Flashback botnet, which it claims had infected over 600,000 Macs in 2012, was still in existence, albeit with a much-reduced number of infected machines (22,000). Reports such as these should serve as a warning to anyone who believes that the Mac OS is immune to malware attacks and that Mac users do not need to consider security issues.

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* (e.g. malicious programs disguised as 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

---

<sup>1</sup> <http://www.zdnet.com/cross-platform-java-bot-found-7000025736/>

## Review of Security Software for OS X 10.9 Mavericks

We have reviewed and tested the following products for this report, using the newest version available in July 2014:

- **avast! Free Antivirus for Mac 9.0.42061**
- **AVIRA Free Antivirus for Mac 2.0.5.100**
- **Bitdefender Antivirus for Mac 3.1.8203**
- **ESET Cyber Security Pro 6.0.13.0**
- **Intego Mac Premium Bundle X8 10.8.2**
- **Kaspersky Internet Security for Mac 14.0.1.46c**
- **KromTech MacKeeper 3.0.2.127**
- **Sophos Anti-Virus for Mac 9.0.11**





## Review format

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

### 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 if the following items, which we consider the most important, can be accessed from the main window: Status; Scans; Update; Settings; Help; Subscription information.

### Mac menu bar

We look for a System Tray icon and menus in the Mac menu bar, to see what additional commands are available there.

### Finder context menu

We note whether a scan be started by right-clicking a file, folder or drive.

### Maintenance

We check whether signatures 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 disable the protection.

### Scanning

We check whether a quick scan, full scan, custom scan and scheduled scan all 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 a phishing page is accessed (tested using AMTSO Phishing Test Page<sup>2</sup>), malware is downloaded from the Internet (tested using EICAR test file<sup>3</sup>), malware is found by real-time protection on a flash drive (tested using genuine Mac malware samples), and a full scan of the flash drive is run (also real Mac malware).

We note how clear its clear whether the user needs to take action, and how easy is it to make a bad decision (e.g. allow the malware to run).

### 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.

---

<sup>2</sup> <http://www.amtso.org/feature-settings-check-phishing-page-intro.html>

<sup>3</sup> <http://www.amtso.org/feature-settings-check-download-of-malware.html>

## 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 65 recent and prevalent samples of Mac malware that are not blocked by Mac OS X Mavericks itself. All are distinctly malicious, functioning programs and were seen in-the-field in 2014. 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 65 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 65 malicious Mac apps represent a substantial part of all in-the-field Mac malware from the first half of 2014.

The number of malicious programs that can currently attack Mac OS X Mavericks is very 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 14<sup>th</sup> July 2014. 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.

There was also a false-positives test, in which 100 common, safe Mac programs were obtained from a popular download site and scanned by the antivirus program.

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 500 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. With the exception of Intego, all the programs detected all the Windows malware samples.

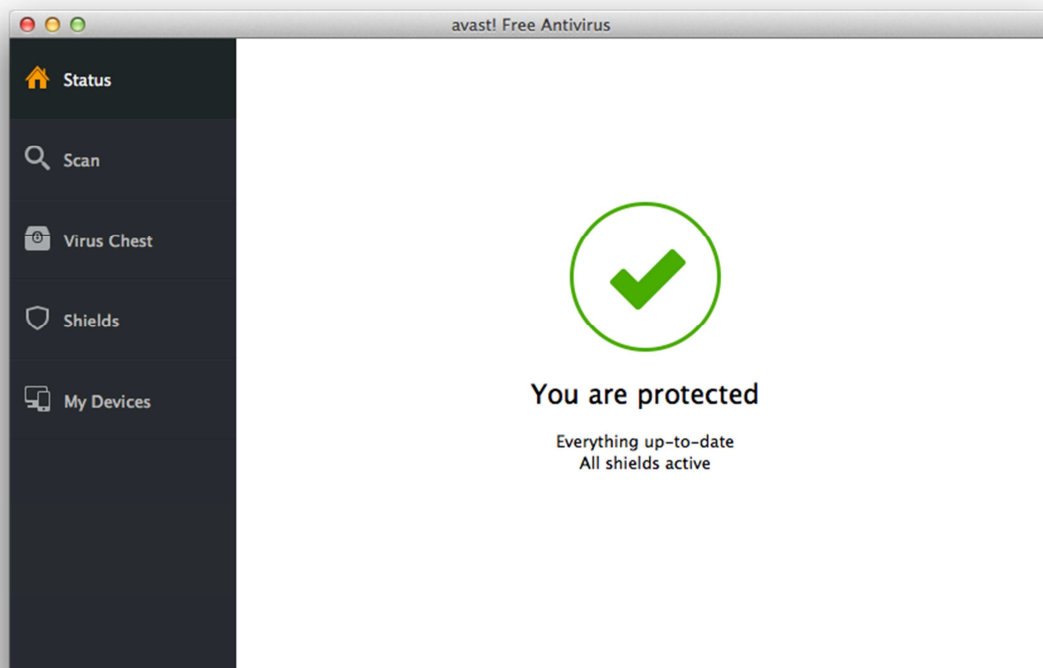
	Mac Malware Protection (65 recent samples)	Windows Malware Detection (500 most-prevalent samples)	False Alarms (100 popular Mac apps)
<b>avast! Free Antivirus for Mac</b>	<b>100%</b>	100%	0
<b>AVIRA Free Antivirus for Mac</b>	<b>91%</b>	100%	0
<b>Bitdefender Antivirus for Mac</b>	<b>98%</b>	100%	0
<b>ESET Cyber Security Pro</b>	<b>100%</b>	100%	0
<b>Intego Mac Premium Bundle</b>	<b>100%</b>	49%	0
<b>Kaspersky Internet Security for Mac</b>	<b>97%</b>	100%	0
<b>Kromtech MacKeeper</b>	<b>80%</b>	100%	0
<b>Sophos Anti-Virus for Mac</b>	<b>100%</b>	100%	0

The test was conducted on the 14<sup>th</sup> July 2014. All participating vendors have by now updated their definitions so that they recognise all the Mac 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/>

## avast! Free Antivirus for Mac



### Additional features

avast! Free Antivirus for Mac includes phishing protection. There is also a feature called My Devices, which describes itself thus: “avast! Account enables you to find or remotely control your phone or tablet and manage all of your avast! protected devices in one place.”

### Installation

The installation process is very simple, with the only option being to install Google Chrome as an additional browser.

The program can be uninstalled using the Uninstall avast! Item in the avast! menu.

### Main window

The main program window is dominated by a single large white pane which displays the current security status. A smaller left-hand pane serves as a menu, with the items Status, Scan, Virus Chest (=quarantine), Shields (=logs), and My Devices. As the product is free, subscription information is not applicable. The Shields item displays information about threats encountered by the

File System/Mail/Web Shields, but does not provide any configuration options. Once a scan has been run, an additional menu item, Reports, appears between Scan and Virus Chest. It provides logs of scans run.

The main program window is in our opinion very clean and uncluttered. However, we feel that some important functions, such as Update and Help, could be added to the left-hand panel to make them more accessible. The use of the term “Shields” to describe what is actually the Logs feature strikes us as confusing; we would expect to find the configuration options for the protection components here.

### Mac menu bar

avast! Free Antivirus adds its own icon to the Mac System Tray, which can be used to open the program window. It also adds four menus to the menu bar: avast! (update, uninstall, settings), Edit, Window, Help.

## Finder context menu

avast! adds a scan entry to the Finder context menu, so that drives, folders and files can be scanned by right-clicking on them.

## Maintenance

Malware signatures can be updated using the "Update virus database" item in the avast! menu. If any of the shields (File System, Mail, Web) is disabled, the status display changes to warn the user:



The text at the bottom indicates what the problem is – in the case above, it shows that the File System Shield is inactive.

Whilst we find the status display warning to be clear and informative, we note that there is no "Fix-All" button provided to rectify the problem, or any instructions as to what to do. An obvious course of action would be to click on the Shields menu item just to the left of the warning, but this does not allow any configuration changes. To solve the problem, the user must go to Preferences in the avast! menu in the menu bar. We feel that this would not be obvious to non-expert users, and suggest that a Fix-All button would be a big improvement.

## Non-administrator access

When logged on with a non-administrator account, a user cannot deactivate any protection components, unless administrator credentials are entered.

This is as it should be, in our opinion.

## Scanning

The Scan item in the left-hand menu panel provides the options Full Scan, Removable Volumes Scan, and Custom Scan. The latter allows particular folders or files to be selected for scanning. We could not find a quick scan or means of scheduling a scan.

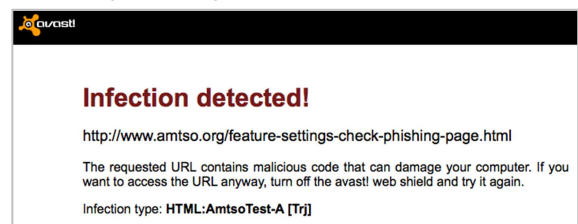
We feel that a quick scan and a scheduled scan would be useful additions to the program.

## Settings, quarantine and logs

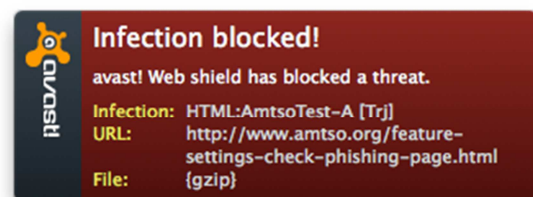
Program configuration options are available from the Preferences item in the avast! menu. Quarantine is found by clicking Virus Chest in the left-hand menu panel of the main window, and the logs can be seen by clicking the Shields item in the same panel.

## Malware and phishing alerts

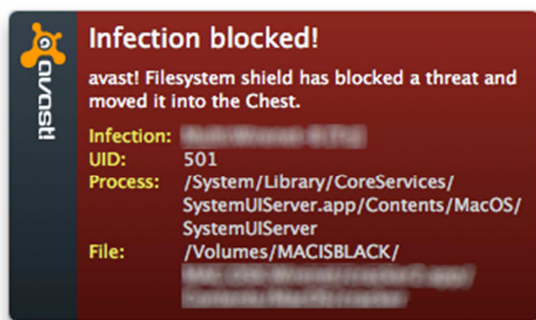
avast! Free Antivirus for Mac recognises the AMTSO phishing test page and displays the following warning in the browser:



Additionally, a pop-up is shown in a corner of the screen:



This persists until the user clicks on it. Similar warnings – both in the browser and pop-up – are shown if the EICAR test file is downloaded. A pop-up alert is also shown when the real-time protection detects malware on a flash drive:



Again, this persists until the user clicks on it. When a flash drive is scanned, malware found is displayed in a list, with options to quarantine (“Chest”) or delete the items:

Removable Volumes Scan		
Scanned files: 3029   Items: 3183   Infections: 261   Unable to scan: 0		
Scanned paths: /Volumes/MACISBLACK		
Scan started: 22 July 2014 12:07:37		
Scan duration: 1 min 21 s		
<input checked="" type="checkbox"/> PATH	INFECTION DETAILS	STATUS
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld	Rootkit-Worms-8 (Fig)	
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
<input checked="" type="checkbox"/> /Volumes/MACISBLACK/.../Contents/.../dyld		
		<input checked="" type="checkbox"/> Chest <input checked="" type="checkbox"/> Delete

We found Avast’s phishing and malware alerts to be very good. The pop-up messages make clear that the threat has been blocked, and provide useful information for advanced users, such as the URL or file path. Not everyone will like the fact that the pop-up alerts persist until clicked, but they can be set to a shorter time or disabled altogether in the program’s preferences. We feel that it is better to have a persistent message than one which comes and goes too quickly to read.

### Malware protection test

Mac malware detected: 100%

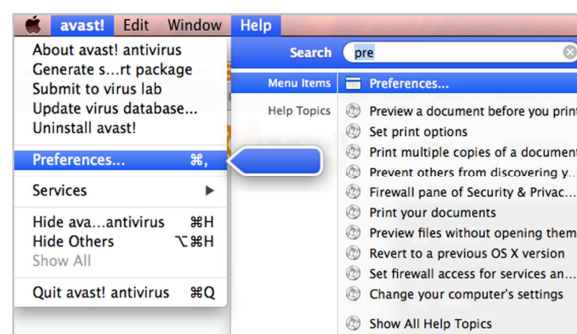
False positives: 0

Windows malware detected: 100%

### Help

The only help function available directly from the program itself is the search box in the Help menu. This uses the OS X menu search

feature, which shows the user where to find the search item in the menus:



The support section of the avast! website (which has to be accessed manually) has a support section for avast! Free Antivirus for Mac. However, at the time of writing (July 2014), all the instructions here related to the previous version of the program, 8.x. The interface of this version is clearly significantly different to the current one, meaning that most of the help topics are irrelevant.

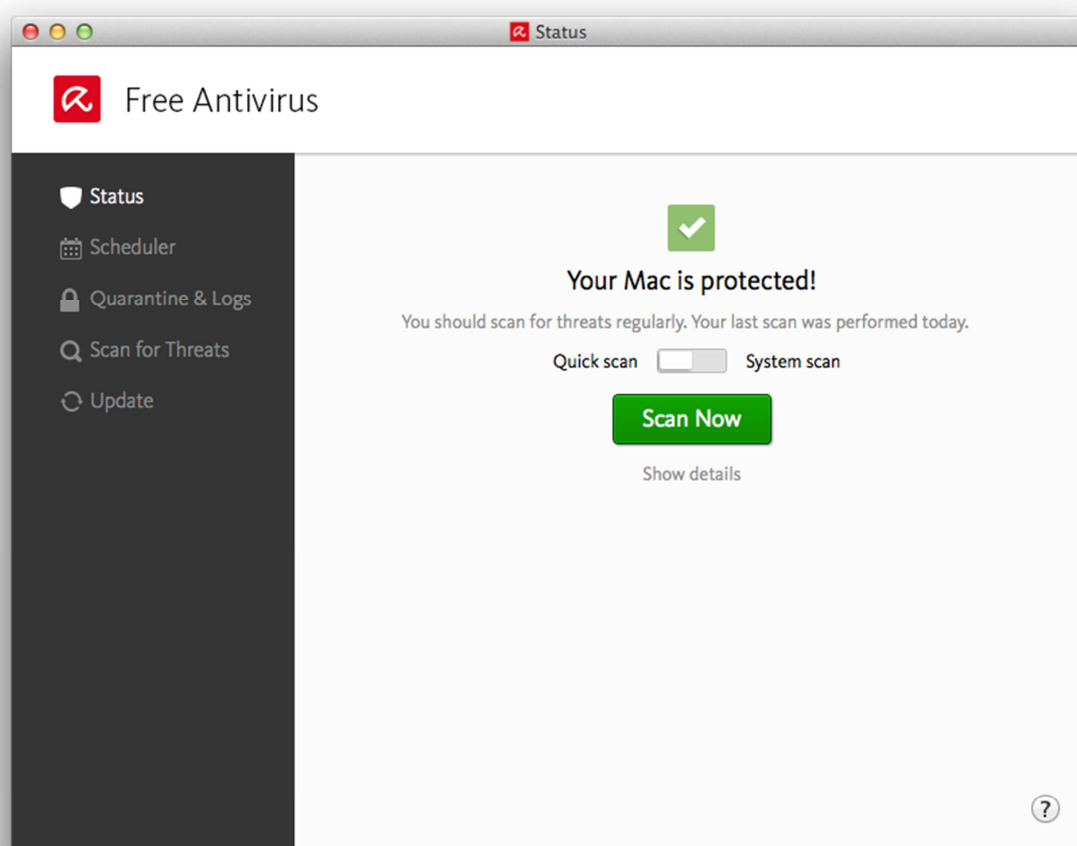
We can only describe Avast’s current help features as being non-existent. Although there is a forum, we do not regard this as an acceptable help service on its own, as it is very much the luck of the draw as to whether there is a contributor who is willing and able to answer a user’s question. Although the program is essentially simple and easy to navigate, we suggest that a manual or support pages applicable to the current version would be very valuable for non-expert users.

### Verdict

avast! Free Antivirus for Mac identified 100% of samples in both Mac malware and Windows malware tests, and has a largely very straightforward program interface, albeit with the odd quirk.

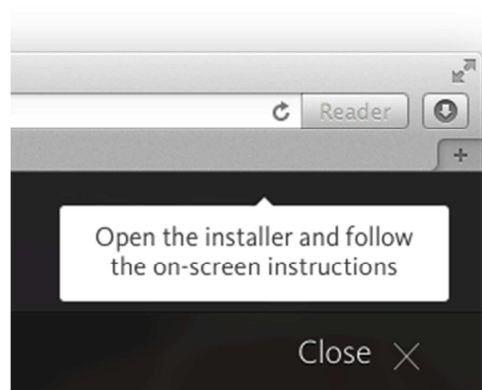
The program interface is very clean, although we would suggest that some improvements such as a Fix-All button. We could not find any help features relevant to the current version, and hope that the manufacturers will release updated instructions soon.

## Avira Free Antivirus for Mac



### Installation

We note that the Avira website provides a hint for non-expert users as to what to do when the download is complete:

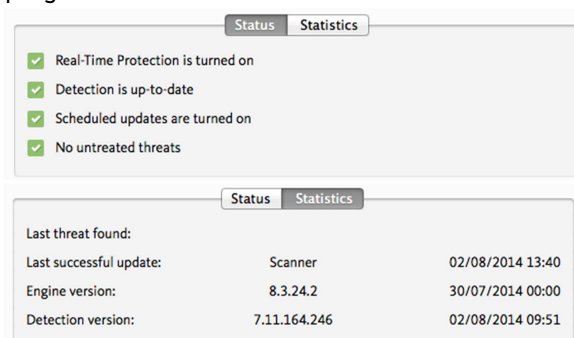


Installation completes with just a few clicks, the only option is which hard disk to install the software to. The program can be uninstalled by dragging the Avira icon in the Applications folder to the Trash. This is described in the online help. There is also an

Avira-Uninstall program in Applications\Utilities.

### Main window

Status, scans, update, quarantine and logs are all accessible from the home page. As the product is free, subscription information is not applicable. The “Show Details” link below the Scan button displays a panel with more detailed information in the lower part of the window. This can display component status or program statistics:





We feel this is a very effective way of making the program suitable for both expert and non-expert users.

### Mac menu bar

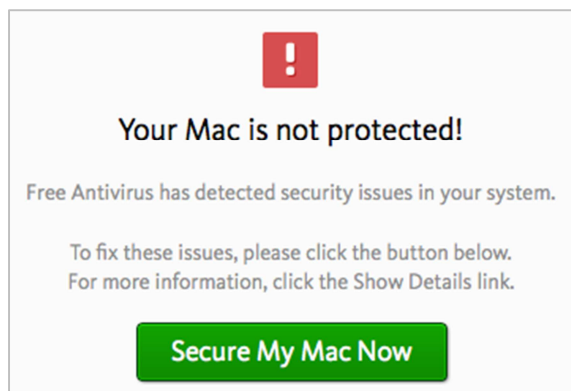
Avira Free Antivirus installs a System Tray icon from which the main program window, preferences, scans and updates can be accessed. There is also an item for disabling the real-time protection. The Mac menu bar is used to display an Avira menu and Help menu.

### Finder context menu

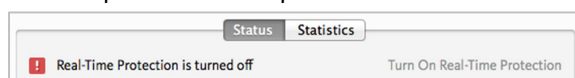
There is no addition to the right-click menu.

### Maintenance

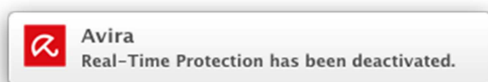
Signatures can be updated from the Update link in the left-hand panel of the window. If the real-time protection is disabled, the status display changes to show this, and provides a big "Secure My Mac Now" button to correct this:



If the details section is displayed, there is an additional warning, and the user can see exactly what the problem is. A link to turn on the component is also provided:



As well as the alerts in the program window, a pop-up message is displayed for a few seconds:



Finally, Avira's system tray icon changes from an open umbrella to a closed one.

We feel that Avira Free Antivirus for Mac warns very clearly in the event that protection is disabled, and makes it very easy to rectify the situation.

### Non-administrator access

In order to disable protection, administrator credentials must be entered, regardless of the account with which the user is currently logged on. Protection can be re-enabled from any account without having to enter an admin password.

This is as it should be, and we find the latter point particularly sensible.

### Scanning

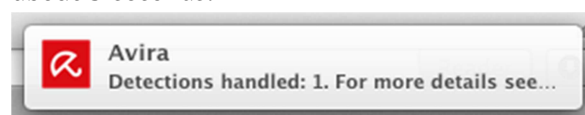
Quick and full scans can be run directly from the home page of the program. The "Scan for Threats" link in the left-hand column additionally provides a custom scan, while the Scheduler link in the same place allows a scheduled scan to be set.

### Settings, quarantine and logs

Quarantine and logs share a link on the left-hand side of the program window, while settings can be accessed from the Avira System Tray icon or Avira menu.

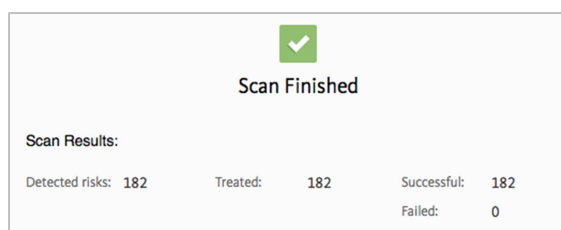
### Malware and phishing alerts

The product does not include phishing protection, so the AMTSO phishing test page is not blocked. When the EICAR test file is downloaded, the following alert is shown for about 5 seconds:



An identical alert is shown when malware on a flash drive is discovered by real-time protection. When a flash drive scan is run, a simple summary of results is shown in the main pane of the window, with no user action required:





The pop-up alert seems rather uninformative to us; we suggest “Malware deleted” would be clearer. In any event, the alert disappears so quickly that most users will not have time to read it. However, with regard to the scan, quarantining all items detected as malware strikes us as ideal for inexperienced users, as there are no decisions to be made and no chance of making a mistake. Expert users can retrieve individual files from quarantine if necessary.

### Malware protection test

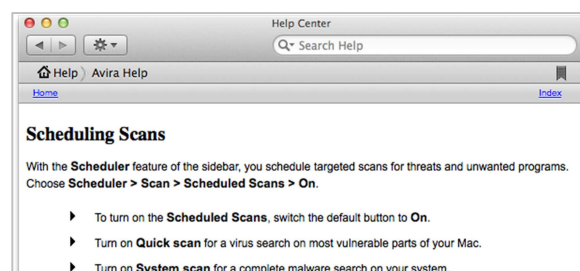
Mac malware detected: 91%

False positives: 0

Windows malware detected: 100%

### Help

Clicking on the question-mark symbol in the bottom right-hand corner of the program window opens Avira’s local help service. This is context-sensitive, that is to say, the help page that opens relates to the page of the program window currently being viewed. For example, if the user clicks on Scheduler in the left-hand column of the window, and then on the question-mark button, the Help window will open the article on scheduling scans:



Clicking on “Avira Help” in the Help menu opens the start page of the local help, which has a prominent link to the Avira Help Center, its online knowledge base. This could be described as an online manual, covering installation, configuration and use of the program. The start page is an index of the various topics; clicking on a topic takes the user directly to the relevant explanation.

We found Avira’s local and online help services to be easily accessible, with clear and straightforward instructions.

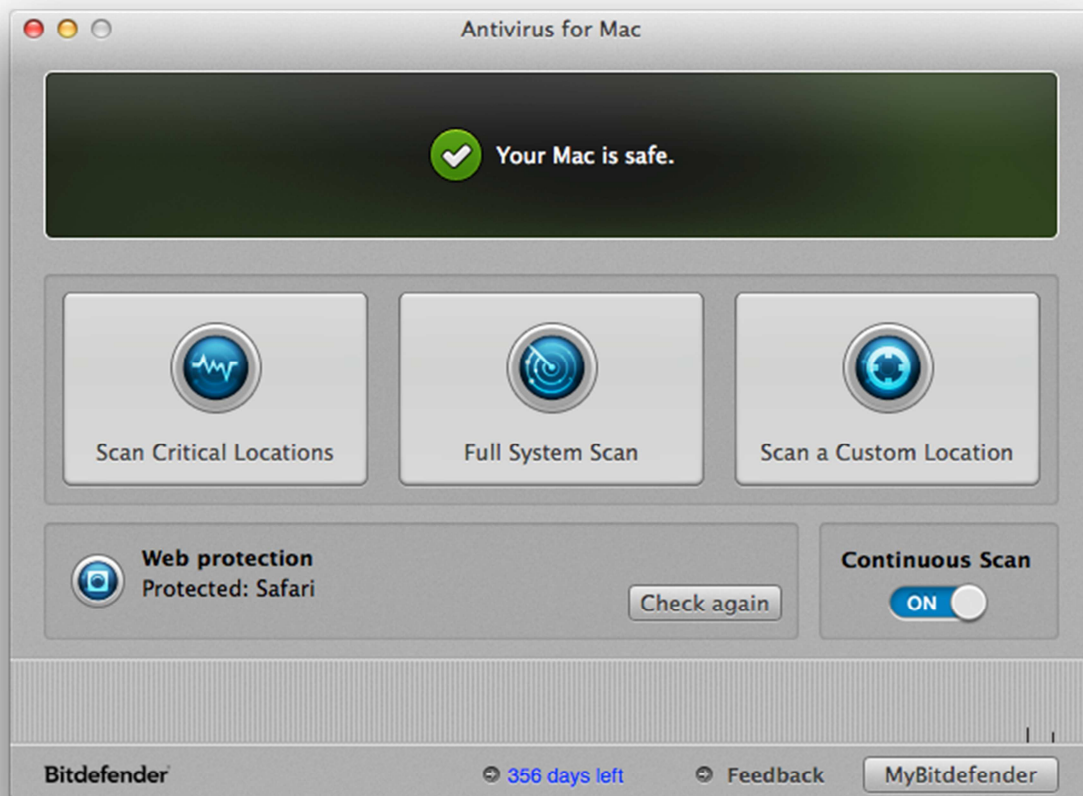
### Verdict

Avira Free Antivirus for Mac combines good malware protection with a very well-designed interface.

The design of the program is clean and simple, and provides easy access to all the essentials. We particularly liked the “Show details” link in the main window, and the fact that admin credentials are required to switch protection off, but not to switch it on.

Avira’s detection score of 91% of Mac malware samples is good. It had no false positives, and recognised all of our Windows malware samples.

## Bitdefender Antivirus for Mac



### Additional features

Web filter, phishing protection for Safari, Chrome and Firefox.

### Installation

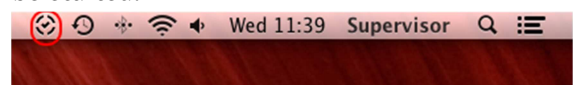
The setup wizard displays a Read Me file, which includes system requirements, support contact information, and instructions for testing the program with the EICAR test file. Installation takes only a few further clicks, with the only option being which hard disk to install the program on. When the main program window is opened, it displays a link from which the web-protection add-on for Safari can be installed. The program can be uninstalled by running the DMG installer file again, which displays a link to the uninstaller file; this is explained in the program's local help file.

### Main window

Status is shown in the top pane of the window. Three buttons below start different scans: Full, Custom and Critical Locations. Subscription information is shown in the form of number of days remaining, and can be found at the bottom of the window. Settings, Help and Update are not shown in the main window but can be found in the menus.

### Mac menu bar

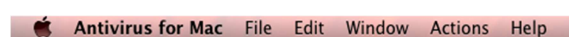
Bitdefender Antivirus for Mac displays a SystemTray icon from which the program can be started:



We did not recognise the icon used as being anything to do with Bitdefender, and wonder why the "B" graphic was not used.

The vendor informs us that they are planning to optimise the icon in order to make it more recognisable.

Bitdefender shows the following menus in the Mac menu bar:



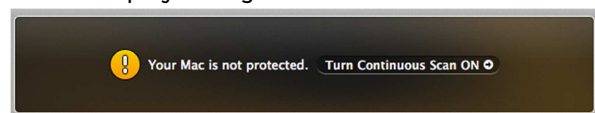
The main Antivirus for Mac menu contains the Preferences item, whilst the Actions menu allows scans and updates to be started.

### Finder context menu

There is no addition to the right-click menu. Bitdefender inform us that this is in keeping with Mac OS X, which does not use context menus as extensively as Windows.

### Maintenance

If the real-time protection is turned off, the status display changes to warn of this:



The button to the right of the warning can be used to reactivate Continuous Scan (=real-time protection), as can the dedicated on/off button in the lower right-hand corner of the window. Signatures can be manually updated from the Actions menu, in addition to the normal automatic update.

### Non-administrator access

When logged on with a non-administrator account, the user cannot deactivate protection without entering administrator credentials.

This is as it should be, in our opinion.

### Scanning

Quick, Full and Custom scans can be run directly from the main window, using the big buttons below the status display. The program does not include a scheduler, so scheduled scans cannot be run.

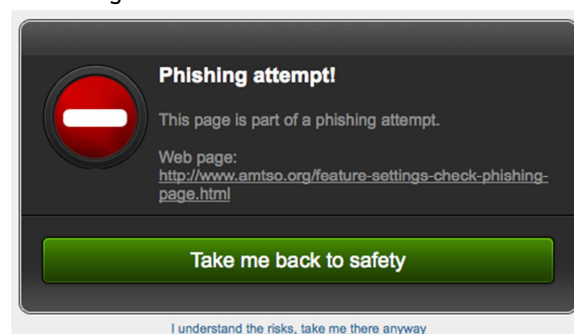
We feel a scan scheduler would be a useful addition.

### Settings, quarantine and logs

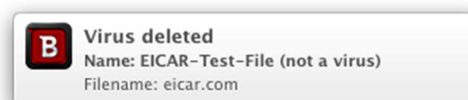
Preferences and History (=logs) can be found in the Antivirus for Mac menu, while quarantine is located in the Actions menu.

### Malware and phishing alerts

Bitdefender Antivirus for Mac recognises the AMTSO phishing test page and displays the following alert in the browser:



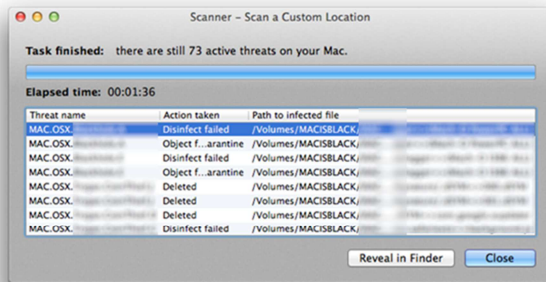
When the EICAR test file is downloaded, the following pop-up alert is shown for about 4 seconds:



When we copied Mac malware samples from a flash drive to the local hard disk, Bitdefender displayed a similar alert to the one above.

We feel that the malware alerts disappear too quickly for most people to read, and that they should be shown for longer. Bitdefender tell us that they currently use the OS X notifications system, so messages are displayed for the standard time; they are looking into improving this.

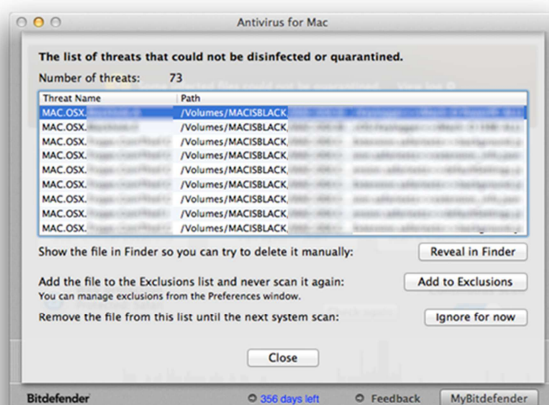
After we had scanned a flash drive containing Mac malware, Bitdefender displayed the following dialog box:



Please note the summary, "There are still 73 active threats on your Mac", and that the dialog offers no means of deleting or quarantining these. After the computer was restarted, the status display in the main window showed the following alert:



Clicking on "View log" opened the following window:



The warning in the program window persisted after a restart of the computer, with the log showing the same as above.

It would appear that Bitdefender Antivirus for Mac was unable to remove many of the malware samples it detected on the flash drive. This surprises us, as no attempt had been made to run any of the malicious files, hence they could not be regarded as active. We feel many users may be alarmed by an antivirus program which detects malware but cannot remove it, even though it is inactive.

Bitdefender have let us know that because of the way OS X works, deleting a file without deleting all references to it in the system (made by the malware itself) may cause the OS to hang. They are working on a means of automatic cleaning.

## Malware protection test

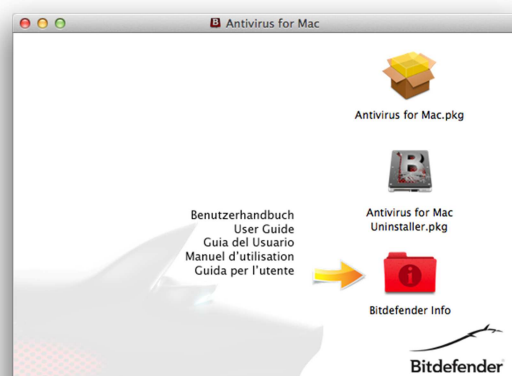
Mac malware detected: 98%

False positives: 0

Windows malware detected: 100%

## Help

Bitdefender Antivirus for Mac has what might be called a quick-start guide which uses the Mac help system, and can be launched from the Help menu. This covers important everyday tasks and FAQs. The support pages of the Bitdefender website also provide instructions for common tasks, illustrated with screenshots where applicable. Additionally, there is a 50-page manual in PDF form, covering all aspects of installation, configuration and use. It has been bookmarked and has a clickable contents page, and is well illustrated with screenshots. It can be accessed from the initial page of the installer:



The manual has been produced to a very high standard, in our opinion. We also like the fact that it can be accessed from the installer file, so there is no need to search the vendor's website. Overall, we would describe the product's help facilities as excellent.

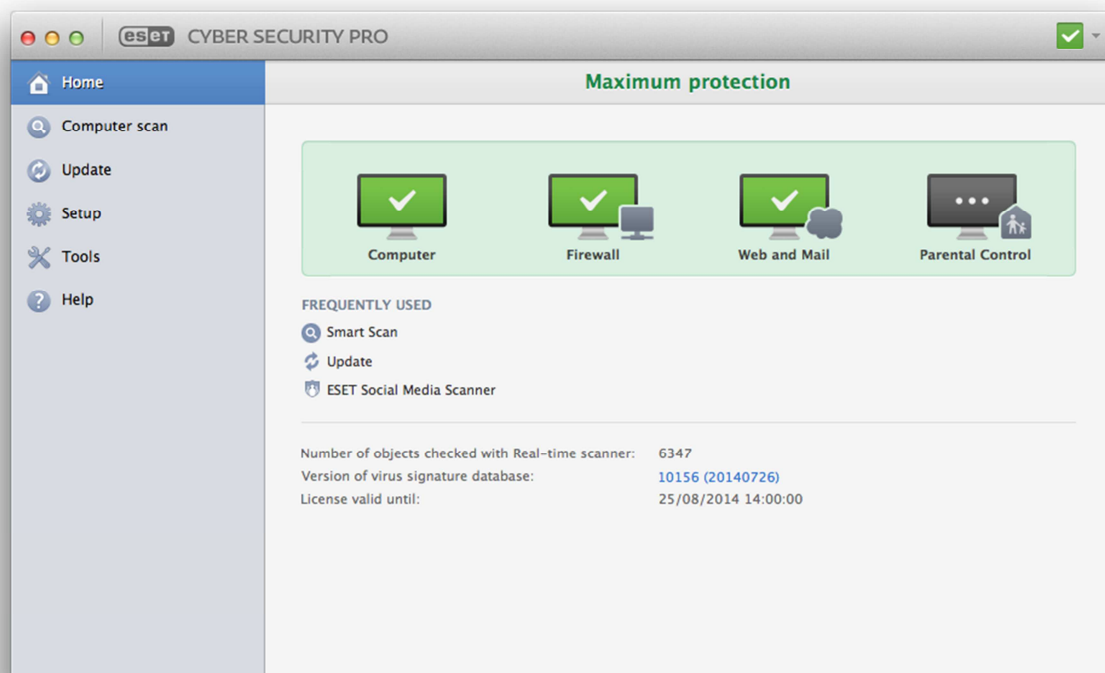
## Verdict

Bitdefender Antivirus for Mac combines very good malware detection with a largely very straightforward interface, but may have difficulty removing the malware detected.

The program interface is largely very well designed and makes important information and tasks easy to access. Help facilities are excellent. Our one concern is that the program appears to be unable to remove many inactive malware samples from a flash drive.

Bitdefender achieved a very good score in our Mac malware test, with no false positives. Its detection of Windows malware was flawless.

## ESET Cyber Security Pro



### Additional features

Phishing protection, parental control, firewall

### Installation

At the start of the installation process, the setup wizard displays the system requirements. Before proceeding, it checks for a newer version of the software. Options are joining Live Grid (malware-information sharing and early-warning scheme); detection of potentially unwanted applications (which we selected); the hard drive to install to. As the product contains a firewall, the user is then prompted to define the current network as home, work or public:



The software can be uninstalled by rerunning the setup process from the original media, or locating the uninstaller in Finder. Both methods are described in the User Guide.

### Main window

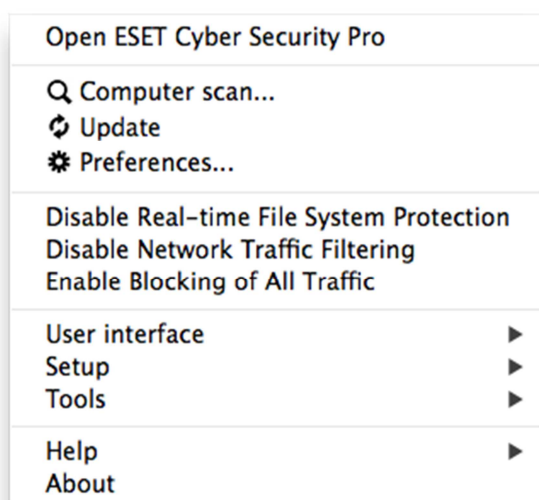
The main pane of the program window includes a status display, links to update and Smart Scan, and licence information. The left-hand panel displays links to further scan options, settings and help.

We feel ESET's main program window is very clear, and makes all essential functions and information easy to access.

### Mac menu bar

By default, ESET Cyber Security Pro does not display any menus in the Mac menu bar (all the controls can be found within the program window itself). However, menus can be activated in the settings. There is a System Tray icon, which can be used to open the menu shown below:



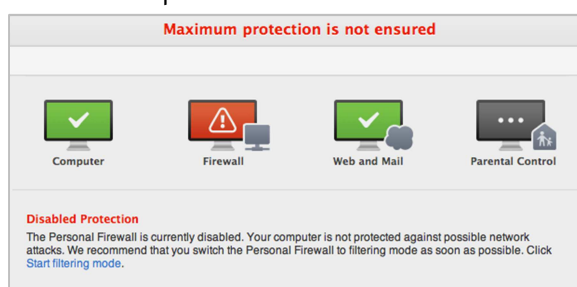


### Finder context menu

In the standard configuration, there is no addition to the right-click menu, but this can be activated via the settings if desired.

### Maintenance

Signatures can be updated from the home page, the menu panel on the left of the window, or from the System Tray icon. If either the firewall or real-time protection is disabled, the status display changes to show this, and a link is provided to reactivate the disabled component:



The alert strikes us as very clear, and makes it very easy to rectify the problem.

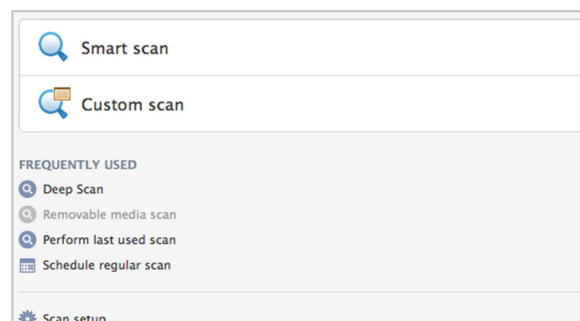
### Non-administrator access

If the user logs on with a non-administrator account, the components settings are greyed out, meaning that protection cannot be disabled. The System Tray icon's menu is also modified, so that options to disable protection components are removed.

This is ideal, from our point of view.

### Scanning

Clicking Computer Scan in the left-hand panel of the window opens a range of scanning options, including quick, full, custom and scheduled scans:



### Settings, quarantine and logs

Settings are accessed by clicking Setup in the left-hand panel of the window; the Tools item just below this provides access to quarantine and logs.

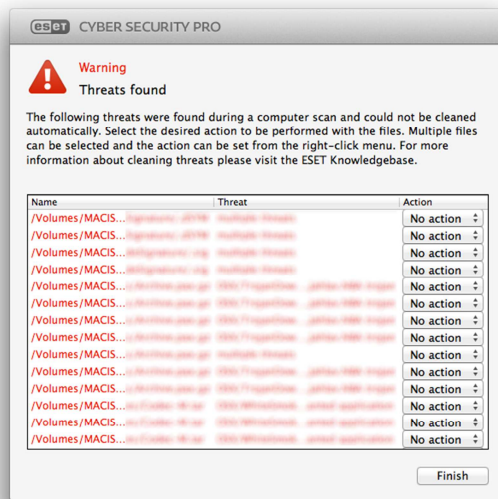
### Malware and phishing alerts

If the user attempts to visit the AMTSO phishing test page, the page does not open, and an ESET alert is displayed:



Similar alerts are shown when the EICAR test file is downloaded or local malware is detected by the real-time protection. In both cases, the alert states that the malware has been quarantined.

When a flash drive containing malware is scanned, the results are presented thus:



We feel the pop-up alerts make reasonably clear that the malware has been dealt with, although it would not hurt to emphasise the relevant word (“blocked” or “quarantined”). We understand that ESET intend to do precisely this in the next version. The note about selecting multiple files by right-clicking strikes us as a usable alternative to a “Select All” button.

### Malware protection test

Mac malware detected: 100%

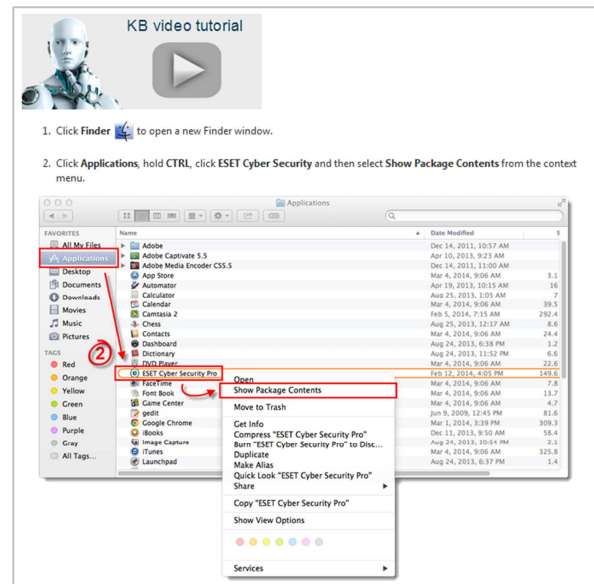
False positives: 0

Windows malware: 100%

### Help

The download page for the software also includes links to two manuals in PDF form, the Quick Start Guide and the User Guide. The former is brief (12 pages), but covers the essentials of installation and maintenance. The User Guide is more comprehensive at 25 pages, but is easy to navigate using bookmarks and a clickable contents page.

Both documents have been produced to a very high standard and are illustrated with screenshots. Additionally, there is an online knowledge base on the ESET website. A search for “uninstall” found comprehensive instructions with annotated screenshots and a video:



We would describe ESET’s help facilities as outstanding.

### Verdict

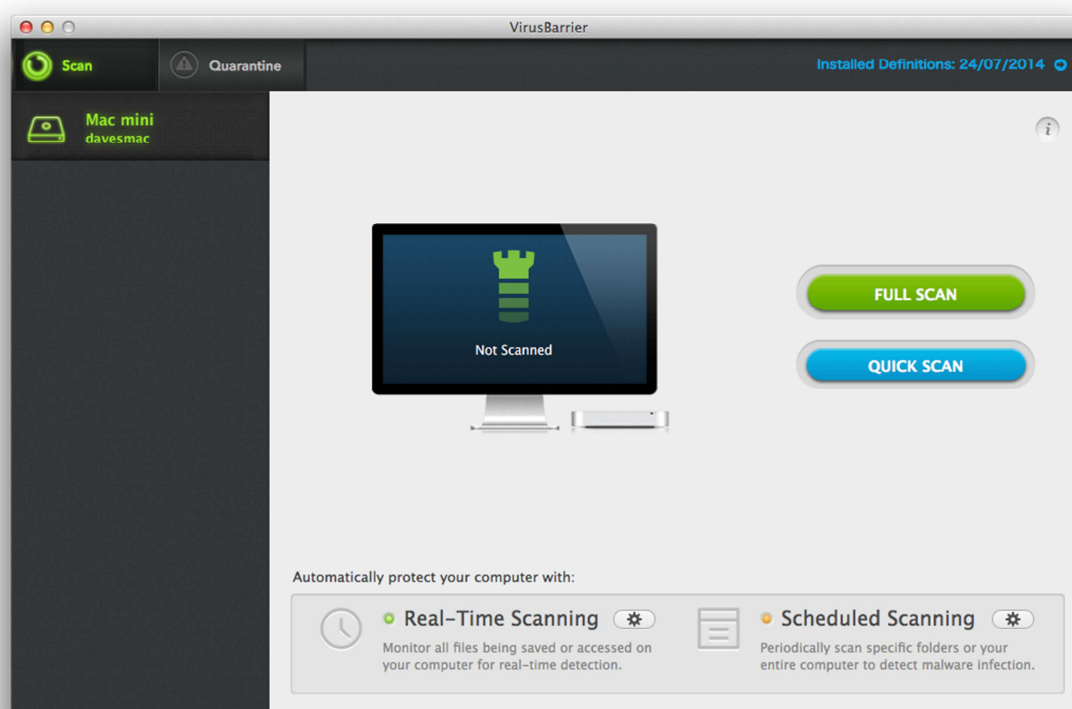
ESET Cyber Security Pro provides outstanding protection against malware with a well-designed user interface.

The main program window makes essential functions and information easily accessible and alerts are sensible. The help facilities are exemplary.

ESET produced a perfect score in our malware tests, identifying all samples of both Mac and Windows malware.



## Intego Mac Premium Bundle X8



### Additional features

In addition to antivirus, the Intego Mac Premium Bundle X8 includes a firewall, parental controls, system optimisation, and backup.

### Note on the nature of the suite

The Mac Premium Bundle is a software package that includes all the programs/components/functions that Intego make for home users of Mac OS X: antivirus; firewall; parental controls; system optimisation; backup.

The antivirus (VirusBarrier) and firewall (NetBarrier) components, along with the integrated update function (NetUpdate) can be purchased together as the Internet Security X8 suite. Both parental controls (Family Protector) and system optimisation (Mac Washing Machine) are available both as standalone products, and in combination with the security features (Family Protector Secure X8 and Mac Washing Machine Secure X8, respectively). The Mac Premium Bundle also includes a backup feature, which is not

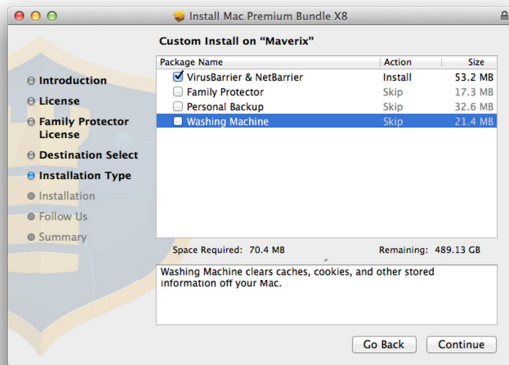
available as a standalone program or with any of the other suites.

### Features covered in this review

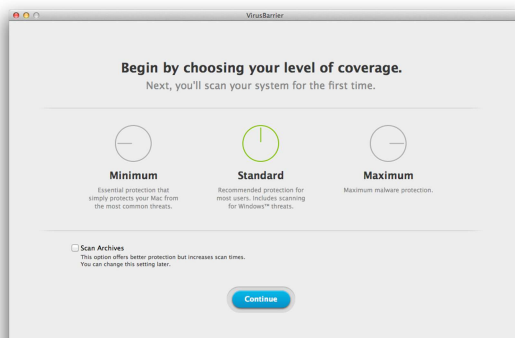
As this review only covers protection against malware, we have not considered Mac Premium Bundle's parental controls, system optimisation or backup features. We have made mention of the firewall, however, as there is no option to install the antivirus component without it, and users will be confronted by it after setup has completed, and when updating the virus signatures (please see "Note on the firewall component" below).

### Installation

Installer file Installation process allows the user to decide which components to install:

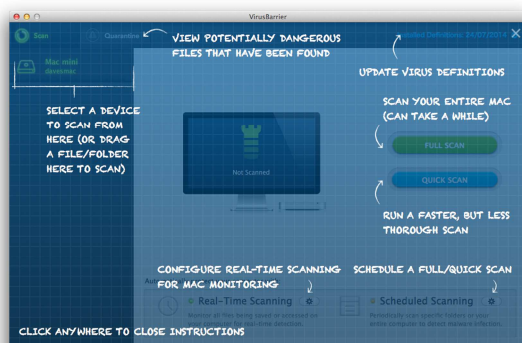


A restart is required after the setup process. When the suite is started for the first time, the licence key has to be entered, and a protection level chosen:



Whilst there is a clear recommendation to choose Standard, which should help non-expert users, we feel it would be helpful to say a little more about the advantages and disadvantages of each option, and provide a recommendation as to whether to scan archives.

When the protection level has been chosen, the program window opens covered by a mask, which is used to label the functions in the program window:

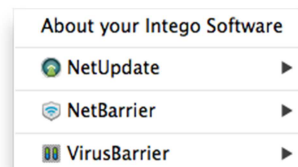


We feel this is a very simple but effective way of explaining the program's controls.

The software can be uninstalled by deauthorizing from the program's main menu in the Mac menu bar, and then downloading and running the latest installer package, which has an Uninstall option. This is described in the online knowledge base.

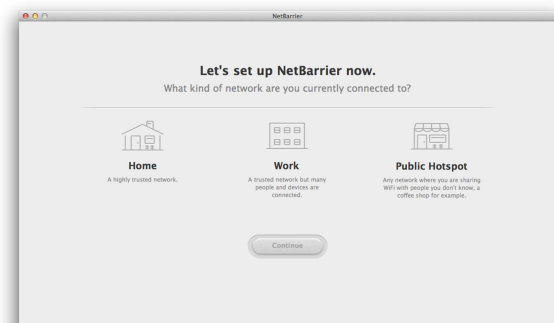
### Note on the program interface

There are three separate program windows, one each for the antivirus component VirusBarrier, its associated update function NetUpdate, and the firewall component NetBarrier. All can be accessed from the Intego icon in the System Tray, which displays the following menu:



### Note on the firewall component

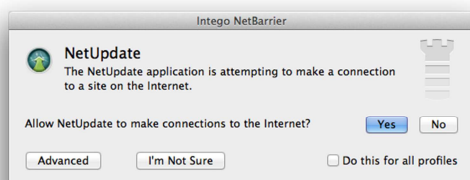
When the computer has been restarted, the firewall component of the suite, NetBarrier, prompts the user to define the current network as Home, Work or Public:



We chose Home, after which access to our Mac's file share was restored, having been blocked during the installation.

We regard the network-type prompt as appropriate (given that the firewall has been installed), and feel that it describes the different network types very clearly and succinctly.

When we attempted to update VirusBarrier (the antivirus component), we were met with the following prompt from NetBarrier, which asked whether to allow access to the Internet for the update process:



We also saw prompts from NetBarrier for its very own processes, that is to say, NetBarrier asks whether NetBarrier should be allowed to access the Internet.

We noted similar Intego firewall prompts in last year's report. At the time, Intego explained that they did not think the program's own processes should be given preferential treatment. We retain the same view that we expressed then, namely that such prompts are counterproductive and confusing for non-expert users. We note that Safari, the web browser integrated into Mac OS X, is immediately recognised by Intego as a safe application, meaning it can access the Internet without any prompt from the firewall. We suggest that Intego should afford its own programs the same privilege.

## Main window

VirusBarrier's main program window provides buttons or links for updating the signatures, accessing quarantine, and running full or quick scans. There are also buttons for configuring real-time protection and scheduled scanning. Both of these have a very subtle status display, in the form of coloured dots. Program preferences can be found in the VirusBarrier menu. Clicking the Help menu |VirusBarrier Help opens the online knowledge base in a browser; additionally, clicking the "i" symbol in the top right-hand corner of the window re-displays the overlay of annotations which was initially shown after installation. We could not find a means of displaying subscription information.

We found Virus Barrier's main window to be clear and well laid-out, but we would like to see an easy means of finding out when the current subscription expires.

## Mac menu bar

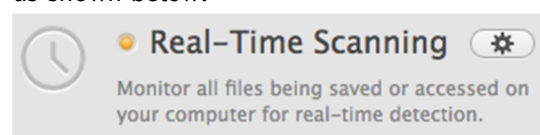
There is an Intego System Tray icon which displays individual sub-menus for each of the three components, as shown in "Note on the program interface" above. There are also six menus, VirusBarrier (About, Preferences, Update, Setup assistant...), File (scans), Edit, View, Window and Help.

## Finder context menu

A "Scan with VirusBarrier" entry is added to Finder's context menu, so individual files, folders and drives can be scanned by right-clicking.

## Maintenance

Signatures can be updated by clicking on the blue update status definition text in the top right-hand corner of the program window, or from the VirusBarrier menu, or the NetUpdate sub-menu, accessible from the System Tray icon. If real-time protection is turned off, the only indication is that the green dot next to the text "Real-Time Scanning" turns orange, as shown below:



We do not feel that this provides adequate warning that real-time protection is disabled, and suggest a much clearer warning should be employed.

## Non-administrator access

When logged on with a standard user account, a user cannot disable real-time protection without entering administrator credentials.

This is as it should be, in our opinion.

## Scanning

Full, quick and scheduled scans can be run using their respective buttons in the main program window. Custom scans are accomplished by dragging a drive, folder or file to the graphic of the Mac in the centre of the window.

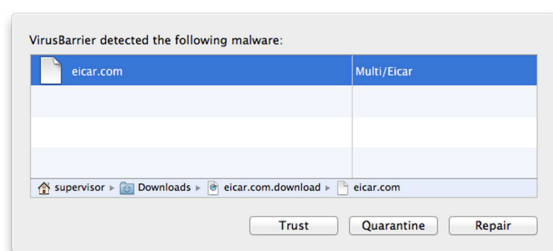
We did not find the custom scan method to be very obvious, and suggest a note underneath the graphic would be helpful.

## Settings, quarantine and logs

Program preferences can be found in the VirusBarrier menu, there is a Quarantine button in the main program window, and logs are located in the Window menu.

## Malware and phishing alerts

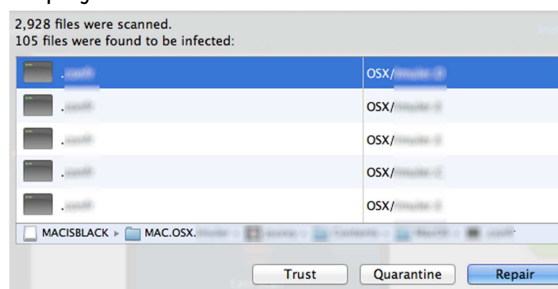
The AMTSO phishing test page is not blocked as the product does not include phishing protection. When the EICAR test file is downloaded, the following alert is shown:



We feel that non-expert users may be confused as to what to do, as there is no recommended action. Making the "Trust" option as obvious and accessible as the other options also strikes us as risky. Finally, we wonder how relevant the "Repair" option actually is. We suggest that making "Quarantine" the default and recommended option, with "Trust" much less obvious and accessible, would be an improvement.

A very similar dialog box was shown when the real-time protection found malware on a flash drive, although the quarantine option was disabled.

When a full scan of a flash drive containing malware is run, the following dialog box is displayed:



We could not see an obvious means of selecting multiple items to apply the action to. Expert Mac users will be aware of the CMD + A keyboard shortcut to select all items, but non-experts would surely appreciate a Select All button. Again we feel the Trust button is too obvious and easily accessible. Finally, we note that quarantining items does not remove them from their original location, which we found confusing.

## Malware protection test

Mac malware detected: 100%

False positives: 0

Windows malware detected: 49%

## Help

The help feature for VirusBarrier comes in the form of a knowledge base and online user manual on Intego's support website. The knowledge base covers frequently asked questions that relate to all Intego products, such as how to install or uninstall the software. The online user manual is specific to VirusBarrier, and covers all aspects of configuration and use of the software.

We found both the knowledge base and manual articles to be simply and clearly explained and very well illustrated with screenshots, some annotated.

## Verdict

Intego VirusBarrier provides outstanding protection against Mac malware, and would be an ideal program for experienced Mac users. The current version does not provide very effective detection of Windows malware, though, and we have also noted a number of areas in the user interface which we feel are not ideal for non-expert users. However, Intego inform us that upcoming releases slated for autumn 2014 will address the user-interface issues and also bring Windows-malware detection up to standard.

## Kaspersky Internet Security for Mac



### Additional features

Phishing protection; web filter; parental control

Kaspersky Lab inform us that the version 15 of the software, due for release in October 2014, will also include their "SafeMoney" feature, the purpose of which is to ensure secure online banking transactions.

### Installation

The installation process is completed with a couple of clicks. The only option is whether to join the Kaspersky Security Network (malware information-sharing scheme). The installer window includes a link for uninstalling the product, and the procedure is described in the online knowledge base.

### Main window

This features a status display, along with buttons for updates (refresh symbol), scans (magnifying glass), licence information (the key symbol), settings and help.

### Mac menu bar

The Mac menu bar menus are Kaspersky Internet Security (updates and preferences), Edit, Protection (scans, updates, switch protection on or off), Window, and Help. There is also a System Tray icon which displays the following menu:



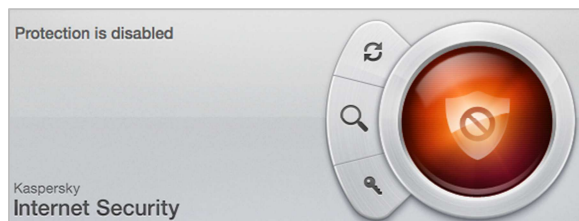
### Finder context menu

A "Virus Scan" entry is added to Finder's context menu, so files, folders and drives can be scanned by right-clicking them.



## Maintenance

Updates can be run by clicking the uppermost of the three symbols to the right of the big button. If real-time protection is turned off, the status display changes accordingly:



Clicking the big red button allows protection to be reactivated.

## Non-administrator access

Users with standard user accounts are not restricted from changing settings, and can switch protection components off without having to enter administrator credentials.

We do not regard this as ideal, but Kaspersky Lab inform us that it will be fixed in the upcoming version 15.

## Scanning

Clicking the scan button in the main program window provides a choice of full, quick or custom scan. Scheduled scans are not available.

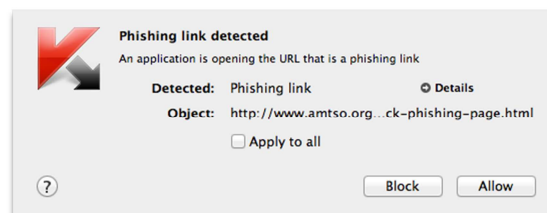
Whilst we would normally regard a scheduled scan as a useful feature, Kaspersky Lab say that they have not included it as they feel that other features in the program, such as a background scan and real-time protection, make it unnecessary.

## Settings, quarantine and logs

The Reports button in the main window provides access to logs and quarantine; settings are available from the Preferences button.

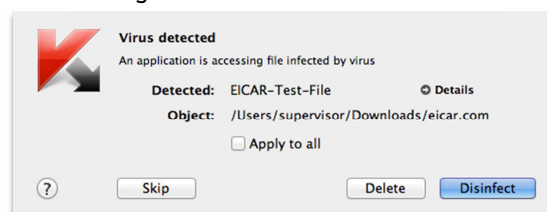
## Malware and phishing alerts

When the user tries to open the AMTSO phishing test page, the following alert is shown:

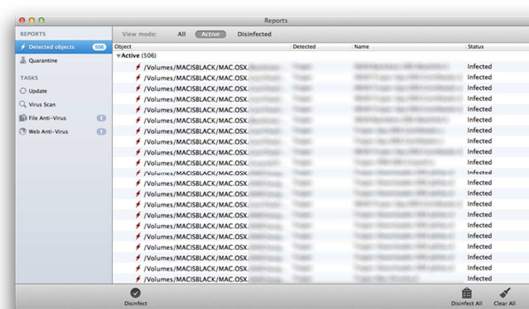


We note that the Allow button is just as big and prominent as the Block button, although we are informed by Kaspersky Lab that this will be changed in an upcoming release.

If the user attempts to download the EICAR test file, a very similar alert to the one above is shown. If the user chooses to allow the download, the local real-time protection detects the file and displays the dialog shown below, with a choice of skipping, deleting or disinfecting the file:



The same dialog is shown when real-time protection discovers malware on a flash drive. When we ran a scan of a flash drive containing malware, Kaspersky Internet Security for Mac displayed the results thus:



We note that if the Clear All button is clicked, an information box appears to explain that this will not treat the malware found, merely clear the display of the scan log. We understand that the release of KIS for Mac 15 will feature an improved dialog with a prominent "Fix All" button.

## Malware protection test

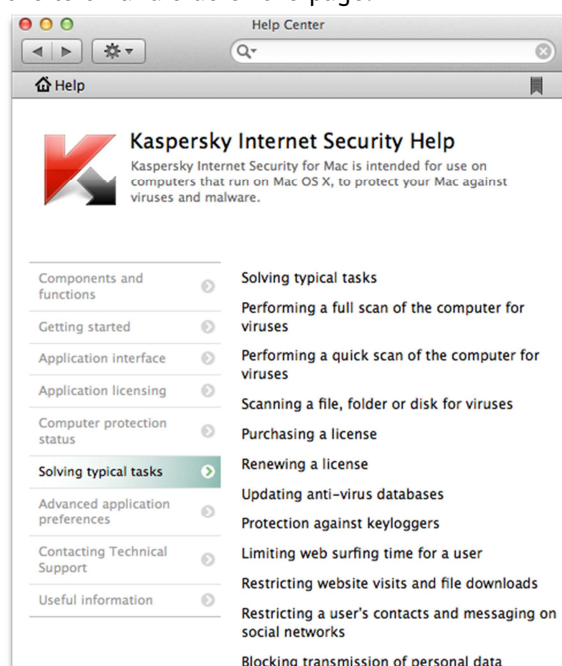
Mac malware detected: 97%

False positives: 0

Windows malware detected: 100%

## Help

Clicking “Kaspersky Internet Security Help” in the Help menu opens the local help service. This provides comprehensive assistance for a wide range of tasks, sorted into categories on the left-hand side of the page:



Additionally, there is a knowledge base on the Kaspersky Lab website. This provides extensive answers to FAQs, well-illustrated with annotated screenshots.

We would describe the help facilities for Kaspersky Internet Security as excellent.

## Verdict

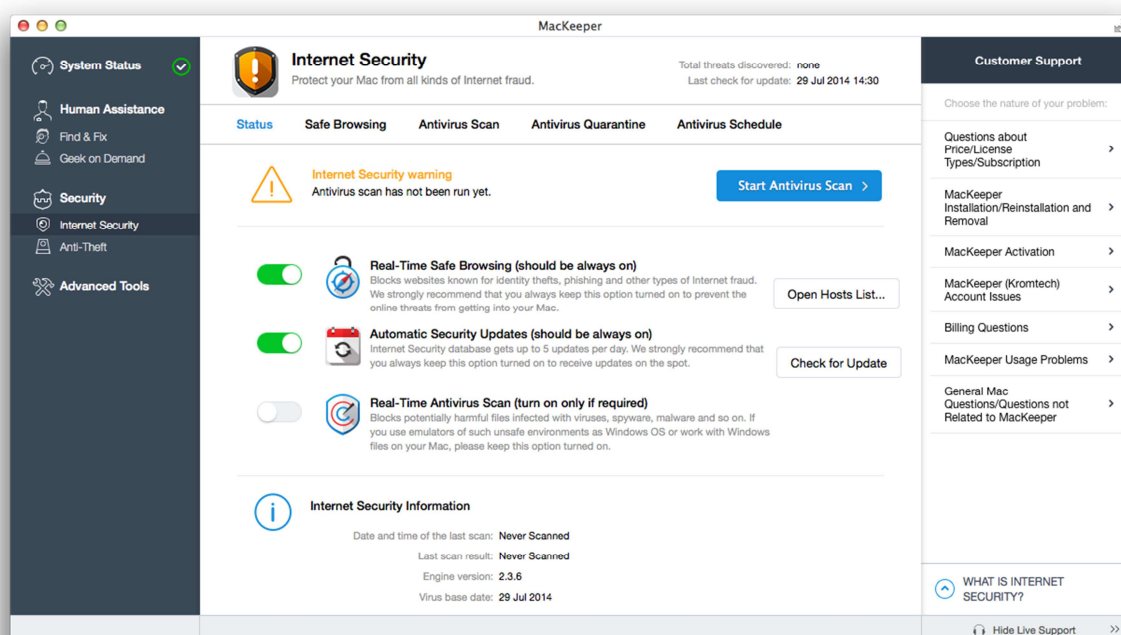
Kaspersky Internet Security combines very good malware protection with a very usable interface.

The program window is well-designed and makes it easy to find the essentials. Malware alerts are largely clear, and further improvements are scheduled for the next release. Help facilities are excellent.

Kaspersky Internet Security for Mac detected 97% of Mac malware in our test, along with all the Windows samples.



## Kromtech MacKeeper



### Additional features

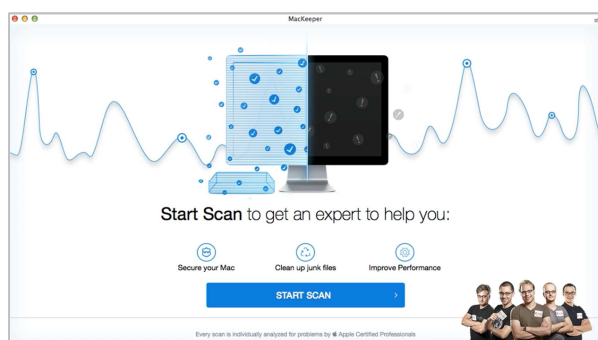
Anti-theft; system optimisation; backup; shredder.

### Installation

The installation process itself is very simple, with the only option being the hard disk to install to. The program can be installed by dragging its icon in Finder/Applications to the Trash.

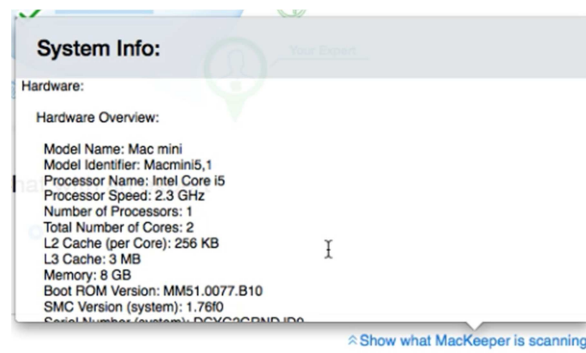
### Starting the program

When the program is first started after installation, the program window requires the user to run a scan; this is the only option available:

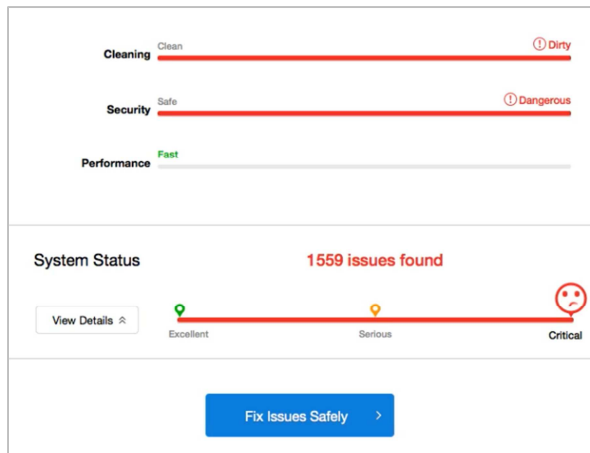


While the scan is running, there is a button entitled "Show what MacKeeper is scanning".

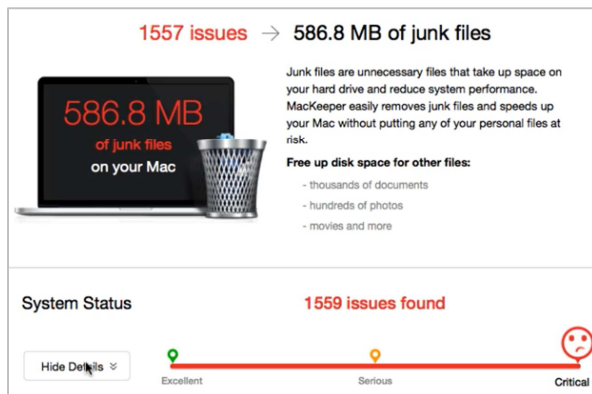
Clicking this displays hardware information about the computer, such as memory and CPU, but nothing about the files or folders being examined:



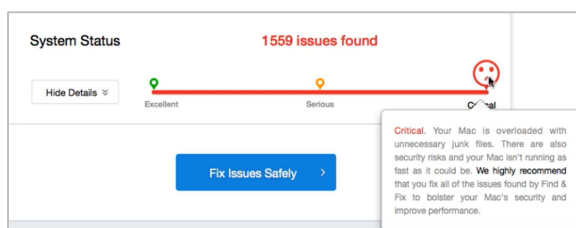
When the scan has completed, the results are displayed. According to the program, our newly-installed Mac was "Dirty" and "Dangerous" but "Fast"; apparently as dirty as is possible, as dangerous as is possible, but also as fast as possible:



The System Status report displayed 1,559 “issues found”, putting it in a “Critical” state<sup>4</sup>, according to the graphic. Clicking on Details displayed a message that there were 586.6 MB of “junk files” on the hard drive, and warned that these could “reduce system performance”, despite the program’s earlier diagnosis of our Mac as being as fast as possible:



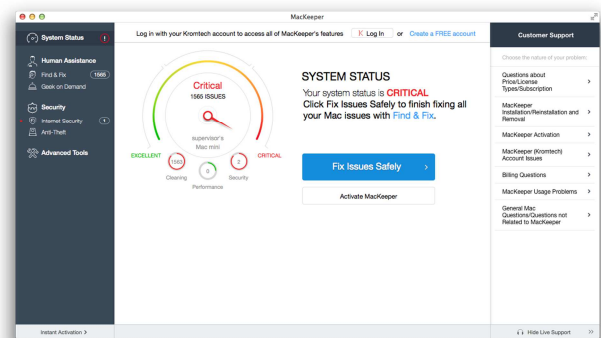
Clicking on the unhappy face representing our Mac’s position at the “Critical” end of the scale produced the following analysis: “Critical. Your Mac is overloaded with unnecessary junk files. There are security risks, and your Mac isn’t running as fast as it could be”.



We note that even after installation of MacKeeper, the hard disk of our Mac still had 488.87 of 499.25 GB free. When we logged on with a non-administrator account as part of the test, we found that we had to run the scan again and sign in again.

We were surprised to see that the computer has to be scanned, and the program activated, for each individual user.

When the scan has completed, the user is urged to activate the product (purchase a licence) in order to fix the problems the program claims to have found:



## Update

Since writing the report, we have tested version 3.1.5 of MacKeeper. In this, the wording on the System Status scale has changed from “Excellent/Serious/Critical” to “Excellent/Aggravated/Serious”. Our Mac, freshly installed once again, was deemed to be in “Serious” condition, i.e. still the worst score possible. There was a slight improvement in the number of problems found: a mere 1,544 instead of 1,559 with the previous version.

Kromtech, the manufacturer, provided us with the following explanation: “MacKeeper detects junk files even on a brand new Mac because most of the Applications are supported by the old PPC architecture which may not comply with the type of processor installed in the computer. Also each application has a huge variety of localizations (languages) that you would probably never use, therefore our software defines the unused languages as junk files, and due to their amount the System

<sup>4</sup> Please see section entitled “Update” below.

*Status may be identified as “Aggravated” or even “Serious”.*

We would suggest that readers consider for themselves the plausibility of the idea that a freshly installed OS X Mavericks system could be “overloaded” and consequently in a “serious condition” (lowest possible score) due to “junk files”, and also the sense in having a graphic that indicates the system is running at maximum speed, combined with text that states that “your Mac isn’t running as fast as it could be”.

### Note on the Internet Security component

This has to be installed separately, although this is done very quickly and easily by clicking the appropriate button in the MacKeeper window.

### Main window

The main program window displays a warning in the event that signatures are out of date or a scan has not been run recently. Full and custom scans can be run from the Antivirus Scan tab, and a scheduled scan set in Antivirus Schedule. Update is available from the Status tab. There is a “lifetime licence” for MacKeeper, so subscription information is not required.

### Mac menu bar

MacKeeper installs a System Tray icon, from which scans can be started, and protection features switched on or off. There are also MacKeeper, Edit, Window and Help menus.

### Finder context menu

There is no addition to the right-click menu.

### Maintenance

Updating signatures can be done from the main Internet Security window or the MacKeeper menu. As the real-time protection is turned off by default, it is perhaps not surprising that there is no warning in this case.

We were surprised to see that real-time malware protection is inactive by default, and only recommended for users who work with Windows files; we would regard it is an essential feature for protecting the computer.

### Non-administrator access

There is no restriction on changing settings using standard-user accounts.

We do not find this ideal, especially for a family computer.

### Scanning

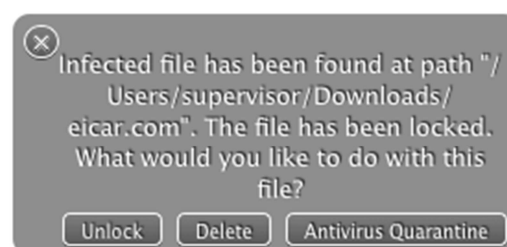
Full and Custom Scans can be run by clicking “Antivirus Scan”, whilst scheduled scans can be set from “Antivirus Schedule”.

### Settings, quarantine and logs

Settings can be changed by clicking the MacKeeper menu, Preferences. There is a tab entitled Antivirus Quarantine at the top of the Internet Security page. We could not find scan logs.

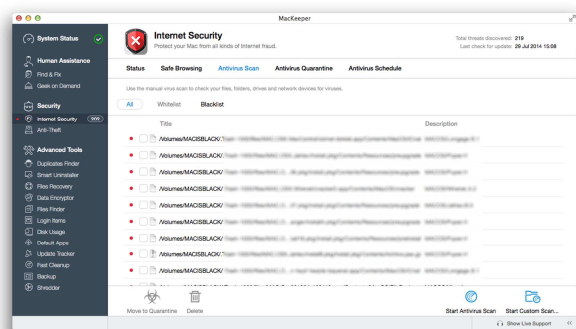
### Malware and phishing alerts

The AMTSO phishing test page is not blocked. When the EICAR test file, is downloaded, the following alert is shown:



We note that the Unlock item is as obvious and easy to click as Delete, and suggest that it should be smaller and less prominent.

A very similar alert is shown when the real-time protection detects malware on a flash drive. When we ran a scan of the flash drive, results were displayed thus:



We could not find a means of selecting all items at once, and so had to tick the box for each item individually.

### Malware protection test

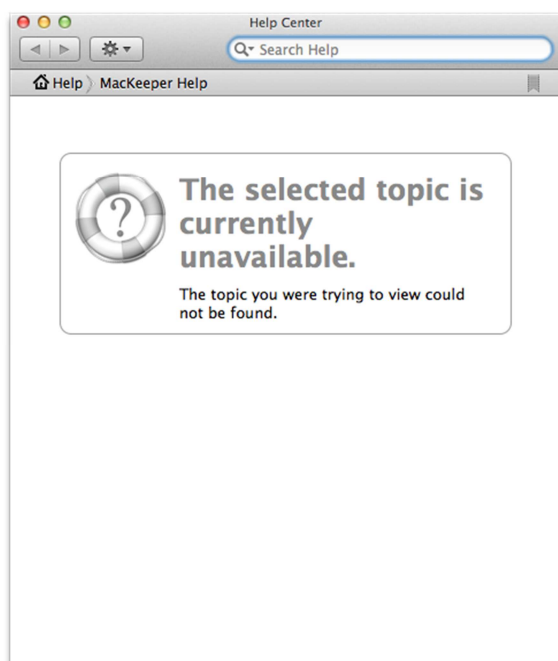
Mac malware detected: 80%<sup>5</sup>

False positives: 0

Windows malware detected: 100%

### Help

At the time of writing (late July 2014), we could not find any help facilities for the current version of MacKeeper. Clicking the Help menu, MacKeeper help opens a local window with no content:



## Verdict

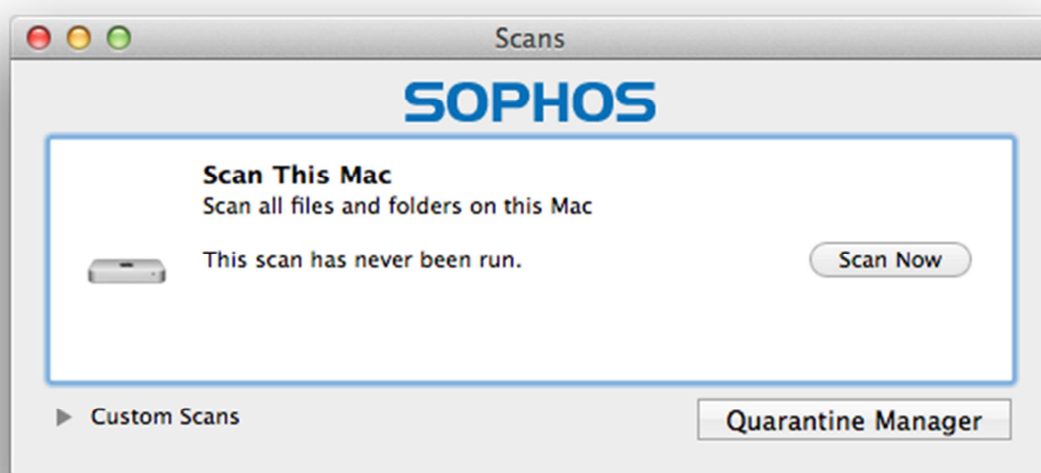
Kromtech MacKeeper has a usable interface and good Windows malware detection, but is not very effective at detecting Mac malware. Not everyone may agree with the program's initial analysis of their system.

The program's user interface is essentially straightforward, although real-time protection is not regarded as essential. We were surprised to see the program's analysis of our newly-installed Mac OS X system, which declared that the system was "overloaded with unnecessary junk files" and consequently in a "Serious" condition.

Although MacKeeper successfully identified all our Windows malware samples, its detection rate of 80% of Mac malware samples was disappointing.

<sup>5</sup> MacKeeper uses the Avira engine, but failed to detect some Mac malware samples that Avira's own program identified.

## Sophos Antivirus for Mac



### Additional features

Phishing protection

### Installation

The first page of the installer informs the user how to find help, and how to uninstall the product. The only option is which hard disk to install the product to. The program can be removed from the computer using the "Remove Sophos Anti-Virus" icon in the Applications folder. This is explained at the beginning of the Setup Wizard.

We found the information on uninstalling and finding help to be useful.

### Main window

Sophos Antivirus for Mac does not have a main window, i.e. a window that provides access to all the program's features. Instead, there are separate windows for Updates, Preferences, Scans and Quarantine. Subscription information is not applicable, as the program is free. Help can be started from the Help menu.

### Mac menu bar

Menus in the Mac menu bar are Sophos Anti-Virus, File, Edit, Scan, Window, and Help. Sophos installs its own System Tray icon,

which can be used to run updates and scans, change preferences, and view quarantine.

### Finder context menu

A scan entry is added to Finder's context menu, so files, folders and drives can be scanned by right-clicking them.

### Maintenance

Signatures can be updated from the Sophos Anti-Virus menu or System Tray icon. There is the most minimalist of status displays provided by Sophos. If real-time protection is turned off, the Sophos system tray icon turns from sharp black to light grey. If the icon is clicked, the first entry at the top of the menu (also in light grey) reads "On-Access Scanning is Disabled". There is no additional information on how to reactivate the protection.

We regard the "status display" as so minimalist that it is actually pointless.

### Non-administrator access

To change protection settings, all users must enter administrator credentials, regardless of the account used to log on to the Mac.

This is as it should be, in our opinion.

## Scanning

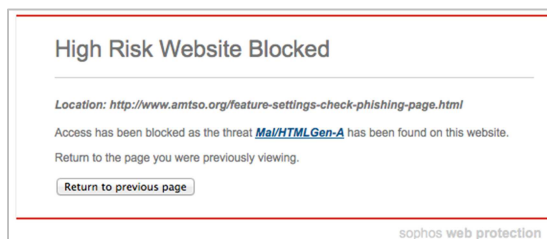
Full and custom scans can be run from the Scans window. There is no quick scan or scheduled scan available.

## Settings, quarantine and logs

Preferences and Quarantine Manager are available from the Sophos System Tray icon. Logs can be found by opening Scans, and right-clicking on the type of scan (Full or Custom); the shortcut menu contains the item "View Scan Log".

## Malware and phishing alerts

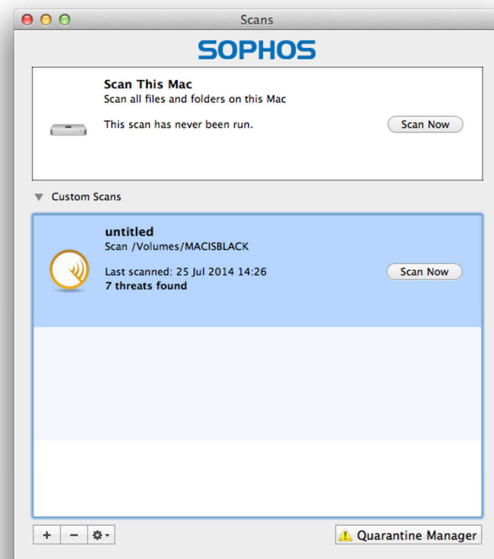
When the AMTSO phishing test page is opened, the following alert is shown in the browser:



A very similar warning is displayed when the EICAR test file is downloaded. When Sophos' real-time protection discovers malware on a flash drive, the following alert is displayed:



Opening Quarantine Manager displays the malware found. An actual scan of the flash drive lists the number of threats found and provides a link to the Quarantine Manager:



Quarantine Manager lists the threats found and provides a "Clean Up Threat" button. There is no means of selecting multiple items, unless the user is aware of the CMD + A shortcut key in Mac OS X.

## Malware protection test

Mac malware detected: 100%

False positives: 0

Windows malware detected: 100%

## Help

Clicking on Sophos Antivirus Help in the Help menu opens the local help service, which provides simple instructions (with occasional screenshots) for everyday tasks, organised into headings:



There is also an online knowledge base, which has instructions for common tasks such as removing malware.



We found the knowledge base articles to be very clear and comprehensive, and very well illustrated with screenshots. We would describe Sophos' help overall as good.

## Verdict

Sophos Antivirus for Mac is extremely effective at protecting against Mac malware, and also at detecting Windows threats.









We feel the program's minimalist user interface would be fine for experienced Mac users who have some understanding of antivirus software. Non-expert users might prefer a single program window with a status display, amongst other things.

Sophos was very effective at detecting both Mac malware and Windows malware, identifying all samples of both in our test.

## Summary

Seven of the products we have reviewed receive our Approved Security Product award. Unfortunately, we were unable to give Kromtech MacKeeper an award, due to limited Mac malware protection and puzzling system analysis<sup>6</sup>.

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><b>avast! Free Antivirus for Mac</b> identified 100% of samples in our Mac malware test. The user interface is modern and largely very straightforward to use, albeit with a couple of quirks.</p>
	<p><b>Avira Free Antivirus for Mac</b> combines fair protection against Mac malware (91% detected) with a very well-designed interface.</p>
	<p><b>Bitdefender Antivirus for Mac</b> provides very good Mac malware detection (98%), but may have difficulty removing the malware detected. The program is mostly very easy to use.</p>
	<p><b>ESET Cyber Security Pro</b> has a very clearly laid-out user interface and identified 100% of our Mac malware samples.</p>
	<p><b>Intego Mac Premium Bundle X8</b> identified 100% of our Mac malware samples, and the interface would be fine for experienced Mac users. Detection of Windows malware was weak, however.</p>
	<p><b>Kaspersky Internet Security for Mac</b> combines excellent protection against Mac malware (97% detected) with a very usable interface.</p>
	<p><b>Sophos Antivirus for Mac</b> is a free program that is extremely effective at protecting against Mac malware (100% detected). Its minimalist interface would be fine for experienced Mac users.</p>
	<p><b>Kromtech MacKeeper</b> has a usable interface and good Windows malware detection, but is not very effective at detecting Mac malware (80% detected). Not everyone may agree with the program's initial analysis of their system.</p>

<sup>6</sup> Please see comments on page 30.



Featurelist Mac (as of August 2014)	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE
Product name:	avast! Free 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	Kromtech MacKeeper	Sophos Antivirus for Mac Home Edition
Supported OS X versions:	10.6.8 and up	10.8 and up	10.7 and up	10.6 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, French, Italian, Korean, Portuguese	German, English	English, German, French, Italian, Spanish	Czech, Danish, Dutch, English, Finnish, French, German, Hungarian, Chinese, Italian, Korean, Norwegian, Polish, Portuguese, Russian, Slovak, Spanish, Swedish, Thai, Turkish	English, French, German, Japanese, Spanish	Chinese, Danish, Dutch, English, 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, Spanish, Japanese
<b>Protection</b>								
Real-Time protection	•	•	•	•	•	•	•	•
On-demand scanner	•	•	•	•	•	•	•	•
Detects also threats for other platforms (e.g. Windows malware)	•	•	•	•	limited detection of windows threats	•	•	•
Cloud Scanning (requires internet connection)			•	•	•	•		•
Prevent access to malicious and phishing web sites (which browsers are supported?)	All		Safari, Firefox, Chrome	All		YES, all	Safari, Firefox, Chrome	Safari, Firefox, Chrome, Opera, curl, wget
Safe search (which browsers are supported?)	Safari, Firefox, Chrome				All	Safari, Firefox, Chrome		
Quarantine	•	•	•	•	•	•	•	•
Whitelisting for specific files/folders	•		•	•	•		•	•
Scheduled Update	•	•		•	•	•	•	•
Scheduled On Demand Scan		•		•	•		•	•
Statistics	•	•	•	•		•	•	
<b>Additional features</b>								
Parental Control				•	•	•		•
Mail Protection	•		•	•	•			
Removable media blocking				•	•			•
Firewall				•	•			
Game/Presentation mode				•				
<b>Support</b>								
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, German, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malay	English, German, French, Italian, Spanish, Portuguese, Romanian, Turkish	All	English, French, Japanese	Arabic, Chinese, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English	English, French, German, Spanish, Japanese, Italian, Chinese
<b>Price (may vary)</b>								
Price 1 Mac / 1 year (USD/EUR)	FREE	FREE	USD 40 / 40 EUR	USD 45 / 34 EUR	USD 90 / 75 EUR	USD 40 / 40 EUR	USD 90 / 90 EUR	FREE
Price 2 Macs / 2 years (USD/EUR)			USD 90 / 90 EUR	USD 83 / 63 EUR	USD 280 / 250 EUR	USD 120 / 120 EUR	USD 178 / 178 EUR	

## Copyright and Disclaimer

This publication is Copyright © 2014 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 (August 2014)