

# Mac Security Review



## Mac Security Review

Language: English

July 2013

Last revision: 19<sup>th</sup> August 2013

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

# Contents

Introduction: Macs and Security Software .....	3
Malware Protection/Detection Test .....	6
Avira Free Mac Security .....	7
ESET Cyber Security Pro .....	11
F-Secure Anti-Virus for Mac .....	14
Intego Mac Premium Bundle .....	17
Kaspersky Security for Mac .....	21
Quick Heal Total Security for Mac .....	25
Sophos Anti-Virus for Mac Home Edition .....	28
KromTech MacKeeper .....	31
Summary .....	35
Copyright and Disclaimer .....	37

## Introduction: Macs and Security Software

In February 2013, Reuters<sup>1</sup> and many other news agencies reported that Mac computers used by Apple's own staff had been infected by malware and then used to launch an attack on Facebook. Apple admitted that some of their systems had indeed been compromised. Whilst this is in itself only a single small incident, it nonetheless proves that the Mac OS cannot be regarded as immune to malware attacks. The growing number of Mac users means that cybercriminals are increasingly targeting the platform, and there have been a number of other reliable reports of Mac malware attacks. Even if the number of malicious programs and successful infections is very small compared to those affecting Windows PCs, it is clear that the issue of Mac security needs to be taken seriously. As with Windows computers, Macs can be made safer by employing good security practices. We recommend the following:

1. Never 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
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. Consider employing security software on your Mac

---

<sup>1</sup> <http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219>

## Review of Security Software for OS X Mountain Lion

We have reviewed and tested the following products for this report, using the newest version available in July 2013:

- **AVIRA Free Mac Security 10.0.0.64**
- **ESET Cyber Security Pro 5.0.110**
- **F-Secure Anti-Virus for Mac B12533.C740**
- **Intego Mac Premium Bundle 10.7.5**
- **Kaspersky Security for Mac 14.0.0.177**
- **Quick Heal Total Security for Mac 1.0**
- **Sophos Anti-Virus for Mac Home Edition 8.0.15c**
- **KromTech MacKeeper 2.5.1**



In this year's review of antivirus programs for the Mac, we have taken a detailed look at the most important features and functionality of each program, using a similar format to our Summary Review for Windows programs. Even if there are fewer malicious programs aimed at Macs than at Windows PCs, the nature of those that do exist is essentially similar to their Windows counterparts, and so we feel that Mac antivirus software should function in a similar way, too.

First, we look at the installation routine of the software. At the very least, this should have a simple option for non-expert users, though a custom option that allows expert users a variety of configuration options is a welcome bonus. We also check what means are available to uninstall the program. After installation, we start the program and check whether the main window offers essential status information and protection functions. We would expect to see a status display that indicates whether the virus definitions are up to date and real-time protection is enabled, as these are the most important factors in ensuring the computer is protected. We also check (if possible) to see what sort of warning is shown when real-time protection is turned off; we feel that a clear warning should be shown, along with an easy means of rectifying the problem, such as a button or link that either reactivates the protection or opens a dialog box where this can be done manually. Another item we consider important is an update button, so that the user can ensure malware definitions are completely up to date. Of course, this does not apply to programs that are entirely cloud-based. The program interface should in our opinion also provide an easy means of running a scan, whereby we would hope to find options for a full system scan and a custom scan of a

particular folder or drive. We check the OS X Finder context menu to see if the program has added a scan entry; this is not essential, but nonetheless a very convenient method of running a scan on a particular drive or folder. In the case of paid programs, we look to see if the subscription information (or a link to it) is displayed in the main program window; the user should know when it would be necessary to renew the subscription, in order to keep the Mac protected at all times. Finally, we check whether the help feature is easily accessible.

Particularly for a family computer, it is important that users with non-administrator accounts should not be able to deactivate important functions of the antivirus program such as real-time protection. We therefore log on to our test Mac using a non-administrator account (specified as such in the settings of the antivirus program, if necessary) and attempt to disable real-time protection, and then to uninstall the program completely.

A useful function in an antivirus program is the ability to schedule a scan, so that the computer will be checked regularly for malware without the user having to remember to do it. We look to see if each program in our test configures a scheduled scan by default, and how to set one up if not. We also note any options as to what should happen if a scheduled scan is missed.

We try to find out what sort of notification each program provides in the event that a threat is discovered. To do this, we use AMTSO's Feature Settings Check pages (<http://www.amtso.org/feature-settings-check.html>). This is intended to test the functionality of the features of antivirus programs using the EICAR test file (manual and drive-by download), a similar PUA (potentially unwanted application) test file, a test phishing site, and a test of cloud protection. The latter works by using a test file similar to EICAR, the definition for which is only ever kept in the cloud, not locally, by all participating vendors. We must stress that using the Feature Settings Check is NOT a detection test, and a program should not be considered inferior if it fails to respond to one of these tests. We have used it in this review purely as a means to demonstrating the alerts produced by a Mac antivirus program when a threat is discovered. We feel that when a threat is discovered, a good antivirus program should inform the user that this has happened; if a web page or download is blocked without any explanation, the user will very probably just be confused as to why this has happened. A warning message should make either clear that the threat has already been blocked/quarantined, and that no further action is necessary, or have a clear default option such as Block/Delete/Quarantine, which does not require the user to make a decision about whether a page or file is safe. Any option to view the page/download the file, to be used by advanced users, should be significantly less obvious/less accessible than the default "safe" option.

The last area of each program that we look at is the documentation and help features offered by each vendor. These may include user manuals, a local help feature, online help and knowledge base articles. We feel that at a minimum, a program should provide some guide to everyday tasks such as updating and scanning, ideally illustrated with screenshots. A search function, whereby the user can type in a term such as "scan exclusions" without having to browse through all available articles, is also highly desirable.

To conclude our review of each Mac antivirus program, we summarise our overall impressions and note any areas where we feel the software is very good, as well as suggesting possible improvements.

## Malware Protection/Detection Test

In addition to the interface review described above, we have also conducted actual malware protection tests to see how effectively the Mac security products protect the system against malware. For this test, we used 20 recent and prevalent samples of Mac malware that are not blocked by Mac OS X Mountain Lion itself. All are distinctly malicious, functioning programs and were seen in-the-field in 2013. 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 components to be irrelevant. We ended up with a test set consisting of 20 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 20 malicious Mac apps represent a substantial part of all recent Mac malware from the first half of 2013.

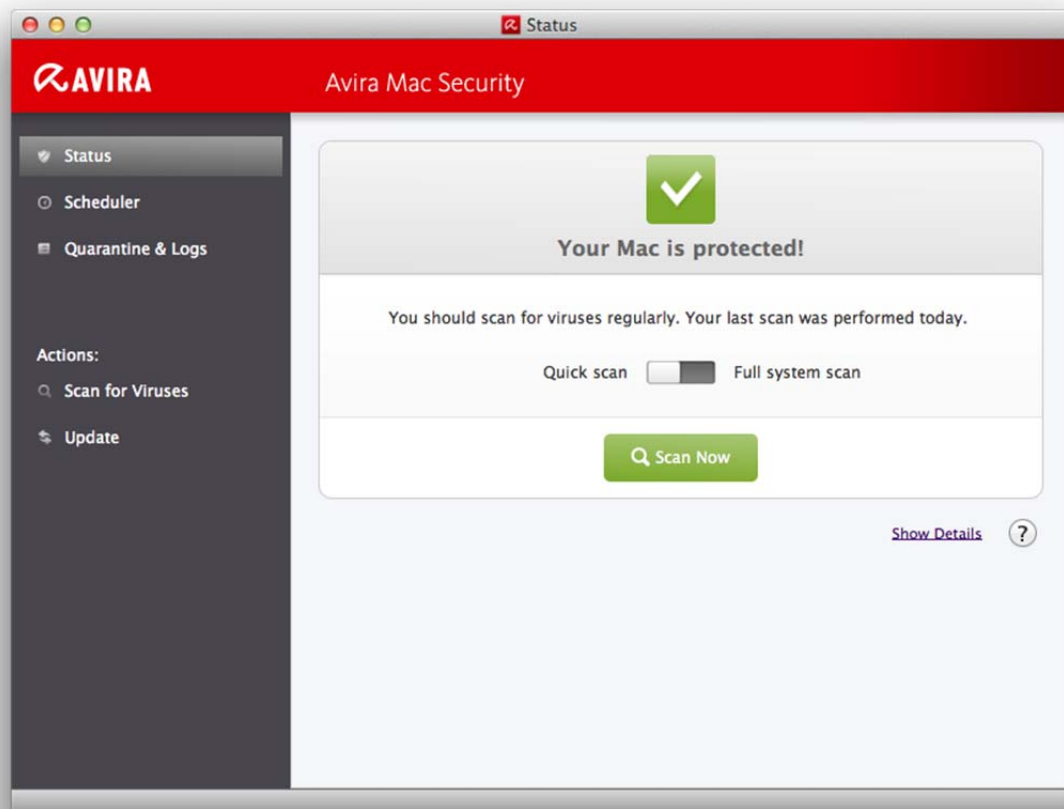
The number of malicious programs that can currently attack Mac OS X Mountain Lion is thus very limited. However, as most Mac systems do not run any third-party security software, even these few threats could cause widespread damage. Precisely because a Mac security product only has to identify a small 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 19<sup>th</sup> July 2013. 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. Finally, we attempted to run any of the malware samples that had not yet been detected.

Of the Mac security products tested, all except Quick Heal protected against every one of the 20 Mac malware samples. No false alarms were encountered with any of the products (over a small set of very common installed Mac apps).

Some (but not all) 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 have also checked if the Mac antivirus products in our review detect Windows malware. We used around 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. AVIRA, ESET, Kaspersky, QuickHeal, Sophos and KromTech detected all the Windows malware samples. F-Secure and Intego did not detect all the prevalent Windows malware samples (although the majority of them), whereby F-Secure state that they provide only limited coverage of Windows malware in their Mac products.

## Avira Free Mac Security



### Introduction

Avira Free Mac Security is an antivirus program without any additional features. Nature and size of the installer: 121 MB full installer

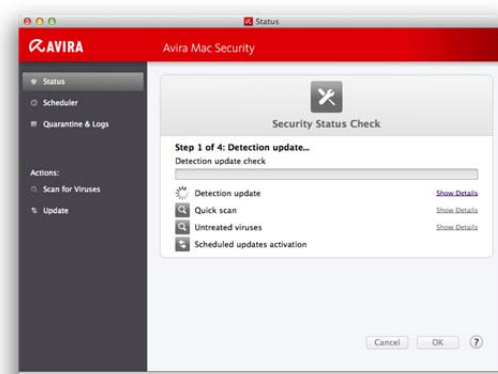
### Installation

Avira Free Mac Security uses a .pkg file for the installer. Simply double-clicking this in the Finder window displays this message:  
The user has to right-click the package and

then click "Open"; the program can then be installed. This may not be obvious to non-expert Mac users.

Steps in the installation process are accepting the licence agreement, then choosing an installation disk and folder. There are no other options. Immediately after installation, the main program window opens, and an update and quick scan are run:

We note that while the update is being



carried out, the Avira program icon in the Dock shows a warning symbol:

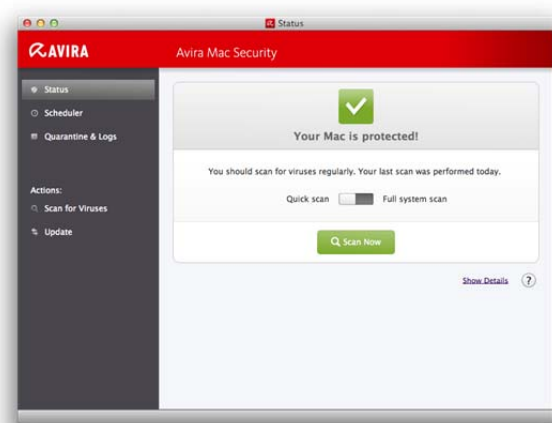


We found the installation process to be very quick and simple.

The user manual suggests two methods of uninstalling the program: moving the application to Trash, or using the command line. Additionally, an uninstaller program can be found under Applications/Utilities.

### Program interface

The Status page of the main program window

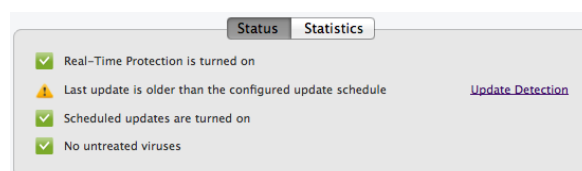


features a status display, with the words *"Your Mac is protected!"* and a tick in a green box to show all is well. Clicking on *"Show Details"* shows the status of individual items: real-time protection, signatures, scheduled updates, and untreated viruses. It is not possible to manually disable the real-time protection, which is our usual means of testing status warnings. However, if the malware signatures are out of date, Avira

Mac Security displays the following warning in the status section:



Clicking on *"Details"* informs the user what the problem is:



Clicking on *"Secure My Mac Now"* takes the necessary steps to solve the problem, in this case by running an update.

The Status page also includes a very obvious scan button, with the choice of Quick or Full scans. The Scan for Viruses button in the menu pane on the left also allows a custom scan to be run. An update button can be found in the same place, along with the Scheduler, Quarantine and Logs. The local Help function is also available from the home page. Subscription information is not applicable as Avira Mac Security is a free product.

An Avira icon appears in the System Tray section of the Mac Menu Bar after installation; clicking it displays the following menu:

Open Avira  
Open Preferences  
Update Detection  
Perform Quick Scan  
My Messages  
Go to Avira Website



Avira does not add an entry to Finder's context menu, so custom scan have to be initiated from the console.

Overall, we found the interface of Avira Mac Security to be very clear and uncluttered, with all necessary functions and information easily accessible.

### Non-administrator access

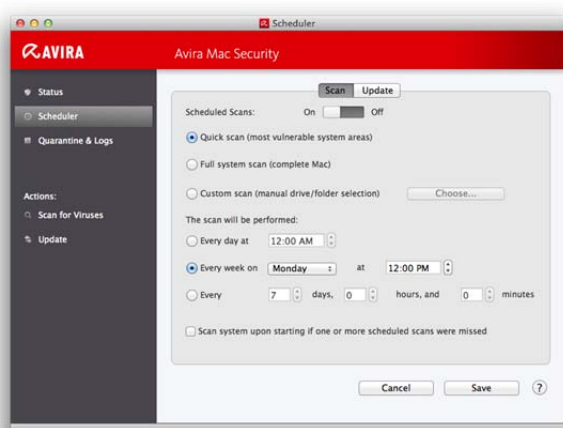
As mentioned above, it is not possible to disable real-time protection *with* administrator rights, let alone without. We were unable to remove the program without administrator rights.

### Scheduled scanning

A scheduled scan is set by default for every Monday at 12 o'clock midday. There is an option to run the scan at the next system startup if the scheduled time is missed. The scheduled scan dialog box, which we regard as optimally simple, is shown below:

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks were as follows:



EICAR.COM test file manual download: file is quarantined without any notification  
 EICAR.COM test file drive-by download: file is quarantined without any notification  
 EICAR potentially unwanted application: file is quarantined without any notification

AMTSO phishing test page: the page is displayed. We note that Avira is among the vendors listed as supporting the anti-phishing test feature, but we assume this only applies to Windows suites.

CloudCar testfile: file is downloaded. Avira is not shown amongst the vendors supporting this test feature.

We note that when Avira detects and quarantines the test files, it does not provide any sort of message to inform the user what has happened. We suggest that a message stating that malware has been quarantined would be helpful to the user and point out the effectiveness of the antivirus software.

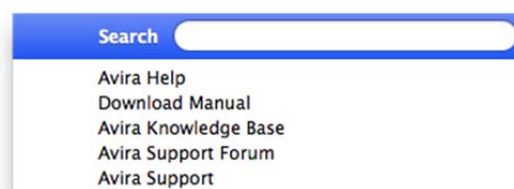
Real-time protection test: we were able to copy a folder of Mac malware from a USB flash drive to the Mac desktop, without Avira taking any sort of action or providing any warning.

### Malware protection/detection test

Avira Free Mac Security detected all the malware samples, both Mac and Windows, used in our tests.

### Help and Documentation

All the help and support features of Avira Mac Security can be found in the Help menu, which we find very convenient:



The search box at the top of the menu can be used to search the local help feature, which provides simple and clear text instructions for everyday tasks. We note that if the window of the local help service is used to type queries (rather than the search box in the Help menu), results are very context-sensitive. That is to say, the results found relate only to the

currently displayed page of the program, so searching for “schedule” when on the home/status page shows no results. We suspect some users may find this confusing.

The manual is a comprehensive 48-page document in .pdf format. It covers installation and deinstallation, and all other features and functions of the program. There is a full, clickable index at the beginning, and the text has been fully bookmarked, making individual sections easily accessible from Adobe Reader’s bookmarks bar. Our only criticism is that aside from a few pictures of the Avira logo in the Dock, there are no screenshots.

Clicking on Avira Knowledge Base in the Help menu opens the appropriate page of the Avira website. The search function on this page applies to all Avira products and operating systems, so any search query must include the name of the particular product being used. We also note that the answers found for Avira Mac Security are contained within the .pdf manuals; clicking the link for a particular answer simply downloads the relevant manual, which must then be opened and searched. We suspect some readers might prefer to be taken directly to a page showing the answer to their question.

By and large we found the help functions of Avira Mac Security to be very good, even if they sometimes take a little patience to understand.

## Summary

Avira Security for Mac provides all the essential features of an antivirus program for free, and proved highly effective at detecting both Mac and Windows malware. It receives our Approved Security Product award. Overall, we found it to be extremely easy to use. The user interface could be regarded as optimal in terms of providing easy access to all important features. Suggestions for improvement include notifications when malware is found, and increasing the sensitivity of real-time protection so that malware is detected on-access as well as on-execution.

## ESET Cyber Security Pro



### Introduction

ESET Cyber Security Pro includes the typical features of a Windows Internet security suite, namely antimalware, firewall and parental control.

Nature and size of the installer: 51MB full installer. We were pleased to note that the installer checks to see if a newer version is available before commencing.

### Installation

The installation package provides Install, Uninstall and Read Me options. The Read Me file has simple installation and deinstallation instructions, plus system requirements. As usual, there is a licence agreement to accept. Unusually for Mac security programs, a custom installation is available. The options are: proxy server settings; defining privileged users (i.e. which users will have administrator rights for the program); enabling Live Grid (malware sharing); whether to detect potentially unwanted programs; and firewall mode (automatic or interactive). Once the

product has been activated with a username and password, an automatic update is carried out.

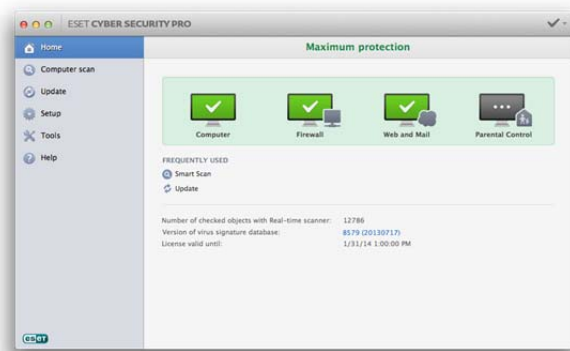
We note that in order to re-enable file sharing on our Mac, we had to go into the firewall settings and change the network type from Public to Home. However, ESET inform us that in the upcoming build of the product, a dialog box at the end of the installation will ask the user whether file sharing should be enabled for each network adapter.

With the exception of enabling file sharing, we found the installation of ESET Cyber Security Pro to be very straightforward, whilst offering a variety of sensible options.

The program can be uninstalled by opening the installation package again, which has an obvious Uninstall icon. We found deinstallation to be quick and straightforward.

### Program interface

The main program window of ESET Cyber Security Pro uses a similar format to its Windows counterpart. A narrow left-hand column serves as a menu bar for important tasks and features, including Computer Scan, Update and Help. The larger right-hand column serves as a status display, with the status of the individual components Computer, Firewall, Web and Mail, and Parental Control, shown as Mac monitor icons: The icon for Parental Control is clearly different from the others, as this feature has to be configured and is not active by default. There are links to Smart Scan and Update;

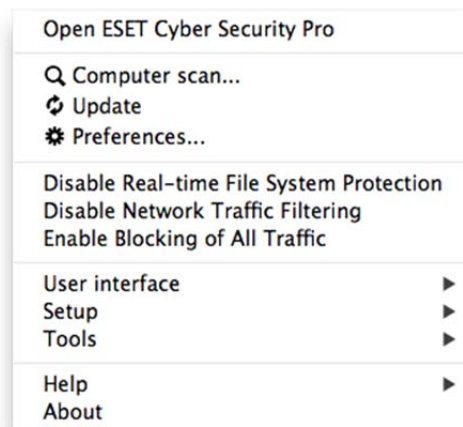


licence and update status information are also displayed. If real-time protection is disabled, the status page changes, showing a clear warning, with various items in red:



Protection can be reactivated by clicking "Enable real-time file system protection", the warning symbol in the top right-hand corner, or the Computer icon.

ESET Cyber Security Pro creates an icon in the System Tray, with a comprehensive menu of tasks and features:



By default, there is no addition to the Finder context menu, although this can be enabled in the program's settings.

Overall, we found the interface of ESET Cyber Security Pro to be exemplary, with important information and functions easy to find in a clean and uncluttered window.

### Non-administrator access

When we logged on to our test Mac with a "non-privileged" account (as defined in the setup process), we were unable to disable the real-time protection; the window controls are greyed out and the System Tray menu is altered so that the item is not available.

We were also unable to uninstall the program without administrator rights.

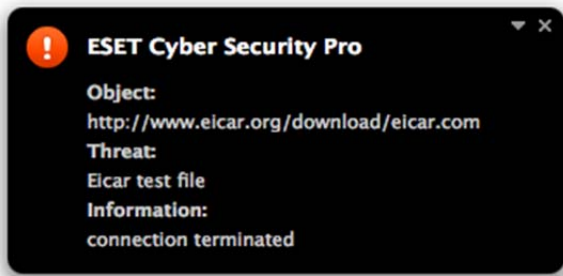
### Scheduled scanning

A scheduled scan is not configured by default, but can easily be set by clicking Computer Scan, Schedule Regular Scan. The user can decide in the scan options what to do if the scheduled scan is missed.

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks were as follows:

EICAR.COM test file manual download: the download is blocked, and a warning message is displayed. This makes reasonably clear that the threat has been removed:



EICAR.COM test file drive-by download: the same reaction was noted as for the manual download

EICAR potentially unwanted application: ESET Cyber Security Pro displays a warning dialog box, with a choice of Disconnect or No Action.

AMTSO phishing test page: the download page is blocked, and replaced by ESET's own warning page, which states "The web page is on the list of websites with potentially dangerous content". A separate pop-up warning message is also displayed.

CloudCar test file: A warning message appears, similar to the one for the Eicar file.

When we plugged a USB flash drive containing malware into our test Mac, ESET Cyber Security Pro immediately warned of the malicious content, before we had even opened the drive in Finder. Overall, we found ESET's warning messages to be good.

### Malware protection/detection test

ESET Cyber Security Pro detected all of the malware samples, both Mac and Windows, used in our tests.

### Help and Documentation

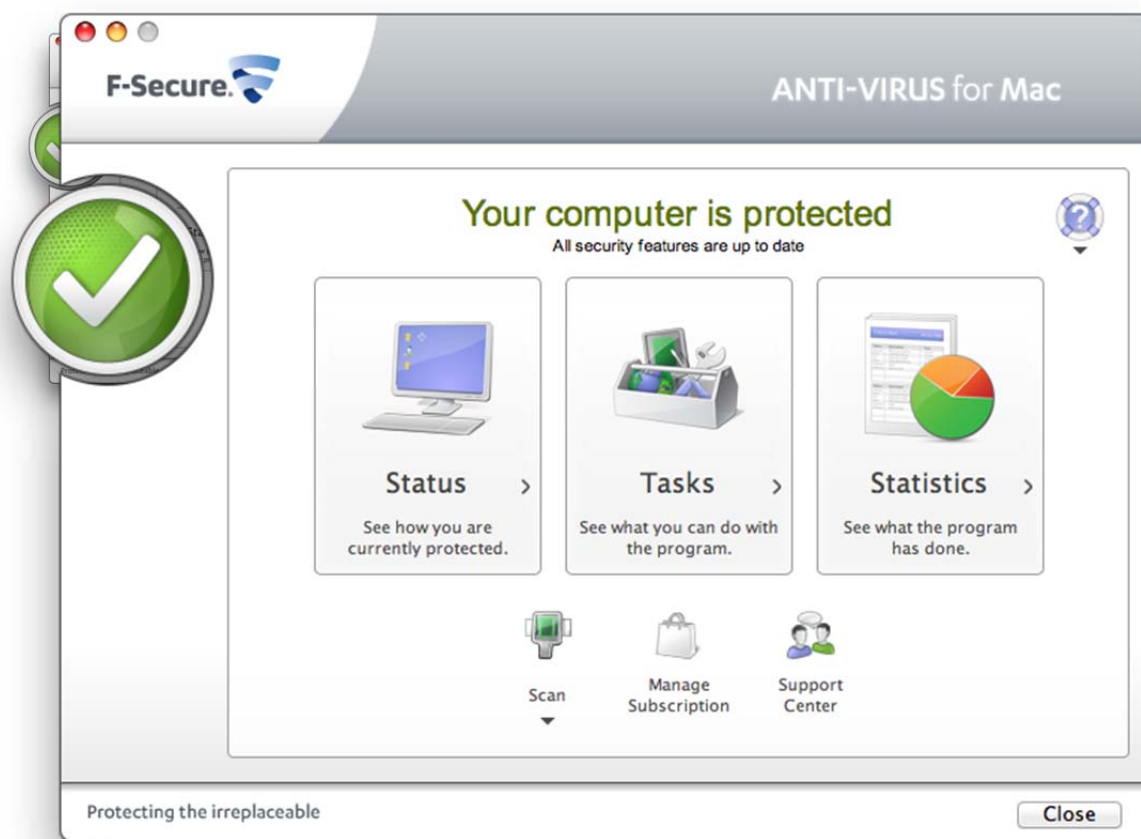
ESET produce two manuals for Cyber Security Pro. There is a very simple 12-page, large-print Quick Start Guide, which covers the essentials of installation and use, and a much more comprehensive 24-page User Guide. The latter covers all aspects of the installation and use of the program in detail, and has been appropriately illustrated with screenshots. A clickable index page and thorough bookmarking make it easy to access a particular section with a single click.

There is a local Help feature, which is searchable and has a comprehensive, clickable index page. Finally, a searchable knowledgebase is available on ESET's website, which features not only text instructions, but also videos for important common tasks such as creating a scheduled scan. Overall, we found the help facilities for Cyber Security Pro to be of the same excellent standard as with other ESET products.

### Summary

Overall, we found ESET Cyber Security Pro to be an excellent anti-malware solution for Mac OS X, and it receives our Approved Security Product award. The program is simple to install and use, and status displays and warning messages are clear. Help facilities are exemplary.

## F-Secure Anti-Virus for Mac



### Introduction

F-Secure Anti-Virus for Mac is a straightforward antivirus program. Nature and size of the installer: 19 MB full installer

### Installation

The installation process requires the acceptance of a licence agreement, but does not have any other options. At the end of the installation, a message appears that the "system firewall" has been enabled; this refers to the OS X firewall. We found the installation to be very quick and straightforward.

F-Secure provide an uninstaller for Anti-Virus for Mac. This can be found by double-clicking the F-Secure icon in the Applications folder.

### Program interface

The main program window will be familiar to anyone who has used F-Secure products for Windows. The status is shown by means of a big circular button, which is green with a white tick (checkmark) if all is well, along with the text "Your computer is protected" at the top of the window.

We could not find a means of disabling real-time protection, and so cannot say how the program reacts when protection is not ensured.

There is no update button anywhere in the program window, although the menu under the F-Secure System Tray icon contains a "check for updates" entry. Clicking on this produces no visible reaction, regardless of whether the program window is open or not.



The user can confirm that an update has taken place by clicking on Statistics; Last Successful Update Check will show “a moment ago”. Nonetheless, we feel that automatically displaying a message along the lines of “Your malware signatures are up to date” would be much clearer.

A scan button can be found on the home page. There are only two options: “Scan Home Folder” and “Choose what to scan”; the latter can be used to run a full scan by selecting the Mac’s hard disk, but we would not regard this as ideal for non-experts, and suggest that an additional option to run a full scan would be an improvement.

There is a help button in the top right-hand corner of the window, which provides links to the Help and Support pages of F-Secure’s website. There is also a Support button, which provides some essential system information, along with a non-functioning, corrupted hyperlink:



The Manage Subscription button on the home page allows the key to be changed and displays the message “Your subscription is valid”, but to find out how long for you have to click on the Statistics button on the home page; it would seem more obvious to all the subscription information together in one place.

Even when the program window is open and active, F-Secure Anti-Virus for Mac does not appear in the Dock or the list of running programs displayed by pressing cmd + tab.

There is however a permanent F-Secure icon in the System Tray, which displays the following mini-menu:



The program does not integrate itself into the Finder context menu, so scans must be started from the program window.

As already noted, the main program window of F-Secure Anti-Virus for Mac is very similar to that of its Windows counterpart. We feel that simply porting the design to the Mac OS does not work very well; for example, the Mac version has fewer features and options than the Windows version, and that these could be made more accessible if there were correspondingly fewer buttons in the main program window. We would also suggest that Mac users would find the program more comfortable to use if it were better integrated into the Dock.

### Non-administrator access

As mentioned above, the program does not provide any means of disabling the real-time protection, even with administrator rights.

We were not able to uninstall the program with a non-administrator account.

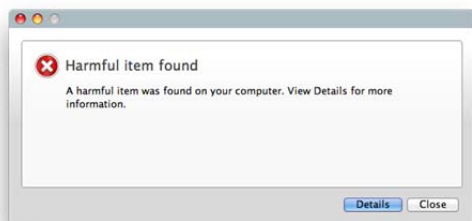
### Scheduled scanning

F-Secure Anti-Virus for Mac does not include a scheduler, so it is not possible to set up a scheduled scan.

### AMTSO Feature Settings Checks

The program reacted to the AMTSO feature settings checks as follows:

EICAR.COM test file manual download: the file is deleted, and the following message displayed:



Clicking on Details shows that the file has been “trashed”. We would suggest that it would be better to display this in the initial message, so that the user knows the threat has been removed and no further action is needed. We note that to see the log file, the user has to click on the Tasks button, whereas we would find it much more logical to put this item under Statistics (subtitle: “See what the program has done”).

EICAR.COM test file drive-by download: the file is deleted, and the same message displayed as above.

EICAR potentially unwanted application: The same message as above is displayed, but the file is not deleted or quarantined. Clicking on Details shows that the file has been “reported”; there is no other information given about the file or why it might be harmful.

AMTSO phishing test page: the page is displayed. We note that F-Secure is shown amongst the vendors supporting this feature, though we assume that this only applies to Windows programs.

CloudCar test file: the file is downloaded. Again, F-Secure is shown as supporting this feature, presumably only in programs for Windows.

We would suggest that the warning message shown when a threat is downloaded should be changed to show clearly whether the threat has been deleted or not.

Real-time protection test: when we plugged in a USB flash drive containing Mac malware samples, the program immediately displayed a message stating that a harmful item had been found; the real-time protection had in fact already detected a number of the malware samples.

### Malware protection/detection test

F-Secure Anti-Virus for Mac detected all the Mac malware samples used in our test. It also detected a small portion of our selected Windows malware. We note that F-Secure does not make any claim that the program will detect Windows malware.

### Help and Documentation

A 12-page manual in .pdf format is available to download from the F-Secure website. There are in fact only 7 pages of text, the other 5 pages being index or cover pages. However, given the simple nature of the program, we feel there is sufficient explanation provided. Although it is not really necessary in a document of this size, the manual has been indexed with a clickable contents page, and bookmarked, making accessing particular sections extremely easy.

The help function accessible from the Help button on the main program window appears to have identical content to the manual, but as a page of the F-Secure website. There is no local help function as such.

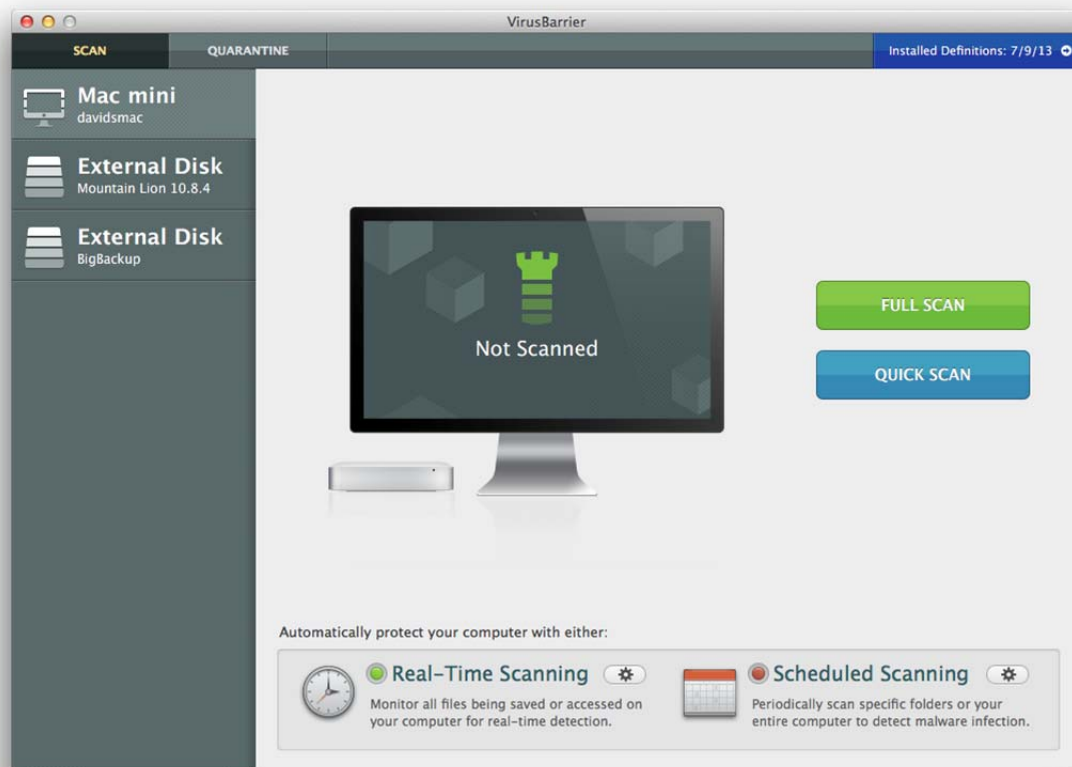
We would describe the help features for F-Secure Anti-Virus for Mac as simple but adequate.

### Summary

F-Secure Anti-Virus for Mac is a simple antivirus program with all essential features. It features excellent Mac malware recognition and real-time protection, and receives our Approved Security Product award. We would however suggest that the program interface could be better adapted to the Mac software, and that malware warnings might be clearer.



## Intego Mac Premium Bundle



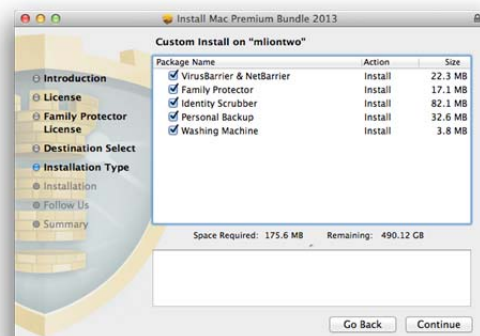
### Introduction

Intego Mac Premium Bundle 2013 combines an antimalware component (VirusBarrier), a firewall (NetBarrier), parental controls (Family Protector), identity protection (Identity Scrubber), backup (Personal Backup), and privacy controls (Washing Machine).

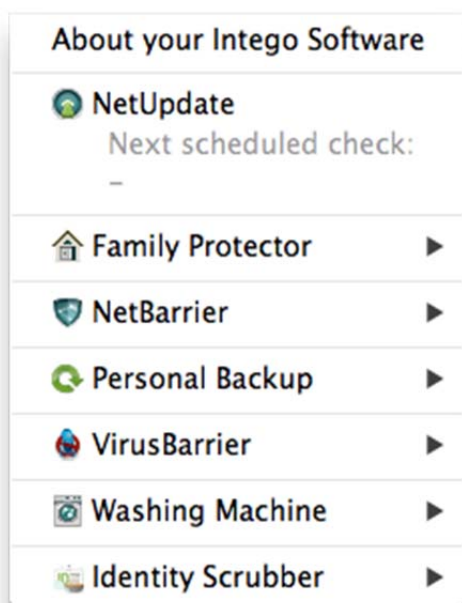
Nature and size of the installer: 73 MB full installer

### Installation

The setup program provides a choice of components to be installed:



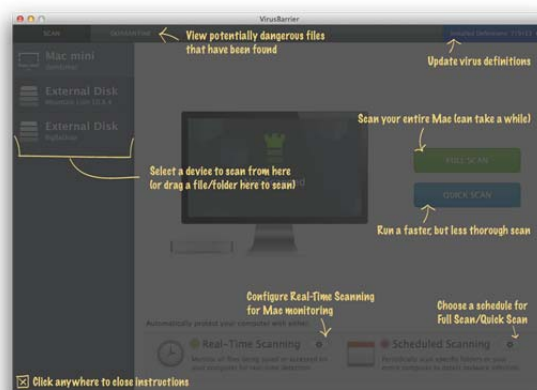
The installer warns that a restart will be required at the end of the installation. The process is completed with just a few clicks. After a restart, the various programs can be opened from the Intego icon in the Mac System Tray:



Each of the components has its own program window. When the VirusBarrier window is opened, configuration options are offered, which include the level of protection and the option to scan archives (these options can be changed later in the program's preferences).



After this, a guide to the main VirusBarrier program window is displayed, using an overlay to illustrate the various screen elements. We found this to be a simple, effective and innovative way of explaining the program's features:

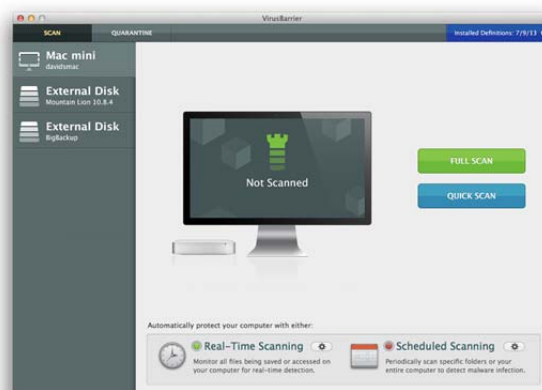


We found the setup process to be very simple and straightforward.

Re-running the installation package provides an option to uninstall the software. This provided the opportunity to remove the components (antivirus/firewall etc) separately from each other. Dragging the Intego icon from the Applications window in Finder to the Trash also allows the software to be uninstalled, albeit in its entirety without any choice of components.

### Program interface

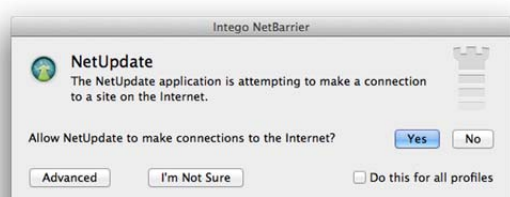
The main program window of VirusBarrier is dominated by a graphic of a Mac Mini and Mac Monitor. We initially assumed this has no function, as clicking on it has no effect, but later discovered that files or folders can be dragged on to it from Finder, in order to scan them. Next to it are very big, obvious buttons for full and quick scans:



A custom scan can be run from the File menu in the Mac Menu Bar.

A section at the bottom of the main window serves as a status display for both real-time protection and scheduled scanning; the former is activated by default, the latter not. The status of each item is shown by a small button, which is green when active and red for inactive. A configuration button next to each item allows it to be switched on or off very conveniently. Other than the colour of the buttons, no warnings are shown if a component is deactivated.

The status of updates is shown in a button in the top right-hand corner; clicking on this runs an update check. The update dialog box shows the subscription expiry date. We were very surprised to see that when we attempted to run an update, the suite's own firewall asked whether the process should be allowed:



Intego tell us their stance is that the application firewall should not special case their own software; however, this strikes us as counterproductive and confusing, and we suggest that Intego should rectify it.

The Help menu in the Mac Menu Bar offers the choice of Show Basic Help (which displays the overlay of key features, as on first use), VirusBarrier Help (which opens the support pages of the product's website), and a search box, although this searches the Mac OS X help files.

VirusBarrier adds a scan entry to the Finder menu, so that drives/folders can be scanned by right-clicking.

Folder Actions Setup...  
Scan with VirusBarrier...

Overall, we found the program's interface to be clear and simple, although we feel a more effective warning could be shown when real-time protection is disabled.

### Non-administrator access

We were unable to disable the program's real-time protection, or uninstall it, using a non-administrator account.

### Scheduled scanning

A scheduled scan is not set by default, but can easily be configured from the button on the program's main window.

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks were as follows:

EICAR.COM test file manual download: a warning message is shown, with the options Trust, Quarantine, Repair:



EICAR.COM test file drive-by download: the same message/dialog box as above is shown  
EICAR potentially unwanted application: The file is not recognised and is downloaded without any sort of reaction from the program  
AMTSO phishing test page: the page is shown  
CloudCar testfile: the file is downloaded without any notification

Real-time protection test: real-time protection appears to be limited. We were able to copy folders of Mac malware from a USB stick to the Desktop without any intervention. However, when we attempted to run Mac malware samples, the same warning/dialog box was displayed as for the EICAR test file.

We found the warnings displayed when malware is discovered to be very clear and simple. We suggest it might be better if the “Trust” button were made smaller and/or moved, to discourage non-expert users from using it.

### Malware protection/detection test

Intego Premium Bundle detected all of the Mac malware samples we used in our test. However, it was only able to recognise two thirds of the prevalent Windows malware samples we tested it against. As the manufacturer’s website claims that the program “detects Windows malware to prevent your Mac from acting as a carrier”, we feel that this is a disappointing score.

### Help and Documentation

Clicking on VirusBarrier Help in the Help menu of the Mac Menu Bar opens the product’s User Guide, which is actually a page of the Intego website. It provides clear and simple instructions for basic tasks, beginning with choosing the settings when the program is first run after installation, and covering what to do when malware is found, and how to run a scheduled scan. The instructions are abundantly illustrated with big, clear

screenshots. We would however point out that the scope of the guide is very limited, even for a simple, easy-to-use product. There is a link on the page to the Knowledge Base, which contains a few links to other relevant pages, such as running a custom scan or installing/uninstalling the program. The instructions given on these pages are again brief but very clear.

Overall, we would describe Intego’s help functions as clear and well-illustrated, but rather limited.

### Summary

Intego Premium Bundle for Mac 2013 detected all our samples of Mac malware and receives an Approved Security Product award. We were however a little bit disappointed with the level of Windows malware recognised.

Overall, we found the program to be clear and easy to use, with all important functions easily accessible. Our major recommendation for improvement would be to ensure that the integrated firewall automatically allows the update of virus signatures, without asking the user for permission.

## Kaspersky Security for Mac



### Introduction

Kaspersky Security for Mac includes antivirus and parental control components, and a virtual keyboard.

We installed the program from a 180MB .dmg file; this is a full installer, but checks for a newer version before proceeding, which we find optimal.

### Installation

The Kaspersky Security installer is extremely simple, the only option being whether to participate in the Kaspersky Security Network (malware information sharing):



Installation then proceeds. After about a minute, the wizard indicates that installation is complete, and the options Try, Activate and Buy are offered. We activated the full version with a key provided by Kaspersky. We felt the installation process for Kaspersky Security was very quick and straightforward. The installation package includes a separate Uninstaller program, which we found to be very quick and easy to use.



## Program Interface

The program window is dominated by a big circular button on the right-hand side, which serves as the status display. This is coloured green if all is well, amber (yellow) for minor problems and red for major problems. The status is confirmed by a text message on the left-hand side of the window, which reads “Protection enabled”, “Protection disabled”, or e.g. “Web antivirus disabled”, as appropriate.



If either of the two main malware protection components is disabled, clicking on the status button opens a dialog box from which the component can easily be reactivated:



Around the left-hand side of the status button are three buttons for update, scan, and licence key. Although these do not have text labels, we found the symbols used to make clear enough what the functions are. If the update button is clicked, the progress of the signature download is shown as a percentage under the status text. Clicking the scan button provides a choice of Full Scan, Quick

Scan and Virus Scan. We found the term “Virus Scan” unclear – it is in fact a custom scan.

The Help function is easily accessible from a button above the status display; the Support button in the same row provides key system information and links to Kaspersky’s technical support webpage and forum.

Kaspersky Security creates its own status icon in the Apple menu bar; clicking it displays the menu shown below:



Kaspersky Security for Mac also adds a Virus Scan entry to Finder’s right-click menu, so that a file or folder can be scanned simply by right-clicking it.

Along the bottom of the main program window are buttons for each of the 3 main components, namely File Anti-Virus, Web Anti-Virus and Parental control; clicking on one of these buttons opens the relevant configuration dialog box. There is another row of buttons along the top of the window, for Reports, Preferences, Support and Help, each illustrated with an appropriate icon.

We found the interface of Kaspersky Security for Mac to be clear and straightforward, displaying all important information clearly and enabling easy access to the most important functions.

## Non-administrator access

If a user without administrator privileges attempts to disable real-time protection from the main program window, the control is locked and cannot be unlocked without entering administrator credentials. However, the same user can disable protection by clicking the Kaspersky icon in the System Tray and then clicking "Turn Protection Off" – this is not locked and does not require any additional credentials. For a suite that is obviously intended for family use, this strikes us as inappropriate. We have informed Kaspersky of this, and they say they will rectify it in the near future.

### Scheduled scanning

Kaspersky Security for Mac does not provide any means of scheduling a scan, which we consider an omission.

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks were as follows:

EICAR.COM test file manual download: the following dialog box is displayed:



Clicking Block prevents the file from being downloaded.

EICAR.COM test file drive-by download: the same dialog box as above is shown, and again clicking Block prevents the download.

EICAR potentially unwanted application: the program was downloaded without any sort of action or message from Kaspersky Anti-Virus for Mac. Kaspersky is shown among the vendors supporting this feature, though we assume this only applies to Windows versions.

AMTSO phishing test page: a warning message, very similar to the one above, was shown; clicking Block prevented the page from being shown.

CloudCar testfile: The familiar warning dialog was again shown, and again clicking Block prevented the download.

Real-time protection test: As soon as we plugged a USB flash drive containing Mac malware samples into our test computer, Kaspersky warned that threats had been detected.

We found the warning messages provided by Kaspersky Security to be perfectly clear. However, we note that in the warning dialog displayed when malware is detected, the options "Block" and "Allow" are equally prominent; we would suggest that Block should be made the clear default option.

### Malware protection/detection test

In our scan tests, Kaspersky Security identified all the malware samples, both Mac and Windows, used in our tests.

### Help and documentation

There is a comprehensive 64-page manual for Kaspersky Security for Mac, which can easily be downloaded from the manufacturer's website. It has been produced to the same excellent standard found in other Kaspersky documentation. The text has been appropriately bookmarked, making it easy to find sections from Adobe Reader's Bookmarks Bar, and the contents page has been hyperlinked to enable the reader to go straight to the page or section concerned. The manual has been clearly written and is suitably illustrated with screenshots.

There is also a searchable online knowledge base, with a range of FAQs (frequently asked questions). Answers given are clear, comprehensive and well illustrated with screenshots.

Overall, we found the help and documentation provided for Kaspersky Security for Mac to be excellent.

#### **Additional feature: Virtual keyboard**

Kaspersky's virtual keyboard is an additional security feature. It appears when the user moves the cursor into the password box of a website login field. With the exception of some (irrelevant) function keys, its design accurately mimics that of the physical Mac keyboard:



The virtual keyboard allows the user to enter passwords without any danger of a keylogger capturing the content, as the physical keyboard is not used at all. We were impressed to see that the virtual keyboard never appears in the same place twice; each time it is used, it appears in a different position on the screen, which also defends against mouseloggers. A button in the bottom left-hand corner shows the current language setting; clicking on it allows the user to change between a number of common European language layouts. As soon as login is completed (or the cursor is moved to a different field), the virtual keyboard disappears again. The automatic display of the keyboard when the cursor moves to a password field can be deactivated, though we do not think it would interfere with users who prefer to use a physical keyboard to enter passwords. We would describe the virtual keyboard as a simple, effective and very well thought-out security feature. Our only suggestion for improvement would be to display an explanation message the first time it is used.

#### **Summary**

Kaspersky Security for Mac is a highly effective antivirus program that receives our Approved Security Product award. The interface is very largely clear and easy to use, and the virtual keyboard is a valuable added security feature. Our only significant suggestion for improvement would be to enable scheduled scanning.



## Quick Heal Total Security for Mac



### Introduction

Quick Heal Total Security 2013 for Mac is a straightforward antivirus program.

Nature and size of the installer: 258MB full installer

### Installation

The installer includes a page with a summary of the program's functionality, system requirements and known issues, as well as a link to the support forum and advice on keeping the Mac OS X up to date. There are no options provided in the setup routine, other than whether to register (activate) the program immediately.

After installation, the program updates itself automatically (although this is done silently). We found the installation process to be quick and simple.

Quick Heal Total Security for Mac can be uninstalled very easily using the uninstaller program provided in the setup package.

### Program interface

The main program window includes a very obvious status display, in the form of a grey horizontal bar towards the top of the window, with a small graphic of a Mac. If all is well, a tick (checkmark) on a green background is shown, along with the text "System is secure. System is being actively protected. No action required". There are also individual green buttons specific areas of protection: Virus (real-time), Browsing, Phishing, Email and Spam Protection, as shown below:



If the real-time protection is disabled, the button for Virus Protection turns red, and the status bar text and graphic change to a warning. An obvious “Resolve Now” button appears; clicking this immediately reactivates the protection.



We found the status display, warnings and “Resolve Now” button to be excellent. We were a little surprised to see ladybirds (ladybugs) used to indicate a threat, as these are an ecologically safe method of pest *control*, not pests.

The manual update feature can be found in the Quick Heal Total Security menu in the Mac Menu Bar; we were surprised that this was not more obviously positioned in the main window. However, the automatic update logs show that the software checks for updates approximately every 15 minutes, i.e. very frequently. A very obvious “Scan My Mac” button can be found in the bottom left-hand corner of the main program window, which provides the options of a full scan or custom scan.

The program’s local help consists of a 52-page manual in .pdf format, which can be accessed from the Help Menu in the Mac Menu Bar.

Subscription information can be found by clicking Quick Heal Total Security, About... in the Mac Menu Bar. Again, we felt this could have been a made a little more obvious.

Quick Heal does not add an entry to the Finder context menu, so scans have to be started from the program window.

We found the overall design of the program to be very clear and uncluttered, with a very clear status display and warnings. However, we feel that adding the update function and subscription information to the main window would be an improvement.

### Non-administrator access

When logged on with a non-administrator account, we were able to deactivate the real-time protection without providing any additional credentials. However, we were not able to uninstall the program.

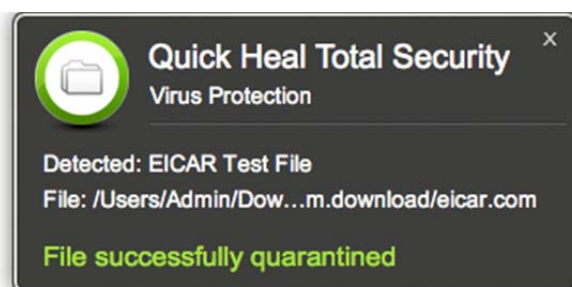
### Scheduled scanning

A scheduled scan is not set by default in Quick Heal Total Security, although it is fairly straightforward to configure this by clicking on Mac Security, Scheduled Scans.

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks were as follows:

EICAR.COM test file manual download: A clear warning message indicates that the file has been quarantined:



A file by the name of eicar.com.download is found in the Downloads folder. Clicking on it produces a message from Mac OS X that it is not a valid download file.

EICAR.COM test file drive-by download: as for the manual download above

EICAR potentially unwanted application: the web page is blocked, and Quick Heal displays a warning message. The file is not downloaded.

AMTSO phishing test page: Access to the page is blocked, and a warning message shown:



CloudCar testfile: the file is downloaded without any sort of warning. Quick Heal is not among the vendors listed as supporting the test.

Real-time protection test: when we inserted a USB flash drive into our test Mac, Quick Heal immediately began recognising and quarantining the malware, even before a Finder window had been opened.

We found Quick Heal's warning messages to be clear and appropriate.

### Malware detection

Quick Heal identified half of our Mac malware samples. This is a disappointing result for a program designed to protect Mac computers against malware. We sent the manufacturers the missed samples after the test, and the program now detects all of them.

Quick Heal Total Security for Mac did produce a perfect score with Windows malware, detecting all samples in the test-set.

### Help and Documentation

The program's local Help feature, accessed from the Help menu in the Mac Menu Bar, is a 52-page manual in .pdf format. It is very comprehensive, and covers installation, registration and use of the program. There is a clickable index page, and the document has been well bookmarked, making it easy to find a section from Adobe Reader's Bookmarks Bar. Our only criticism is that there are absolutely no screenshots.

There is an FAQ section of the Quick Heal website for "Quick Heal Total Security", although as far as we could see, this only applies to the Windows version.

Whilst we found Quick Heal's help to be good as far as it goes, we feel it could be improved by having a searchable online knowledge base for the Mac version.

### Summary

We found the interface of Quick Heal Total Security for Mac to be clear, simple, and easy to use, even if we could suggest some minor improvements. Whilst detection of Windows malware is excellent, we are concerned by the fact that the program did not protect against all the malicious Mac samples used in the test, and for this reason, we are not able to give it our Approved Security Product award.

We note, however, that Quick Heal Total Security for Mac is a brand new product, and expect that more experience will allow the manufacturers to improve it.

## Sophos Anti-Virus for Mac Home Edition



### Introduction

Sophos Anti-Virus for Mac Home Edition is a straightforward antivirus program. Nature and size of the installer: 78MB full installer

### Installation

The downloaded package includes not only the installer, but also an .html document entitled "Before You Install". This provides links to the Sophos forum and Facebook page, along with a warning that Sophos does not provide telephone or email support.

The installer also includes a "read me" page with more information about the program (e.g. help and deinstallation), plus a licence agreement to accept, and the option to change the installation location. There is a further information page at the end of the installer:



We found the installation process very straightforward, and consider the information pages at the beginning and end to be helpful. There is an uninstaller provided (Sophos Remove, in the Applications folder) which can be used to easily remove the program.

### Program interface

The program interface of Sophos Anti-Virus for Mac could fairly be described as "minimalist"; it appears to be more like a dialog box than a window:

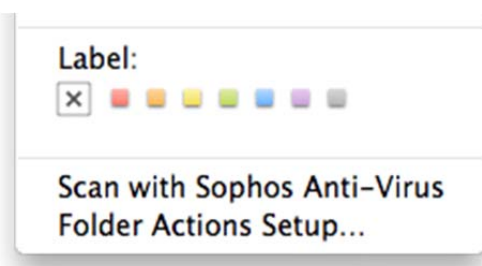


There is no status display (of real-time protection or updates) in the window. In the event that real-time protection is disabled, the only indication is that the Sophos icon in the Mac System Tray becomes light grey rather than the usual black. Whilst the information page at the end of the installation process points out that protection is enabled when the icon is black, we nonetheless feel that this is very ineffective as a warning and would be overlooked by all but the most diligent users. The menu that appears when the icon is clicked will indicate "On-Access Scanning is Disabled" when appropriate, although there is no obvious means of correcting this. The user has to open the Preferences dialog and reactivate the protection there. The status of updates can be found by clicking the Sophos System Tray icon and then Show AutoUpdate Window.

The Sophos Anti-Virus window does include buttons for a full scan and custom scans. There is also information about the last scan run and threats found, along with a button for Quarantine Manager.

The help feature is accessed from the Help menu in the Mac Menu Bar. It opens a search box which can be used to query the local help service. There is no subscription information as Sophos Anti-Virus for Mac Home Edition is a free product.

Sophos adds a scan entry to the Finder context menu, so that folders can be scanned by right-clicking:



Overall, we would describe the user interface as being somewhat too minimalist, and suggest that a status display for real-time protection and updates, along with an "update now" button, would be valuable additions to the main program window.

### Non-administrator access

We were unable to disable real-time protection or uninstall the program without administrator rights.

### Scheduled scanning

A scheduled scan is not set by default, but any custom scan can easily be scheduled as part of the configuration process.

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks were as follows:

EICAR.COM test file manual download: the file was quarantined and the following message displayed:



To delete the file from the Quarantine Manager, we had to enter the administrator password, which we felt was an unnecessary complication.

EICAR.COM test file drive-by download: the file was quarantined, and the same message displayed as above.



EICAR potentially unwanted application: the file downloaded successfully without detection by Sophos; scanning the Downloads folder afterwards did not detect the program either. Although Sophos is listed amongst the vendors supporting this feature, we assume this only applies to its Windows programs.

AMTSO phishing test page: We were able to open the phishing test page without any warning or action from Sophos. Again, Sophos is shown as supporting the feature, presumably only in Windows software.

CloudCar testfile: The file was quarantined and the same message shown as for the EICAR test file above.

Real-time protection test: Detection begins as soon as a USB stick with Mac malware is inserted.

#### Malware protection/detection test

Sophos Anti-Virus for Mac identified all the Mac malware samples in our test. It also detected all of the Windows samples we used.

#### Help and Documentation

Sophos produce a 48-page manual in .pdf format for Anti-Virus for Mac. It is comprehensive, covering updating, scanning for and dealing with threats, and uninstalling the program. There is a clickable contents

page, and the document has been well bookmarked, enabling easy access to any section from Adobe Reader's bookmarks bar.

The local help function is accessible via the query box in the Help menu, and provides clear and concise information on everyday tasks.

There is a very brief FAQ page on the Sophos website, along with a user forum for support.

Overall, we found the help functions to be more than adequate for a simple, free program.

#### Summary

Sophos Anti-Virus for Mac has excellent Mac malware recognition and earns an Approved Security Product award. Windows malware is also effectively detected. We felt the interface is rather minimalist, and could be made friendlier for non-expert users.

## KromTech MacKeeper



### Introduction

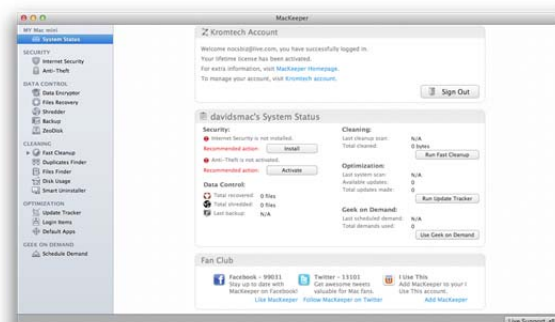
KromTech MacKeeper (previously known as ZeoBIT MacKeeper) is a comprehensive suite of Mac utilities; please see the *"Other features"* section for details.

Nature and size of the installer: 370KB downloader (downloads over 70MB)

### Installation

Installation is a very simple and quick affair, the only option being to change the drive on which MacKeeper is installed. Once setup has completed, the program has to be registered with an email address and licence key.

When the main program window is opened, a warning in the System Status section makes clear that the Internet Security component of MacKeeper is not installed by default, and has to be added as an extra:



This involves merely clicking *"Install"* and entering the administrator password; the installation then completes in less than a minute.

We found installation of MacKeeper to be very straightforward, despite the extra step for the setup of Internet Security.

The program does not have an uninstaller visible, but the online manual provides clear deinstallation instructions.

## Program interface

The Status page of the program only indicates whether the Internet Security component is installed, not whether it is up to date, real-time scanning is on or if a scan has been run recently. Immediately after installation, the Internet Security page indicates that a scan needs to be run, but does not show any kind of warning even if all the protection components are switched off. After the scan has been run, no further warnings can be seen on the Internet Security Status page. On investigating the status of individual components, we were very surprised to see that real-time antivirus protection is not enabled by default, and the program only recommends switching it on if the user works with Windows files or a Windows emulator. Given the existence of Mac botnets created by Trojans such as Flashback, we consider it inappropriate to suggest that real-time protection is not necessary to protect the OS X operating system. We also find it incompatible with the claim on the Status page that *"MacKeeper makes the Internet a safer place by blocking all threats and vulnerabilities automatically"*. We note that when activated, MacKeeper's real-time protection can instantly detect and protect against Mac malware samples, hence our surprise that it is not activated by default.



There is a *"Check for Update"* button on the Internet Security Status page. Clicking it has no very obvious effect, that is to say there is no progress report or message that the program is up to date. Observant users will however notice that the date/time shown

under *"Last check for update"* in the status area at the top has been updated.

Clicking on the *"Antivirus Scan"* allows either full or custom scans to be run.

We could not find any form of subscription information in the MacKeeper window. To find out when the subscription expires, the user has to open a web browser and log in to the KromTech account. We find this inconvenient, and, given the lack of warnings about the antivirus status, potentially risky. It would seem very easy for the licence to expire, and updates to cease, without the user realising it.

Clicking *Help/MacKeeper Help* in the Mac Menu Bar opens the local help function. MacKeeper installs its own icon in the Mac System Tray, which can be used to open the program, start scans, and switch real-time protection features on and off:



There is no MacKeeper item added to the Finder context menu, so scans have to be started from the program itself.

Our overall opinion of the program interface was that the Internet Security component does not have an especially prominent position within the suite, and that real-time protection has a very subordinate role within Internet Security. Hence, we feel that although the suite is capable of protecting the Mac effectively, neither its interface nor



its default configuration has been designed to do this effectively.

### Non-administrator access

We found that we could disable MacKeeper's real-time protection using a non-administrator account, without having to enter any additional credentials. This is perhaps not surprising, given that KromTech do not assign great importance to real-time protection anyway. We were not able to uninstall the program without administrator credentials.

### Scheduled scanning

A scheduled scan is not set by default, but can easily be configured using the Antivirus Schedule tab. It is not clear what happens if a scheduled scan is missed.

### AMTSO Feature Settings Checks

Results for the AMTSO Feature Settings Checks (with RTP enabled) are shown below. Please note firstly that we switched on the real-time antivirus protection before conducting the tests, and secondly that KromTech is not shown amongst the vendors supporting any of these tests.

EICAR.COM test file manual download: the file is downloaded, but "locked"; a message asks what action to take:

EICAR.COM test file drive-by download: the file was downloaded, but treated as above.

EICAR potentially unwanted application: file is downloaded without any warning.

AMTSO phishing test page: page opens without any sort of warning or message.

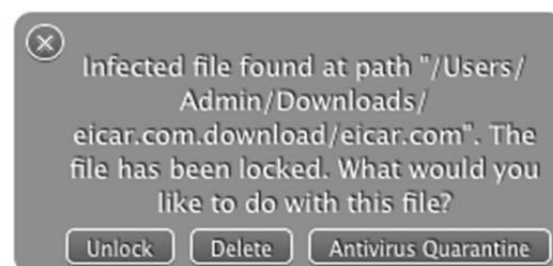
CloudCar testfile: the file is downloaded without any sort of warning.

When we attempted to copy Mac malware from a USB flash drive onto our Mac's Desktop, KromTech's real-time protection detected the malware.

We found KromTech's warning messages to be good, as far as they go.

### Malware protection/detection test

KromTech identified all the samples of Mac malware, and all but two of the Windows malware samples, used in our tests.



### Help and Documentation

The local help feature, accessed by clicking Help\MacKeeper Help in the Mac Menu Bar, provides an overview of various functions available in MacKeeper; it should be noted that only one of these is relevant to the Internet Security component. Clicking this item, "Protecting your Mac with Internet Security", opens a Flash video in a browser. This video takes the user through the basic functionality of the program, including scanning for and removing malware. We found this video to be simple but informative, a good introduction to the essentials of the program. The program's own webpage has a link entitled "Manual" on the Support page; this opens a page with links to detailed descriptions of individual functions, such as setting a scheduled scan. We feel the instructions given are clear and simple, and very well illustrated with screenshots. Our only reservation about the Help facilities in MacKeeper is that the detailed instructions are not directly accessible from the main program window.

### Other features

The MacKeeper suite includes a wide range of other components: Data Control (Data Encryptor, Files Recovery, Shredder, Backup, ZeoDisk cloud storage); Cleaning (Fast Cleanup, Duplicates Finder, Files Finder, Disk Usage, Smart Uninstaller); Optimization (Update Tracker, Login Items, Default Apps);

Geek on Demand (online support). We did not test any of the additional features, as the review concentrates on malware protection.

### Summary

KromTech's Internet Security is an effective security program for the Mac, which protects against Mac malware and intercepts Windows malware too. It has all the essential functionality of a good antivirus program. Consequently, it receives our Approved Security Product award. However, it should be noted that it is only one component of many within MacKeeper, and is arguably assigned a minor role within the suite, given that it is not even installed by default and has to be added afterwards. We were very surprised to see that real-time protection is not enabled by default, and that the program itself states that it is only necessary when working with Windows files, despite the fact that it effectively detects Mac malware when activated. The program interface also hides away elements such as subscription information, which we would expect to see more prominently displayed. Consequently, we feel KromTech Internet Security would be very well suited to enthusiasts who have a good understanding of security issues, but not ideal for non-expert users who need pre-configured optimal security for their Macs.

## Summary

Seven of the products we have reviewed receive our Approved Security Product award. Unfortunately, we were unable to give Quick Heal Total Security an award, due to misses in the Mac malware test at the time of testing.

The review covers protection against Mac malware, Windows malware detection, ease of use and help functions; potential buyers should also consider additional features and price before choosing a product. We always recommend installing a trial version of any product before making a purchase.

**Avira Security for Mac** is simple to use and effectively detects Mac malware. It is an ideal choice for anyone wanting a good basic antivirus program for free. Windows malware detection is also included.

**ESET Cyber Security Pro** is a full security suite with firewall and parental control functions. Its recognition of Mac malware is excellent, and the clarity of its interface and outstanding help features make using the program very comfortable. The program also recognises Windows malware.

**F-Secure Anti-Virus for Mac** provides effective protection against Mac malware, in a familiar interface.

**Intego Premium Bundle for Mac** provides virus protection, a firewall, parental controls, backup, identity protection and privacy controls. VirusBarrier has a simple, modern interface, and protection against Mac malware is excellent.

**Kaspersky Security for Mac** includes parental controls and a virtual keyboard as well as antivirus. Its recognition of Mac malware is first rate, while interface design and help features are both of a very high standard. The program includes Windows malware detection.

**Sophos Anti-Virus for Mac Home Edition** is a free program that provides effective protection against Mac malware. Its minimalist interface may be best suited to expert users. Windows malware is also detected.

**KromTech MacKeeper Internet Security** is part of the very comprehensive MacKeeper suite, which is well suited to Mac experts and enthusiasts. Its detection of Mac malware is excellent. Windows malware detection is also included.



FeatureList Mac (as of July 2013)	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL
Product name:	Avira Free Mac Security	ESET Cyber Security Pro	F-Secure Anti-Virus for Mac	Intego Mac Premium Bundle	Kaspersky Security for Mac	Quick Heal Total Security	Sophos Antivirus for Mac Home Edition	KromTech MacKeeper
Supported operating systems:	Mac OS X 6 and higher	Mac OS X 6 and higher	Mac OS X 6 and higher	Mac OS X 6 and higher	Mac OS X 6 and higher	Mac OS X 6 and higher	Mac OS X 6 and higher	Mac OS X 5 and higher
Supported Program languages:	English, German	English, Spanish, French, German, Chinese, Russian, Polish, Portuguese, Italian, Dutch, Swedish, Finnish, Danish, Norwegian, Thai, Japanese, Slovak, Czech, Turkish, Korean, Hungarian	English, Chinese, Czech, Danish, German, Greek, Spanish, Estonian, Finnish, French, Hungarian, Italian, Japanese, Dutch, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Swedish, Turkish	English, German, Japanese, Spanish, French	English, French, German, Russian, Spanish, Italian, Portuguese, Norwegian, Japanese, Chinese, Polish	English	English, German, Spanish, French, Japanese	English, French, German, Japanese, Spanish, Italian, Dutch, Russian, Portuguese, Danish, Swedish, Korean, Finnish, Czech, Norwegian, Polish, Chinese, Turkish
<b>Protection</b>								
Real-Time protection	●	●	●	●	●	●	●	●
On-demand scanner	●	●	●	●	●	●	●	●
Detects also threats for other platforms (e.g. Windows malware)	●	●	limited detection of windows threats	limited detection of windows threats	●	●	●	●
Scheduled On Demand Scan	●	●		●	●	●	●	●
Quarantine	●	●		●	●	●	●	●
Whitelisting for specific files/folders		●		●	●	●	●	●
Cloud Scanning (requires internet connection)		●			●		●	
Scheduled Update	●	●	●				●	
Prevent access to malicious and phishing web sites (which browsers are supported?)					Safari, Chrome, Firefox	All	Safari, Chrome, Firefox, Opera, OmniWeb, Cruz, curl, wget	All
Mail Protection		●		●	●	●		
Safe search (which browsers are supported?)				All	Safari, Chrome, Firefox			
Statistics		●		●	●			●
Eventtriggered Tasks		●		●	●			●
Firewall		●		●				●
Block all network traffic		●	●	●				
Applications Audit / Security info about installed programs		●		●				
<b>Parental Control</b>								
Explicit URL blocking/allowing		●		●	●	●	●	●
Category blocker for website contents		●		●	●	●		
Daily Internet time limit and scheduled Internet access				●	●	●		
Age profiles		●		●				
Log all visited URLs				●	●			
Personal data blocker & Social network control					●			
<b>Support</b>								
User manual	●	●	●	●	●	●	●	●
Online Help and User Forum	●	●	●	●	●		●	●
Email and Phone Support	●	●	●	●	●	●		●
Online Chat	●			●	●	●		●
Supported languages (of support)	English, German, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malay	All	English, Finnish, French, Dutch, Danish, German, Chinese, Italian, Norwegian, Polish, Swedish	English, French, Japanese	English, French, German, Russian, Spanish, Italian, Japanese, Chinese, Polish, Dutch, Turkish, Portuguese, Arabic	English, Hindi, Marathi, Tamil, Telugu, Malayalam, Japanese	N/A	English
<b>Additional features</b>								
Removable media blocking		●		●				●
Backup (including scheduled data backup)				●				●
Anti-Theft (Remote location, remote snapshot of thief)								●
Keep programs up-to-date (report new versions of third-party programs)								●
Game/Presentation mode		●						
Taskmanager (display running processes)		●						
Mac optimization utilities (remove junk files, uninstall programs, recover deleted files, file shredder, disk usage stats, etc.)				●				●
<b>Price (may vary)</b>								
Price 1 Mac / 1 year (USD/EUR)	FREE	USD 45 / 35 EUR	USD 30 / 20 EUR	USD 80 / 60 EUR	USD 60 / 40 EUR	USD 55 / 50 EUR	FREE	USD 40 / 30 EUR
Price 2 Macs / 2 years (USD/EUR)	FREE	USD 80 / 60 EUR	USD 120 / 80 EUR	USD 320 / 220 EUR	USD 240 / 160 EUR	USD 220 / 200 EUR	FREE	USD 80 / 60 EUR

## Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. 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 e.V., prior to any publication. AV-Comparatives e.V. 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 e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (August 2013)