Independent Tests of
Anti-Virus Software

Mac Security Test & Review

TEST PERIOD: JUNE 2019
LANGUAGE: ENGLISH
LAST REVISION: 20TH JUNE 2019

WWW.AV-COMPARATIVES.ORG

Contents

Macs and Security Software

It is an often-heard view that macOS computers don't need antivirus protection. Whilst it is certainly true that the population of macOS malware is very tiny compared to that for Windows and Android, there have been instances of macOS malware[1] getting into the wild. Moreover, Apple Mac security needs to be considered in the wider context of other types of attacks[2].

In addition, it should be noted that Apple themselves ship some anti-malware capabilities within macOS. Firstly, there is "Gatekeeper", which warns when apps without a digital signature are run. Then there is "XProtect", which checks files against known-malware signatures. Finally, Apple provide the MRT (Malware Removal Tool). Gatekeeper and MRT are essentially invisible to users and have no direct user interface for the user. System updates are installed automatically using the update process. The effectiveness of Apple's built-in anti-malware features have been questioned[3], however, and some security experts recommend strengthening the defences by adding in a third-party antivirus package. There are many good reasons for this. Firstly, the approach taken by Apple might be adequate for well-established malware, but might not respond quickly enough to emerging threats. Secondly, you might want a broader base of malware evaluation. Thirdly, macOS is not immune to bugs. This year, researchers at AV-Comparatives found a security-related flaw in Apple's operating system. Details are given later on in this report.

Some vendors' macOS security products can detect malware aimed at other operating systems too. Hence an AV program on your macOS computer could effectively handle Windows and Android malware too. Of course, there is no method by which Windows or Android malware could directly infect a macOS device. However, there are scenarios where you might well benefit from scanning for such threats. For example, if you are given a USB stick of photos by one friend, who asks you to make a copy for a second friend. They both use Windows, but you are using a macOS computer. There is Windows malware on the USB stick, and you make a copy of all the files. In this scenario, it is useful to be able to ensure that malware is not inadvertently passed on from one friend to another, even if your own machine is not at risk.

Mac security programs can offer other capabilities too. For example, browser extensions can identify web sites which are potentially phishing locations. Readers should note that Mac users are just as vulnerable to phishing attacks as users of e.g. Windows, as phishing sites function by deceiving the user rather than by altering the operating system or browser.

Other packages might offer VPN (virtual private network) capabilities which can be useful when you need to operate your computer in an untrusted environment, or a public location such as an Internet café, where you are not sure of the integrity of the connection. You might also want to replace macOS' built-in parental control capabilities with third party tools, if you believe this is more appropriate to your family needs.

[1] https://www.macworld.co.uk/feature/mac-software/mac-viruses-malware-security-3668354/
[2] http://www.itpro.co.uk/malware/31443/dumb-malware-targets-macos-devices-by-getting-cryptocurrency-users-to-infect
[3] https://business.blogthinkbig.com/antimalware-xprotect-macos/

Before purchasing a Mac security solution, you also need to decide on the size and scope of the protection you wish to deploy. It might be for a single computer, or for a laptop and desktop. Or you might have a family environment. There might be a mixture of macOS laptops and desktops, but also other devices too like Windows desktops and laptops, along with iOS and Android phones and tablets. For this environment, a broader and more flexible licensing package might well be appropriate.

This could allow you to purchase e.g. 5 licenses and then distribute them amongst your collection of devices. It could also give you the flexibility to transfer licensing from one device to a new item, e.g. if you need to replace an aging Windows laptop with a new MacBook. Some packages offer cloud-based management interfaces. Usually this is to cover the licensing of the packages, but some can also be used to initiate malware scans and device updates and manage parental control capabilities.

Then there are packages which are really aimed at the business and corporate space. Here the macOS support is but one component of a much larger deployment and management infrastructure. This will cover all devices and operating systems, often running thousands of managed devices. Although it might be tempting to go for a larger and stronger solution than is appropriate for your organizational size, be aware that the larger platforms have significant up-front design, management and deployment overheads. This is required to allow these tools to scale to the sizes that they can support, and they usually bring in a level of day-to-day commitment which, although entirely proper and required in a larger enterprise, is simply beyond the capabilities and resourcing of a small company.

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

Readers who are concerned that third-party security software will slow their Mac down can be reassured that we considered this in our test; we did not observe any significant performance reduction during daily operations with any of the programs reviewed.

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

1. Do not use an administrator account for day-to-day computing
2. Keep your Mac operating system and third-party software up-to-date with the latest patches
3. Use secure passwords (the Mac includes the KeyChain password manager)
4. Deactivate any services such as Airport, Bluetooth or IPv6 that you don't use
5. Be careful about which programs you install and where you download them from

Security bug in macOS found by AV-Comparatives in 2019

AV-Comparatives found a security flaw on macOS Mojave 10.14.4 and earlier versions, and reported the issue to Apple in March 2019. The issue allows Gatekeeper to be bypassed, and unsigned apps from outside the App Store to be executed. The method used does not require any specialist knowledge or programming ability. Anyone who can create, copy and rename folders in Finder could do it, with a few very simple instructions.

Apple recognized AV-Comparatives' discovery and released a security update for Mojave in mid-May 2019. However, at the time this report was published (late June 2019), the older versions (e.g. High Sierra) exhibiting the same flaw had still not been patched.

We will update this report as soon as patches for these are released.

APPLE-SA-2019-5-13-2
DesktopServices
Available for: macOS Mojave 10.14.4
Impact: A malicious application may bypass Gatekeeper checks
Description: This issue was addressed with improved checks.
CVE-2019-8589: Andreas Clementi, Stefan Haselwanter, and Peter Stelzhammer of AV-Comparatives

After finding the OS vulnerability, we repeated the test with different, well-known antivirus products for macOS installed. In all cases, the AV products blocked the threats that Gatekeeper had allowed to run. This demonstrates that it does make sense to use antivirus programs with macOS, as an AV program would have protected the system against the threats that had bypassed Gatekeeper.

A video showing the issue can be seen here: *(link will be provided as soon as bug is fixed; see above)*

Security Software for macOS Mojave

We have reviewed and tested the following products for this report, using the newest version available in June 2019:

- **Avast Security for Mac 13.12**
  https://www.avast.com/free-mac-security
- **AVG AntiVirus for Mac 19.0**
  https://www.avg.com/avg-antivirus-for-mac
- **AVIRA Antivirus Pro for Mac 3.10**
  https://www.avira.com/en/avira-antivirus-pro
- **Bitdefender Antivirus for Mac 7.3**
  http://www.bitdefender.com/solutions/antivirus-for-mac.html
- **CrowdStrike Falcon Prevent for Mac 5.10**
  https://www.crowdstrike.com/products/falcon-prevent/
- **Fortinet FortiClient for macOS 6.0**
  https://www.fortinet.com/products/endpoint-security/forticlient.html
- **F-Secure SAFE for Mac 17.5**
  https://www.f-secure.com/en/web/home_global/safe
- **Intego VirusBarrier X9 10.9**
  https://www.intego.com/mac-protection-bundle
- **Kaspersky Internet Security for Mac 19.0**
  http://www.kaspersky.com/security-mac
- **Trend Micro Antivirus for Mac 9.0**
  https://www.trendmicro.com/en_us/forHome/products/antivirus-for-mac.html
- **Webroot SecureAnywhere AntiVirus for Mac 9.0**
  https://www.webroot.com/us/en/home/products/antivirus-for-mac

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

Malware Protection Test

The Malware Protection Test checks how effectively the security products protect a macOS system against malicious apps. The test took place in June 2019, and used macOS malware that had appeared in the preceding few months. We used a total of 585 recent and representative malicious Mac samples.

In the first half of 2019, several tens of thousands of unique mac samples were collected. However, this figure includes many samples which could be classified as "potentially unwanted" – that is, adware and bundled software – depending on interpretation. Very many of the remaining (true malware) samples are often near-identical versions of the same thing, each with a tiny modification that just creates a new file hash. This enables the newly created file to avoid detection by narrow blacklist-based protection systems such as XProtect. There were in fact almost no new families, and only some dozens of really new variants, of true Mac malware seen in 2019. Some of these will only run on older versions of the macOS operating system. Consequently, the 585 samples used for the test represent an accurate guide to the current threat landscape, even if the sample size seems very small compared to what is commonly used for Windows.

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 most (if not all) of the threats, so the protection rate required for certification is relatively high (99%).

Before the test, the macOS systems were updated and an image created; no further OS updates were then applied. Each program was installed on the freshly imaged machine and the definitions updated to the 3rd June 2019. 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 recognized some of the samples. If available, we then ran a scan of the flash drive, either from the context menu or from the main program window. Samples found were quarantined or deleted. After this, any samples which had not been deleted or disabled by the real-time protection or scan were copied to the Mac's hard disk. These remaining samples were then **executed**, providing the security product with a final chance to detect the malware.

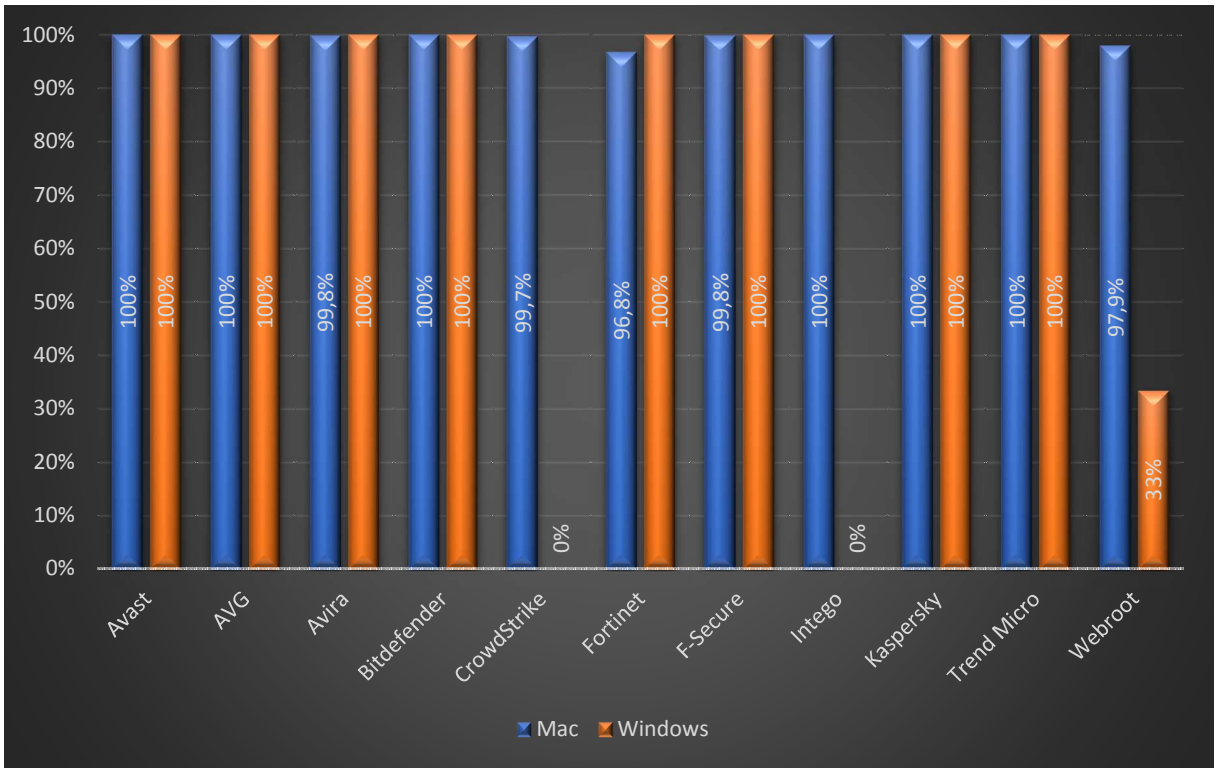
In addition to the Mac malware samples, we also scanned and executed a set of clean Mac programs to check for false positives. **None of the programs we tested produced any false alarms.**

Most of the Mac security products in our review claim to detect Windows malware as well as Mac malware, thus ensuring that the user's computer does not inadvertently act as a conduit for programs that could attack Windows PCs. For this reason, we also checked if the Mac antivirus products detect Windows malware. We used 500 prevalent and current 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 macOS.

We also check that the vendor's claims in the feature list they provide for this review are correct. As part of this process, we verify that any claims by vendors to detect potentially unwanted apps (PUA) are correct. However, this is not part of the test, and all the features reported to us in 2019 were verified as correct.

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

Product	Mac Malware Protection 585 recent Mac samples	Windows Malware Detection on macOS[4] 500 prevalent Windows samples
Avast Security for Mac	**100%**	100%
AVG AntiVirus for Mac	**100%**	100%
Avira Antivirus Pro for Mac	**99.8%**	100%
Bitdefender Antivirus for Mac	**100%**	100%
CrowdStrike Falcon Prevent for Mac	**99.7%**	0%
Fortinet FortiClient for macOS	**96.8%**	100%
F-Secure SAFE for Mac	**99.8%**	100%
Intego VirusBarrier X9	**100%**	0%
Kaspersky Internet Security for Mac	**100%**	100%
Trend Micro Antivirus for Mac	**100%**	100%
Webroot SecureAnywhere AV for Mac	**97.9%**	33%



A list of antivirus programs for Mac can be seen here: https://www.av-comparatives.org/list-of-av-vendors-mac/

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

Summary

This year, the following Mac security programs receive our Approved Security Product award: **Avast**, **AVG**, **Avira**, **Bitdefender**, **CrowdStrike**, **F-Secure**, **Kaspersky** and **Trend Micro**.

Unfortunately, the products made by **Fortinet**, **Intego**, and **Webroot** did not reach certification standard this year. In the case of Fortinet and Webroot, this was due to missing the 99% protection rate against Mac malware. With Intego, although its protection score was 100%, we found a number of issues in the version available at time of testing.

A summary of the reviewed products is shown below. If you are thinking of getting a security product for your Mac, we recommend that you consider also other factors, such as price, additional features and support, before choosing a product. We also recommend installing a trial version of any paid-for product before making a purchase.

Avast Security for Mac is a simple, easy-to-use antivirus program for home users. It uses the "freemium" model, i.e. some features are only available in the paid-for premium version.

AVG AntiVirus for Mac is a consumer antivirus program that is easy to set up and use. It also uses the freemium model.

Avira Antivirus Pro for Mac is a straightforward antivirus product suitable for home users and small businesses. It is simple to install and use.

Bitdefender Antivirus for Mac is an antivirus product that includes ransomware protection. It has a very well-designed interface and excellent user manual, and is suited to home users and small offices.

CrowdStrike Falcon Prevent for Mac is part of an endpoint protection package for enterprise networks. It has no user interface on client machines, and is managed using a web-based console.

Fortinet FortiClient for macOS is intended to be used in business networks. It has a fairly minimalist interface, and is intended to be managed using the FortiClient Enterprise Management Server console.

F-Secure Safe for Mac is a security product for home users and small offices. It includes a parental control feature, and is simple to install and use.

Intego VirusBarrier X9 is an antivirus program targeted at small businesses, although it is also included in Intego's consumer security suites. On macOS Mojave, we found some unexpected behaviour while using the product.

Kaspersky Internet Security for Mac is a consumer security product with parental controls. It is suitable for home users and small offices. Its interface is well designed and easy to use.

Trend Micro Antivirus for Mac includes camera and microphone protection and an anti-ransomware feature, in addition to malware protection. It is suitable for home users and small offices, and ideal for non-expert users due to its very straightforward design and operation.

Webroot SecureAnywhere Antivirus for Mac is an antivirus program that is suitable for home and home office users. It is simple to use, and fast in operation.

AV-Comparatives' Certification requirements

AV-Comparatives have strict criteria for certifying security programs. These are updated every year to take new technological developments into account. Certification by AV-Comparatives indicates that a product has proven itself to be effective, honest, transparent and reliable.

Possible reasons why a product may fail certification are listed below, though this is not necessarily an exhaustive list.

- Poor Mac-malware detection rates (under 99% for Mac malware) or false positives on common macOS software
- Significant performance issues (i.e. slowing down the system) that have a marked impact on daily use of the system
- Failure to carry out essential functions, such as updating, scanning, detecting and deleting malware, reliably and in a timely fashion
- Being detected as PUA (or malware) by several different engines on multi-engine malware scanning sites (e.g. VirusTotal), either at the time of the test, or in the six months prior to it
- Scareware tactics in trial programs: exaggerating the importance of minor system issues, such as a few megabytes of space taken up by harmless but unnecessary files; fabricating security issues that do not exist
- Confusing or misleading functions, alerts or dialog boxes that could allow a non-expert user to take an unsafe action, or make them worry that there is a serious problem when in fact none exists
- Mac AV products must include real-time/on-access or on-execution scanning/protection. Providing only an on-demand scanner does not qualify for certification.
- For consumer products, very short trial periods (a few days only) combined with automatically charging for the product unless the user deliberately cancels the subscription. We regard 10 days as the minimum amount of time needed to assess a program
- "Trial" versions that do not make available all essential protection features such as real-time protection or ability to safely disable detected malware
- Untrue claims, such as stating that a macOS app also detects Windows malware, despite tests showing that detection of even prevalent Windows malware is (close to) non-existent
- Bundling of other programs or changing existing system/app preferences (e.g. default search engine), without making clear to the user that this is happening and allowing them to opt out easily

Review format

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

Summary

Here we describe the nature of the product and its features, including whether it is free or requires a subscription, and give an overview of our experience with it.

Installation

This describes how to get the product up and running on your Mac(s), starting with downloading the installer, and finishing with any post-setup tasks needed. These might include installing and allowing browser extensions, for example. We note any options available, and whether you have to make any decisions during installation. There is also a note on how to uninstall the product, should you need to.

Finding essential features

Here we consider how easy it is to find the most important functionality in each program: status, update, different types of scan including scheduled scans, subscription information (not applicable to free programs), quarantine, logs, settings and help.

Status alerts: It's important to know whether your security program is working properly. We look at how the current status is displayed, what sort of warning is shown if real-time protection is disabled, and how to correct this.

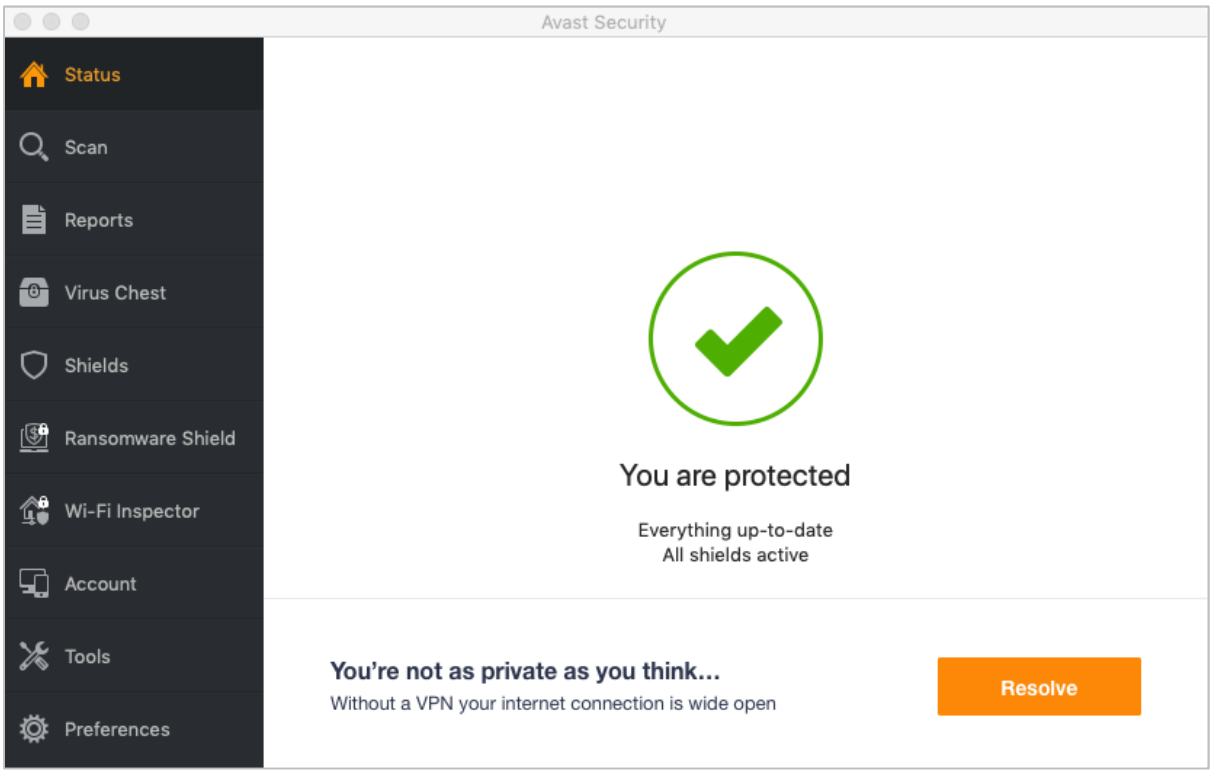
Behaviour on malware detection: We run a functionality test to determine how each program behaves when it encounters malware. This is entirely separate from the malware protection test, and is run on different systems. We connect a USB flash drive containing a few samples of common Mac malware, which all the tested programs are known to detect. Some security programs will automatically detect the malware without the user needing to do anything; if not, we attempt to copy the malware samples onto the Desktop of the currently logged-on user. We note at which stage the malware is detected, and what sort of alert is shown. For programs that do not automatically detect and delete/quarantine the malware when the external drive is connected, we attempt to run the malware directly from the external drive.

Quarantine and logs: We check the functionality that shows you which malicious items have been found, what information is provided about them, and what the options are for dealing with them (e.g. delete or restore).

Help: There is a brief description of each program's main help feature (accessible from the program interface)

Advanced Options: We check to see if both administrators and standard users can disable protection features, make scan exclusions, restore items from quarantine, or uninstall the program.

Avast Security for Mac



Summary

Avast Security for Mac is a free antivirus program with a password manager. The default installation includes a VPN service, but you have to pay for this to use it beyond a 7-day trial period. The program is very simple to install, and most common features are easy to find in the clean, well-laid out GUI. Avast Security has highly effective on-access protection, which instantly detects any malware and prevents it being copied to the system. Suggestions for improvement would include a "Fix-All" button to resolve issues such as disabled protection, and an update button on the home page. We felt that the advertising displayed for Avast SecureLine VPN service rather overstated the risks of using a standard unencrypted Internet connection.

Installation

To set up Avast Security on your Mac, you just download and run the installer file, then double-click *Avast Security*. There are no decisions to make. You can opt out of installing the password manager and VPN functions, and change the installation folder, if you so choose. The installer file also includes an uninstaller, should you need to remove the program for any reason.

Finding essential features

Status, **scan options**, **quarantine** (*Virus Chest*), **logs** (*Reports*) and **settings** (*Preferences*) are all found in the left-hand menu bar in the main program window. **Subscription information** is not applicable, as the program is free. **Updates** can be run by clicking *Preferences, Updates* (as is standard for modern security programs, Avast Security for Mac runs automatic updates as well). You can **scan a drive, folder or** file from the Finder context menu, by clicking *Scan with Avast*. The help file is accessible from the *Help* menu in the Mac menu bar.

Status alerts

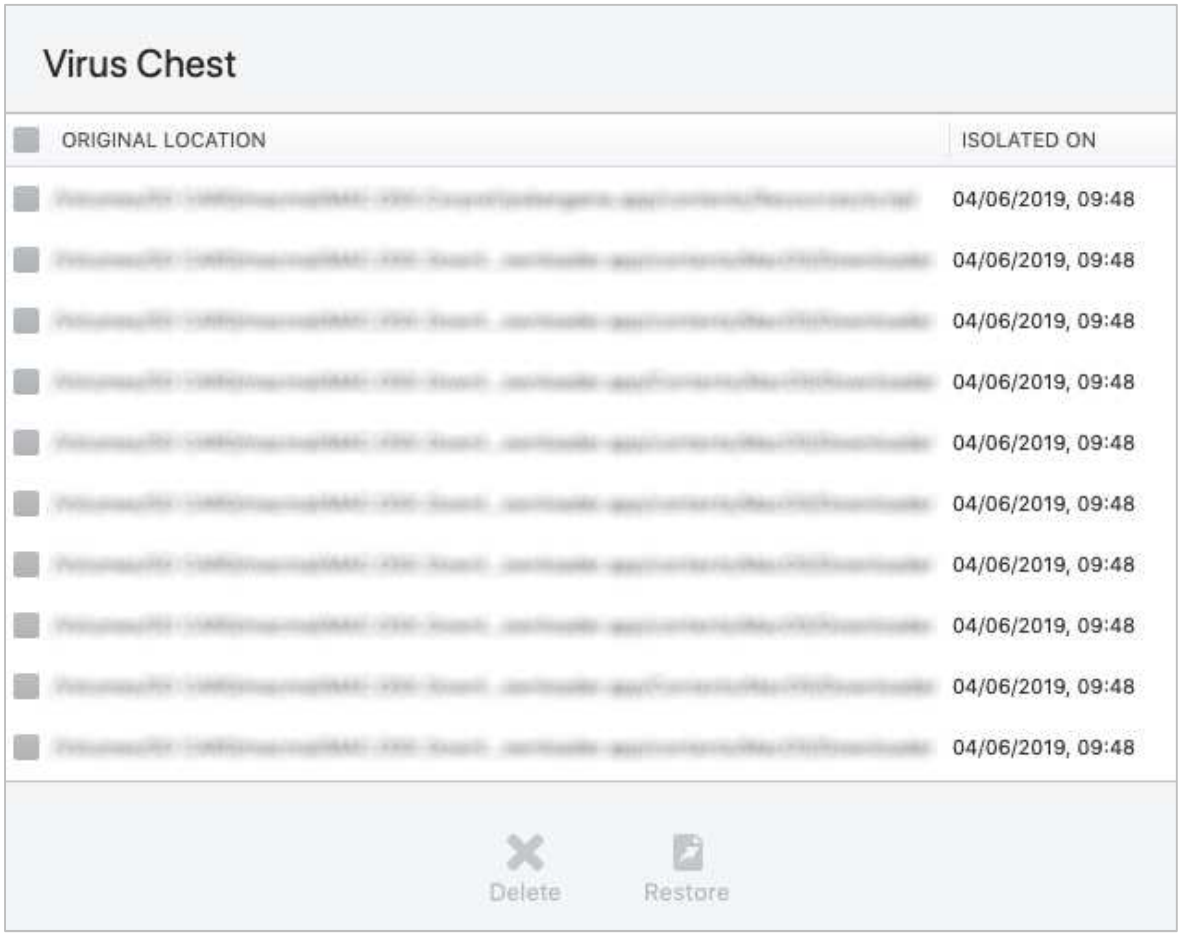
If a real-time protection is disabled, a warning is displayed on the *Status* page. To reactivate the protection, you need to go into *Preferences* and click *Shields\Enable*.

Behaviour on malware detection

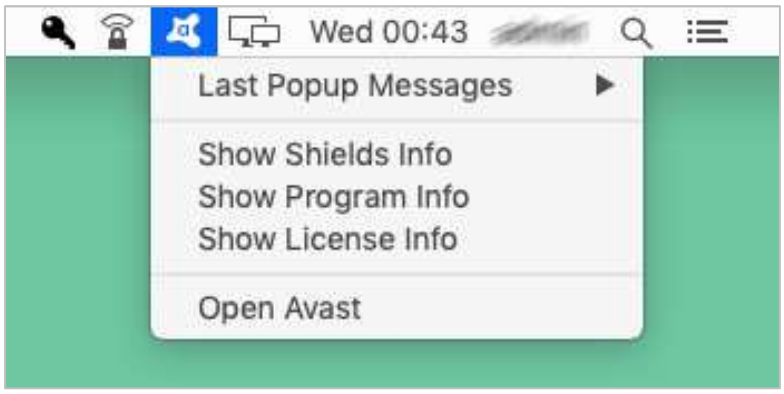
When you connect an external drive, Avast Security takes no action. However, as soon as you start browsing through folders containing malware, the on-access detection springs into action and starts detecting the malicious files. There is one alert box per discovered item. The alerts persist until you click on them. Clicking *Learn more* in the alert just opens an advertisement for the Pro version of the program.

Quarantine and Logs

Virus Chest displays files that have been quarantined, and allows you to delete or (with an administrator account) restore any/all items.



System Tray menu



Help

A help file with basic FAQs and clear, simple text answers is provided. You can open it from the *Help* menu in the Mac menu bar.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

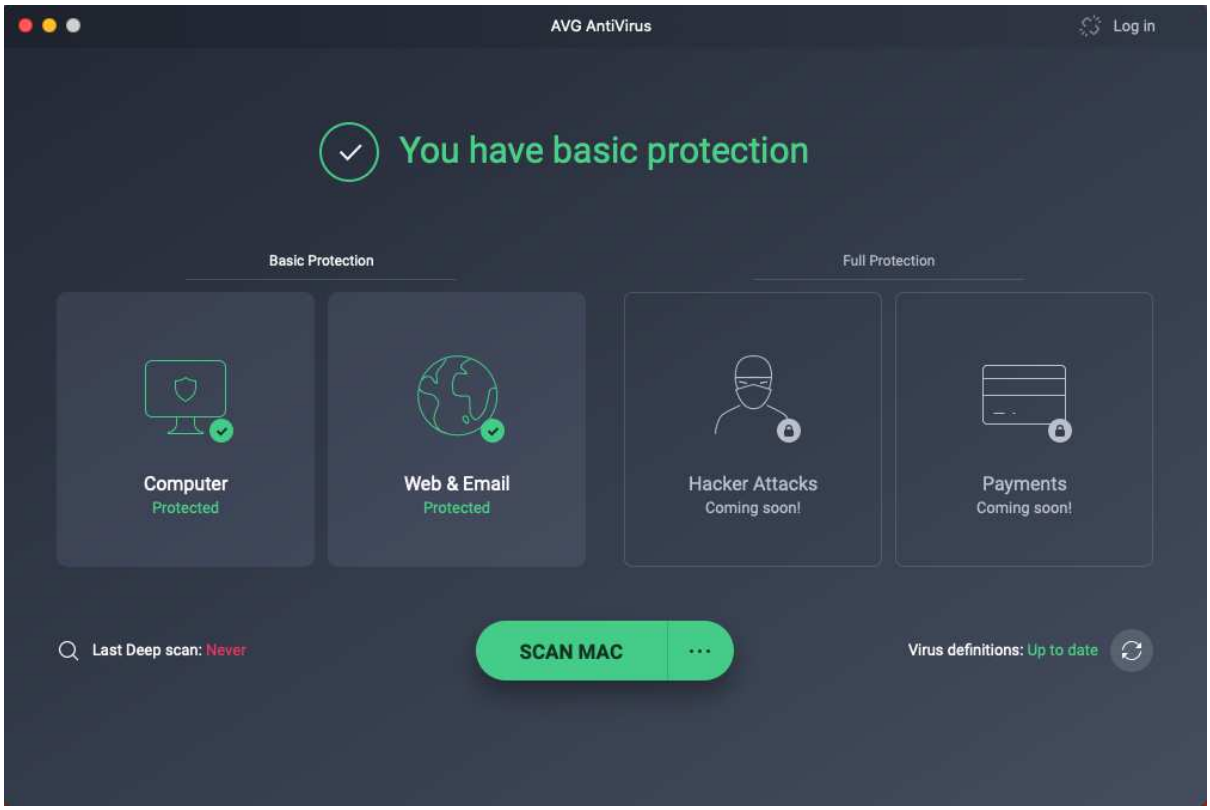
- Disable protection features Yes (under *Preferences\Shields*)
- Uninstall the program (using the *Uninstall* button in the installer file)
- Restore items from quarantine

Standard macOS users (i.e. accounts without administrator rights) cannot perform either of these tasks, which we regard as optimal.

Other points of interest

An advertising strip along the bottom of the main program window promotes Avast's paid-for SecureLine VPN service. If you click on the *Upgrade* button, the installation prompt page states "Your Internet connection is not secure and anyone can see what you're browsing".

AVG AntiVirus for Mac



Summary

AVG AntiVirus for Mac is a free antivirus program with web and email protection. The program is extremely simple to install and use, making it very suitable for non-expert users. It has all the essential features of a good antivirus program, and executes them all well. AVG's on-access detection dealt with malware samples on an external drive very effectively, and displayed a well-designed alert dialog box. We were able to find almost all the functions very easily. We do have one suggestion for improvement, however. The configuration options for the protection components are not found in the general settings dialog; you have to click the relevant tile on the home page to get to them. This was not immediately obvious to us. We felt that the advertising for AVG's paid VPN product somewhat exaggerates the risks of using a standard unencrypted Internet connection.

Installation

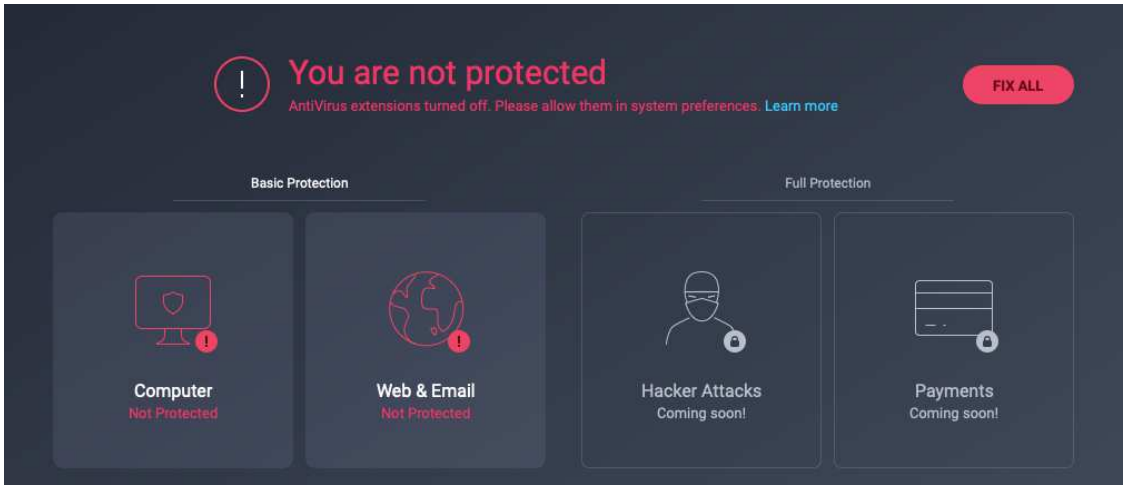
To set up AVG AntiVirus for Mac, just download and run the installer, and double-click *Install AVG AntiVirus*. The installation wizard is very simple. There are no decisions to make, but you can change the location of the installation folder if you want. You can uninstall the program by clicking *AVG AntiVirus* in the Mac menu bar, then *Uninstall AVG AntiVirus*.

Finding essential features

On the program's home page you can find **status**, **update**, **default scan** and **scan options**. You can scan a drive, folder or file by right-clicking it and clicking *Scan with AVG* in the Finder context menu. There is no means of setting a scheduled scan. You can open **quarantine** by double-clicking the *Computer* tile on the homepage. There is no separate log feature. **General Settings** can be found in the *AVG Antivirus menu* in the Mac menu bar, as is normal for macOS programs. **Protection settings** for the *Computer* and *Web & Email* components can be found by clicking their respective tiles on the home page. The **help** feature is also found in the menu bar. Subscription information is not applicable, as the program is free.

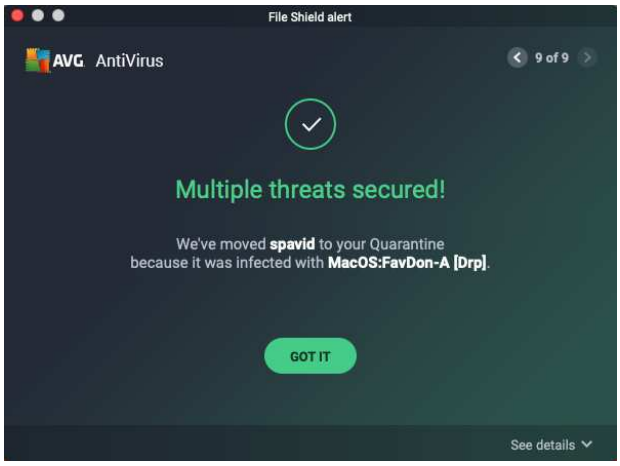
Status alerts

If real-time protection is disabled, very obvious red warning messages are shown on the home page. You can reactivate the protection by clicking *Fix All*.



Behaviour on malware detection

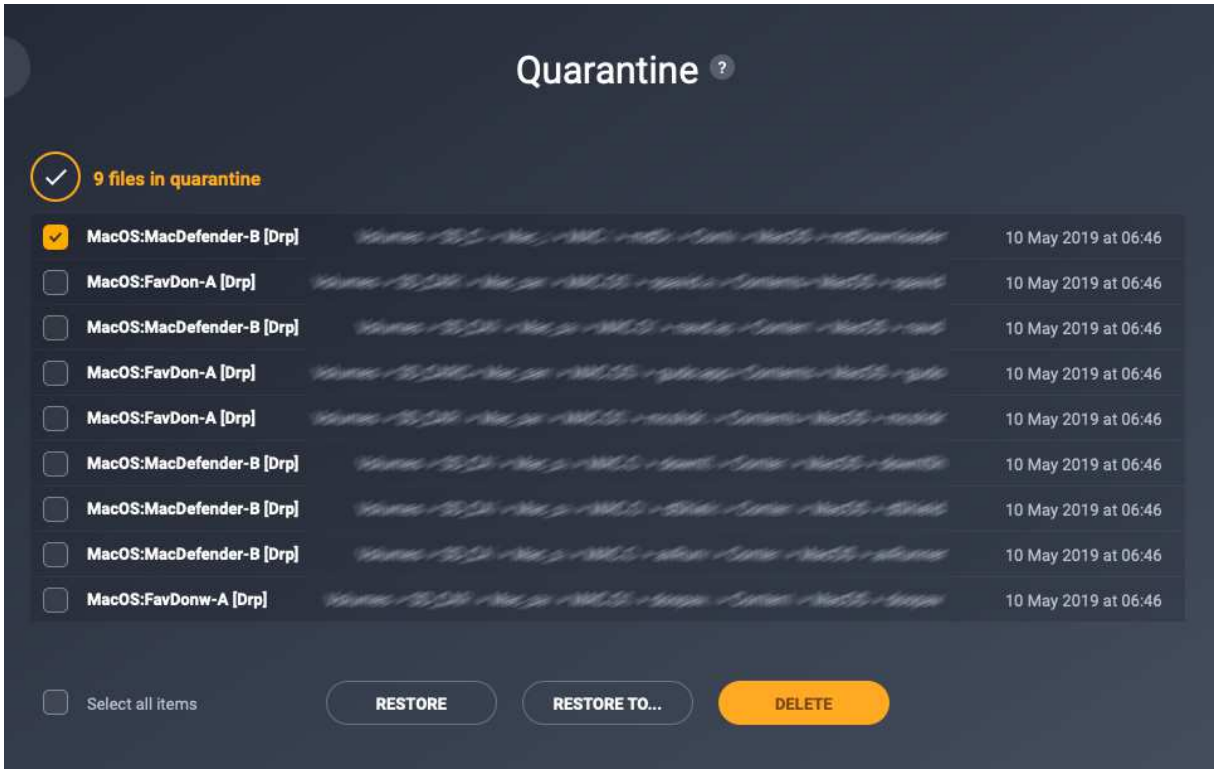
When you connect an external drive to your Mac, AVG does not take any action. However, if you open a folder containing malware in Finder, AVG's on-access protection immediately detects and quarantines the malicious files. The alert below is shown:



The alert persists until you close it. You can browse through the detected threats using the arrow buttons in the top right-hand corner. You can also get more information about each threat by clicking *See details* in the bottom right-hand corner. This area includes a convenient link to quarantine.

Quarantine/Logs

The quarantine and logs features are combined in the *Quarantine* window. Here, you can see a list of quarantined threats, along with the path to their original location, plus date and time of detection. You can delete or restore any or all items here. The "breadcrumb trail" used to show the location where the malware was detected uses a clever trick. Many of the steps in the trail are compressed, so as to fit the entire trail into the window. However, if you mouse over any compressed step, the text is expanded so that you can read it in full. No additional information about the detected malware is available, however.



System Tray menu

Help

Clicking *Help* in the Mac menu bar, then *Antivirus help*, opens a simple help file with basic FAQs, such as "How do I keep my Mac secure?" and "What is File Shield?". Simple but clear text answers are provided.

Advanced options

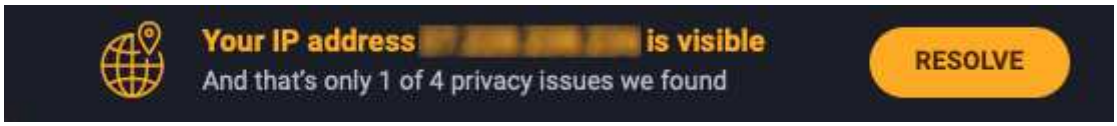
Power users with a macOS Administrator account can perform the following tasks (caution is advised):

- Disable protection features
- Make scan exceptions (*Preferences* dialog box)
- Restore items from quarantine
- Uninstall the program

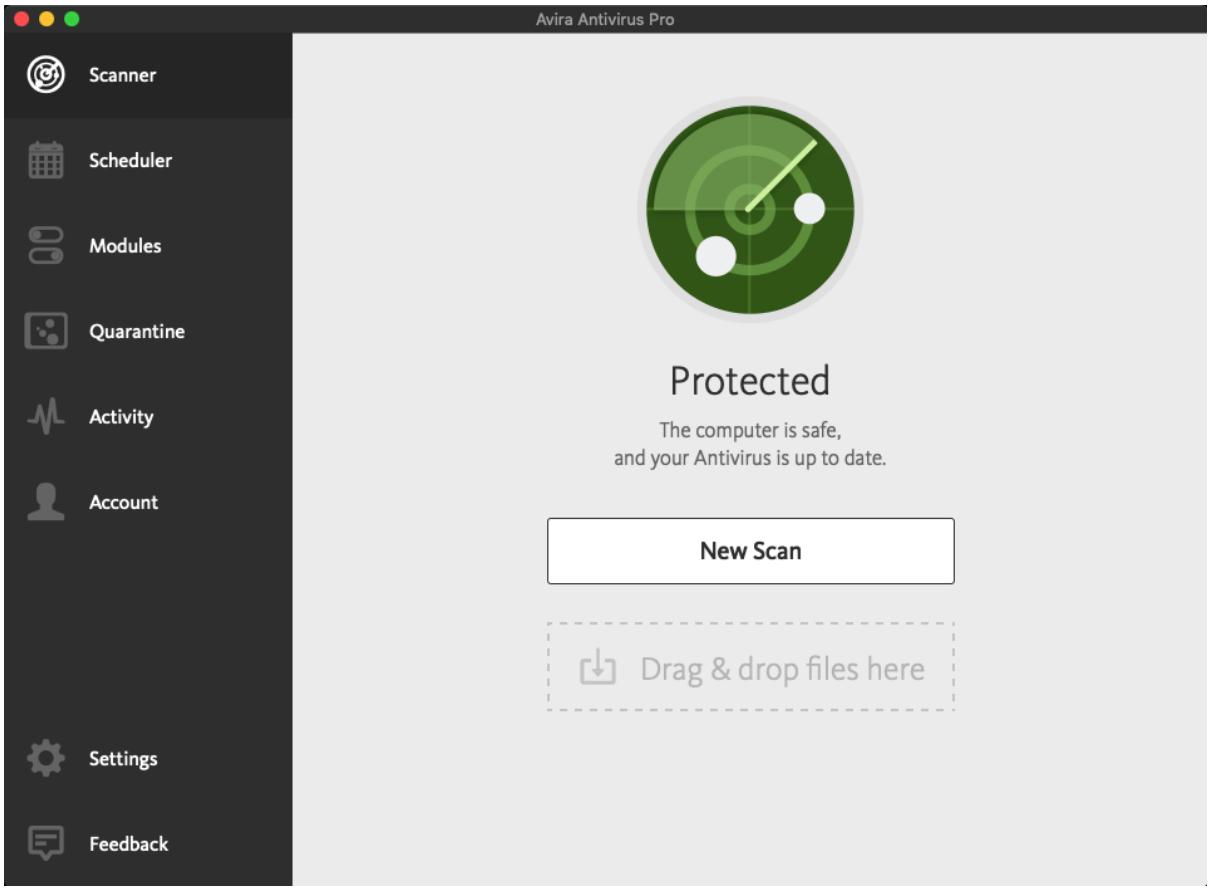
Standard macOS users (i.e. accounts without administrator rights) cannot perform any of the above tasks. We regard this as ideal.

Other points of interest

An advertising strip frequently appears along the bottom of the program, as shown below. This states that "privacy issues" have been found. Clicking on *Resolve* opens a separate window, which displays a number of warnings such as "Anyone can see what you do online". If you click on *Resolve All*, a purchase page for AVG Secure VPN opens.



Avira Antivirus Pro for Mac



Summary

Avira Antivirus Pro for Mac is a straightforward, paid-for antivirus program. It is very simple to install, and all the important features are easy to find in the interface. Real-time protection is very sensitive, and the program offers to scan external drives when you connect them. In our functionality test, we found a minor bug in the quarantine feature (which does not affect system security). However, overall the program is well designed and offers effective protection.

Installation

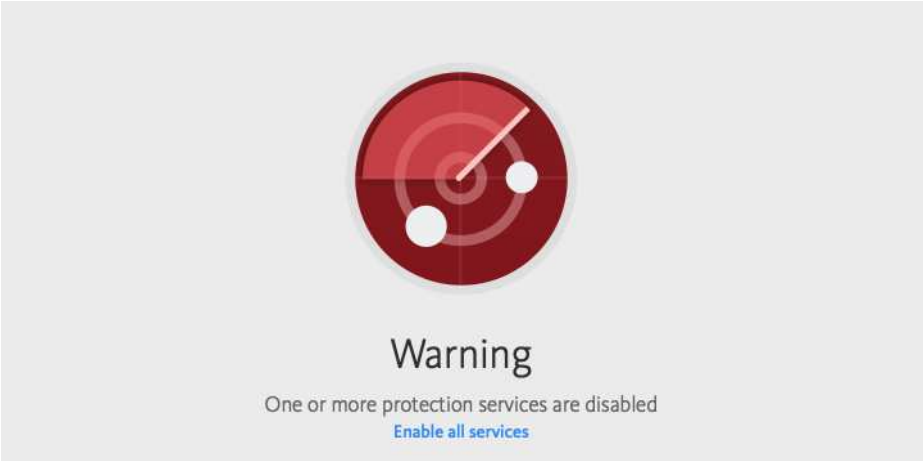
To set up Avira Antivirus Pro for Mac, you need to log in to your Avira account. You then download and run the installer, double-click the Avira icon, then click *Accept and install*. There are no options or decisions to make. If you have already installed the Free version of the product, you can upgrade this to the Pro version by adding a licence key, without having to reinstall. You can uninstall the program by clicking *Help* in the Mac menu bar, then *Open Uninstaller*.

Finding essential features

Status, default scan, scheduled scan, scan options, quarantine, settings and subscription information (*Account*) can all be accessed from the *Scanner* (home) page of the program window. You can update signatures from the System Tray icon menu. The help feature is found in the *Help* menu in the Mac menu bar. You can scan a drive, folder or file from the Finder context menu. You can also drag and drop items to be scanned onto the appropriate area of the *Scanner* page.

Status alerts

If real-time protection is disabled, an alert is shown in the main program window. You can reactivate protection by clicking *Enable all services*.

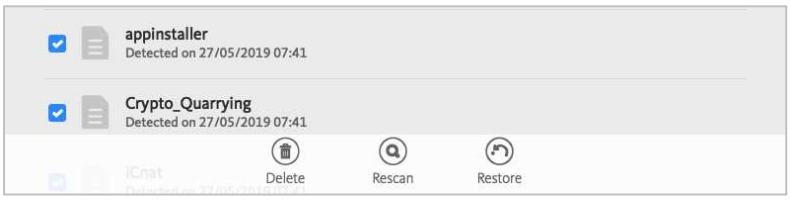


Behaviour on malware detection

When you connect an external drive, Avira offers to scan the drive. If you don't do this, and try to copy malware from the external drive to the system, Avira immediately blocks the copy process, quarantines the malware found, and displays an alert. This closes automatically after a few seconds.

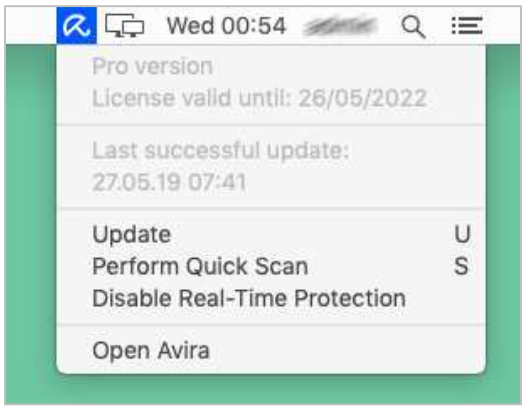
Quarantine and Logs

The *Quarantine* page of the program shows you all the items that have been quarantined, along with the date and time this happened. There are options to delete, rescan and restore any of the detected files. There is also a *More info* link for any individual file, although this only tells you the date on which it was discovered. In our functionality test, we found an occasional glitch in the restore-from-quarantine function. Avira have informed us that they are aware of this issue, and are working on making it 100% reliable.



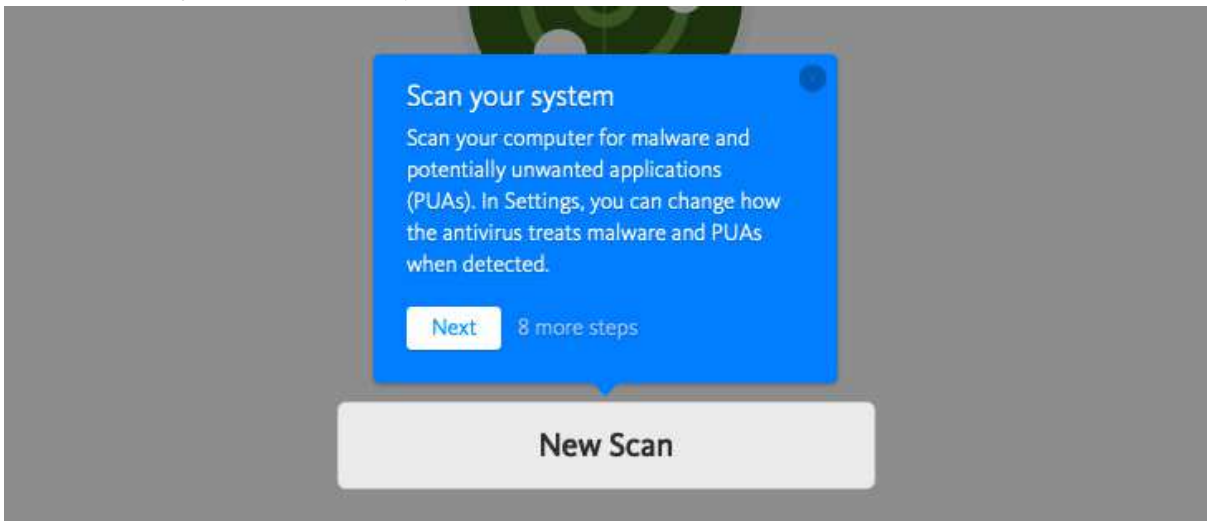
Activity shows a log of all system events, including detections, scans, updates and component activation/deactivation.

System Tray menu



Help

Avira Help (in the *Help* menu in the Mac menu bar) displays overlay balloons explaining the menu items in the program interface. This provides a clear and simple introduction to the program's features, but is obviously limited in its scope.



Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

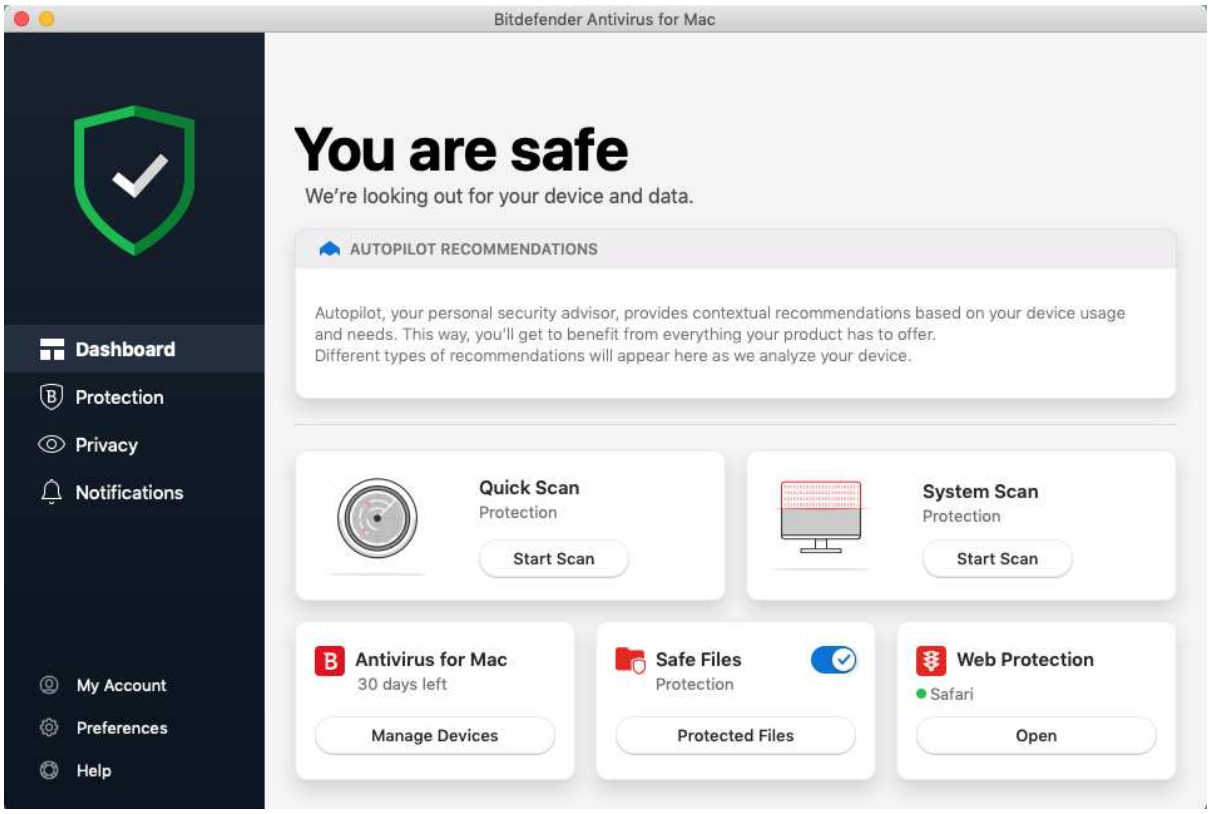
- Disable protection features (*Modules* page)
- Uninstall the program

Standard macOS users (i.e. accounts without administrator rights) cannot do either of these, which we regard as ideal.

Other points of interest

Avira Antivirus Pro for Mac makes unusually good use of the Mac menu bar. Only two menus are displayed – *Avira and Help* – which makes it easy to find what you want.

Bitdefender Antivirus for Mac



Summary

Bitdefender Antivirus for Mac is a paid antivirus program with ransomware protection, a data-limited VPN feature, and a browsing-protection add-in for Safari. We found it very straightforward to install and use. The user manual is easy to find, comprehensive, and very well produced. Effective real-time protection immediately detects and cleans malware on first contact. Overall, the product gets every important detail right, providing solid protection features in a very well-designed interface. Both expert and non-expert users should find it suitable for their needs.

Installation

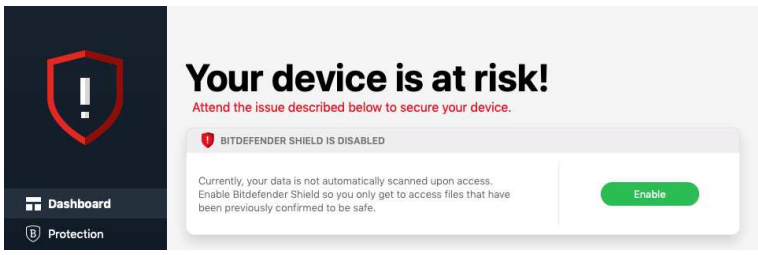
After downloading and starting the installer file, you just need to double-click the setup package icon to start the setup wizard. You do not need to make any decisions, and the only option is to change location folder. There are however some further steps to take in order to maximise protection. Firstly, you need to grant Bitdefender full disk access. Next, you need to create a Bitdefender account and sign in. An optional introductory tutorial then starts, after which the program window displays a recommendation to install the *Traffic Light* extension for Safari. After that, the Bitdefender window recommends configuring *Safe Files*, the product's ransomware protection feature. Next, Bitdefender suggests setting up Apple's Time Machine backup feature, and finally running a system scan. Whilst the setup process is certainly longer than for most other antivirus programs, everything is clearly explained as you go along. You can uninstall the program from the Bitdefender icon in the Finder Applications window.

Finding essential features

Status, **quick** and **full scans**, **subscription information**, **settings** and **help** are all directly accessible from the program's *Dashboard* (home page). You can find **custom scan**, **quarantine** and **scan exceptions** under *Protection*. **Update** is in the *Actions* menu in the Mac menu bar. There is no scheduled scan function, but you can scan a drive, folder or file using the Finder **context menu**. **Logs** are shown under *Notifications*.

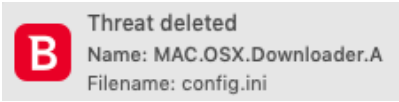
Status alerts

If real-time protection is disabled, an alert is shown in the status area of the main window.
You can reactivate the protection by clicking *Enable*.



Behaviour on malware detection

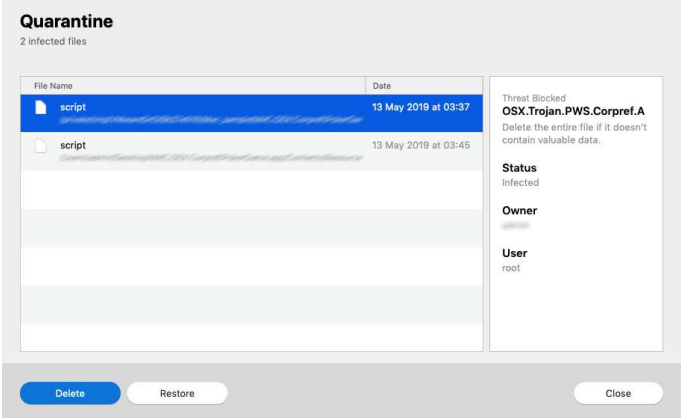
If you connect an external drive containing malware, Bitdefender's real-time protection immediately detects and cleans the infected files. The alert below is shown:



The message box closes itself once all detected items have been shown.

Quarantine and Logs

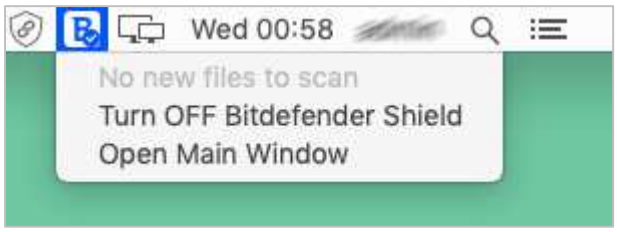
The *Quarantine* window lets you view and delete quarantined files. If you are using a macOS admin account, you can also restore files from here.



The right-hand pane of the quarantine window shows you the threat name. However, there is no means of accessing any more information about this.

Notifications is the log feature. It displays events such as updates, component activation, and malware detections.

System Tray menu



Help

Antivirus for Mac Help in the Mac menu bar opens a very comprehensive manual in .PDF format. This covers all aspects of using the program, and includes a glossary of malware types. It is fully indexed, and very well illustrated with screenshots.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

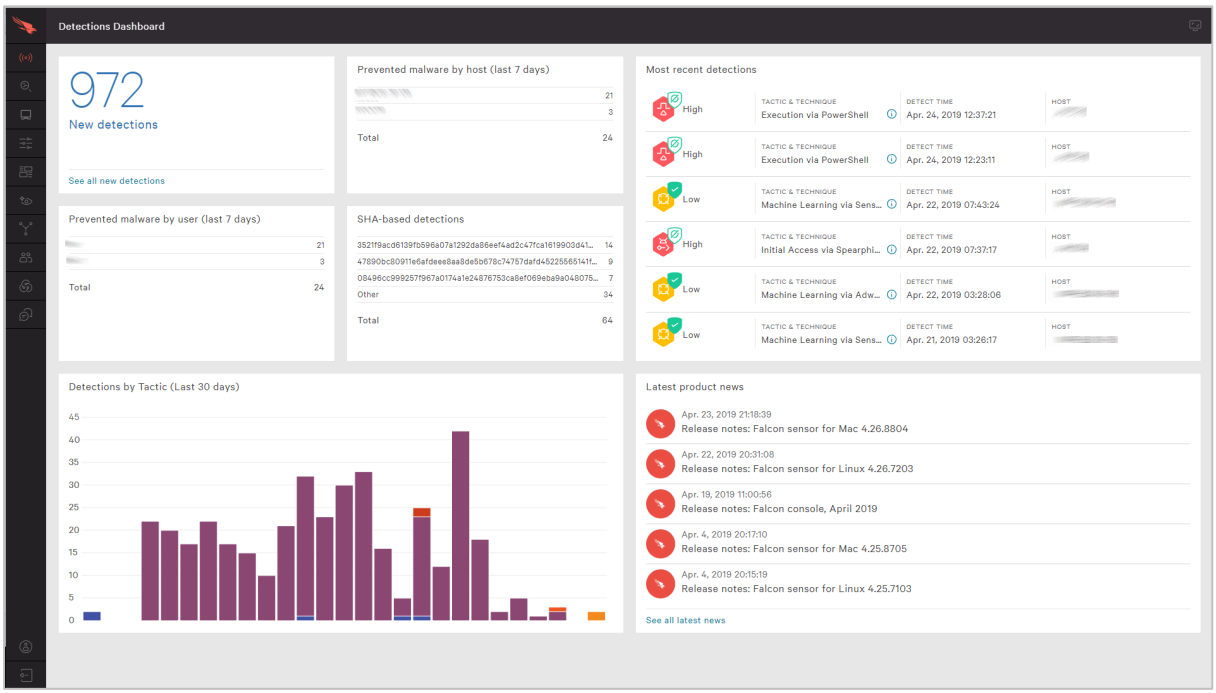
- Disable protection features (under *Preferences*)
- Make scan exclusions
- Restore items from quarantine
- Uninstall the program

Standard macOS users (i.e. accounts without administrator rights) cannot perform any of these tasks, which we regard as ideal.

Other points of interest

If you install the *Traffic Light* extension for Safari add-in, safety ratings are added to Google searches. For example, green tick (checkmark) symbols are used to indicate safe sites. There are similar add-ins for Firefox and Chrome.

CrowdStrike Falcon Prevent for Mac



About the product

Crowdstrike Falcon is a cloud-based endpoint protection platform. Endpoint protection software is provided for macOS computers, Windows clients and servers, and specific Linux client and server distributions. As the endpoint software has no user interface at all, we have described the functionality of the cloud console in this report.

Verdict

CrowdStrike Falcon is a very comprehensive platform. It provides not only AV services within an organization, but also a comprehensive set of detection and analysis services. We note that CrowdStrike Falcon is available as a fully managed service for organizations that desire a more hands-off solution to endpoint protection. Otherwise, it is aimed at the larger organization, and is not really a “fit and forget” product. Basic everyday monitoring and management tasks are simple enough, even with minimal understanding of its operations. However, the product’s capabilities are sufficiently deep that making some investment of time for learning is worthwhile to realize maximum value. CrowdStrike tell us that learning modules are available on-line or via external consultancy.

Getting up and running

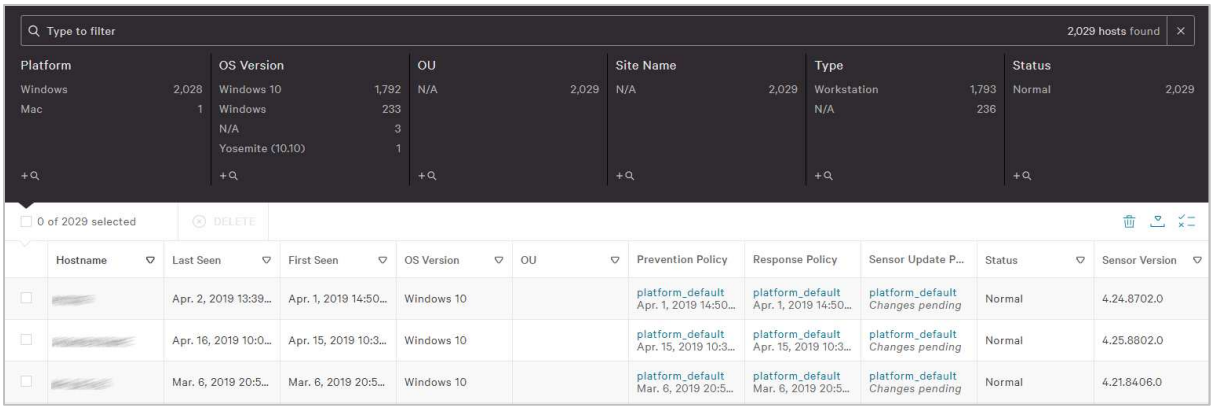
To install the sensor (endpoint protection software) on a Mac, you download the installer file from the console. You need to run this using a command prompt – instructions for this are provided in the documentation.

Everyday management

The management console is based in a web browser, as you would expect from a cloud-based solution. Two-factor authentication is required to log in, and support for single sign-on solutions is available. There is a menu of buttons down the left-hand side, and this menu can be expanded by clicking on the Falcon icon at the top left. The major items are *Activity*, *Investigate*, *Hosts*, *Configuration*, *Dashboards*, *Discover*, *Intelligence*, *Users*, and *Support*.

Activity is the first place to start work once the platform is up and running. There is a strong dashboard here, with the most important items brought into view. Good graphics show detections by scenario over the last 30 days, and you can click through here into the *Detections* submenu to view more detail. You get a strong reporting infrastructure, with a good choice of filter options presented front and centre here. You can also examine quarantined files and real-time response sessions here too.

The *Investigate* menu takes you into a comprehensive search facility. This covers hosts, hashes, users, IP addresses, domain and event searching. This is aimed at locating specific issues across the network estate in the recent history. The default is 24 hours, pre-set filters are provided up to 60 days, and customization options are available.



The *Hosts* page, shown above, lists all the host installations, by version and platform. It provides immediate understanding of which hosts are offline or disconnected. From here, you can go to the *Sensor Download* menu and download sensor installations for all the platforms.

The *Configuration* menu is the heart of the policy driven process within CrowdStrike Falcon. From here, you create policy definitions which cover all aspects of the AV and prevention processes of the platform. And then you apply that process to groups of installations. You can have different policies for Mac, Windows and Linux clients here too.

The *Dashboards* menu gives access to the executive summary view of the estate. There are detailed graphics for detections by scenario and severity, and identifications of the top 10 users, hosts and files with most detections. This is just the tip of a very deep iceberg allowing for comprehensive analysis of what is happening. You can search by almost anything, and use this to discover what has happened on the network during an outbreak. This includes where something entered, how it attempted to execute, what processes it used, and how it was contained. Getting through this is not for the fainthearted, but it cannot be denied that you have very powerful set of audit and analysis tools here.

The *Discover* menu allows you to discover devices, users and applications on the network. You can search by application inventory, asset, mac address, accounts and other app/process-based inventory. You can also review user account information including domain accounts, local accounts and their password reset status.

The *Intelligence* menu takes you into an overview of the current landscape threat as perceived by CrowdStrike. This can be categorised by different factors. Examples include geographical origin of threat, target industry, target country, and motivation (espionage/criminal/Hactivist and destruction). Each threat is detailed by these parameters. Clicking *View Profile* on the threat takes you to a comprehensive analysis and explanation of that specific threat. This is a comprehensive resource which is unusual and most welcome.

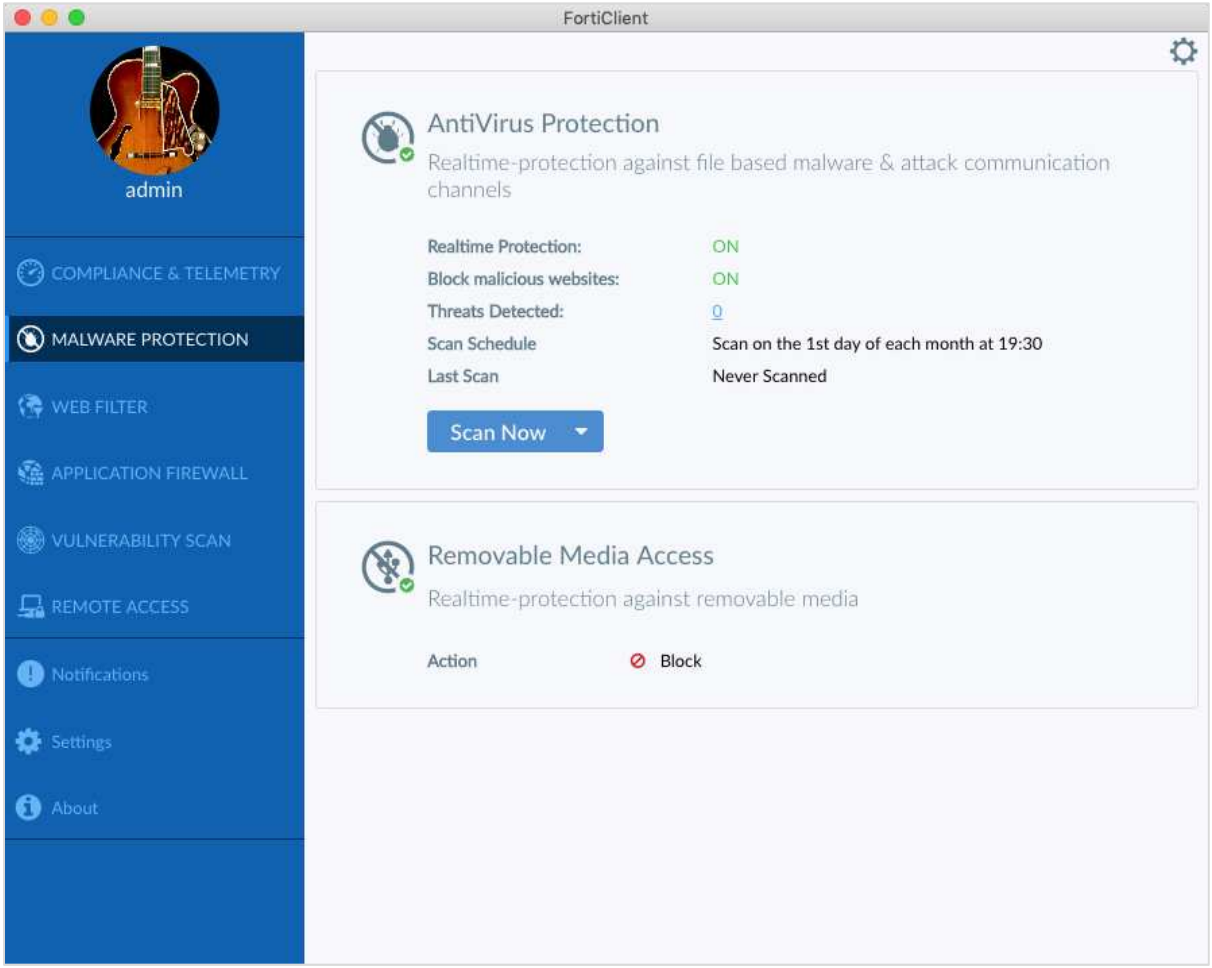
The *User* menu allows you to create the usual user profiles for administrators and other activities within the platform. There are pre-built roles already created for *Endpoint Manager*, *Event Viewer*, *Administrator*, *Analyst*, *Investigator*, *Real Time Responder*, and others. You can map these roles onto existing internal working structures, or to custom-build new roles as required.

The *CrowdStrike Store* allows you to extend the capabilities of the Falcon platform with a host of ready-to-go partner apps and add-ons.

macOS endpoint protection software

On the end-user client, the default setting is to have the client invisible to the user. There is no interface, and no alerts are shown. In our functionality test, we were able to connect a flash drive containing a folder of malware to our test system, and copy the folder to the Mac desktop. However, when we tried to execute some malware samples, execution failed, and the detection was immediately shown in the cloud console.

FortiClient for macOS



Summary

FortiClient for macOS is a business endpoint protection program with a sandbox, web filter, firewall, vulnerability scanner and VPN. It is primarily designed to be managed using the FortiClient Enterprise Management Server (EMS), but can be used as a standalone product as well. EMS was reviewed in AV-Comparatives' Business Security Test 2018 (August – November); please see that report for details of the management console.[5] In keeping with its status as a server-controlled endpoint protection product for business networks, FortiClient for macOS has a fairly minimalist user interface. Consequently, it should not be compared to the consumer products in this report.

Installation

To install FortiClient on a Mac, you open a browser and enter the name or IP address of the management server. You can then download and run the installer. The administrator can alternatively send the installer URL to users for them to install themselves. The setup wizard is very straightforward. It is also possible to deploy the software to endpoints via 3rd-party remote installation tools.

[5] https://www.av-comparatives.org/tests/business-security-test-2018-august-november/#fortinet

Finding essential features

Because the product is managed from a server-based console, users (whether or not they have macOS admin rights) are only able to run scans and updates. They cannot disable protection, make scan exclusions, or restore items from quarantine.

The *Malware Protection* page of the program window has a status display for real-time protection, web protection, and removeable media access. It also shows the number of threats detected, the schedule for scans, and the date and time the last scan was run. The *Scan Now* button gives you a choice of quick, full, custom and removeable media scans.

The *About* page functions as a de facto update feature, in that opening it will check for updates and download any new ones if necessary.

The *Settings* page shows the current configuration, but does not allow users to make any changes. Settings can be controlled by policy from the administration console.

Notifications shows a log of events. Help features can be accessed from the *Help* menu in the Mac menu bar, though these are only relevant to network administrators.

Status alerts

The status of real-time protection is shown in the status area of the *Malware Protection* page. The component can only be switched on or off from the server console.

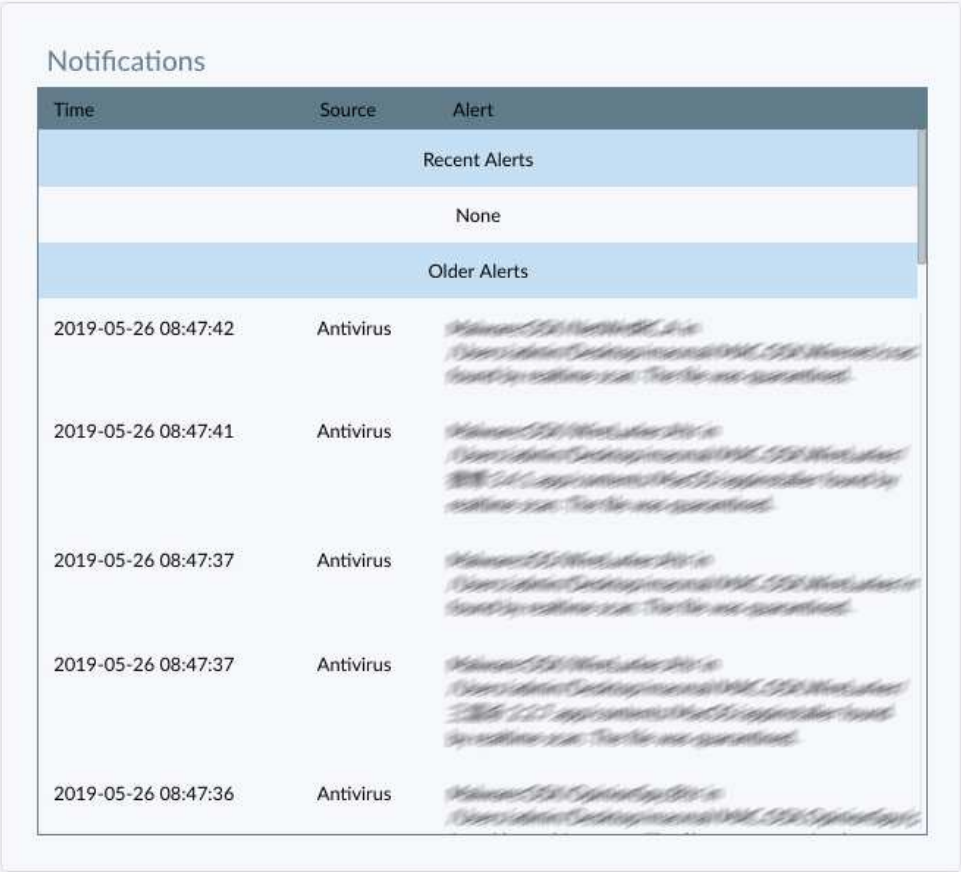
Behaviour on malware detection

How FortiClient for Mac reacts on discovering malware depends on how it is configured. For our funcitionality test, we had the policy set so that an alert would be shown, and the malware quarantined. This is exactly what happened when we tried to copy malware from an external drive to the Mac Desktop; the alert is shown below:

We note that access to USB drives can be disabled by policy.

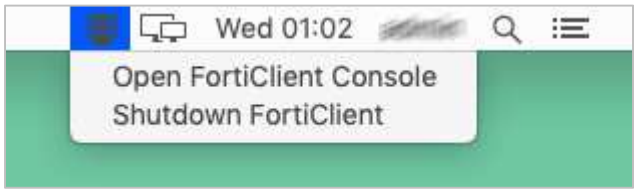
Logs and quarantine

The notifications page, which displays malware detections, is shown below:

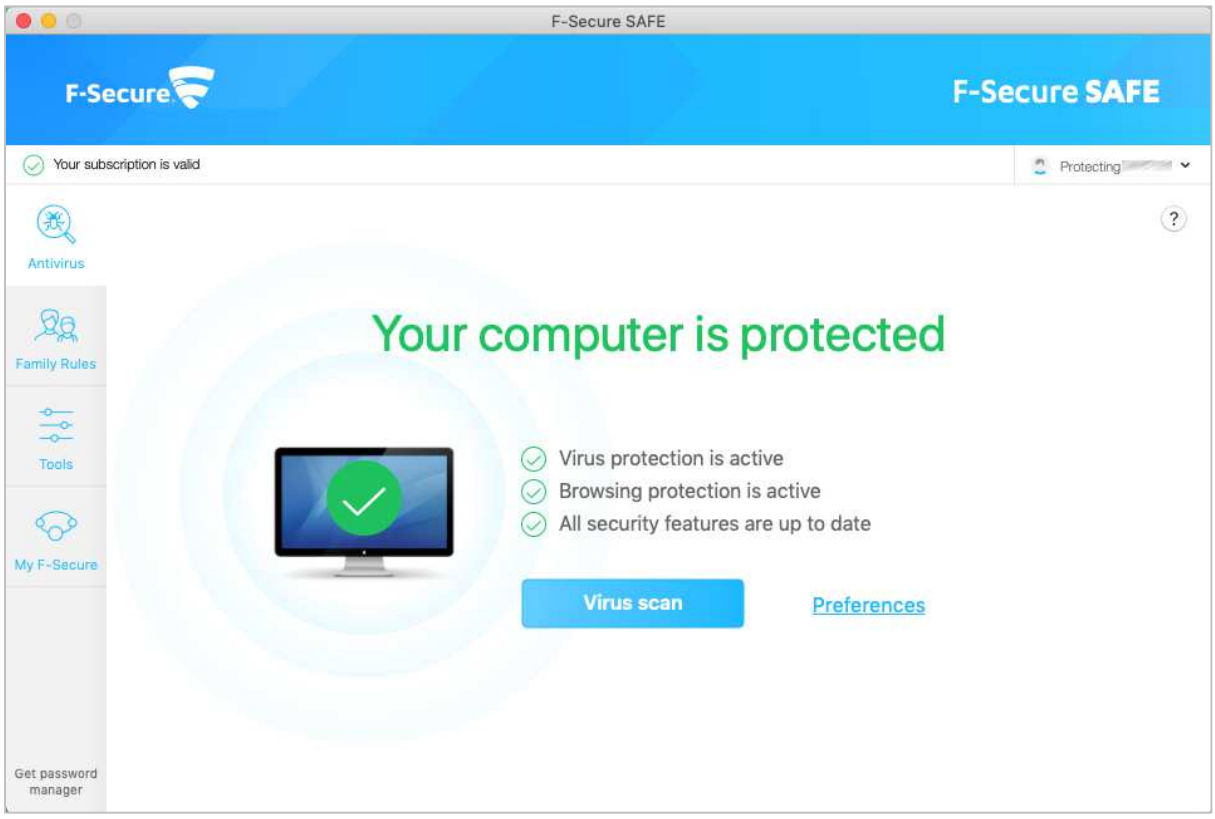


Quarantine is not accessible from the client GUI.

System Tray menu



F-Secure Safe for Mac



Summary

F-Secure Safe for Mac is a paid-for antivirus program with parental controls and a URL blocker. It features very simple installation, and effective on-access protection that prevents malware from being copied to the system. Most important features are easy to access from home page, and the program is simple enough for non-experts to use comfortably. Suggestions for improvement would be a "Fix-All" button to e.g. reactivate protection, and a quarantine feature.

Installation

To install F-Secure Safe, you need to create an F-Secure account and log in. You can then download and run the installer, which asks if you want to protect your own device, a child's, or someone else's device. Other than this, there are no options or decisions to make. Should you need to, you can uninstall the product using the uninstaller in the *Applications\F-Secure* folder.

Finding essential features

Status, **default scan**, basic **subscription information**, **settings** (*Preferences*) and **help** are all found on the *Antivirus* (home) page of the program window. **Scan options**, **updates** and **logs** (*Infection report*) are accessed from the menu of the System Tray icon in the Mac menu bar. We could not find scan scheduler, context-menu scan, or a quarantine feature.

Status alerts

If real-time protection is disabled, an alert is shown in the main program window. To reactivate the protection, you need to go into *Preferences*.

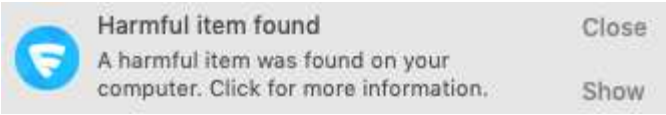
Your computer is not protected

Turn on virus protection

Browsing protection is active

Behaviour on malware detection

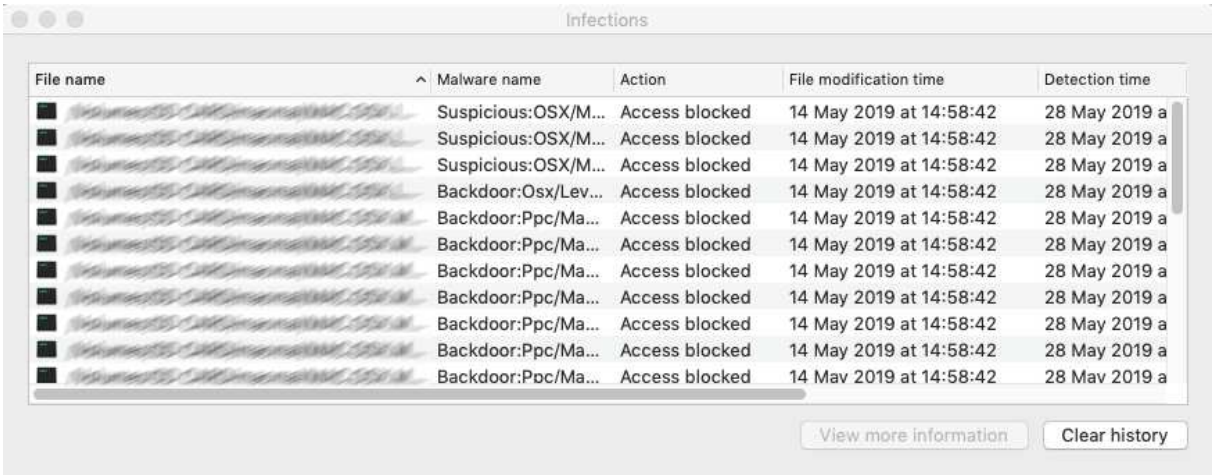
When you connect an external drive, F-Secure does not take any action. However, if you try to copy any malicious files from the drive to the local system, F-Secure immediately detects the malware and prevents it being copied. The alert below is shown.



Harmful item found

A harmful item was found on your computer. Click for more information.

The alert persists until you close it. If you click on *Show*, the scan log with detected items will be displayed. There is a *View more information* button here, but this only provides a generic description of macOS malware.

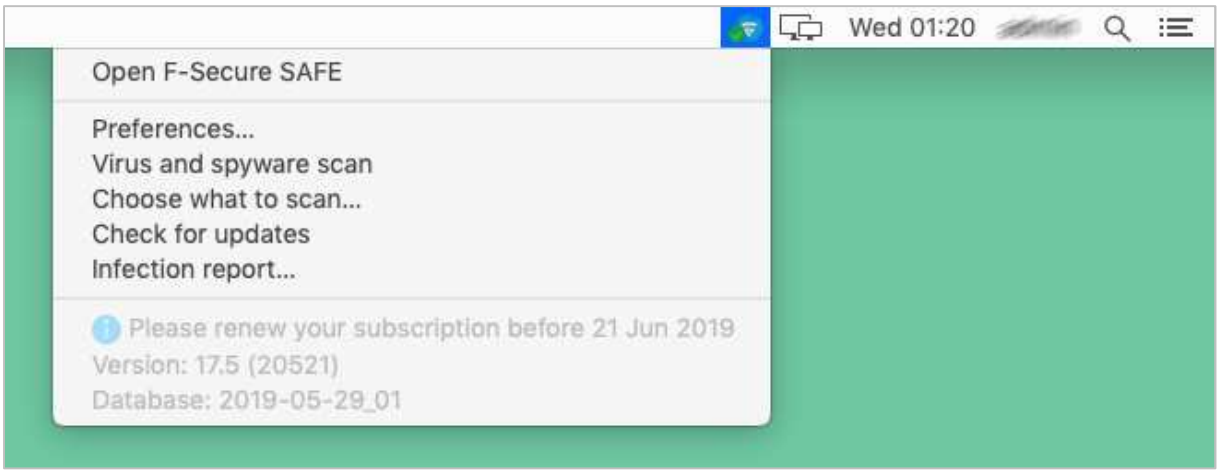


File name	Malware name	Action	File modification time	Detection time
[redacted]	Suspicious:OSX/M...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Suspicious:OSX/M...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Suspicious:OSX/M...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Osx/Lev...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a
[redacted]	Backdoor:Ppc/Ma...	Access blocked	14 May 2019 at 14:58:42	28 May 2019 a

Quarantine

The program does not include a quarantine feature. The scan logs window can be re-opened by clicking *Tools\Infection Report*.

System Tray menu



Help

Clicking the *?* symbol in the main program window opens the program's online help window. This gives simple text explanations and instructions for using the main functions.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

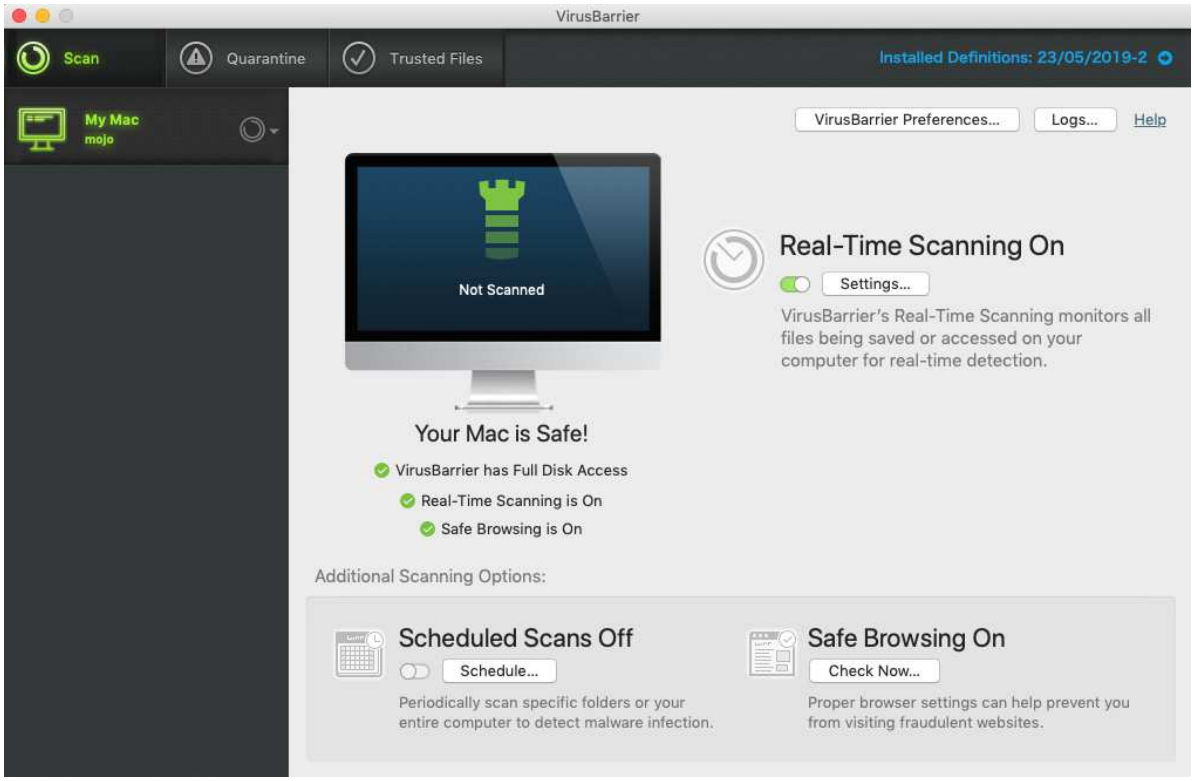
- Disable protection features (in *Preferences*)
- Uninstall the program

Standard macOS users (i.e. accounts without administrator rights) cannot perform either of these tasks, which we consider ideal.

Other points of interest

After installing the program, you are prompted to allow the Safari extension. This provides search ratings, such as a green tick for safe sites, in Google searches.

Intego VirusBarrier X9



Summary

Intego VirusBarrier X9 is a straightforward, paid-for antivirus program. Its interface is well designed and provides easy access to all the important functions. Standard users without administrator rights cannot take any potentially risky actions. There are two effective help features: a simple overlay that explains the GUI, and an online user manual. We found two of the program's functions – *Quarantine* and *Safe Browsing* – to be rather confusing, however.

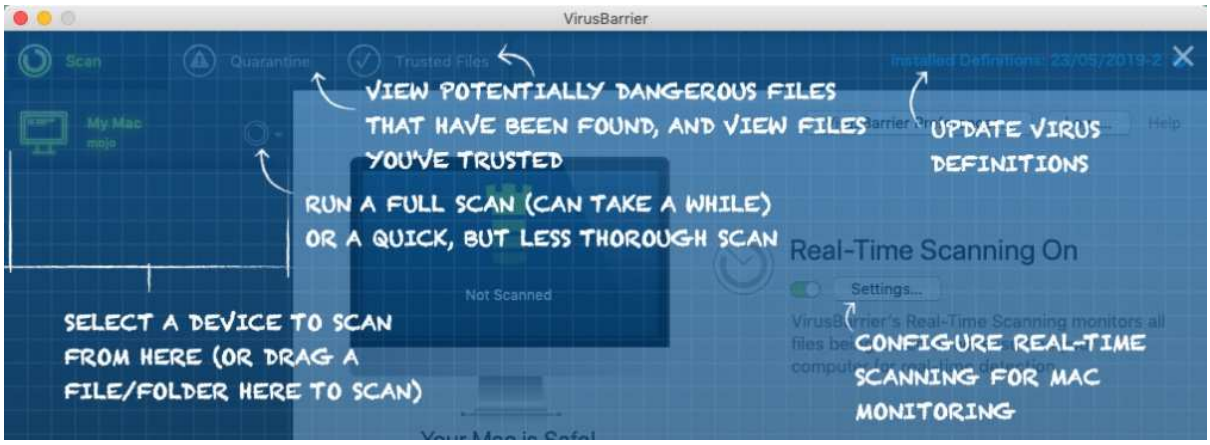
Problems with version 10.9.18 of the program on macOS Mojave

For this report, we tested and reviewed all products on macOS 10.14 (Mojave), which was released in September 2018. We used VirusBarrier 10.9.18, as this was the current version at the time of the review. Although Intego's website specifically stated that this version was compatible with Mojave, we discovered a number of serious malfunctions with it in our functionality check. These are listed at the end of the review under Appendix. It appears that these problems are related to new security measures in macOS Mojave, as they did not occur when we tested the same program version on older versions of Apple's operating system. In order to verify the intended behaviour of VirusBarrier for the purposes of the review, we repeated our functionality test on a system running macOS 10.13 (High Sierra).

We reported the Mojave-related issues we had found to Intego, who to their credit immediately started working on an updated version of the product that will rectify these problems. This is due to be released soon as VirusBarrier X9 v10.9.19. It will also include additional prompts/alerts when protection is disabled, and options for action when an external drive is connected.

Installation

To set up VirusBarrier X9 on your Mac, download and run the installer, then double-click the aptly named *Double Click to Install* button. A quick and simple setup wizard then runs. At the end of this, you are prompted to choose a protection level; there is a choice of *Minimum, Maximum* and *Standard*, with an explanation of the difference between them. When you first run the program, a semi-transparent overlay is shown over the program window, which points out the main features of the GUI:



If you are using an administrator account, you can uninstall the program by rerunning the installer file and double-clicking *Uninstall*.

Finding essential features

Status, **scheduled scans** and **scan options**, **quarantine**, **logs**, **preferences** and the "Quick Start" **help** overlay can all be found on the home page of the program window. You can **update definitions** from the *VirusBarrier* menu in the Mac menu bar, and the **logs** and main **help** functions are also found here. A *Scan with VirusBarrier* entry is added to the Finder context menu, with which you can scan individual drives, files and folders. **Subscription information** can be seen by clicking the *Installed Definitions* link in the top right-hand corner of the program window.

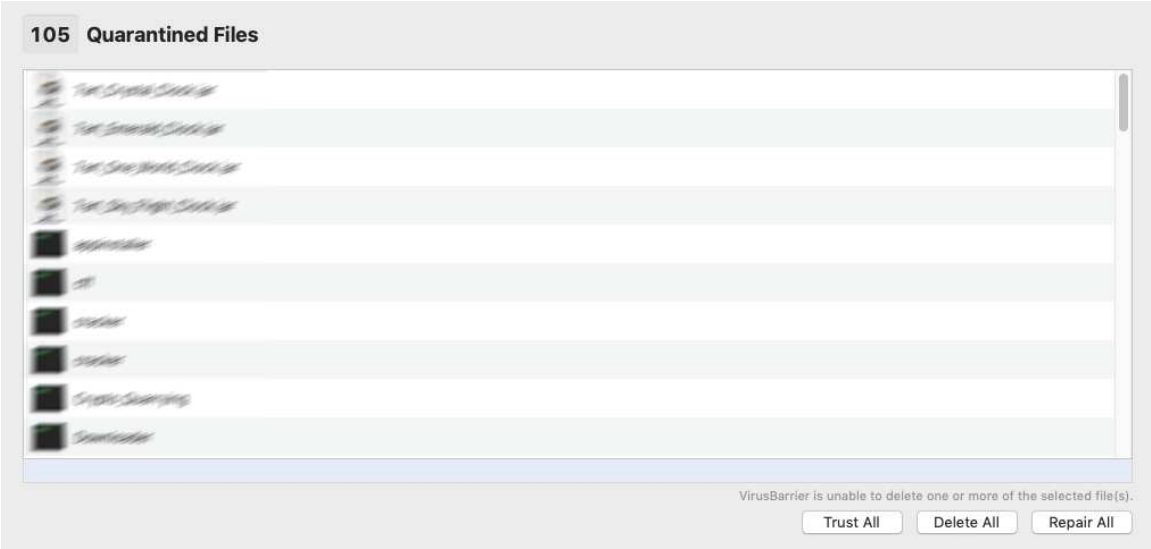
Status alerts

If real-time protection is disabled, a (somewhat subtle) warning is shown in the status area of the main program window. You can reactivate the protection by clicking *Turn On*, or using the slider switch in the real-time scanning area.

Behaviour on malware detection

When you connect an external drive, VirusBarrier does not take any action by default. There is however an option in the settings to scan external drives on connection.

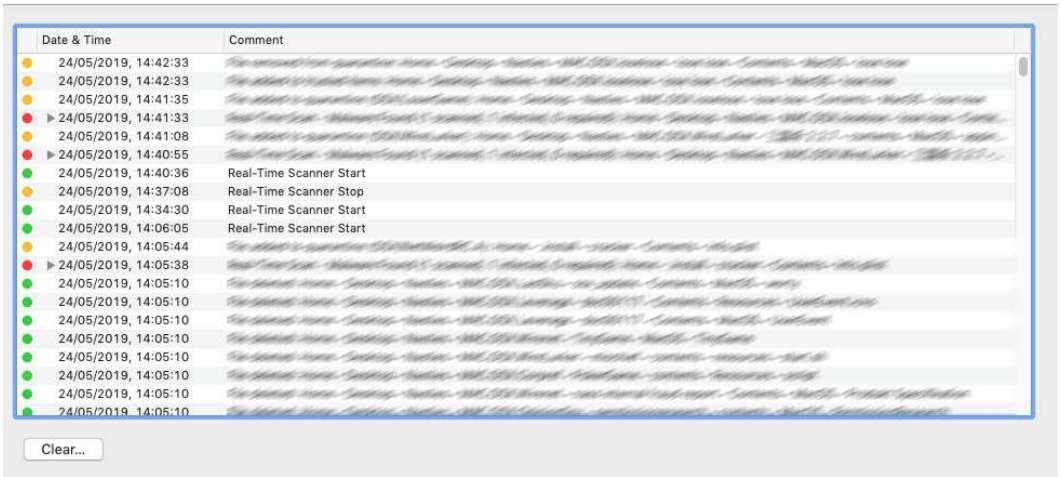
If you try to copy malware from an unscanned USB drive to the macOS system Desktop, the program immediately detects the malicious files and displays the quarantine/detection alert window, shown below:



The alert persists until you close it.

Logs

The *Logs* window shows the date and time of events such as malware detections, deletions, quarantine management and real-time protection being started or stopped:



Quarantine

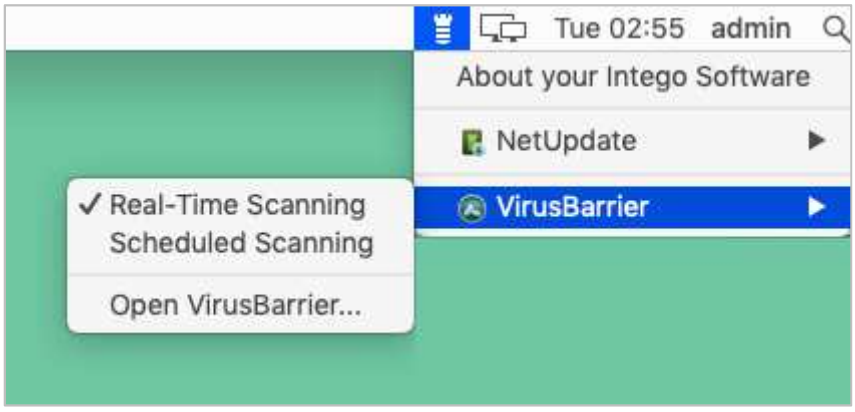
The *Quarantine* page of the program window (which is the same thing as the detection dialog, see screenshot above) shows malicious files that have been detected and quarantined, and provides the options *Trust, Delete* and *Repair*. You can carry these out on individual files by clicking on them, or use the *Trust All/Delete All/Repair All* buttons to apply the same action to all the files.

We note that when malware is quarantined by VirusBarrier, it is not removed from its original location, and appears in Finder windows just the same as before. If you attempt to execute, copy or move it, VirusBarrier will block the action, and a message box appears, stating "The operation can't be completed because you don't have permission to access some of the items". Sometimes an AV alert stating "Quarantine file access blocked" is also shown:

In the event that you rescan a folder containing items that have already been quarantined, VirusBarrier will detect them again, in just the same way as in the original scan. We found this behaviour to be very confusing, and suggest that moving quarantined items to a hidden folder/repository – as is the norm for antivirus programs – would be much simpler for users to understand. However, Intego tell us that the quarantine behaviour is by design, for a number of reasons.

System Tray menu

When we tested VirusBarrier X9 on an older version of Apple's operating system, a System Tray icon with menu was displayed, as shown below:



Help

Clicking *Help\VirusBarrier Help* in the Mac menu bar opens a clear, simple online manual, well illustrated with screenshots, with comprehensive instructions and information for using the program.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

- Disable protection features
- Make scan exclusions - you can do this by making a folder "trusted"
- Uninstall the program, using the *Uninstall* button, which is displayed if you rerun the installer file.

Standard macOS users (i.e. accounts without administrator rights) cannot perform any of the above tasks, which we find ideal.

Other points of interest

The *Safe Browsing* function shown in the VirusBarrier program windows reports on the whether the safe browsing feature in Safari (and Chrome/Firefox if you have them) is enabled. We found it rather misleading, as some users might think that it is a feature of VirusBarrier X9 itself. An alert is shown in the status section of the program window if the feature is deactivated. In the dialog box *Check Now* there is an *Open* link, though this just opens the browser itself rather than its settings – which we found rather frustrating. Intego tell us that in the next release of the product, the description of the *Safe Browsing* function will be improved to make clear what the feature does.

If you test the product by using the trial version, you need to open the program window, and click OK in the info box that appears first, before real-time protection becomes active. This does not apply to the licensed version of the product, whose real-time protection is automatically enabled as soon as you log on. A pop-up alert informs you when RTP is activated after each logon, though this can be supressed. Please also note that the *Repair* function for malware files is only available in the licensed version.

Appendix: details of problems with VirusBarrier 10.9.18 on macOS Mojave

1. The setup wizard crashes after the program has been installed, but before essential configuration can be completed. You have to find the program in the Applications folder and start it manually to complete the setup process.
2. The option to scan external drives on connection does not work reliably.
3. When copying a folder of malware samples from an external drive to the Mac Desktop, not all the samples are blocked by the real-time protection, and an on-demand scan of the copied folder produces additional detections.
4. It is possible to execute malware samples from an external drive, if this has not been manually scanned first. This applies even with samples that would be detected by VirusBarrier in an on-demand scan, or if executed from the Mac's system drive.
5. VirusBarrier sometimes crashes after deleting malware items from quarantine.
6. The System Tray icon is not displayed, and consequently its menu is not accessible.

Kaspersky Internet Security for Mac

Summary

Kaspersky Internet Security for Mac is a paid-for security suite with a browser add-in and parental controls. We found it very straightforward to use, with all the features easily accessible from the main program window or macOS menu bar. In our functionality test, all the features worked exactly as expected. Sensitive on-access detection immediately quarantines any malware copied to the system. Users without administrator rights cannot disable the protection or uninstall the program. Overall, the product provides solid protection for your Mac.

Installation

Having downloaded and run the installer, you need to double-click *Install Kaspersky Internet Security\Download and Install*. The only option is whether to install the browser extension for Safari (and/or other browsers). The program can be uninstalled from the *Kaspersky Internet Security Support* link in the *Help* menu in the macOS menu bar.

Finding essential features

Update, status, scan options and scheduled scan, subscription information, can all be accessed directly from the program's home page. Settings (*Preferences*), logs (*Reports*) and help are all in the Mac menu bar. A link to quarantine is shown on the home page when quarantined items are present.

Status alerts

If real-time protection is disabled, a warning is shown in the main program window. You can reactivate the protection by clicking *Enable*.

Behaviour on malware detection

When you connect an external drive, KIS does not take any action by default (but an upcoming version will prompt you to scan the drive on connection). If you try to copy malware from the external drive to the macOS system, KIS immediately detects and quarantines the malware. An alert like the one below is shown for every malware sample detected:

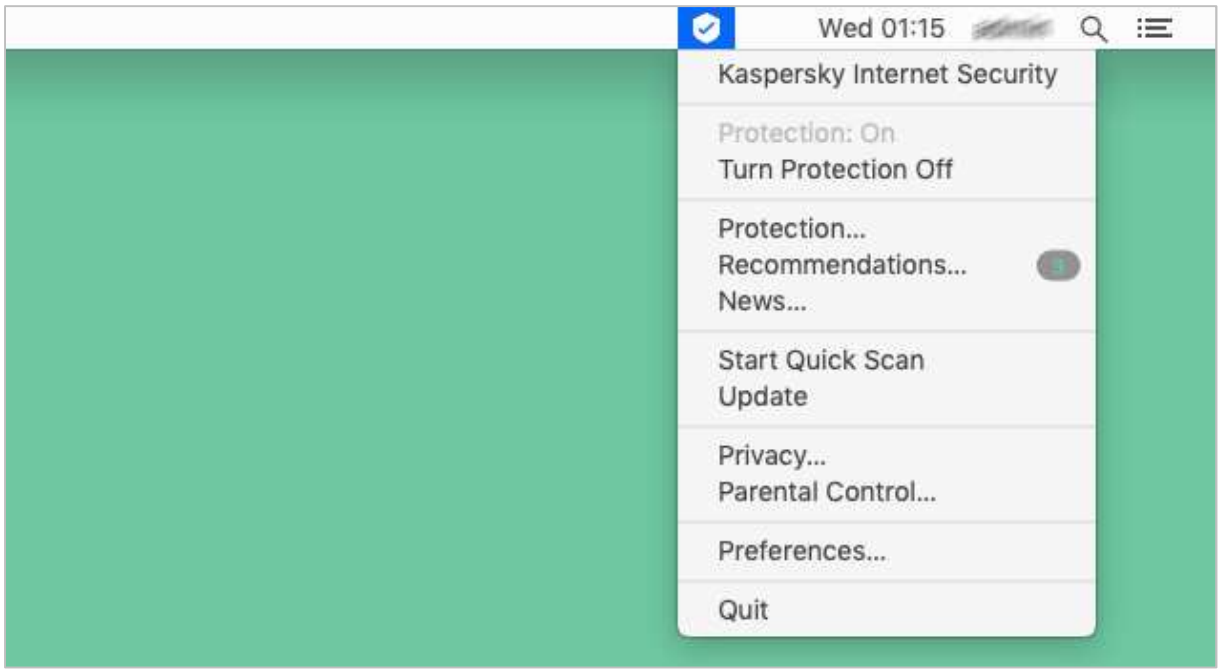
The alerts persist until you close them.

Quarantine and Logs

When there are untreated items in quarantine, a link to the quarantine page is shown on the home page. There is no separate logs feature as such.

By clicking on the"..." at the end of each line, you can delete or restore individual items (the latter only if you have an administrator account). In our functionality test, restored malware items were immediately re-deleted by the on-access protection. You can delete all quarantined items using the *Delete All* button. No additional information about detected malware is provided.

System Tray menu



Help

Kaspersky Internet Security Help is found in the *Help* menu in the macOS menu bar. It contains simple, clear feature descriptions and text instructions for using the program.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

- Disable protection features from *Preferences*.
- Restore items from quarantine – although these are immediately re-deleted by the on-access protection
- Uninstall the program

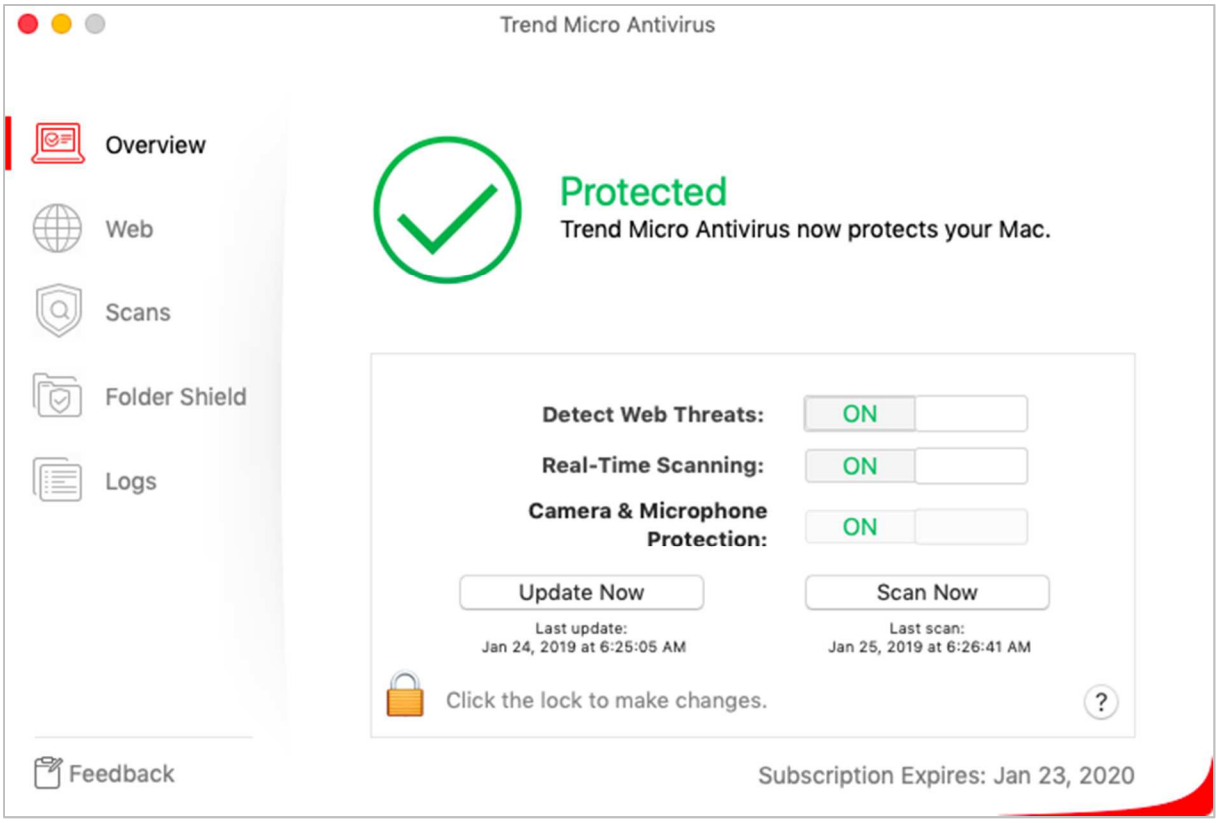
We note that no security prompts are shown when carrying out any of these tasks. However, Kaspersky inform us that the upcoming 2020 release of the product will require all users to enter a password before quitting the program.

Standard macOS users (i.e. accounts without administrator rights) cannot perform any of the above tasks, which we regard as ideal.

Other points of interest

After installing Kaspersky Internet Security for Mac, you are prompted to install an extension for Safari (and other browsers if installed).

Trend Micro Antivirus for Mac



Summary

Trend Micro Antivirus for Mac is a paid-for antivirus program with camera and microphone protection, an anti-ransomware feature, and a web-protection add-in for Safari. This year's version makes a number of improvements on the one we reviewed last year. We were particularly impressed with the very sensitive on-access malware detection. The help features are clear, and convenient to access. Installing and uninstalling are both straightforward, and the clean UI design makes the most important features very easy to access and use. Consequently, Trend Micro Antivirus for Mac would be particularly well suited to non-experts. A couple of minor improvements could be made to the quarantine function, and a context-menu scan would be nice. However, overall the program has been very well thought-out, and gets all the important things right.

Installation

After downloading and running the installer file, you start the setup wizard by clicking *Install Trend Micro Antivirus*. The *User Support* folder on the same page includes a list of system requirements, and a succinct, well-illustrated *Quick Start Guide*. There is also an uninstaller, with which you can quickly and easily remove the program, should you need to.

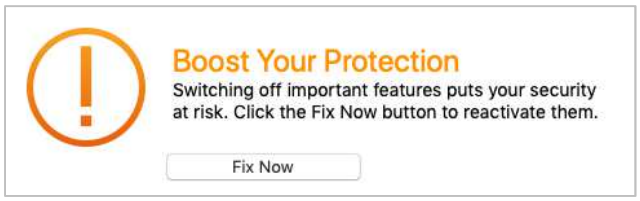
The setup wizard is very straightforward. Aside from choosing whether to enter a licence key or use the trial version, there are no decisions to make. The final page of the wizard has a screenshot of the macOS System Tray, showing you how to access the program from the Trend Micro icon. When you first open the program, it prompts you to set up *Camera and Microphone Protection* and *Ransomware Protection*. For the latter, you can easily customise the default list of folders and drives to be protected.

Finding essential features

Status, **update**, **default scan**, **scan options**, **subscription**, **logs/quarantine** and **help** can be accessed directly from the *Overview* page (please see screenshot above). We note that the logging and quarantine functions are combined under *Logs*. **Settings** are found under *Trend Micro Antivirus\Preferences* in the Mac menu bar, as is to be expected for a macOS program. **Scheduled scans** can be configured in the *Preferences* dialog box. There is no context-menu scan feature (Trend Micro tell us that they feel context menus are out of keeping with macOS user-interface design).

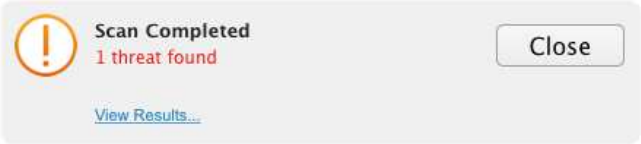
Status alerts

If real-time protection is disabled, the alert below is shown in the main window. You can reactivate the protection by clicking *Fix Now*.



Behaviour on malware detection

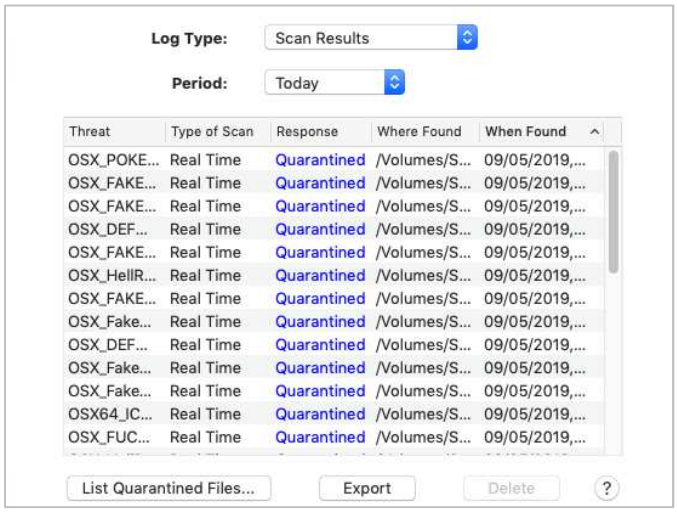
When you connect an external drive, a Trend Micro pop-up suggests scanning this. However, even if you don't do this, the program's on-access protection immediately starts scanning the drive anyway. In our test, malware samples were detected and quarantined immediately in this scenario. We regard this as exemplary behaviour. The alert below is shown when malware is detected:



The alert box remains on display until you close it. If you click on *View Results* in the alert box, it opens the logs/quarantine page and shows you what's been detected.

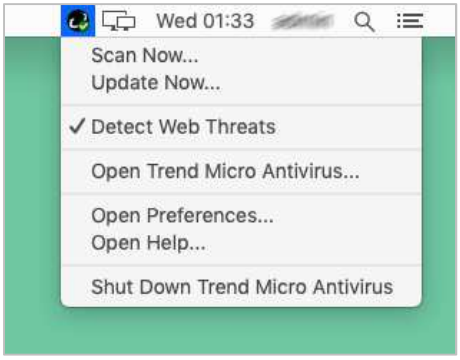
Quarantine and Logs

The quarantine and log functions are combined in the *Logs* page. From here, you can view and delete any or all of the quarantined items.



Whilst viewing and deleting detected items is simple, power users may feel there is some room for improvement in the quarantine functionality. Firstly, as noted last year, the window is small and cannot be resized. This means some scrolling and dragging of columns is required to see all the content (although the list can be exported to a .CSV file). Secondly, threat names are shown by default in the main Logs window, whilst file names are shown in the *List of Quarantined Files*. You can see the file names as well in the *Logs* window (to correlate them with threat names), but you have to expand the *Where Found* column and then scroll to the end of it. Finally, no direct way to find more details of the malware items is provided, although they can be manually looked up in Trend Micro's online threat encyclopaedia.

System Tray menu



Help

Clicking the *?* icon in the main window opens a context-sensitive online manual. This provides a simple, clear guide to the program's features and how to use them, well illustrated with screenshots.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

- Disable protection features (using the slider buttons on the *Overview* page)
- Make scan exclusions (using the diagnostic toolkit)
- Restore items from quarantine (by clicking *List Quarantined Files*)
- Uninstall the program

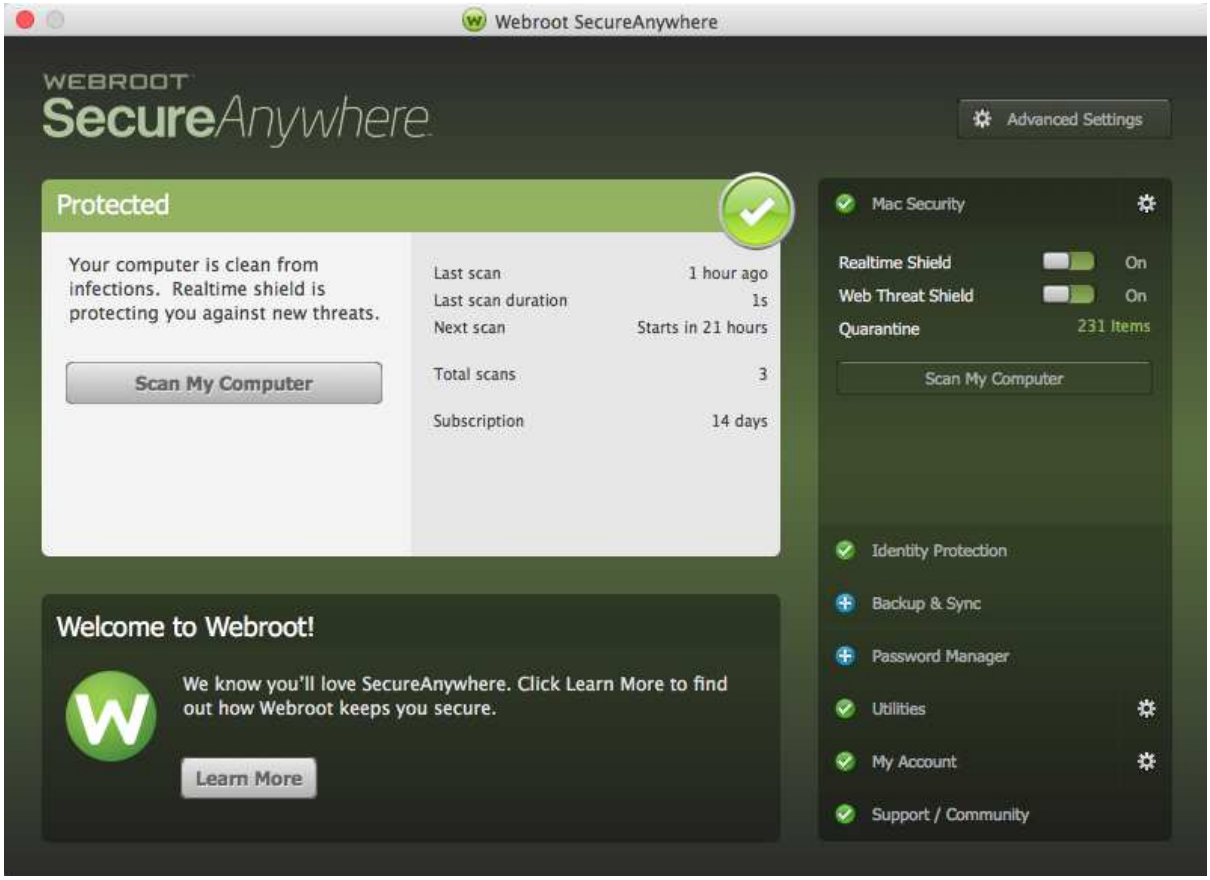
Standard macOS users (i.e. accounts without administrator rights) cannot perform any of the above tasks. We regard this as ideal.

Other points of interest

The Safari add-in shows safety ratings for sites in Google web searches. These use e.g. a green tick icon for safe sites.

In the Trend Micro folder in the macOS Applications window is a diagnostic toolkit. With a macOS Administrator account, you can stop/start components; delete temporary files; uninstall if the standard uninstaller has problems; troubleshoot; collect debugging info; upload quarantined files to the vendor; collect network logs; create scanning exclusions.

Webroot SecureAnywhere Antivirus for Mac



Summary

Webroot SecureAnywhere Antivirus for Mac is a paid-for antivirus program with an add-on for the Safari browser. We found it very quick and simple to install, and all of the features are easy to access from its home page. Even full scans run very rapidly. Real-time protection against malware copy is effective, malware alerts are good, and it is easy to deal with any threats encountered. Currently, there is no means of preventing standard users (without admin rights) from disabling the protection, restoring items from quarantine, or shutting the program down. Webroot are considering changing this, which would make the program more suitable for anyone who uses a shared computer, e.g. in a family or small business.

Installation

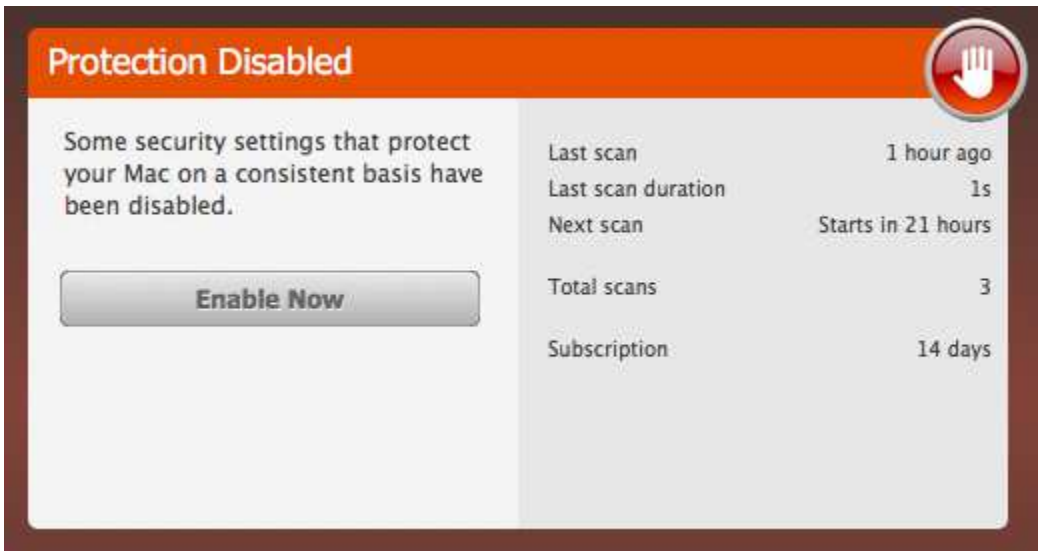
Installation is very quick and simple. To set up Webroot SecureAnywhere Antivirus for Mac, download and run the installer, then double-click the Webroot icon. You can choose the interface language, but otherwise there are no options or decisions to make. You can uninstall the program by dragging its icon from the Applications folder to the Trash.

Finding essential features

Status, **default scan**, **quarantine**, **settings**, **logs** (*Utilities\Reports*) and **subscription** (*My Account*) are all found on the program's home page. **Help** is found in the Mac menu bar. There are no scan options as such, but you can change the **default scan** from *Full Scan* to *Quick Scan* in the settings dialog; you can also **schedule scans** here. There is a *Check for Updates* feature in the Mac menu bar, though this updates the program itself, rather than the malware definitions (which are cloud based).

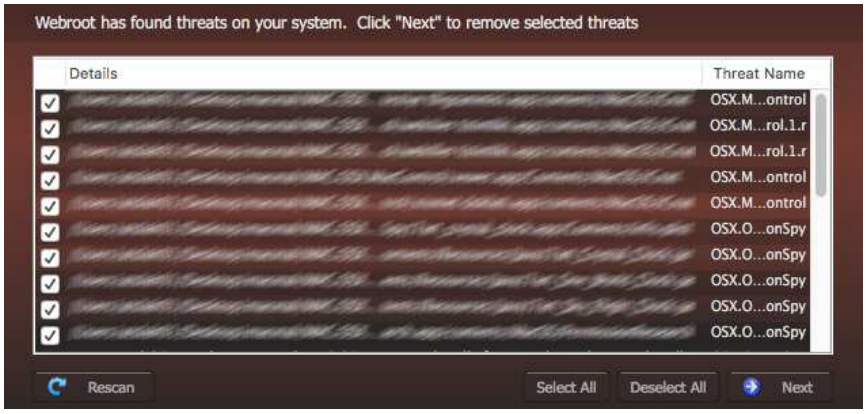
Status alerts

If real-time protection is disabled, a very obvious warning is shown in the program window. You can reactivate the protection by clicking *Enable Now*.



Behaviour on malware detection

When you connect an external drive, Webroot does not take any action by default. However, you can change this in the settings, so that it will scan on connection. As far as we know, this is actually the only way to scan an external drive. If you copy any malware from the drive to the mac Desktop, Webroot immediately detects this, and shows the scan results window:

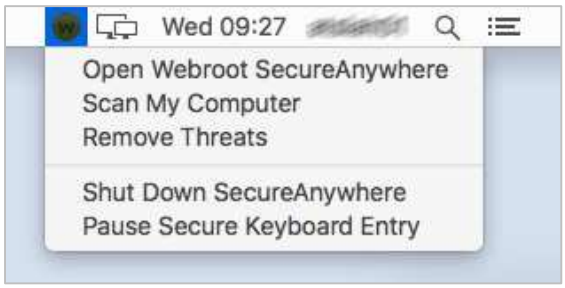


Clicking *Next* runs a quick scan of the system, and then lets you quarantine any and all threats found.

Quarantine and Logs

The quarantine window allows you to restore or permanently delete quarantined items.

System Tray menu



Help

SecureAnywhere Help in the Mac menu bar opens an online manual for the product. This provides clear and simple task-based instructions for using the program, well illustrated with screenshots.

Advanced options

Power users with a macOS Administrator account can perform the following tasks (caution is advised):

- Disable protection features using the slider button on the home page
- Make scan exclusions, using the *Ignore Folder* feature in the settings
- Restore items from quarantine (please see "Other points of interest" below)
- Shut down the program
- Uninstall the program

Standard macOS users (i.e. accounts without administrator rights) can disable protection, shut down the program completely, make scan exclusions, and restore items from quarantine, but not uninstall the program. In the settings, there is an option to prevent the program being shut down. However, this is accessible to all users, and so offers no effective protection. We could not find any means of password-protecting the settings. However, Webroot tell us that they are considering introducing this in a future version.

Other points of interest

We note that if you restore any items from quarantine, the system will regard all of these files as clean, and take no further action. You can then copy and move these files (or exact copies) around the system, including from an external drive, without detection.

Featurelist Mac (as of June 2019)											
Product name:	Avast Security for Mac	AVG AntiVirus for Mac	AVIRA Antivirus Pro for Mac	Bitdefender Antivirus for Mac	Crowdstrike Falcon for Mac	Fortinet FortiClient for Mac	F-Secure SAFE for Mac	Intego VirusBarrier X9	Kaspersky Internet Security for Mac	Trend Micro Antivirus for Mac	Webroot SecureAnywhere Antivirus for Mac
Supported Mac OS versions:	10.9 and up	10.10 and up	10.13 and up	10.10 and up	10.9 and up	10.12 and up	10.11 and up	10.8 and up	10.12 and up	10.12 and up	10.7 and up
Supported Program languages:	English, German, Czech, Spanish, Finnish, French, Italian, Dutch, Polish, Korean, Portuguese, Russian, Swedish, Norwegian	English	English, German, French, Dutch, Italian, Spanish, Portuguese, Russian, Polish, Turkish, Japanese, Chinese, Indonesian	English, German, French, Italian, Spanish, Czech, Dutch, Greek, Japanese, Korean, Polish, Portuguese, Romanian, Turkish, Russian, Vietnamese, Hungarian, Thailandese, Swedish	English	English	English, Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Vietnamese, Chinese	English, French, German, Japanese, Spanish	English, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English, German, French, Spanish, Chinese	English, Chinese, Dutch, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, Turkish
Used scan engine	proprietary	Avast	proprietary	proprietary	proprietary	proprietary	Avira	proprietary	proprietary	proprietary	proprietary
Free Trial version available? (how many days?)	Freemium	Freemium	Freemium	30 days	15 days	Freemium	30 days	30 days	30 days	30 days	14 days
Protection											
Real-Time protection	●	●	●	●	●	●	●	●	●	●	●
Prevents access to malicious and phishing web sites	●	●	●	●		●	●		●	●	●
On-demand scanner	●	●	●	●		●	●	●	●	●	●
Quarantine	●	●	●	●	●	●		●	●	●	●
Detects also PUA on Mac	●	●	●	●	●	●	●	●	●	●	●
Detects also Windows threats on Mac systems	●	●	●	●		●	●		●	●	limited detection of Windows threats
Whitelisting for specific files/folders	●	●		●	●			●	●	●	
Additional features											
Mail Protection	●	●		●	●			●		●	
Parental Control						●	●	●	●	●	
Firewall			●			●		●			●
Removable Media Blocking						●		●		●	●
Other features	Home network security		USB Scanner	Time Machine Protection, VPN, Safe Files	EDR, Managed Hunting, IOC details	Vulnerability Scan, VPN	Banking protection		Webcam protection, Private browsing, Network attack protection, Secured browser for online banking	Folder Shield	
Support											
Online Help and/or User Forum	●	●	●	●	●	●	●	●	●	●	●
Email and/or Phone Support	●	●	●	●	●	●	●	●	●	●	●
User manual				●	●	●	●	●	●	●	●
Online Chat			●	●			●	●	●	●	
Supported languages (of support)	English, German, Spanish, French, Italian, Portuguese, Russian, Czech	English, German, Czech, French, Italian, Dutch, Polish, Spanish, Portuguese, Chinese	English, German, Italian, Spanish, Portuguese, French	English, German, French, Italian, Spanish, Portuguese, Romanian, Turkish, Czech, Dutch, Greek, Japanese, Korean	English	English	English, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Swedish	English, French, Japanese	English, Arabic, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English, German, French, Spanish, Chinese	All
List Price (may vary)											
Price 1 Mac / 1 year (USD/EUR)	FREE	FREE	USD 45 / 35 EUR	USD 40 / 40 EUR	n/a (enterprise)	n/a (enterprise)	USD 60 / 60 EUR	USD 40 / 40 EUR	USD 40 / 40 EUR	USD 40 / 50 EUR	USD 40 / 35 EUR

Copyright and Disclaimer

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

AV-Comparatives
(June 2019)