Mac Security Test & Review

Mac Security Test & Review

Language: English

July 2018
Last revision: 30th July 2018

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 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 which warns when apps without a digital signature are run. Then, there is "XProtect", which checks files against known-malware signatures. Finally, apple provide 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. Despite the built-in capabilities, some security experts recommend strengthening the defenses 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.

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 very useful when you need to operate your computer in an untrusted environment, like a public location, internet café or other place 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.

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 to 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.

[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

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

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

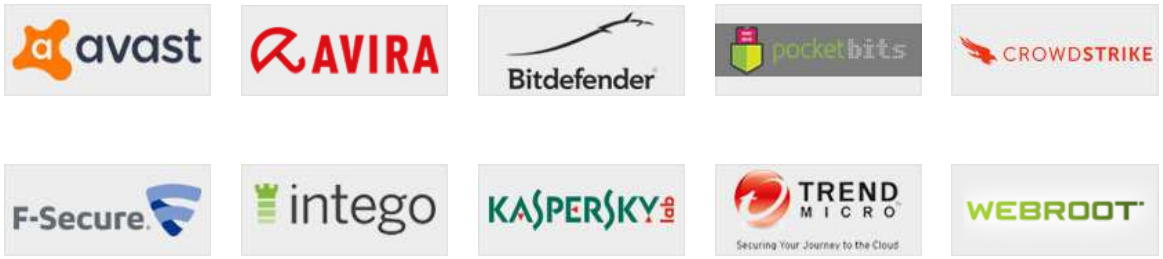
1. Do not use an administrator account for day-to-day computing
2. Use a sandboxed browser such as Google Chrome
3. Uninstall/disable the standalone Flash Player
4. Uninstall/disable Java unless it is essential for you
5. Keep your Mac operating system and third-party software up-to-date with the latest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

Security Software for macOS High Sierra

We have reviewed and tested the following products for this report, using the newest version available in July 2018:

- **Avast Security for Mac Free 13.9**
  https://www.avast.com/free-mac-security
- **AVIRA Antivirus Pro for Mac 3.10**
  https://www.avira.com/en/avira-antivirus-pro
- **Bitdefender Antivirus for Mac 6.2**
  http://www.bitdefender.com/solutions/antivirus-for-mac.html
- **BitMedic Antivirus & Malware Security 2.6**
  http://pocketbitsllc.com/apps/bitmedic-antivirus-malware-security/
- **CrowdStrike Falcon Prevent for Mac 4.9**
  https://www.crowdstrike.com/products/falcon-prevent/
- **F-Secure SAFE for Mac 17.3**
  https://www.f-secure.com/en/web/home_global/safe
- **Intego Mac Premium Bundle 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 8.0**
  https://www.trendmicro.com/en_us/forHome/products/antivirus-for-mac.html
- **Webroot SecureAnywhere Internet Security Complete for Mac 9.0**
  http://www.webroot.com/us/en/home/products/complete

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



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 July 2018, and used very recent macOS malware that had appeared in the preceding few months. We used a total of 310 recent and representative samples of genuine malware that runs on current macOS systems (10.11 and higher).

A survey of Mac security experts showed that in total, several tens of thousands of unique mac samples had appeared in the first half of 2018. However, this figure might include 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 less than one dozen new families, and in total less than two dozen new variants, of true Mac malware seen in 2018. Some of these will only run on older versions of the macOS operating system. Consequently, the 310 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%).

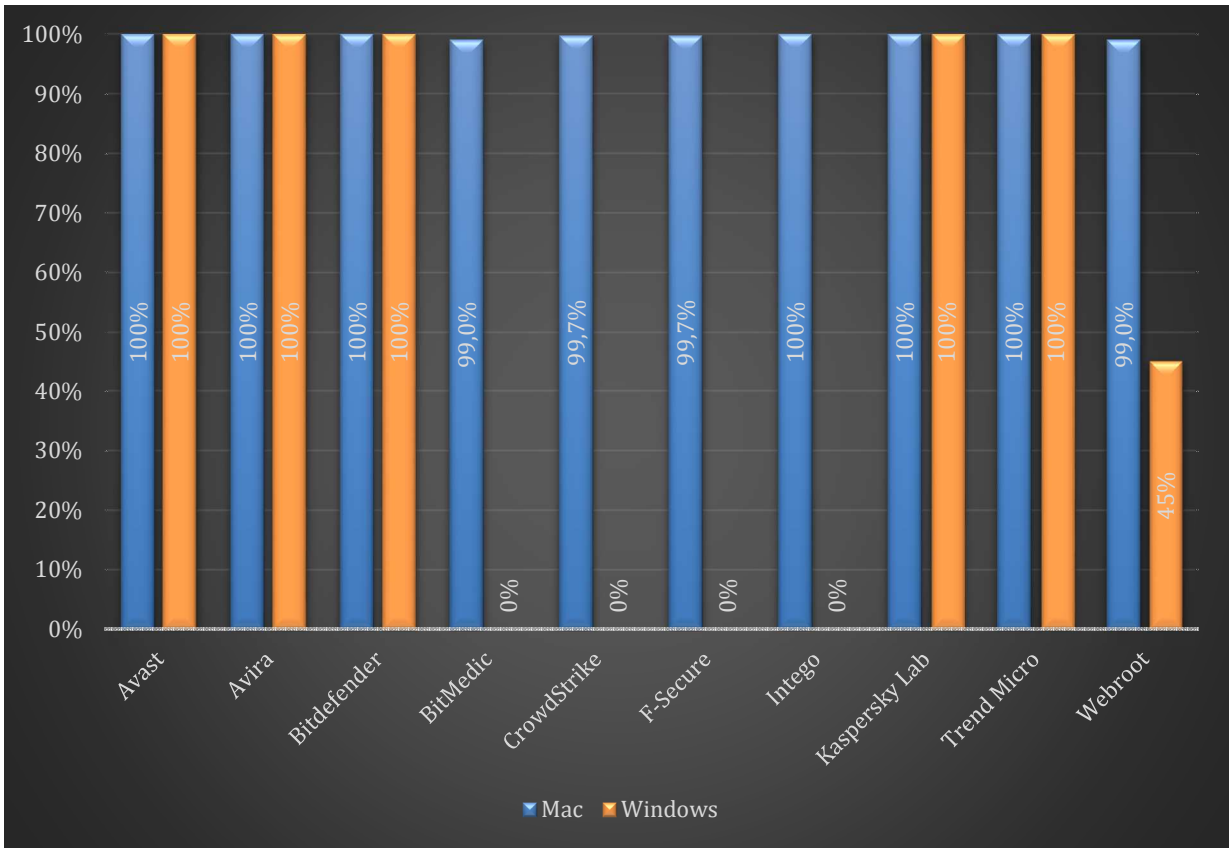
Before the test, the Mac OS systems were updated and an image created; no further OS updates were then applied. Each program was installed on the freshly imaged machine and the definitions updated to the 10th July 2018. The Mac remained connected to the Internet during the tests, so that cloud services could be used. A USB flash drive containing the malware samples was then plugged in to the test computer. At this stage, some antivirus programs recognised some of the samples. We then ran an-on demand scan of the flash drive, either from the context menu if available, or from the main program window if not. Samples found were quarantined or deleted. After this, 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. After each active infection, a full scan was performed, in order to give the products a chance to check for active malware.

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

Most of the Mac security products in our review claim to detect Windows malware as well as Mac malware, thus ensuring that the user's computer does not inadvertently act as a conduit for programs that could attack Windows PCs. For this reason, we also checked if the Mac antivirus products detect Windows malware. We used 1,000 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 Mac OS.

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

Product	Mac Malware Protection 310 Mac samples	Windows Malware Detection[3] 1000 prevalent Windows samples
Avast Security for Mac Free	**100%**	100%
Avira Antivirus Pro for Mac	**100%**	100%
Bitdefender Antivirus for Mac	**100%**	100%
BitMedic Antivirus & Malware Security	**99.0%**	0%
CrowdStrike Falcon Prevent for Mac	**99.7%**	0%
F-Secure SAFE for Mac	**99.7%**	0%
Intego Mac Premium Bundle X9	**100%**	0%
Kaspersky Internet Security for Mac	**100%**	100%
Trend Micro Antivirus for Mac	**100%**	100%
Webroot SecureAnywhere for Mac	**99.0%**	45%



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

[3] 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, all of the products we have reviewed receive our Approved Security Product award.

A summary of the review is shown below. Users should also consider other factors, such as price and support, before choosing a product. We always recommend installing a trial version of any paid-for product before making a purchase.

Looking at the products, there are offerings from all of the well-known vendors: **Avast**, **Avira**, **Bitdefender**, **F-Secure**, **Intego, Kaspersky Lab, Trend Micro** and **Webroot** all offer strong products with a varying mix of capabilities. Always make sure that you are buying the appropriate bundle for your needs, and also be aware that there are often special offers and bundles which can offer a lower cost for first-year purchasing. It is also a good idea to watch out for indications of pricing that will apply from the second year, as this can sometimes be a significant rise in cost.

For each product, especially those with a wide range of capabilities, ensure that all of the functionality that you require has been installed. If there are web browser extensions, for example, then it is wise to enable these. Other functionality might be valuable to you, but not required immediately – parental control, VPN and so forth. Nevertheless, it is wise to ensure that you have a good working knowledge of the capabilities of package when you install it, so you are aware of what can be enabled later on if necessary.

BitMedic might be a good fit for your needs. However, we felt it had room for improvement in its user interface, configuration tools and daily operational performance.

In the business end of the market, **CrowdStrike** brings a very impressive array of capabilities to the medium and larger enterprise. The macOS component is just one part of the larger platform here, and the range of tools, the design and deployment flexibility, and the raw analytical power that it brings places it in quite a different space from normal home/small office-oriented AV packages. Such a platform requires significant investment both in the product itself, but also in the implementation. However, when deployed appropriate, supported within the enterprise, there is no doubt that macOS can be effectively managed within the broader business context.

Review format

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

What is it?

Here we look at the type of scenario the product is aimed at, including whether it is free or paid for.

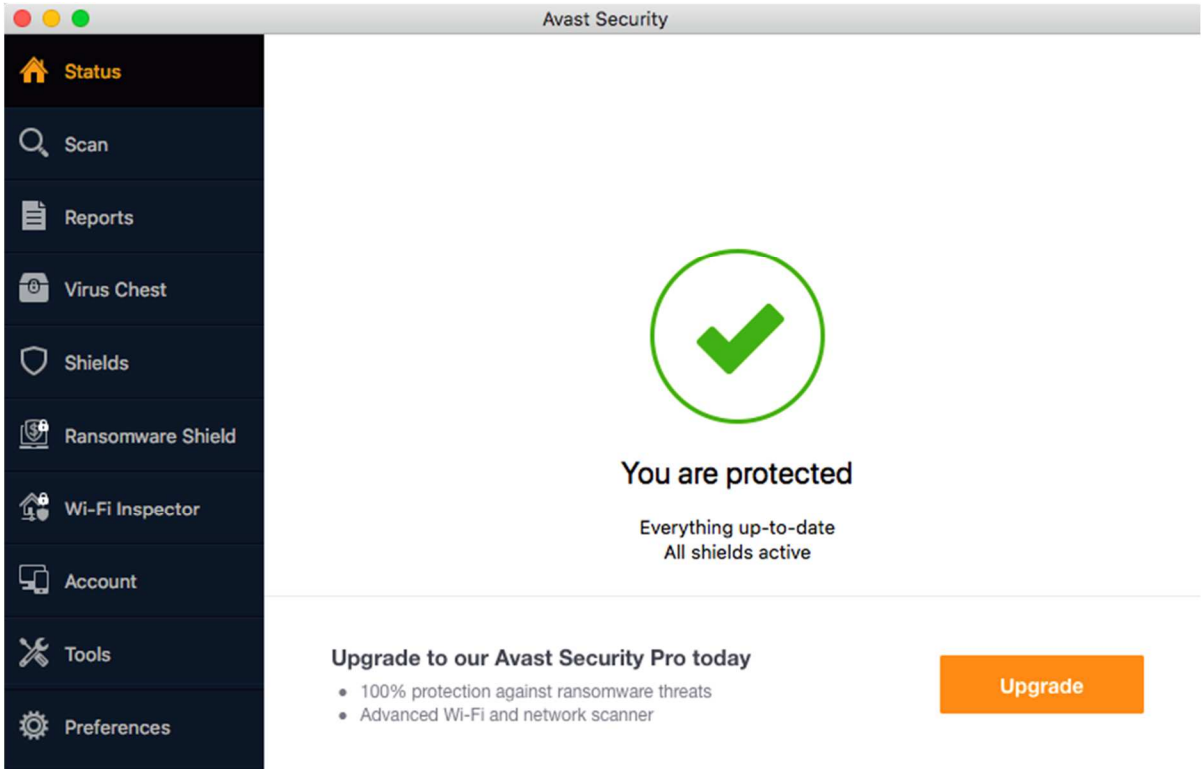
Product installation and configuration

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.

Ongoing use

Here we consider the interaction the user will have with the program when using the GUI to carry out everyday tasks. These include such things as monitoring status, responding to alerts, dealing with malware found, and running scans on the system and removeable devices.

Avast Security for Mac Free



What is it?

Avast Security for Mac is an antivirus product for macOS. Licensing is free. There are adverts within the app enticing you to upgrade to the paid-for features. Some functionality that appears to be built in is either trialware (VPN) or hooks to an upgrade (Ransomware Shield, Wi-Fi Inspector).

Product information on vendor's website: https://www.avast.com/en-gb/free-mac-security

Online support: https://support.avast.com/en-gb

Overall

Avast Security Free for Mac is a solid and competent package. All the components appear to work well, and it catches malware of all types in a competent fashion. It is reasonably easy to use, and comes with useful capabilities. Some of the more powerful capabilities are trialware or demoware, but this is to be expected in a free product. Advertising is not intrusive, and you are left with the feeling that this is a useful free addition to any standalone Mac laptop or desktop computer. It is suitable for users of all levels, and appears to add value to the platform for no financial outlay. As such it is to be recommended.

Part 1: Product Installation and Configuration

Installation is relatively straightforward. Download the installer from the web site and run the installer package. The installer package includes an uninstaller routine, or this can be run from the app itself. During installation you are asked whether you want to install additional items – Avast SecureLine VPN, Avast Passwords and Avast SafePrice. With macOS 10.13, in the final stages of installation, you will get an install warning from macOS stating that a System Extension has been blocked. This is part of macOS security preventing unauthorised system extension installation. Simply click on the Open Security Preferences button and authorise the extension installation.

After installation is completed, your work is not done yet. The web browser extensions are not installed by default, nor are you told that this needs to be done. To fix this, you need to dig into Preferences and then Browsers. Here you will see that both Online Security and SafePrice are not supported in Safari. The extensions for Chrome and Firefox need to be installed by pressing the buttons. This is somewhat fiddly, especially the Online Security plugin for Firefox.

The other components are separate products, and require additional setup, or payment for a full product. For example, SecureLine VPN has a 7-day trial, after which yo have to buy it. Avast Passwords requires full setup too, but this appears to be fully functional. Part of the setup includes installation onto Safari.

Part 2: Ongoing use

By default, you see little of Avast in normal use. There is an icon on the top status bar, along with tools for SecureLine VPN and Avast Passwords if installed. You can choose to see basic status here, including the last status messages, or you can open the main Avast window.

The main Avast window has a set of menu items down the left-hand side, and a minimal set of commands in the main Apple menu bar at the top (this does include an uninstall routine, which is useful).

The main status window is clear and clean – you get a green tick mark, and confirmation that you are protected and that everything is up to date. There is an advert here to ask you to upgrade to Avast Security Pro, but it is not too intrusive. The Scan menu offers full system scan, removable volumes scan, custom scan, home network security scan and a scheduled scan capability. The home network scan does a ping around your home LAN and tries to identify which devices are present. It then digs into deeper information and offers remediation and security changes on devices which it deems to be weakly protected.

Reports gives you a view of recent activity, and Virus Chest allows you to see which malware has been quarantined. You can delete the files or restore them to their original locations from here. Shields shows a real time graphical view of the operational status of the File Shield, Mail Shield and Web Shield components.

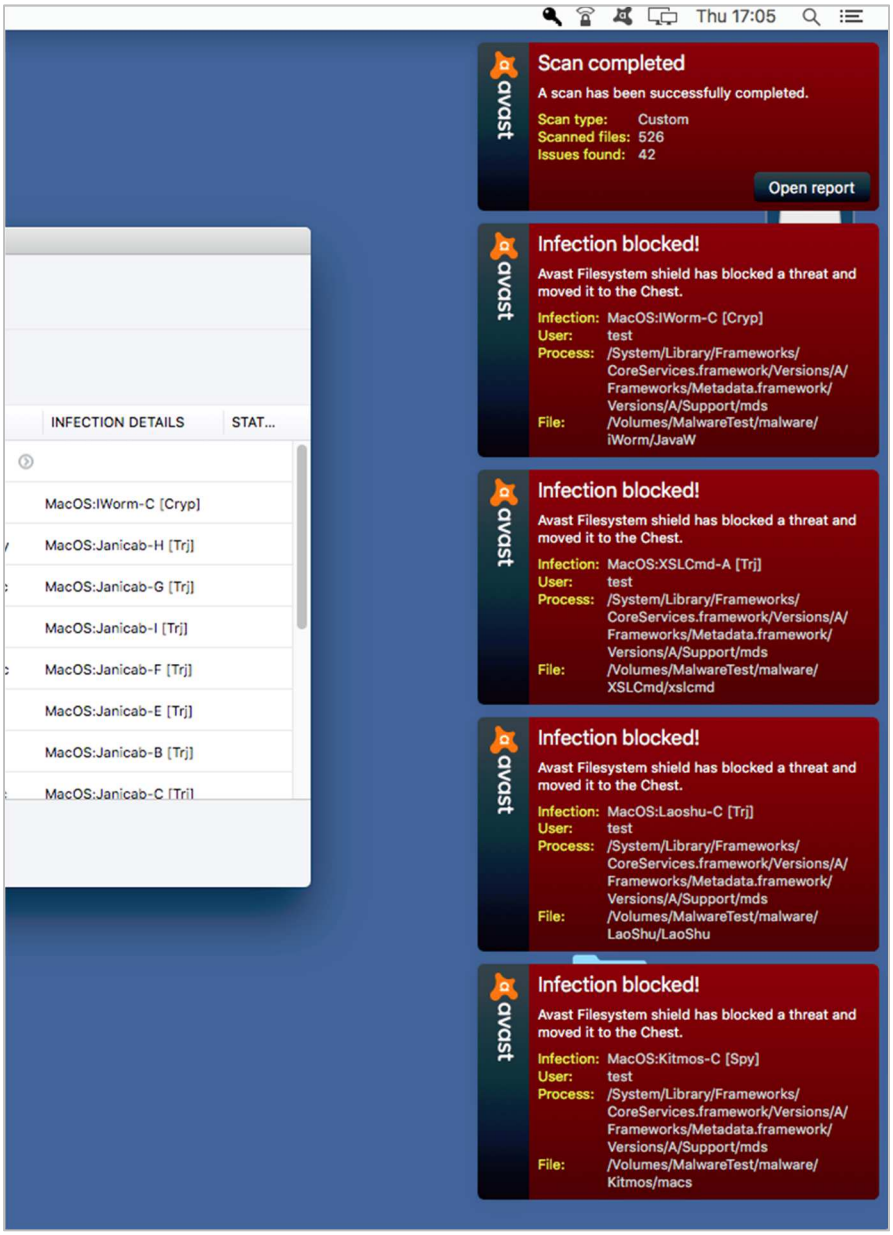
Ransomware Shield and Wi-Fi Inspector require upgrades to the paid-for version for the functionality to be enabled.

Account allows you to log into an Avast account if you have one. Tools lets you open the SecureLine VPN tool and the Avast Passwords app, or to activate them on your iPhone.

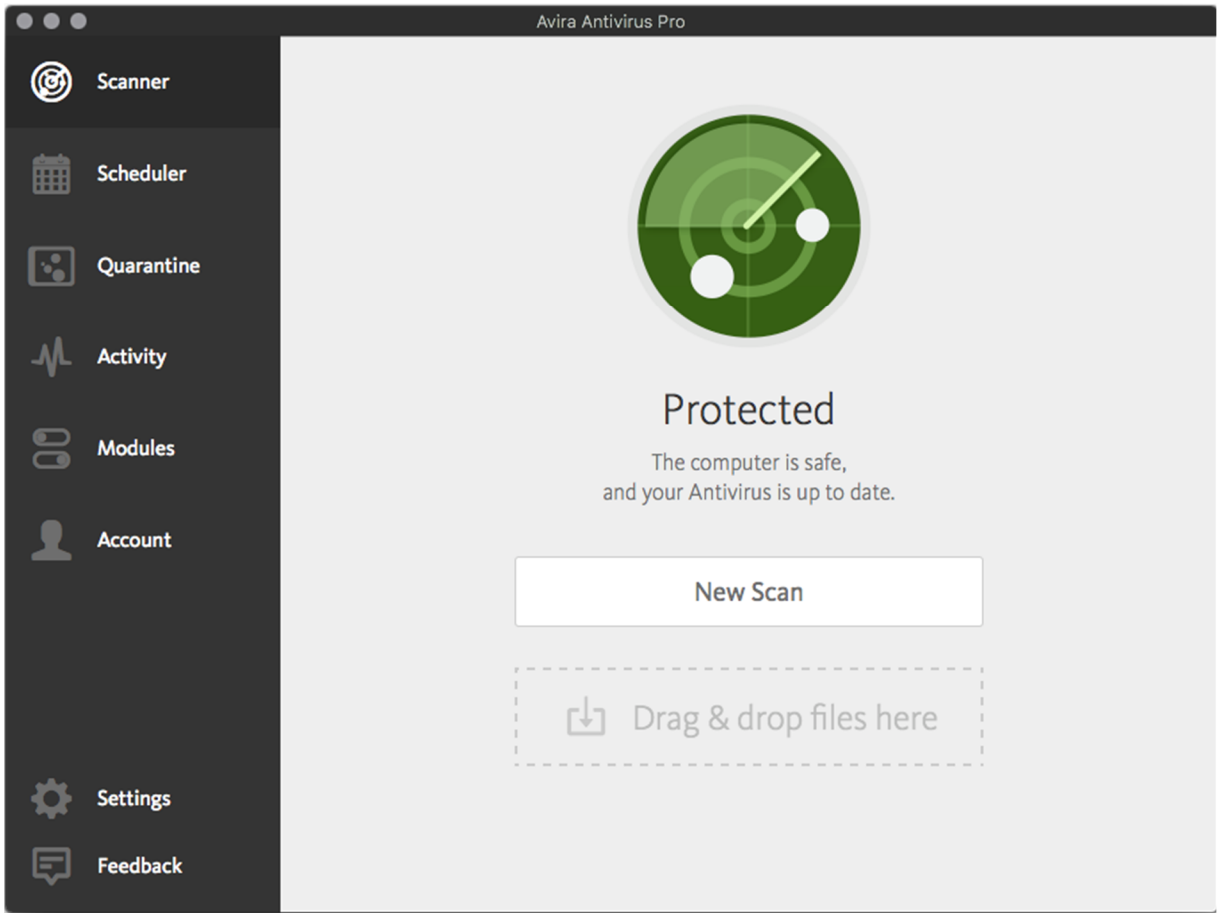
Finally, Preferences has all the settings for the various components of the app.

The app is quite simple to use, and is clear and clean in operation. When you introduce malware to the system, there are status windows which appear in red in the top right corner of the desktop. If multiple malware threats are found, then multiple boxes start stacking vertically down the right-hand side of the screen. In a major malware situation, this can somewhat overflow the screen estate, and a more crafted arrangement here would be an improvement.

The malware warning windows themselves are reasonably useful, if somewhat dense and geeky. The information held within is of value, but it could be a little more customer friendly, especially for the less-experienced user.



Avira Antivirus Pro for Mac



What is it?

Avira Antivirus Pro is a paid-for antivirus product for macOS. There are very many products available on the Avira website, but once you have found the right page for Avira Antivirus Pro (link below), purchasing the license is straightforward, and the main installation is not complicated.

Product information on vendor's website: https://www.avira.com/en/avira-antivirus-pro

Online support: https://www.avira.com/en/support

Overall

The product is competent in what it does, although some users might want more feedback and interaction with the capabilities of the system. If you are looking for a quiet, lightweight and unobtrusive AV package, then this might well be a good choice.

Part 1: Product Installation and Configuration

Purchase and installation are quite straightforward. You make the purchase, download and run the installer, then create a My Avira account which shows you your licence key. Please note that the software initially installs under the name of Avira Antivirus Free, but when you enter the licence key, this immediately changes to Avira Antivirus Pro.

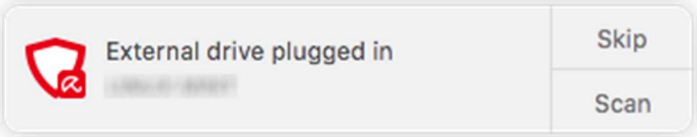
The My Avira webpage allows you to manage licenses and oversee configurations. However, we could find no way of managing tasks such as remotely initiating a scan, although things like this would be useful in a family context.

Part 2: Ongoing use

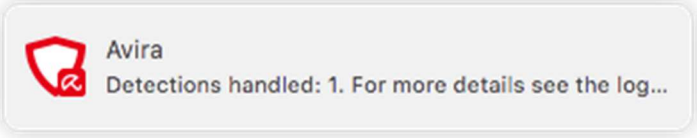
Normally you will see little of Avira in operation. There is a status icon at the top of the screen, and from here you can click to initiate an update, run a quick scan, disable the protection, or open the main app window.

The main app window is clear and clean in operation, and tells you immediately if something is wrong. There are eight menu items down the left-hand side. On the Scanner (status) page, you can initiate a new scan. Scheduler lets you run scans on a schedule, Quarantine is self-explanatory, and Activity displays scan logs. The Modules section allows you to enable or disable the 3 main components of the products (real-time protection, cloud-based protection features, and USB scanner). There is also a Firewall switch, which you can use to enable or disable the macOS firewall that's built into the operating system. Account allows you to log in and log out of the account. Settings allows you to change some very basic settings, such as update notifications and language of the GUI. Finally, Feedback opens a page of the Avira website where you can rate the product.

If you enable the USB Scanning function, then Avira notices when you plug in a USB storage device, and offers to scan it for you. This is a useful capability and one that users should employ, even though it is not enabled by default.

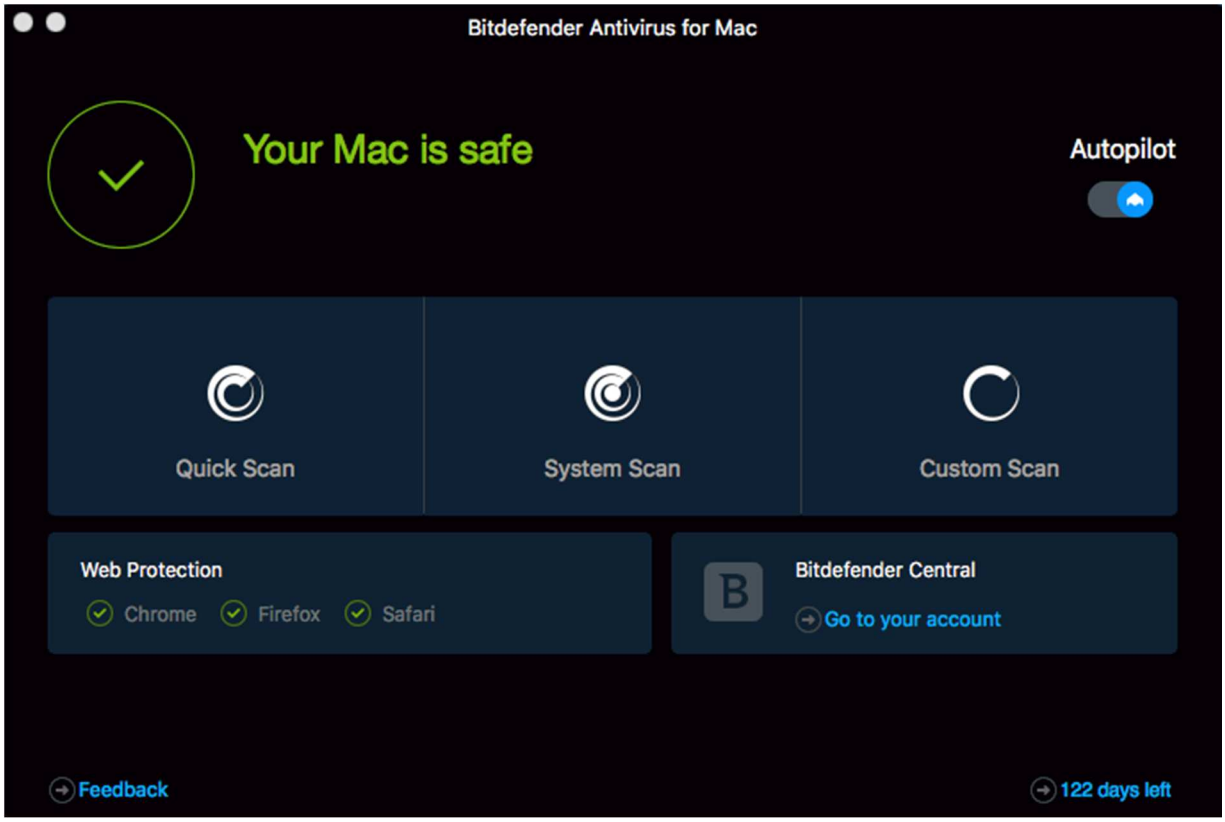


If malware is detected by the real-time protection, e.g. when copying files from an external device, you get an alert appearing in the top right-hand corner of the desktop:



For non-expert users, it might not be clear that "the log" noted in the warning is actually the "Activity" page in the main program window. We also note that the information provided on this page is very spartan – only the detection time and a very concise detection name are provided. However, more information can be found on any individual item by going to the Quarantine page and clicking the relevant "i" button.

Bitdefender Antivirus for Mac



What is it?

Bitdefender Antivirus for Mac is a paid-for antivirus product for macOS. It claims to offer full antivirus features, providing protection against Mac and PC malware. It comes with a VPN capability, which is new, offering 200MB of tunnelled traffic per day for free. This can be increased to unlimited traffic if you purchase a Premium account.

Licensing is straightforward and can be purchased in multiple units and years.

There is a demo version for download, and this runs for 30 days.

Product information on vendor's website: https://www.bitdefender.co.uk/solutions/antivirus-for-mac.html

Online support: https://www.bitdefender.co.uk/consumer/support/

Overall

This is a strong and well-designed package. Setup is straightforward, makes clear that the browser extensions need to be installed, and provides the tools to do this in a simple and logical fashion. The program presents a clear and obvious UI to the user, and the Autopilot feature takes almost all decision-making away from the user. The only time the user has to make a choice is if the handling of a piece of malware has failed, and the user has to decide whether to delete the file. Overall, there is much to like here, and the calm way in which the package operates is praiseworthy.

Part 1: Product Installation and configuration

Installation is easy to do, helped by the trial package which you can download for free. Purchasing is straightforward too. The installer gets the program up and running quickly with minimal interruption to the user.

As part of the installation, you will be asked if you want to enable "Safe Files" by default. This is an anti-ransomware feature which keeps a close eye on key folders for any sign of document encryption by ransomware. The default selection of Desktop, Documents, Downloads and Pictures is a good starting point, and it allows you to add in other folders easily (for example you might choose Music or a cloud-storage folder tree like Dropbox). Additionally, Bitdefender can watch your Apple Time Machine backups, to ensure that your backups have not been tampered with.

After installation, you open the main window of the app. Here it is made clear that the Web Protection features are not installed by default and that you have to continue to this step by pressing the "Fix Now" button. Bitdefender provides browser extensions for Chrome, Firefox and Safari. Installation of these plug-ins is straightforward, and guided by the installer app.

VPN tunnelling is provided as part of the setup program, and this is straightforward to use.

Part 2: Ongoing use

Like most end-user focussed packages, you see little of the operation of Bitdefender in daily use. Opening the main window shows a clear and well-designed layout which is obvious to navigate. The Autopilot feature is enabled, which allows Bitdefender to make decisions on your behalf in an appropriate way. The main window has a rather dark (black and grey) design, which is not maintained through the rest of the app. However, it does not impede operation.

If you want to scan files for malware, it is very simple and straightforward. And, like most AV packages, you can right click a file, folder or drive and choose "scan" for easy access to the functionality.

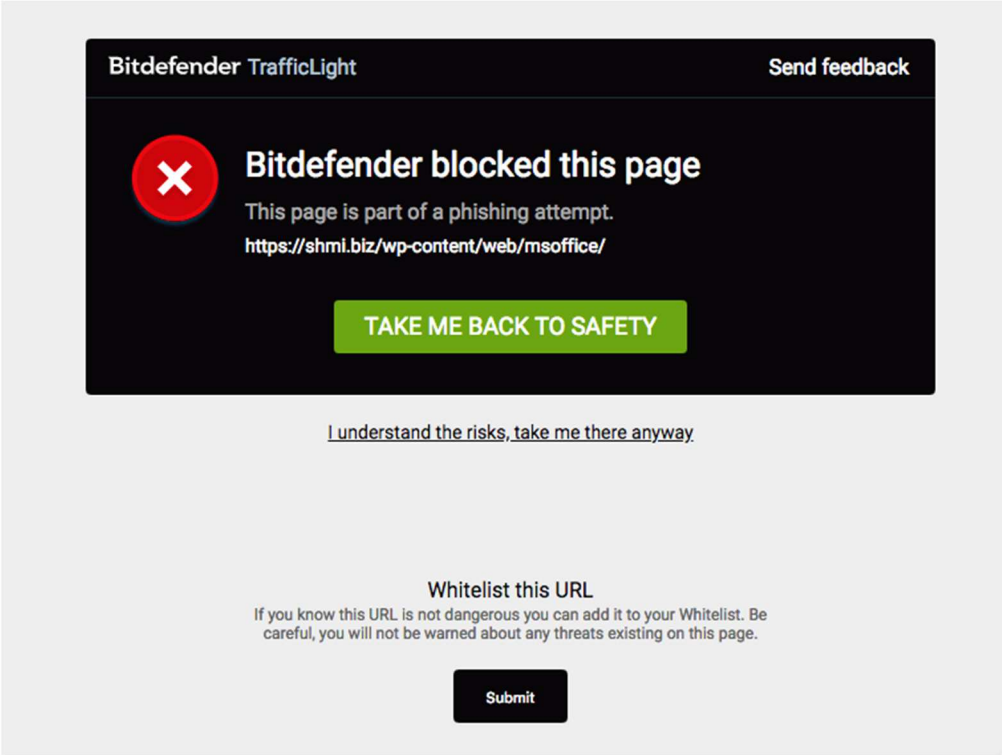
The web browser security works well, and picked up on phishing attempts. The message you get is clear and obvious, and there is a "Take me back to safety" button here. We liked the fact that this worked in all three of the browsers we had running (Chrome, Firefox and Safari).

When malware lands on the computer, the program reacts immediately as you would expect. It even automatically scans USB sticks on insertion, cleaning them without user intervention. We liked this, as it provides a level of protection that others do not offer by default.

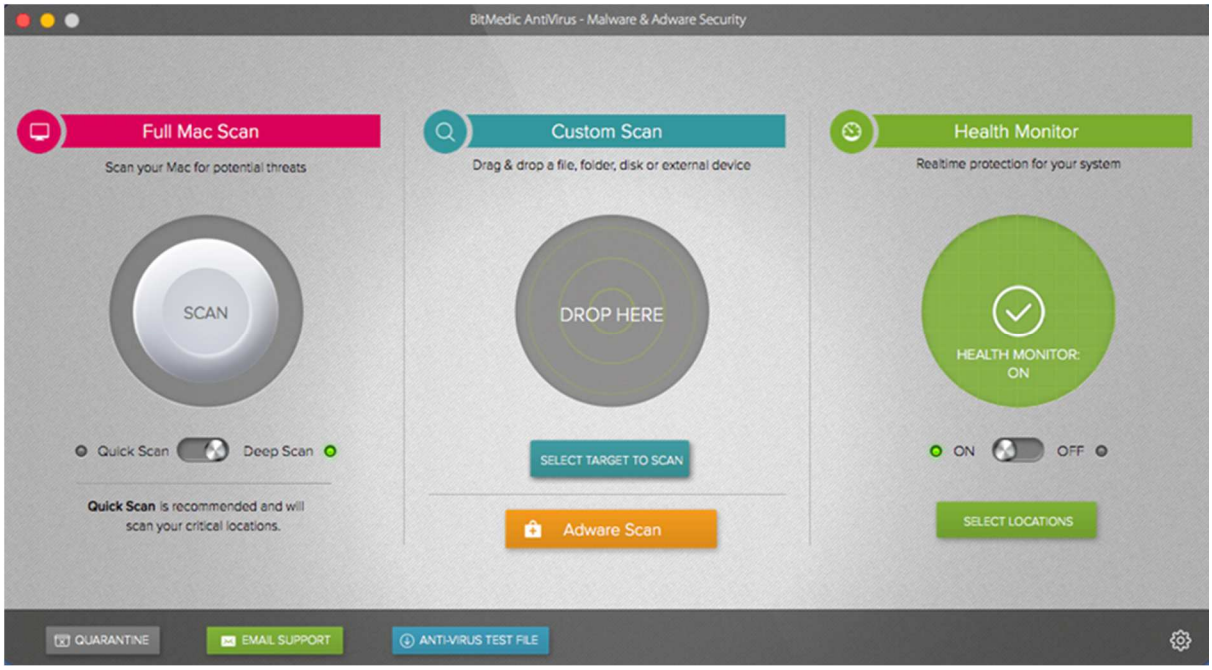
Despite the vendor only claiming that it protects you against Windows and macOS malware, it had no issues discovering and cleaning Android malware too, offering a fully rounded solution here.

The only concern we have is when the package is presented with a lot of malware to clean. It performs this process just fine, but the messaging at the top right can be somewhat laboured, as each message is replaced by the next. There is room for improvement here, without resorting to the vertical stacking of messages which can somewhat overwhelm the screen on other packages. One status window that switches to "handling multiple issues..." would be clearer and more helpful here.

The messaging itself is clear, but it would be improved if there was a link to a virus encyclopaedia detailing each item.



BitMedic Antivirus & Malware Security



What is it?

BitMedic is a paid-for antivirus product for macOS. It is purchased from the Apple Store, and cannot be bought or downloaded from the vendor's website, unlike other AV products from competing vendors. There is no trial period. It appears that you can install it on multiple machines, providing they are logged into the same Apple Store account. There is a "Lite" version of the application available on the Apple Store, called BitMedic AntiVirus Lite, which is free to try. It lets you remove malware found in the first scan; the next time you run a scan and malware is found, you have to pay to remove it.

Product information on vendor's website: http://pocketbitsllc.com/apps/bitmedic-antivirus-malware-security/

Online support: http://support.pocketbitsllc.com/category/bitmedic-antivirus/

Overall

Clearly there is a strong AV engine at the core of this product. However, it is somewhat let down by the UI design, operational issues and rather confusing settings.

Part 1: Product Installation and configuration

Installation is simple and straightforward, as you would expect from an Apple App Store purchase. When you first run the program after installation, you get a five-page tutorial covering the main points of the app. The menu system is the default Mac app menu bar.

At this point, we started to have some doubts about the BitMedic app. The UI has some unusual "hi-fi style" slider buttons, and textual content, including the title bar, which was rather too small to read.

The “Antivirus test file” button takes you to a page where the EICAR test file is described, along with a button to initiate download. We note that this will only be detected by Bitmedic if the real-time protections is switched on, and the app itself is set to autostart (neither of these being default settings).

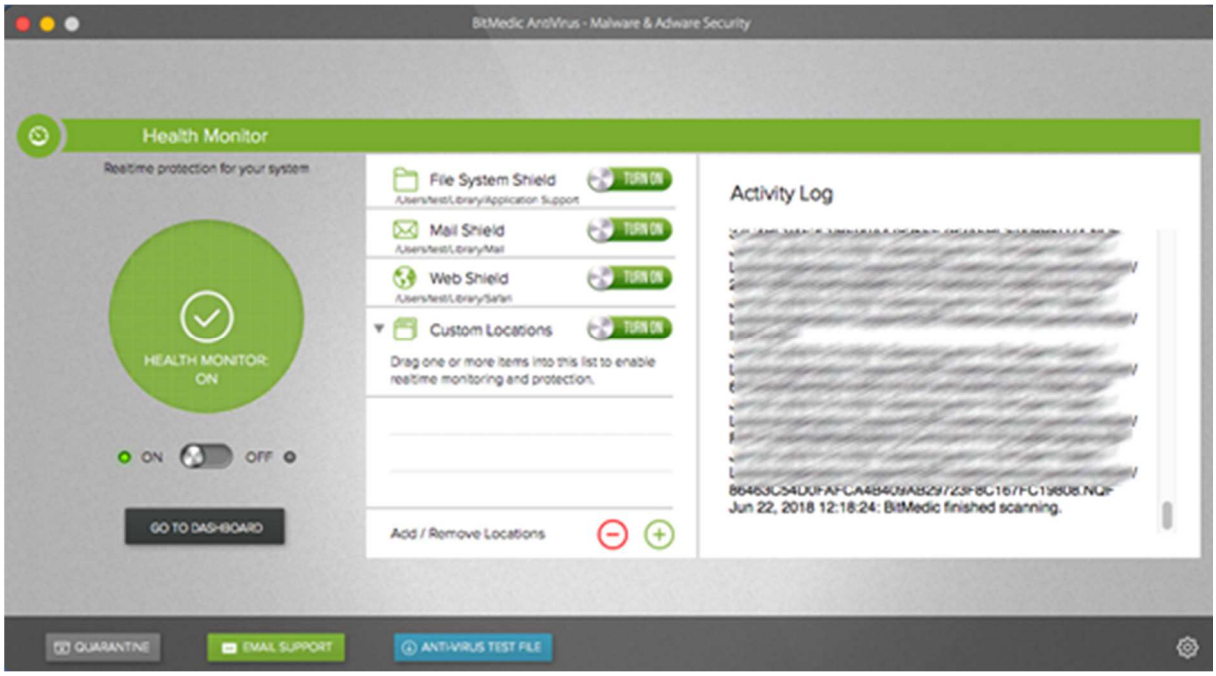
We were a little confused by the On/Off slider buttons and their labels; these have the On state with the slider to the left, as opposed to the more-or-less standard right=on configuration. We also found that the “Scan with BitMedic” menu item has no apparent effect.

Part 2: Ongoing use

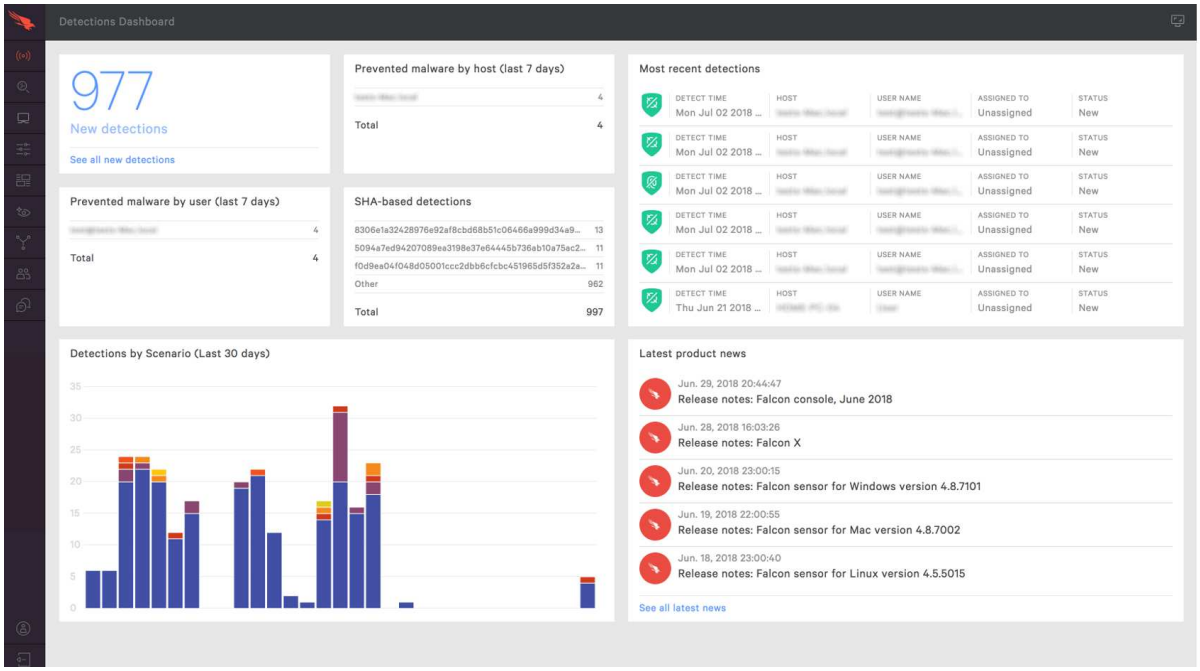
The UI is split between three large areas for scanning: full Mac scan, custom scan, and health monitor. If you go into Health monitor and click on the small unlabelled Preferences button, then the Preferences window opens. Clicking on “open quarantine folder” opens a Mac file system folder view of the quarantine folder. You can drag and drop captured malware out of here with no intervention, although the quarantined items have their file extension replaced by “qua” so they won’t execute.

There was no automatic recognition of the plugging in of a USB stick. There was no real-time file system monitoring either, which meant that a user copying files to USB sticks could pass on malware to friends and family. On attempting to execute Mac malware, we did a full scan and it reported that OSX.Malware.Agent-1438593 was in the file /Application Suport/JavaW/JavaW, but its status for this malware was “Process Failed”. There was no other indication of what to do, or if the cleaning had been successful or not.

Finally, we tried the Adware Scan function. A window popped up saying “We will scan for all known adware and also remove your extensions, cookies and caches to restore your browser. Don’t worry, bookmarks and history will not be affected”. This seems a little excessive if you have known-good extensions in place.



CrowdStrike Falcon Prevent for Mac



What is it?

CrowdStrike is a multi-platform product for business. The product provides protection for Windows and Linux machines as well as macOS. It would be suitable for larger enterprises and organisations that use macOS devices. Please note that management is carried out entirely through a web-based console, and is effectively the same for any client PC, regardless of whether it uses macOS or another operating system.

Product information vendor's website: https://www.crowdstrike.com/products/

Overall

CrowdStrike Falcon is very comprehensive platform, providing not only protection, but also detailed detection and analysis services. However, in our opinion it would require a significant investment of time to discover and make best use of its features, and so is very much aimed at larger organisations that can either train a dedicated team, or make use of specialised external consultancy.

Part 1: Product Installation and deployment

The management console is cloud based, and so requires no installation or configuration. The client protection software is called a "sensor", and is straightforward to deploy to clients by downloading from the console. You have to copy a checksum ID from the console, and execute the installer using the Terminal (command line). Once installed on a macOS computer, the sensor is effectively invisible to the user, i.e. there is no user interface.

Part 2: Ongoing use

The cloud-based management console has 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, Support.

Activity is a dashboard, which provides a good overview of the most important items with clear graphics. You can see detections by scenario over the last 30 days, and you can drill down into the Detections submenu to get more detail. There is a strong reporting infrastructure, with good filtering options prominently presented. You can also check quarantined files and real-time responses.

The Investigate menu has a comprehensive search facility, covering hosts, hashes, users, IP addresses, domain and event searching. This lets you locate specific issues on the network, and allows you to set the time period to be investigated.

The Hosts menu provides an overview of client installations, by version and platform, and shows which clients 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 controls the policy-driven process within CrowdStrike Falcon. It lets you create policy definitions, covering the entire AV and prevention functionality of the platform, which can then be applied to groups of clients. You can set different policies for Windows and Mac clients.

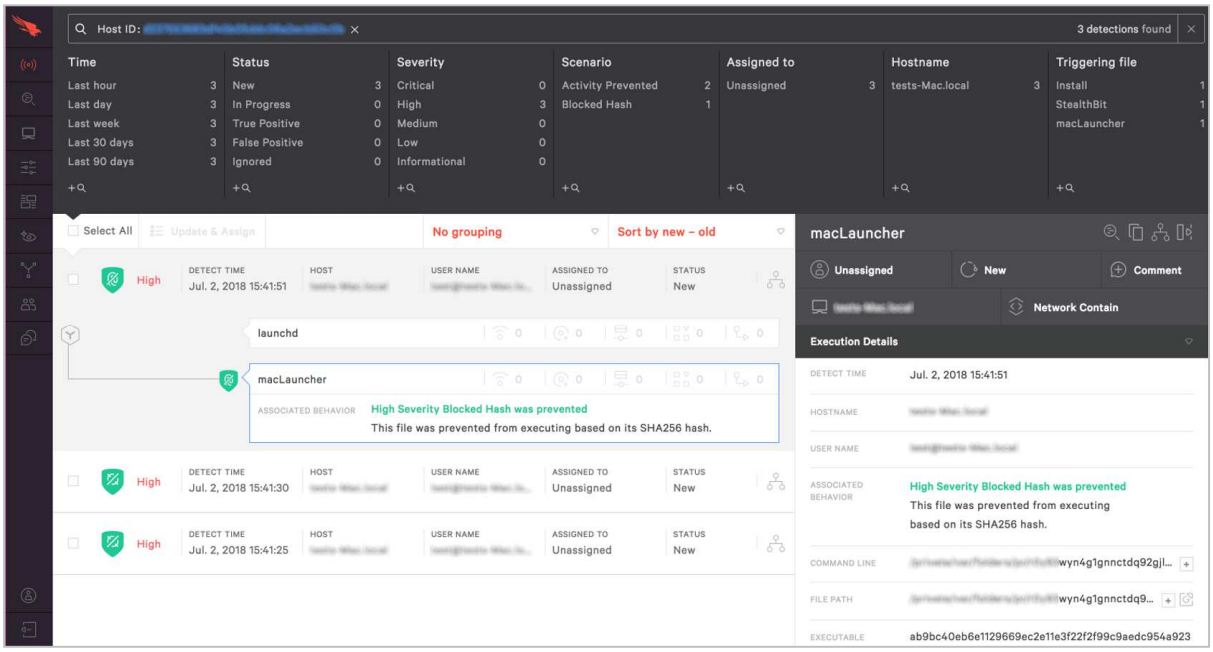
The Dashboards menu shows the executive summary view of the estate, with detailed graphics for detections by scenario and severity, and identifications of the top 10 users, hosts and files with most detections. You can also get comprehensive details of what is happening in any area. It is possible to search using a wide range of relevant items, and use this to discover what has happened on the network during an outbreak, such as where malware entered, how it was attempting to execute, what processes it was using, and how it was contained. Administrators who understand the platform well have a very powerful set of audit and analysis tools here.

The Discover menu lets you explore the network by application inventory, asset, MAC address, accounts and other app/process-based inventory.

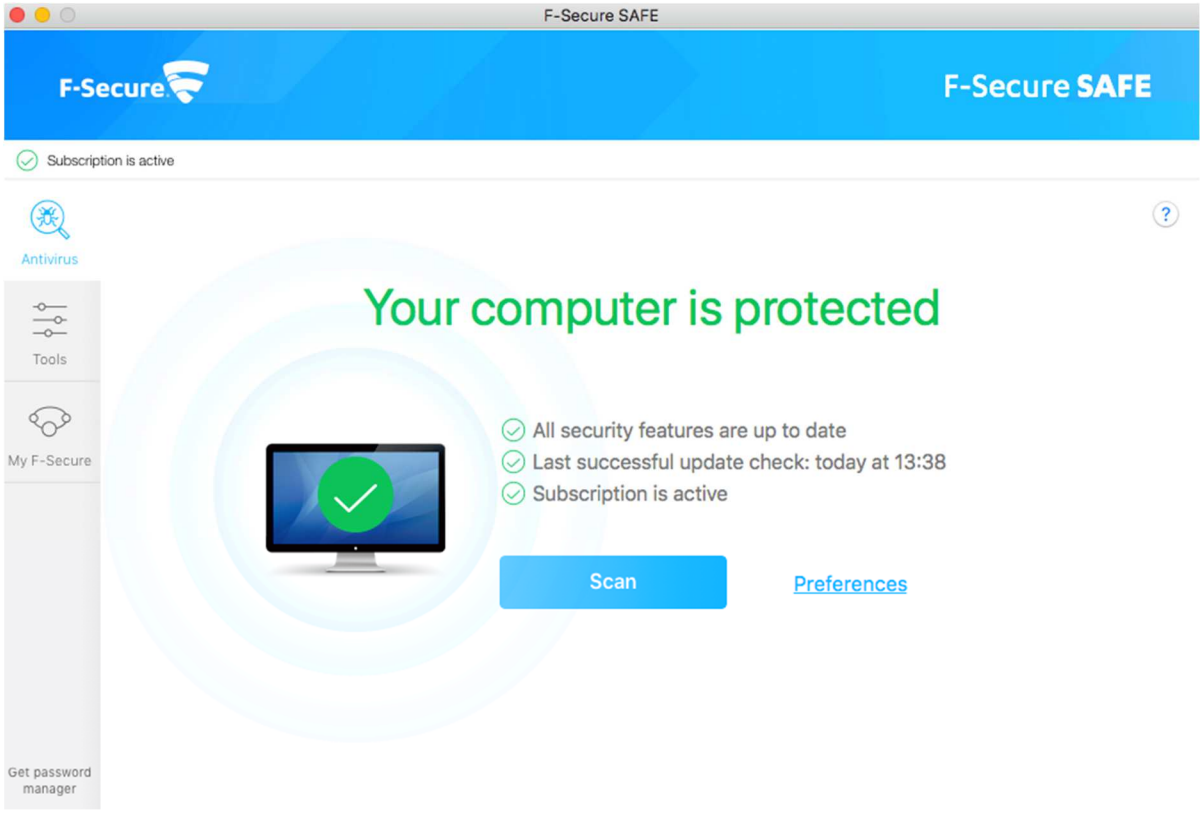
The Intelligence menu displays an overview of the current AV threat landscape according to CrowdStrike. This can be shown by geographical origin of threat, target industry, target country, and even the suspected motivation (e.g. espionage, criminal, Hacktivist or destruction). Each threat is detailed by these parameters, and clicking "View Profile" on the threat provides a comprehensive analysis and explanation of that specific threat. This is a comprehensive resource, which is unusual and most welcome.

The Users menu lets you create user profiles for console administrators and other management roles within the organisation. There are pre-built user profiles already created for Endpoint manager, Event Viewer, Administrator, Analyst, Investigator, Real Time Responder etc, allowing you to map these roles to existing company structures, or to custom build new roles as required. Two-factor authentication appears to be mandatory for all logins here, and this needs to be considered as part of the deployment design.

Finally, there is a comprehensive help and support function within the product, as well as the Intelligence capability.



F-Secure SAFE for Mac



What is it?

F-Secure Safe for Mac is a paid-for AV product for macOS. You can buy subscription bundles covering a number of computers, and these can be a mix of device platforms. Purchasing the license is straightforward, and the main installation is not complicated.

Product information on vendor's website: https://www.f-secure.com/en_GB/web/home_gb/safe

Online support: https://www.f-secure.com/en_GB/web/home_gb/support

Overall

This is a strong product with a well-designed UI and capabilities. The setup and configuration could be more complete, but the only significant area of concern are the browser extension installations. Operationally, the product is easy to use, catches the malware and does a strong job of handling issues thrown at it. Parts of the UI could be clearer, especially around the Firewall capability. The help documentation is comprehensive, but we found some issues with it on specific areas of the functionality. The online web console is useful for managing the accounts and licensing, and to help with installation and deployment, but we would have liked to see the opportunity for a remote initiated update and scan to be delivered to the client. This would allow better control in a home environment, with a parent ensuring that a child's computer is up to date. Or in a small business environment where an IT manager wants to ensure a travelling salesman is kept safe. "My F-Secure" doesn't currently allow access to the family web filtering settings on Mac computers, though this is scheduled for later in 2018. Overall, it is a strong product that works well.

Part 1: Product Installation and configuration

Purchasing and installing the app is not complicated, and the easiest route for installation is to log into My F-Secure and choose to install onto the current machine. This downloads the appropriate installer, which can then be run.

One criticism that can be raised here is that the F-Secure web pages are really quite opaque as to what functionality you get, especially when comparing a cross-platform suite such as SAFE. There is an online tool which allows you to select capabilities important to you, and the website then recommends a product. SAFE claims to cover the areas of antivirus, browsing and banking protection, family rules and ransomware protection. A comparison page can be found here: https://www.f-secure.com/en_GB/web/home_gb/compare-products

Part 2: Ongoing use

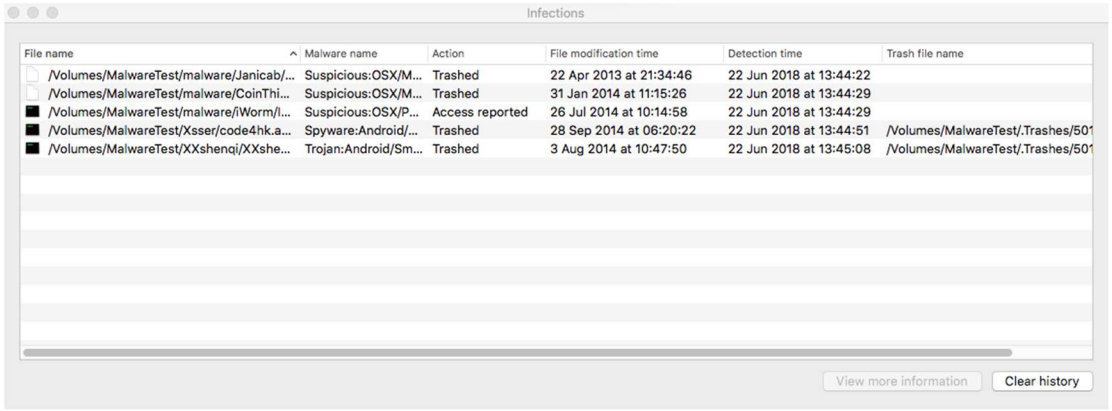
Once you have the product installed, it is a quiet application in normal operation. There is an icon on the top menu bar, and this gives access to the main window. You can also access preferences, malware scanning, updating and reporting from here. Usefully it also tells you that your computer is protected and when it was last updated. The main application window is clear and easy to operate. There are three icons on the left-hand side. Antivirus takes you to a status page which gives an overview of the current system status, and tells you if the subscription is active. The Scan button starts a scan of the system.

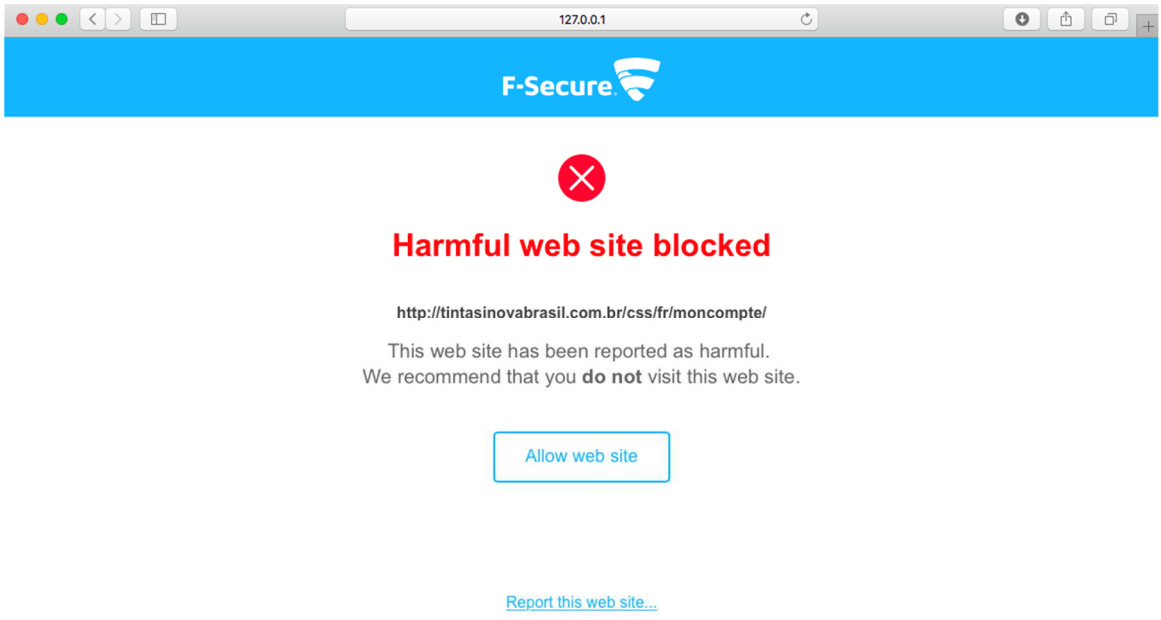
The Tools icon brings up a menu selection of icons to choose from. Virus Scan is the same as Scan on the Antivirus page. “Choose what to scan” lets you choose a file or folder to scan. Check for updates causes the app to look for signature updates and to apply them if necessary. Infection report is the F-Secure term for looking at the quarantine folder. Submit a Sample opens a web page where you can send a file to F-Secure for analysis by their experts. There is one somewhat confusing feature here – Firewall. This allows you to turn the Mac firewall on and off. However, you might not realise it has worked, as the setting shown in the dialog box is only updated after some time. F-Secure tell us you can usually see the change immediately if you quit System Preferences and open it again.

The Preferences button opens the preferences panels. Most settings here are locked to prevent accidental status changes, which we liked. It is possible to temporarily disable the real-time scanning for a fixed period of time, default being 5 minutes. On the Browser Protection tab, you find that browser protection has been enabled, as is banking protection. It isn’t clear what “banking protection” actually does, and the help file doesn’t make this clearer. When you visit a known banking site, the system tells you that it is a banking site, so it is certainly recognising this. But what extra protection is offered is not clear at all. Browser protection requires the installation of browser extensions. These are not detected and installed as part of the application installation which is disappointing, nor does it make it obvious to the user that the browser extensions need to be installed and enabled. Pressing the Install Browser Extension button does do the installation work for you, but this should be automatic and much more obvious.

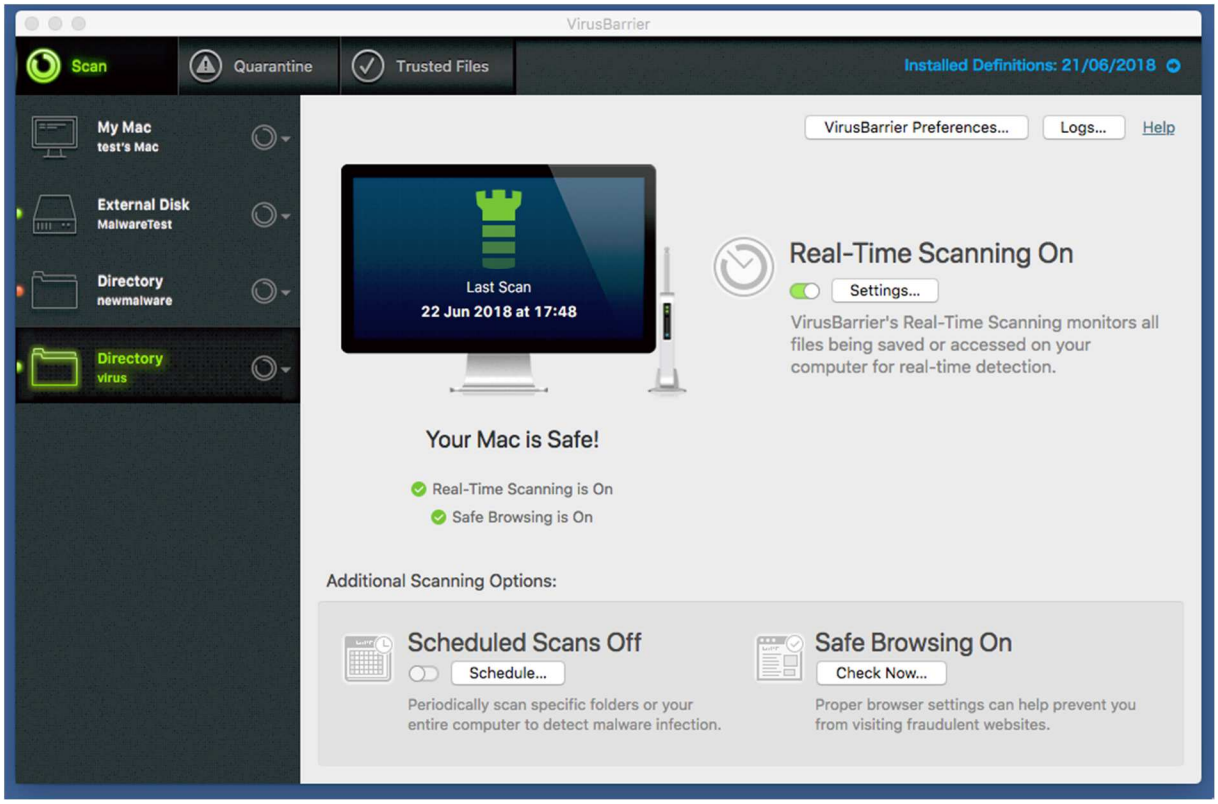
The Parental Control tab lets you turn on content filtering. There are the usual groups of definitions that a parent might want to exclude, including Weapons, Violence, Gambling, Drugs, Date, Adult and so forth. Parents should note that they must not let the child use a macOS admin account, or know the password to such an admin account, as otherwise he/she can unblock a banned site just by clicking “Allow web site”.

Finally, the "My F-Secure" button takes you to the online My F-Secure website where you can manage licenses. We would have liked some means to remote manage clients here, for example being to initiate a scan on a family member's computer. One item which is not clear is that the My F-Secure status item for a Mac says that "Family Rules" is not available: "This device does not support Family Rules". On a Windows machine, you can control the Parental controls remotely from the My F-Secure account, but not Mac devices. It's possible that the feature has been added to the client but not made it through to the administration cloud services page yet.





Intego Mac Premium Bundle X9



What is it?

Intego Mac Premium Bundle X9 is, as the name suggests, a collection of tools. It is a paid-for product. There are bundle offers for 1, 3 and 5 computers, and for 1 or 2 years of subscription.

Unusually, Intego charges a premium for having both Windows and Mac support in the license. They state: "*Intego offers the option for a Dual Protection version of our products that allows you to get protection for both your Mac and Windows computers. We partner with Panda, a Windows antivirus protection company, to provide Windows protection. When you select Dual Protection, you get an additional license for 1 Windows computer in addition to the number of Mac computers chosen*." From this we presume that if you buy 3 Mac licenses you get 1 Windows license in addition if you choose this extra item.

Product information on vendor's website: https://www.intego.com/mac-protection-bundle

Online support: https://www.intego.com/support

Overall:

There is quite a lot to like in this product. However, it appears a little of a "bundle of items" rather than a wholly integrated security platform. Although we like the facility to check that the built-in security capabilities provided by the modern browsers has been properly implemented, we would have been happier with a set of browser extensions provided by Intego themselves. The other functionality in the bundle is definitely useful. As such, there is a lot to find of value in this package.

Part 1: Product Installation and deployment

Purchasing and installation is straightforward. There is a demo version of the tool bundle, but some components are somewhat limited in their capabilities. We examined the fully licensed version. Rather unusually you can have software for both Mac Windows and versions in the license bundle. This is enabled by a deal with Panda for the Windows version, and is at additional cost. The purchasing process is simple enough. However, we noted that the license auto-renews by default, with no option to disable this at purchase time. Also, Intego charge an addition £2.95 to extend the download period from a few days to the full year of the license. We prefer downloading to be available for the entire lifetime of the license at no additional cost.

Installation is quite straightforward. As the name suggests, this is a bundling of tools into one package. The main app is called VirusBarrier, and this is the AV package. There are other components too, called ContentBarrier which is a parental control content filtering solution. NetBarrier is a firewall. Personal Backup is a backup and recovery application. And the rather cutely named Washing Machine is a clean-up tool for your Mac. Once the package is installed, the main window for VirusBarrier can be opened. We immediately noticed that we had some issues reported with Safe Browsing. The app indicated that Safe Browsing was not enabled. In fixing this, we were taken to a UI where it was shown that our browsers were not in safe browsing mode. We initially expected this to mean that we needed to install extensions, to provide in-browser filtering, safety and security in the usual way. However, this was not the case – the Safe Browser tool within Intego simply checks the browser settings to ensure that the built-in protection filters are enabled. In Chrome for example, this is found in chrome://settings, Advanced and check the "Protect you and your device from dangerous sites". Whilst we like the fact that Intego is checking these settings in Chrome, Firefox and Safari, it should be clear that Intego is not adding additional security capabilities itself.

Part 2: Ongoing use

In operation, there is little to see of the Intego apps, as you would expect. The top menu icon allows quick access to the various components of the application bundle. The main VirusBarrier window is quite straightforward. Across the top, you have buttons selecting Scan, Quarantine and Trusted Files which work as you would expect. And there is a status line telling you of the date of the installed definitions.

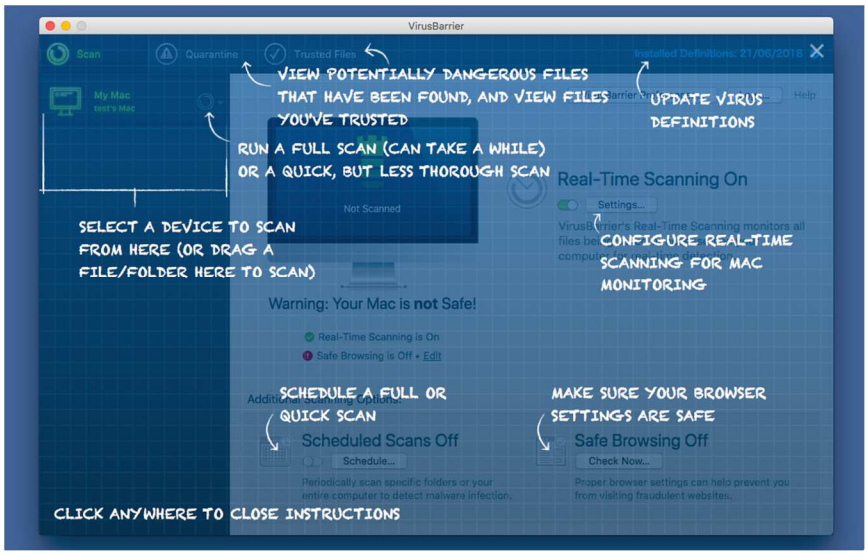
In the scan window mode, the left-hand side holds pre-cooked definitions of scans. For example, My Mac, External Disc and so forth. You can add to this with directories or files to allow for rapid access. As you would expect, you can right click on a file, folder or drive to initiate a scan. Each scan can have its own settings. By default, it detects Mac malware, but it can scan for Windows malware, Linux malware, Malicious scripts, Hacking tools and Keyloggers. In addition, you can set the scan to look inside archives. Scheduled scanning is possible, but this is disabled by default. In basic mode, it looks like you can only set up one scheduled scan, but if you choose the Advanced button the window expands to allow for multiple definitions.

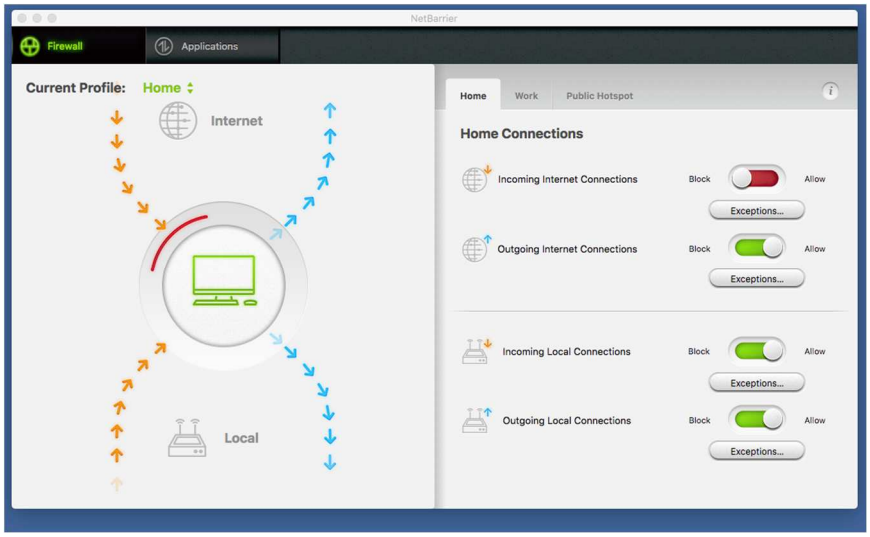
When you introduce malware to the system, you don't get notifications in the usual notification area at the top right. A window pops up with a rather non-descript list of the malware found and its contents. By default, the app does not clean anything. It offers to Trust, Quarantine or Repair the file, with Repair being the default. We would have liked to see automatic options here, especially for the less technically-minded users. In addition, it is possible to push the warning window back in the Z order, so it can become obscured by other windows. A slightly more proactive and nagging UI here might benefit users.

It is not clear whether the quarantine facility is actually a locked-away quarantine. If you select a quarantined item, it shows the path to the malware at the bottom of the window. Double click on this, and the file system browser is opened at that point, showing the malware. It appears to be more of a holding list of malware found rather than a secure quarantine.

The other items in the bundle are useful tools too. Netbarrier is a firewall, with a particularly graphic view of network traffic. Washing Machine can help you look for space that can be reclaimed on your system, by hunting down duplicate files for example. Personal Backup can create backups of your system over the network or to local devices, and claims to be able to make these backups bootable too. However, the value proposition here is somewhat muted when compared to the built-in capabilities of Time Machine, for example. It would help if Personal Backup offered support for backup to cloud. Content Barrier lets you put filtering in place both for web content, but also for scheduled time access, chat access, and to block applications too. Finally, it can take snapshots of the screen taken at prescribed intervals (e.g. all windows every 3 minutes), and to record keystrokes too.

Built-in help is reasonable, and we liked the use of a "crayon drawing" overlay when you first open an app, to point out the major functions and features.





Kaspersky Internet Security for Mac

What is it?

Kaspersky Internet Security for Mac is a paid-for antivirus product for macOS. It is available as a standalone package, or as part of Kaspersky Internet Security and Kaspersky Total Security packages. Kaspersky Internet Security for Mac aims to protect you from malware, viruses and phishing attacks. It has extra security features for when you are doing shopping or online banking, and has parent control features too. An intrusion detection system, called Network Attack Blocker, is also included.

Product information can be found at: https://www.kaspersky.co.uk/mac-security

Overall

Clearly this is a solid and well-thought-out product. It operates in a calm, efficient manner, and provides the core functionality that you need. It performs a solid installation, and doesn't force you to install additional capabilities that you might not need or want. In daily operation, it works very well, and the user interface and general experience is positive. We liked the carefully designed UI which informs without being patronising, or overly complex. We liked the cloud-based management console, and clearly this allows a family or small business to view, manage, update and control their devices. As such, it must be a solid recommendation.

Part 1: Product Installation and Configuration

Installation is simple enough and quite straightforward. In accordance with privacy laws, Kaspersky Lab goes to great lengths to get user consent for its privacy policy and data settings. The installer runs and asks for license credentials. The install process continues and takes little time. We liked how it prompts you before installing the browser extensions and provides good handholding here. This is welcome for the more beginner-level user. Browser extensions are provided for Safari, Chrome and Firefox. Finally, during install you are asked if you want to install Kaspersky Secure Connection, which is a VPN tunnel product, and Kaspersky Password Manager.

You also set up a My Kaspersky account. This is useful because it gives a cloud-based overview of the licenses that you have deployed. In addition, you can remotely manage devices. For example, for our macOS installation, we were able to schedule a Full Scan, Quick Scan, Update and also manage settings through the Components panel.

Part 2: Ongoing Use

As you would expect, there is a menu bar item which provides a drop-down list of common tasks. The first is to open the main application window. You can turn protection off, although you have to enter the macOS administrator password unless you are using an admin account. The menu gives easy access to the main functions, and also allows you to quit the app if required. If you are in the file system view on the desktop, you can right click and choose “Scan with Kaspersky Internet Security” on any file, folder or drive object.

The first thing that strikes you about the main Kaspersky product window is its clean and obvious user interface. It uses colour carefully in a traffic-light arrangement to immediately provide reassurance that all is well, or to highlight issues that need resolving. There are four main buttons: Scan, Update, Privacy and Parental Control.

The Scan window that appears gives you a target on which to drop any file or folder, which will then be scanned immediately. Or you can initiate a full scan, a quick scan or set up a scheduled scan. We liked the scheduled scan capabilities, allowing separate schedules for quick and full scans. And you can choose Weekdays, Weekends, Every Day, or choose particular days of the week, all along with a chosen time. The Scan History panel shows the results of recent activity, and you can easily drill down through this to get to the results of what happened. The Reports page is resizable, which is useful, but it would have been helpful to have encyclopaedia links to the defined malware, to provide more information.

The Update window is simple to use. It tells you that the databases are up to date, and also when they were last updated, so you are reassured that it is recent. Again, you can easily drill down to a report window that logs when updates were applied, and then dig even deeper to get the record of which definitions were affected.

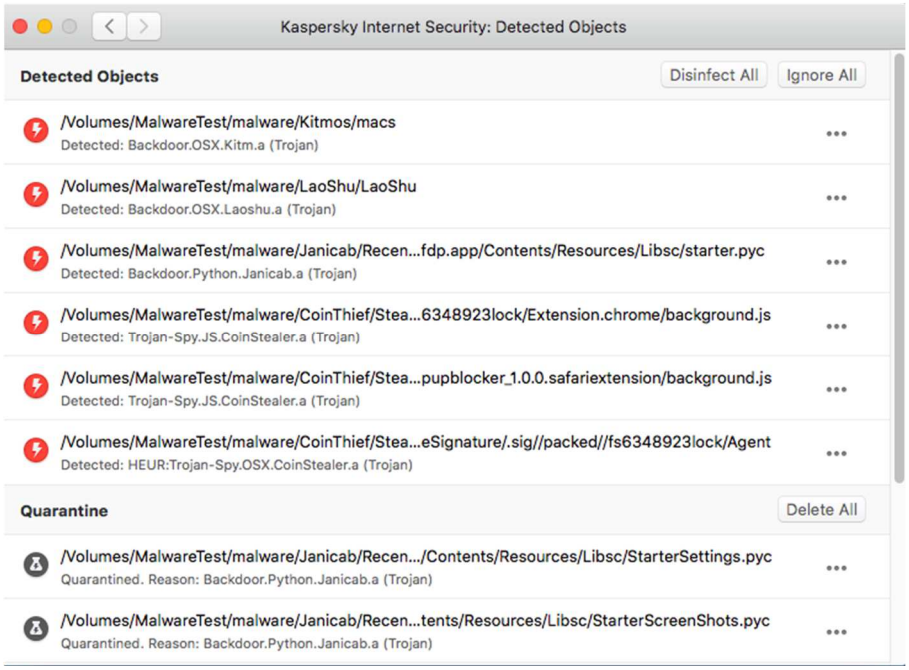
The Privacy tab brings together some straightforward tools: block webcam and block website tracking. It also gives easy access to the Password Manager and Secure Connection components if these have been installed and enabled.

Finally, Parental Control opens a new operational window where you can define all the usual levels and types of parental control for a user. Although there is a fine set of definitions and locks here, it would have been even better if there was a predefined set of child definitions. For example, to be able to select “under 5 years” or “11 years and above” to help set starting values. The Reports tool here is useful, and allows a parent to monitor and then engage with the child about sites visited.

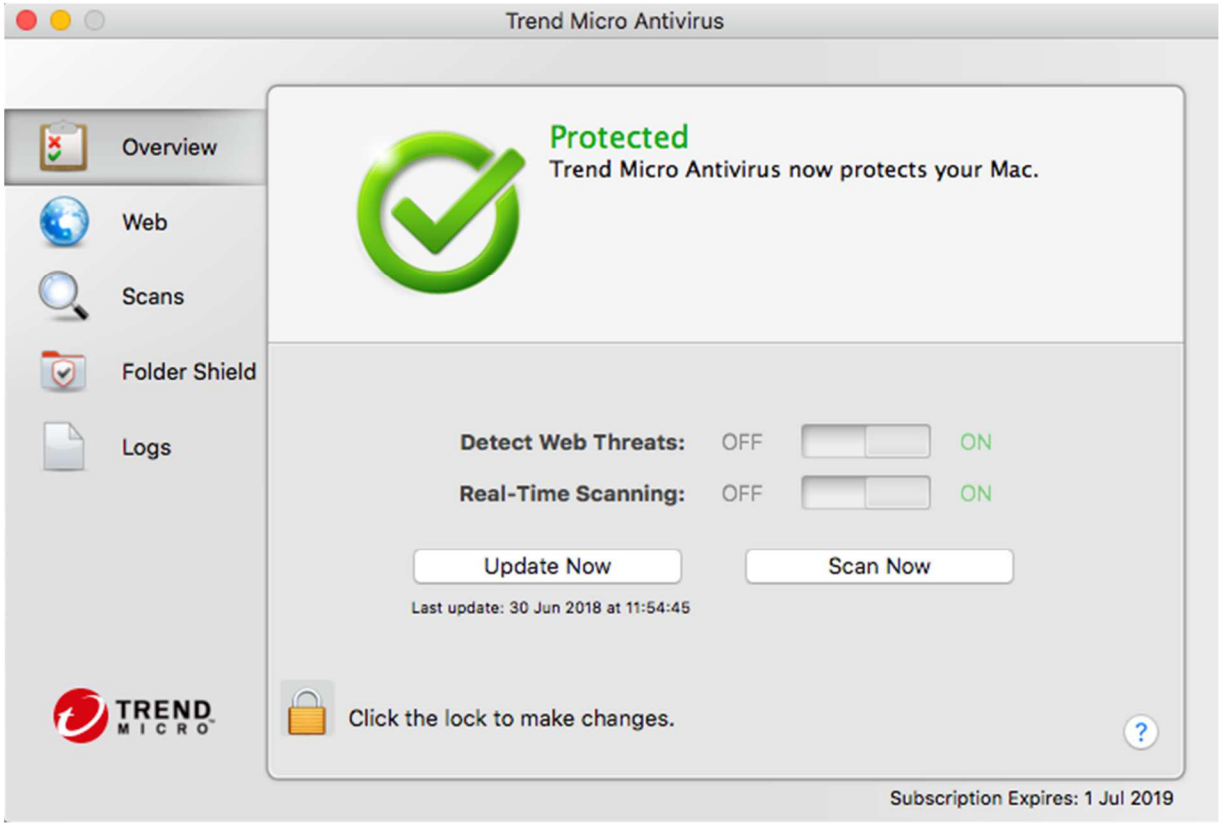
We placed some macOS malware onto the test computer, and asked Kaspersky to scan the files. It immediately sprang into action, and provided a clear report of what was happening. Please see screenshot below. By default, the program attempts to disinfect the computer, and we found this to be efficient and effective. It provided the right balance between alarm and reassurance to the user.

Visiting known phishing sites brought up clear and obvious warnings, against a stark black background. The user is offered the choice to ignore the alert or to go back. We also liked the analysis of web pages, which highlighted bad sites directly within the web page itself.

We liked the on-screen keyboard, and the ability to tap out a password instead of using the keyboard, in case keylogger malware was present.



Trend Micro Antivirus for Mac



What is it?

Trend Micro Antivirus for Mac is a paid-for antivirus product for macOS. It is available as a standalone product, and as part of the Maximum Security package, which adds in Windows, macOS, Android and iOS support. Trend Micro claims that Antivirus for Mac will protect your email, avoid web threats, stop malware and allow you to browse safely.

Product information on vendor's website:
https://www.trendmicro.com/en_gb/forHome/products/antivirus-for-mac.html

Online support: https://esupport.trendmicro.com/en-us/home/pages/technical-support/

Overall

We are left with mixed thoughts regarding Trend Micro Antivirus for Mac. On the one hand, it is an effective antivirus product for the macOS platform, and has a good range of capabilities. On the downside, there are aspects of the installation and daily use which we feel could be improved. A few small changes could significantly improve the usability of the product. At present it feels a little incomplete and lacking in a coherent design and operational strategy.

Part 1: Product Installation and Configuration

Purchasing is quite straightforward, although the current range of special offers and discounts can make the choice rather difficult. There is a temptation to buy one of the bundle offers, even if you don't have an Android phone, for example. This is not helped by the setting up of auto-renewal of the subscription by default. So, although you might be buying a larger product than you need, at a low first year price, the auto-renewal price might be higher. It is not detailed what the auto-renewal price will be at the end of the year. We purchased a license for the straightforward Antivirus for Mac for one computer for one year. Turning off auto-renewal as part of the purchasing process is not difficult, and for that Trend Micro are to be applauded.

Trend Micro offer a backup disc option at extra cost, but this is optional and not placed in the basket by default.

Payment and download of the package is straightforward with no issues.

Installation is mostly quite straightforward. Walking through the setup process is relatively easy, and few users will have issues. We did receive a warning on installation that "Trend Micro Antivirus is not optimised for your Mac", indicating that the app might contain 32-bit components. This is a new warning that Apple issues on app install since macOS 10.13.4. We are confident that Trend Micro will update the installation package to rectify this.

Installing the browser extensions is quite straightforward, and there is handholding for this.

During setup, you are asked if you want to set up Folder Shield. This is a tool which monitors key areas of the disc for malware apps that try to make unauthorised changes to data files (ransomware). At the end of the installation, we opened up the app and discovered that it needed updating, according to the dialog box that was presented to the user. Although it was no problem choosing the update function, it would have been nice for either the download to be up to date, although Trend Micro tell us that the app will automatically initialise an update about 10 minutes after the setup is completed.

Getting to the support area seems to require a Trend Micro account. Unlike other apps which offer an element of cloud control, we found no such capability in the Trend Micro cloud platform after logging in.

Part 2: Ongoing use

As you would expect, there is a status icon in the top bar of the screen. This gives access to Scan Now, Update Now, Open Trend Micro Antivirus, Open Preferences, Open Help, an on/off selector for Detect Web Threats, and Shut Down Trend Micro Antivirus.

As soon as you open the app and start looking at settings, you notice that the app is locked down against casual fiddling, and that you have to enter a password to unlock each page to make changes. The main application window is quite straightforward, with a clean and clear user interface. On the left-hand side is a set of menu items, starting with Overview. This gives a quick view of the status of the app, and allows you to run updates and perform scans.

The Web menu gives access to an overview of the Privacy Scanner, which claims to "check your privacy when you share information on Facebook, Google, Twitter and LinkedIn". The Web Threat Protection element protects you against fraud, malicious software and other threats. The Website Filter is a straightforward parental control filter, which is disabled by default. It has pre-sets for Child, Teenager, Mature Teenager, Adult and Custom settings.

The Scans menu entry allows access to Smart Scan, Custom Scan (which is essentially a files and folders picker), and Full Scan. You can also change the defaults here: for example, it is set up to do a scheduled scan every month on the 15th at midday. Some might prefer a more proactive scanning rate, but this can be set. Scanning compressed files is off by default but can be enabled.

The Folder Shield menu is the tool which prevents mass file encryption by malware. It is set up to monitor the Documents, Music, Pictures and Movies folders by default, but you can add other folders as well. And it can monitor connected USB devices too.

Finally, the Logs menu shows you what has happened.

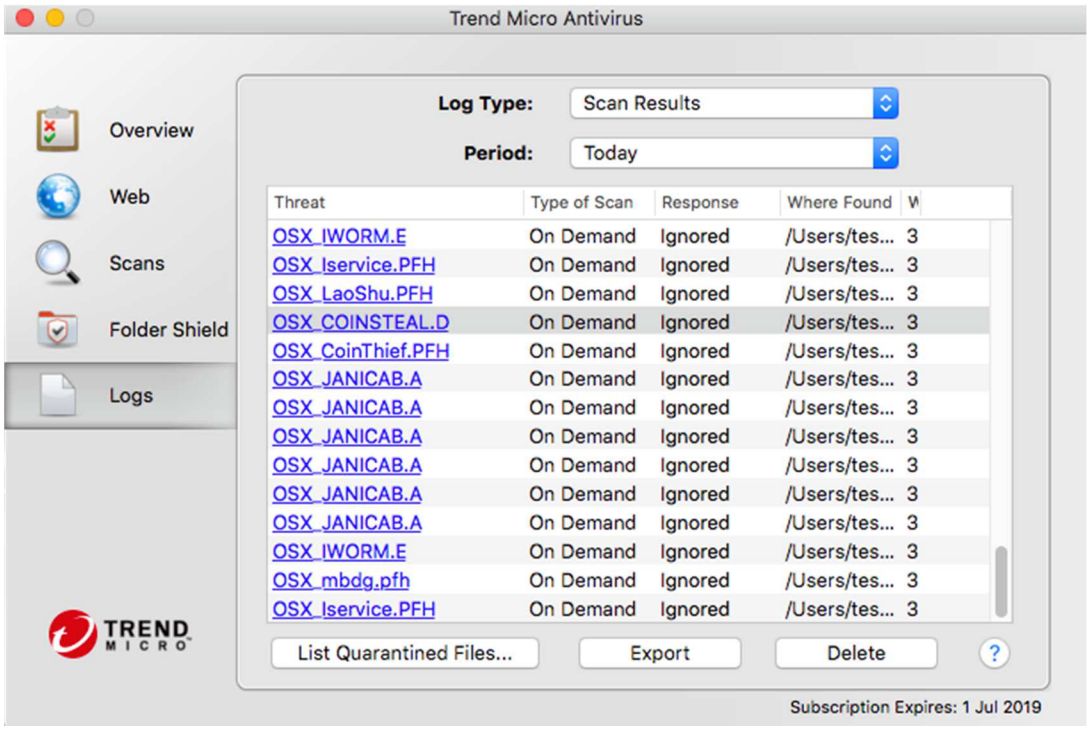
Introducing malware to the system has a mixed response. Firstly, there is no right click feature to scan a file, folder or drive: you have to use the Trend Micro menu system, or drag a file/folder to the main Trend Micro program window. Secondly, there is no on-access scanning on copy, so it is possible drag malware from a USB stick onto the desktop untouched.

However, our biggest concern is what happens when you scan malware. It efficiently scans the malware test folder, and reports that there is malware. However, this is a very muted dialog box and certainly doesn't project any level of concern or worry to the user. Worse still, if you choose the View Results link, you get a view of the log file. This is not a resizable window, and it is much too small for the amount of information it is trying to display. You have to try to resize the columns to fit within the fixed window, and this is awkward. Trend Micro tell us that it is possible to export the information as a .csv file, however.

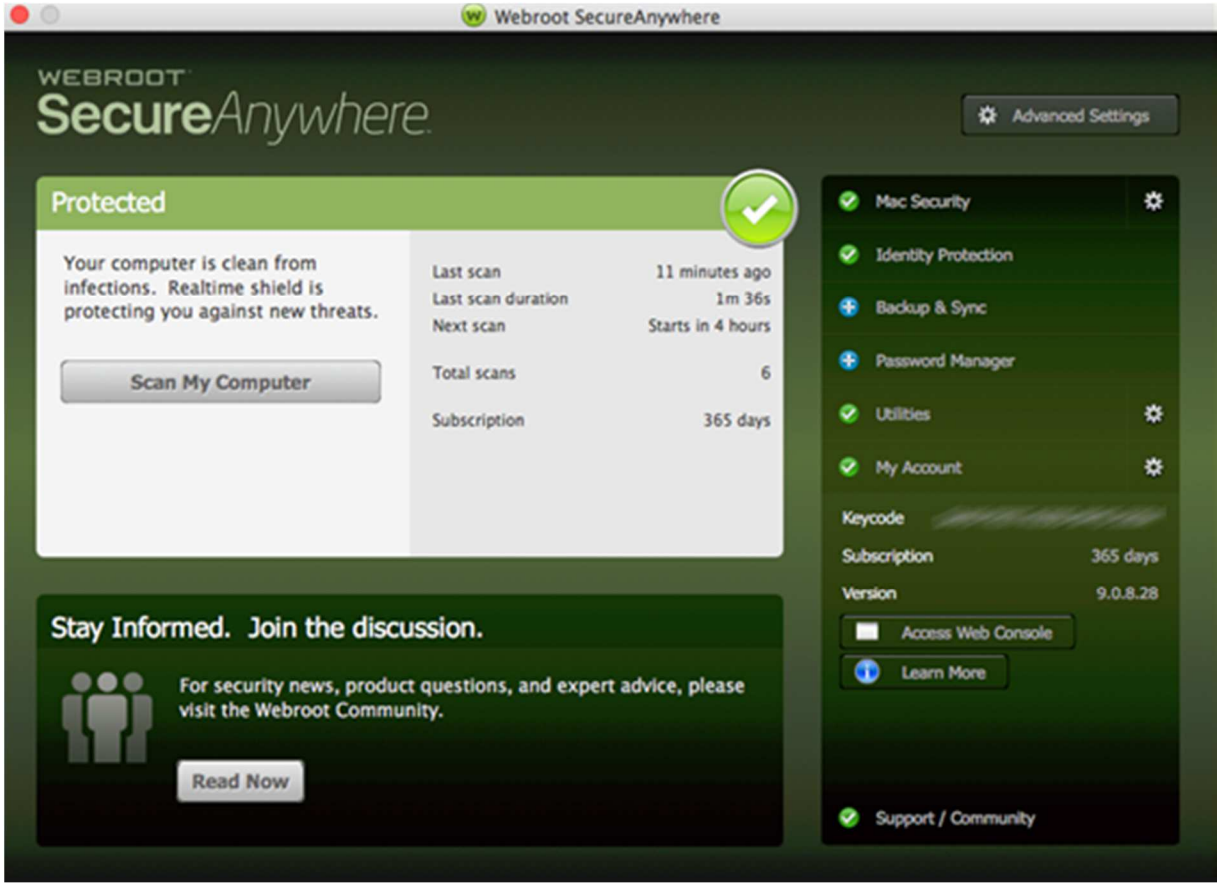
We were not particularly impressed with the application reporting that numerous pieces of malware were detected but "ignored" in the Response column. The report window does highlight each malware type as a clickable URL to take you into the antivirus encyclopaedia at Trend Micro. However, for each item of malware that we clicked on, the Trend Micro website reported that it had no information for that malware type, which was a considerable disappointment. Trend Micro inform us that they have made improvements to the handling and reporting of malware in a later build (8.0.3055).

The lack of phishing support via extensions for Safari was disappointing, but the extensions for Firefox and Chrome appeared to work well. The report page for an attempted phish was clear and obvious, and offered to ask Trend Micro to review the page for you.

The lack of a significant cloud-based management console is a disappointment for the family user.


Trend Micro Antivirus
Overview
Web
Scans
Folder Shield
Logs
Log Type: Scan Results
Period: Today
Threat Type of Scan Response Where Found W
OSX_IWORM.E On Demand Ignored /Users/tes... 3
OSX_Iservice.PFH On Demand Ignored /Users/tes... 3
OSX_LaoShu.PFH On Demand Ignored /Users/tes... 3
OSX_COINSTEAL.D On Demand Ignored /Users/tes... 3
OSX_CoinThief.PFH On Demand Ignored /Users/tes... 3
OSX_JANICAB.A On Demand Ignored /Users/tes... 3
OSX_JANICAB.A On Demand Ignored /Users/tes... 3
OSX_JANICAB.A On Demand Ignored /Users/tes... 3
OSX_JANICAB.A On Demand Ignored /Users/tes... 3
OSX_JANICAB.A On Demand Ignored /Users/tes... 3
OSX_JANICAB.A On Demand Ignored /Users/tes... 3
OSX_IWORM.E On Demand Ignored /Users/tes... 3
OSX_mbdg.pfh On Demand Ignored /Users/tes... 3
OSX_Iservice.PFH On Demand Ignored /Users/tes... 3
List Quarantined Files...
Export
Delete
?
Subscription Expires: 1 Jul 2019

Webroot SecureAnywhere Internet Security Complete



What is it?

SecureAnywhere is a paid-for antivirus product available for macOS and Windows. It is available in three bundle versions: the straightforward SecureAnywhere package itself, then SecureAnywhere Internet Security Plus, which adds in support for tablets and smartphones, along with logins and password support. Finally, there is Internet Security Complete, which adds in 25GB of secure online storage for backup and recovery, and tools for removing any traces of online activity.

Product information on vendor's website: https://www.webroot.com/gb/en/home

Online support: https://www.webroot.com/gb/en/support/support-home

Overall

This is a solid, easy-to-use product that delivers a quality, polished experience for the user. We liked the core AV functionality, along with the antiphishing feature. As is often the case, the value of a cloud backup solution and a password manager must be weighed against the use of existing specialist products. Some users might prefer to be running TimeMachine for local recovery, and a tool like 1Password or Dashlane for password management. However, if you don't have these items in place, then the built-in functionality is worth considering. Overall, the program has very many good points, and impresses with its confident functionality.

Part 1: Product Installation and deployment

Purchasing and installation is straightforward. We purchased the SecureAnywhere Internet Security Complete package, and found the process straightforward. Downloading is easy, and you run the installer in the usual way. As is the case with most security packages, you have to explicitly authorise the package in System Preferences to allow the security modules to be registered with the operating system. At the end of the installation, a scan is run against the computer, which we liked. It is always good to have confidence that you are starting from a known clean state.

As part of the setup process, the relevant extensions are loaded into Safari and Chrome automatically. You simply need to authorise their deployment, but this is straightforward. There is an equivalent extension for Firefox. Please note that if Firefox is running when the extension is installed, you will have to restart the browser before you can use it.

You don't have to create a Webroot account, but it is useful if you are managing multiple machines. And since you get 5 as part of the license, it makes sense to use this. Setting up an account is quite straightforward, and we were impressed by the account security used – not only do you need a username and password, but also a security key number from which two characters are chosen at random during login. Managing devices from the console is simple and definitely worth using. A licensed computer automatically registers with the cloud account here, but this can take some time for a device to become visible. We found it taking upwards of an hour for a test machine to register. Patience is rewarded here.

Part 2: Ongoing use

Like most macOS AV packages, there is a status item in the top bar. This allows you to open Webroot, scan the computer, remove threats, shut down SecureAnywhere and pause the Secure Keyboard Entry. We were a little surprised to see that the SecureAnywhere package could be shut down without requiring an appropriate password, at least by default.

Accessing scanning on a daily basis is simple, and can be done via the usual right click function on any file or storage folder or drive.

The main SecureAnywhere window is quite straightforward in operation, and has a strong green design theme. The default settings are good and everything is enabled. Backup & Sync, and Password Manager were not enabled in our package.

The main window has a large button for "Scan My Computer" and this immediately initiates a system scan. The Scan page is clear and allows you to cancel at any time. The Results page is clear, and hopefully tells you that the system is clean. There is a third tab, Next Steps, which appears if problems are detected.

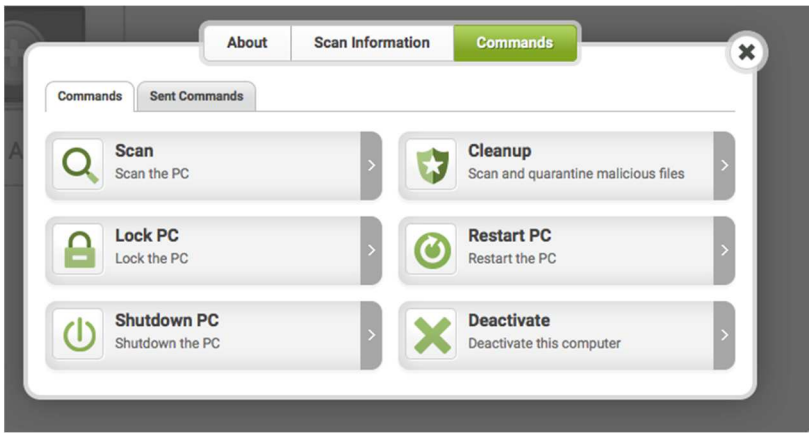
By default, there is no automatic scan on insertion of USB devices (although this can be enabled in the settings). When we ran a manual scan of a USB stick loaded with macOS malware, the main application window almost immediately turned red and indicated that there were issues. We chose the option to resolve the issues automatically, and after that a full system scan was run again to ensure that the machine was clean. Once this had completed, the software returned to its normal green look and feel, showing that there were no issues.

There is one minor inconsistency in this model. If Webroot's real-time protection picks up malware being copied from external drive to desktop, the alert window displayed is green. Webroot tell us that this will be rectified, however.

Moving to the rest of the user interface, there is a vertical stack of items on the right-hand side. At the top is Mac Security, along with a configuration button. By default, all of the settings should be adequate here. Then there is Identity Protection, which is the built-in anti-phishing service. We tried this against known phishing sites and found it to offer clear and concise warnings to the user, with no possibility of confusion. It is possible to submit the URL to Webroot for a review of the security rating of a site, which is useful in the rare case of a false positive.

Then there is Backup and Sync, which uses the bundled 25GB of cloud storage. Password Manager is next, followed by Utilities which covers System Control of processes, and Reports of activity within the package.

The My Account button gives information about the current version of the app, and the remaining subscription. Finally, Support/Community takes you to the online help capability.



Featurelist Mac (as of July 2018)	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL
Product name:	Avast Mac Security Free	AVIRA Antivirus Pro for Mac	Bitdefender Antivirus for Mac	BitMedic AntiVirus & Malware Security	Crowdstrike Falcon for Mac	F-Secure SAFE for Mac	Intego Mac Premium Bundle	Kaspersky Internet Security for Mac	Trend Micro Antivirus for Mac	Webroot SecureAnywhere Internet Security Complete for Mac
Supported Mac OS versions:	10.9 and up	10.12 and up	10.9.5 and up	10.8 and up	10.9 and up	10.11 and up	10.8 and up	10.12 and up	10.11 and up	10.7.3 and up
Supported Program languages:	English, German, Czech, Spanish, Finnish, French, Italian, Dutch, Polish, Korean, Portuguese, Russian, Swedish, Norwegian	English, German, Italian, Spanish, Japanese, Dutch, Polish, Portuguese, Russian, Turkish, Chinese, Indonesian	English, German, French, Italian, Spanish, Czech, Dutch, Greek, Japanese, Korean, Polish, Portuguese, Romanian, Turkish, Russian, Vietnamese	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
Protection										
Real-Time protection	●	●	●	●	●	●	●	●	●	●
Detects also PUA on Mac	●	●	●	●	●	●	●	●	●	●
Prevents access to malicious and phishing web sites	●		●			●		●	●	●
On-demand scanner	●	●	●	●		●	●	●	●	●
Cloud Scanning (requires internet connection)		●	●		●	●	●	●	●	●
Quarantine	●	●	●	●	●		●	●	●	●
Detects also threats for Windows platform	●	●	●					●	●	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	Adware Scanner and Remover	EDR, Managed Hunting, IOC details	Banking protection		Webcam protection, Private browsing, Network attack protection, Secured browser for online banking	Folder Shield	Backup, System optimizer, Identity protection, Password manager
Support										
Online Help and/or User Forum	●	●	●	●	●	●	●	●	●	●
Email and/or Phone Support	●	●	●	●	●	●	●	●	●	●
User manual			●	●	●	●	●	●	●	●
Online Chat		●	●			●	●	●	●	
Supported languages (of support)	English, German, Spanish, French, Italian, Portuguese, Russian, Czech	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
Price (may vary)										
Price 1 Mac / 1 year (USD/EUR)	FREE	USD 45 / 35 EUR	USD 40 / 40 EUR	USD 30 / 30 EUR	not applicable	USD 60 / 60 EUR	USD 70 / 70 EUR	USD 40 / 40 EUR	USD 40 / 50 EUR	USD 60 / 75 EUR

Copyright and Disclaimer

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

AV-Comparatives (July 2018)