Independent Tests of
Anti-Virus Software

Mac Security Test & Review

TEST PERIOD: MAY 2022

LAST REVISION: 22ND JUNE 2022

WWW.AV-COMPARATIVES.ORG

Content

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 still been many 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 (i.e. not certified by Apple) are run. Then there is "XProtect", which checks files against known-malware signatures. Finally, Apple provide the "Malware Removal Tool" (MRT). These features are essentially invisible to the user, other than configuration options and alerts. System and security updates are installed automatically using the macOS 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.

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 as well. 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 to 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 major performance reduction during the course of the test 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 Software for macOS Monterey

We have reviewed and tested the following products[4] for this report, using the newest version[5] available at time of testing (May 2022):

- **Acronis Cyber Protect Cloud for Mac with Advanced Security pack 15.0**
  https://www.acronis.com/en-eu/products/cloud/cyber-protect/
- **Avast Security Free for Mac 15.2**
  https://www.avast.com/free-mac-security
- **AVG AntiVirus FREE for Mac 20.1**
  https://www.avg.com/en-us/avg-antivirus-for-mac
- **Avira Antivirus Pro for Mac 1.11**
  https://www.avira.com/en/avira-antivirus-pro
- **Bitdefender Antivirus for Mac 9.0**
  http://www.bitdefender.com/solutions/antivirus-for-mac.html
- **CrowdStrike Falcon Pro for Mac 6.39**
  https://www.crowdstrike.com/endpoint-security-products/falcon-endpoint-protection-pro/
- **Intego Mac Internet Security X9 10.9**
  https://www.intego.com/antivirus-mac-internet-security
- **Kaspersky Internet Security for Mac 21.1**
  http://www.kaspersky.com/security-mac
- **Trellix Endpoint Security (HX) for Mac 34.28**
  https://www.trellix.com/en-us/products/endpoint-security.html
- **Trend Micro Antivirus for Mac 11.5**
  https://www.trendmicro.com/en_us/forHome/products/antivirus-for-mac.html

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.

[4] Additional information about the products and additional third-party engines/signatures used inside the products: **Acronis** and **Trellix** use the **Bitdefender** engine. **Intego** uses the **Avira** engine for detection of Windows malware. **AVG** is a rebranded version of **Avast**.

[5] Avast/AVG specifically asked us to test their free version.

Malware Protection Test

The Malware Protection Test checks how effectively the security products protect a macOS Monterey system against malicious apps. The test took place in May 2022, and used macOS malware that had appeared in the preceding few months. We used a total of 471 recent and representative malicious Mac samples.

In the first half of 2022, thousands of unique Mac samples were collected. However, this figure included many samples which could be classified as "potentially unwanted" – that is, adware and bundled software – depending on interpretation. Many samples were 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 simple signature-based protection systems. There were in fact almost no new families, and only a few dozen really new variants, of true Mac malware seen in 2022. Some of these will only run on certain macOS versions. After careful consideration, we ended up with 471 Mac malware samples to be used in the test. We feel these reflect 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.

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 23rd of May 2022. 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. We then ran a scan of the flash drive, either from the context menu or from the main program window. Any detected samples were removed. After this, any remaining samples which had not been detected by the real-time protection or scan were copied to the Mac's system disk. These remaining samples were (where possible) then executed, providing the security product with a final chance to detect the samples. In addition to the Mac malware samples, we also performed a false alarm test on a set of clean Mac programs to check for false positives. None of the programs we tested produced any false alarms.

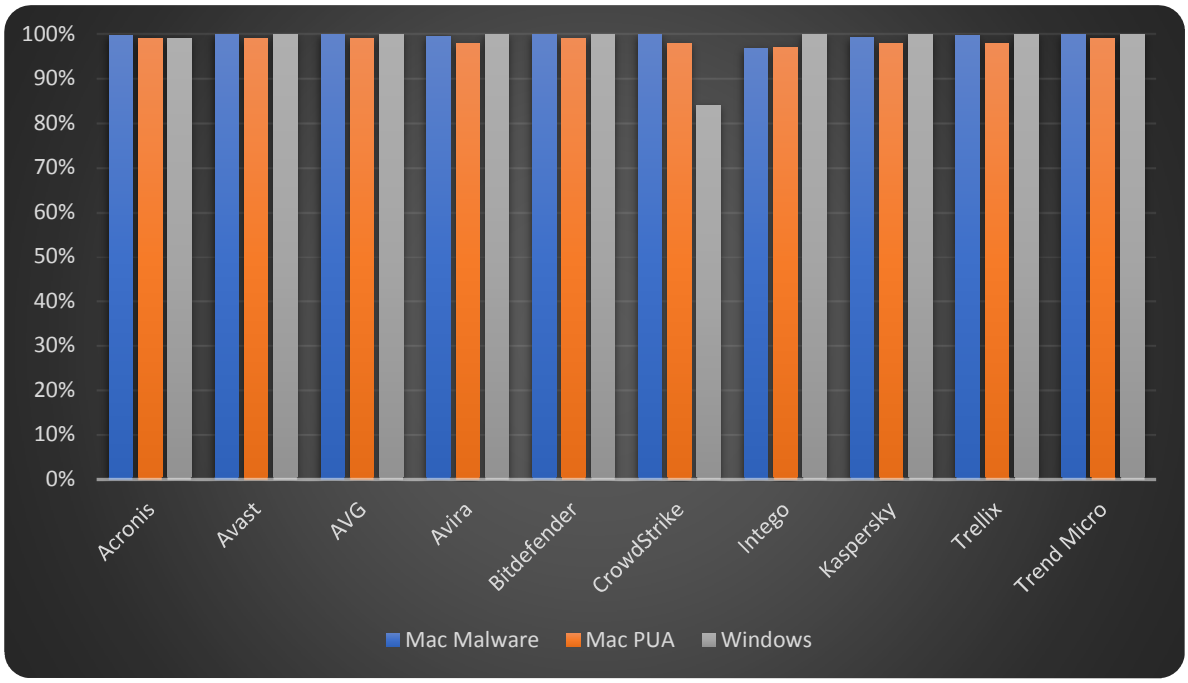
To take account the increasing number of potentially unwanted applications on Mac, we also tested detection of 773 prevalent Mac PUAs. The testing methodology was the same as that for the malware testing described above.

Most Mac security products 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 1000 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.

Results

The table below shows protection results[6] for the products in the review.

Product	Mac Malware Protection 471 recent Mac Malware samples	Mac PUA Protection 773 prevalent Mac PUA samples	Windows Malware Detection on macOS[7] 1000 prevalent Windows malware samples
Acronis Cyber Protect Cloud for Mac	**99.8%**	99%	99%
Avast Free Security for Mac	**100%**	99%	100%
AVG AntiVirus FREE for Mac	**100%**	99%	100%
Avira Antivirus Pro for Mac	**99.6%**	98%	100%
Bitdefender Antivirus for Mac	**100%**	99%	100%
CrowdStrike Falcon Pro for Mac	**100%**	98%	84%
Intego Mac Internet Security X9	**96.8%**	97%	100%
Kaspersky Internet Security for Mac	**99.2%**	98%[8]	100%
Trellix Endpoint Security (HX) for Mac	**99.8%**	98%	100%
Trend Micro Antivirus for Mac	**100%**	99%	100%



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

[6] We would like to point out that while some products may sometimes be able to reach 100% protection rates in a test, it does not mean that these products will always protect against all threats. It just means that they were able to detect 100% of the widespread samples used in this particular test. We do not round up scores to 100% if there are misses. Programs with a score of 100% thus had zero misses.

[7] 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.

[8] If PUA detection is manually enabled. All other consumer products had PUA detection on by default.

Summary

This year, the following Mac security vendors receive our Approved Mac Security Product award: **Acronis, Avast, AVG, Avira, Bitdefender, CrowdStrike, Kaspersky, Trellix** and **Trend Micro**.

Unfortunately, **Intego** app did not quite reach our threshold for Mac malware detection, and so was not certified this year.

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 also consider 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.

Acronis Cyber Protect Cloud with Advanced Security pack is part of an endpoint protection package for enterprise networks. The management is done by cloud console, and there is only a minimalist GUI on client PCs.

Avast Security Free for Mac is a fully-featured but easy-to-use free antivirus program. It displays clear and persistent malware detection alerts.

AVG AntiVirus FREE for Mac is a free antivirus program with a full range of anti-malware features. The tiled user interface can be navigated very simply, and malware detection alerts are persistent as well as clear.

Avira Antivirus Pro for Mac is a paid-for antivirus product with a password (limited) VPN feature. It has a very simple, easy-to-navigate interface.

Bitdefender Antivirus for Mac is a paid-for antivirus product that includes ransomware protection in addition to anti-malware features. The interface is well designed, and there is an excellent user manual.

CrowdStrike Falcon Pro 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.

Intego Mac Internet Security X9 is a paid-for security suite that includes a firewall in addition to malware protection. A simple but useful help feature explains the main functions using an overlay.

Kaspersky Internet Security for Mac is a paid-for security suite with a data-limited VPN. It has a clearly laid-out user interface, which includes intelligent icons in the main program window.

Trellix Endpoint Security for Mac is part of an endpoint protection package for enterprise networks. The management is done by cloud console, and there is no GUI on client PCs.

Trend Micro Antivirus for Mac is a paid-for security suite with camera and microphone protection and an anti-ransomware feature. It features particularly sensitive real-time protection.

AV-Comparatives' Mac 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), poor Mac-PUA detection rates[9] (under 75% for Mac PUA[10]) or false positives on common macOS software. Please note that detection of Windows malware is not a certification requirement.
- 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, and detecting malware, reliably and in a timely fashion.
- Untrue claims, such as stating that a macOS app also detects Windows malware, despite independent tests showing that detection of even prevalent Windows malware is very poor (as noted above, Windows malware detection is not in itself a requirement for certification).
- Lack of real-time/on-access or on-execution scanning/protection. Providing only an on-demand scanner does not qualify for certification. For consumer products, real-time protection has to be enabled by default after installation.
- 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.
- 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.
- 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.

[9] Starting from 2023, for consumer products, the PUA detection threshold must be reached using default settings.
[10] What is "potentially unwanted" might be debatable, and a few apps that we would regard as PUA might be considered to be clean by some vendors. Consequently, this threshold is relatively low.

Review Format

Here we have outlined the features and functionality that we have looked at for each of the consumer programs in this review. With the enterprise products, which are managed using a cloud-based console, we have used a similar review format to that used in the Enterprise Main Test Series reports.

Summary: Here we describe the nature of the product and its security features, including whether it is free or requires a subscription, and give an overview of our experience with it. Please note that all products protect against ransomware in the same way as for other types of malware. Where we have specifically mentioned "ransomware protection", this means that specific user folders are monitored to prevent unauthorised changes.

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 record 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. Please be aware that when installing any antivirus product on macOS Monterey (which was used for the tests and reviews), it is necessary to go into the System Preferences and give the program specific permissions, such as Full Disk Access. As this process is essentially identical for all products, we have not mentioned it in the individual reviews. However, non-expert users might consider asking for help with the installation of their chosen product, if they do not feel confident about doing it themselves.

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.

Alerts: We look at how each program's current protection status is displayed, what sort of warning is shown if real-time protection is disabled, and how to correct this. We also note what sort of alert is shown when malware is discovered, and whether the user needs to take any action in this case.

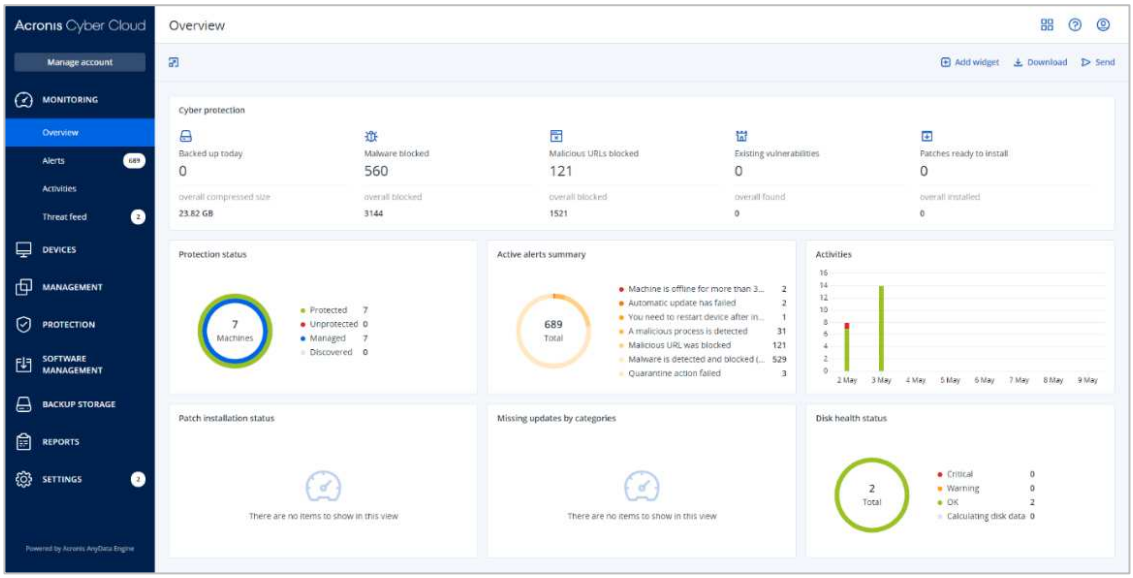
Malware detection scenarios: We run a functionality check to determine whether each program detects malware on access (e.g. when it is downloaded or copied to the system), or only on execution (i.e. when it is run). This is entirely separate from the malware protection test, and is run on different systems. We connect a USB flash drive containing a few samples of common Mac malware, which all the tested programs are known to detect in an on-demand scan. 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. If this is possible, we then check on-execution detection by running the copied malicious files.

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 whether users with macOS Standard User Accounts can disable the antivirus protection features, restore items from quarantine, or uninstall the program. We regard it as ideal if only Administrator Accounts (not Standard User Accounts) can perform these tasks. This means that if you let someone else use your computer, you can create a Standard User Account for them, and they will not be able to compromise your Mac's security. Of course, if you don't share your computer, this point is not relevant to you.

Acronis Cyber Protect Cloud with Advanced Security pack



Advantages

- Has backup, disaster recovery, vulnerability assessment, and secure file-synch
- Well suited to smaller businesses
- Console is easy to navigate
- Pages of the console can be customised
- Geographically aware threat-feed feature

About the product

Acronis Cyber Protect Cloud with the Advanced Security pack is a security package for business networks. It provides a cloud-based console for managing the endpoint protection software. Details of the management console described here are applicable to all supported operating systems. In addition to malware protection, the product contains a variety of other cloud-based services, including backup, disaster recovery, and secure file-synchronisation. This review considers only the malware protection features, however. The product can manage networks with thousands of seats. We feel it would also be suitable for small businesses without dedicated IT support staff.

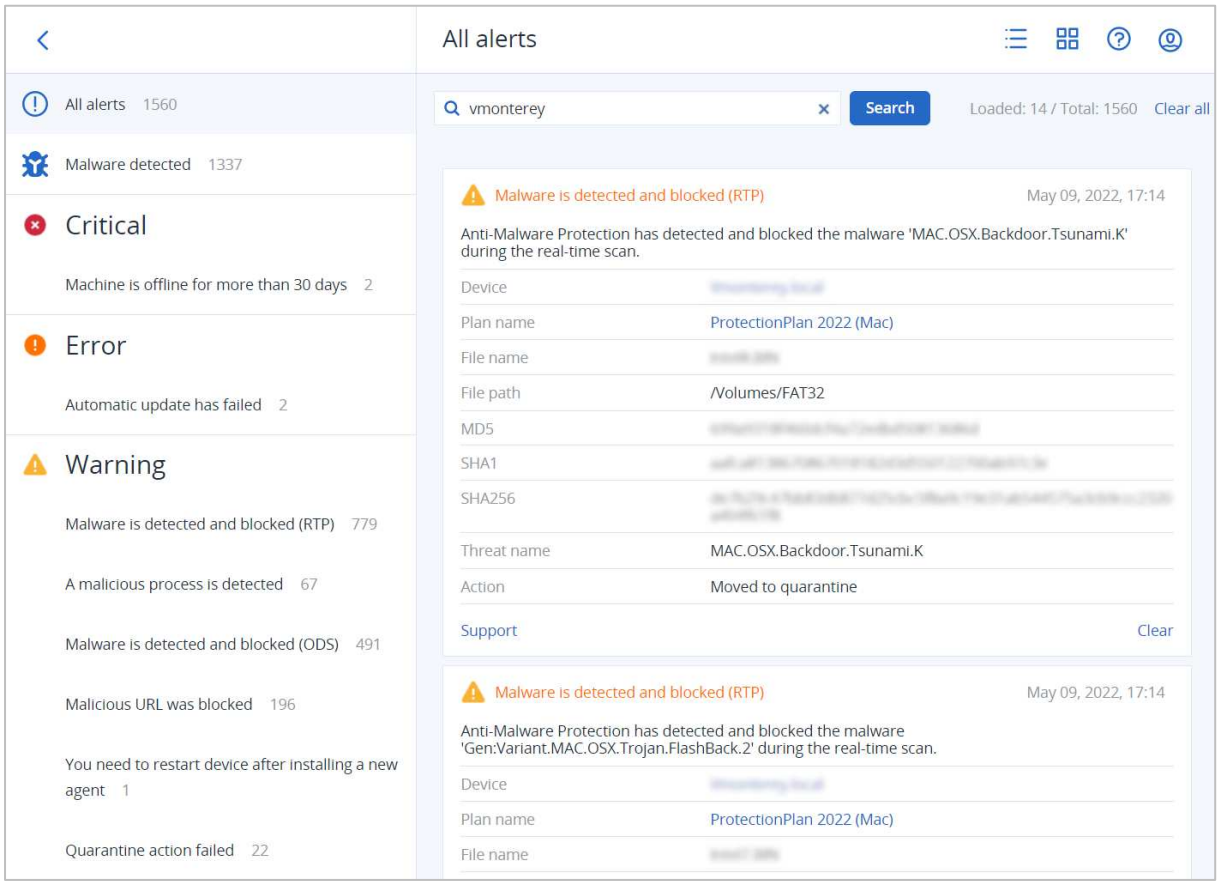
Management Console

The console is navigated from a single menu panel on the left-hand side. There are entries for *Monitoring, Devices, Management, Protection, Software Management, Backup Storage, Reports,* and *Settings*. The numbers shown to the right of each menu item represent items such as threats and alerts that the administrator should look at.

Monitoring\Overview page

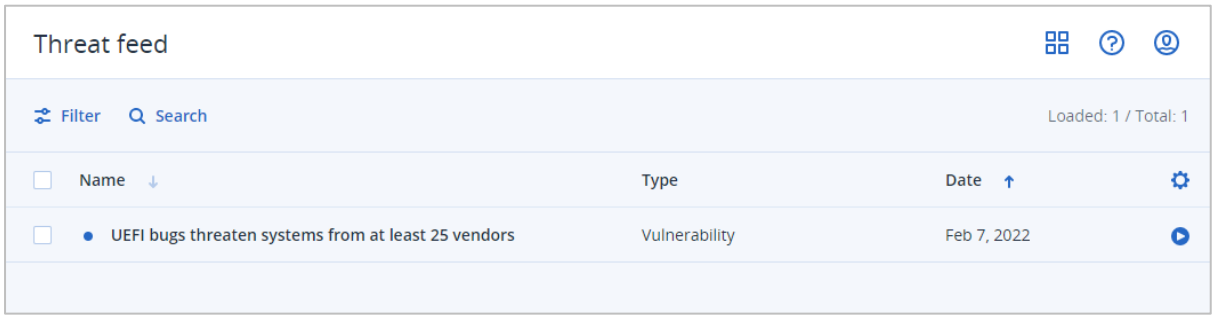
This is the page you see when you first log on to the console. It's shown in the screenshot above. It provides a graphical overview of the security and backup status of the network, using coloured doughnut and bar charts. There are panels for *Protection status, Active alerts summary, Activities, Patch installation status, Missing updates by categories,* and *Disk health status*. *The Cyber protection* panel across the top displays the items *Backed up today, Malware blocked, Malicious URLs blocked, Existing vulnerabilities,* and *Patches ready to install*. Details of recent alerts and other items are displayed in further panels at the bottom. You can customise the page by changing data settings for each panel, or adding/removing panels.

Monitoring\Alerts page



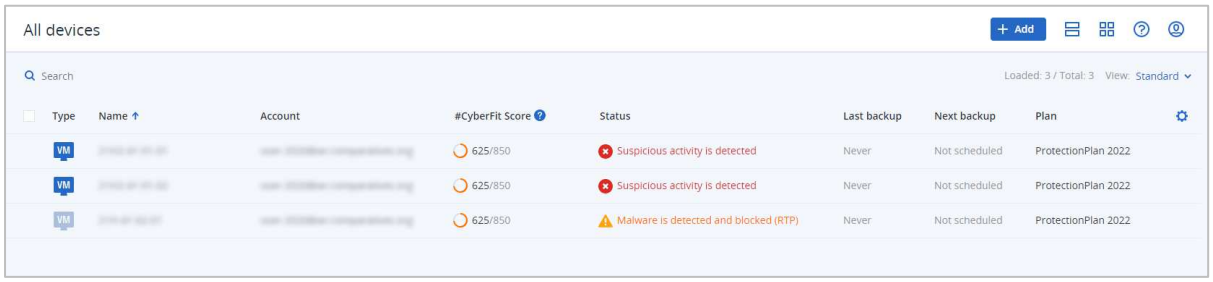
Here you can see alerts relating to malware detection, blocked URLs, and also the backup functions. These can be shown as a list, or as big tiles with details (as shown above). Information for malware detections includes the device, protection policy (*Plan*), file name and path, file hashes, threat name and action taken (e.g. quarantined). Clicking *Clear* removes the item from the *Alerts* page, but not the system logs.

Monitoring/Threat feed page



The *Threat feed* page displays warnings of current attacks and vulnerabilities to watch out for. Acronis tell us that this list is tailored to your geographic location, so that it only displays warnings that are relevant to you. The page may even warn you of natural disasters, where applicable. Clicking on the arrow symbol at the end of a threat entry opens a list of recommended actions to counteract that particular threat. These might be to run a malware scan, patch a program, or make a backup of your PCs or data.

Devices\All devices page



The *Devices\All devices* page lists the computers on the network. Sub-pages allow you to filter the view, e.g. by managed and unmanaged machines. You can see device type (virtual machine or hardware) and name, user account, and security status, amongst other things. The columns shown can be customised, so you can remove any you don't need, and add e.g. IP address and operating system. Devices can be displayed as a list (as in the screenshot above), or large tiles with additional details. Selecting a device in the list opens up a menu panel on the right, from which you can see the applied protection policy, apply patches, see machine details/logs/alerts, change group membership, or delete the device from the console.

Management/Protection plans page

Under Management/Protection plans , you can see, create and edit the policies that control the anti-malware features of the platform. Again, if you click on an icon, an uncluttered menu pane slides out from the right with the appropriate details and controls. Amongst the functions that can be configured are real-time protection, network folder protection, action to be taken on malware discovery, exploit prevention, crypto-mining process detection, scheduled scanning, and exclusions. On other tabs of the menu pane, you can also configure other items such as URL filtering, vulnerability assessments and patch management.

Protection\Quarantine page

Under *Protection*, the *Quarantine* page lists the names of malicious files that have been detected, along with the date quarantined and device name. You can add columns for the threat name and applicable protection plan, using the page settings. A mini menu at the end of each entry lets you whitelist, restore or delete the selected items.

Protection\Whitelist page

The *Whitelist* page displays any applications that have been found during backup scanning and categorised as safe. A backup scanning plan has to be created in order to enable automatic whitelist generation.

Software Management pages

The *Vulnerabilities* page under *Software Management* is populated if a vulnerability assessment has been created in a protection plan and run at least once.

Reports page

The *Reports* page lists a number of topics for which reports can be generated, including *Alerts, Detected threats, Discovered machines, Existing vulnerabilities* and *Patch management summary*. Clicking on a report name opens up a details page for that item. The *Alerts* report page, for example, contains panels showing *5 latest alerts, Active alerts summary, Historical alerts summary, Active alerts details,* and *Alerts history*. Coloured alert icons and doughnut charts serve to subtly highlight the most important items. As with other pages of the console, the *Reports* page can be customised.

Settings pages

Under *Settings/Protection*, you can set the schedule for protection definitions updates, and enable the *Remote Connection* function. The *Agents* page allows you to see the version of the endpoint agent installed on each client, and update this if necessary. If any devices are running outdated agents, an alert will be shown in the *Settings/Agents* entry in the menu panel of the console. This makes clear that you need to take action.

macOS Endpoint Protection Client

Deployment

Installation files in .DMG format can be downloaded by going to the *Devices* page and clicking the *Add* button. After performing a local installation on a Mac client, you have to click *Register the machine* in the client window. You then need to log on to the management console from the Mac client, find the device's entry, and apply a protection plan.

User interface

The user interface on protected endpoints consists of a System Tray icon, which opens a small information panel when clicked. Here you can see the status of the real-time malware protection, and details of any scheduled backups. Settings for backup encryption and proxy server can also be changed here. Users can scan a drive, folder or file for malware by right-clicking it in macOS Finder.

Malware detection scenario

When we connected a flash drive containing malware samples to our test PC, and opened the drive in macOS Finder, Acronis did not immediately take any action. However, as soon as we tried to copy malware from the external drive to the Mac Desktop, Acronis blocked the copy process, and detected and quarantined the malicious files on the flash drive. No alert was shown.

Avast Security Free for Mac

Summary

Avast Security Free for Mac is a free antivirus program. 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 and deletes malicious files when they are copied or downloaded. Alerts are clear and persistent, giving you time to read them. Standard user accounts cannot take any risky actions. The program is well suited to non-expert users due to its ease of use.

Installation

To set up Avast Security on your Mac, you just download and run the installer file, then double-click *Install Avast Security*. You can uninstall the program by clicking *Avast Security* in the macOS menu bar, then *Uninstall Avast Security*.

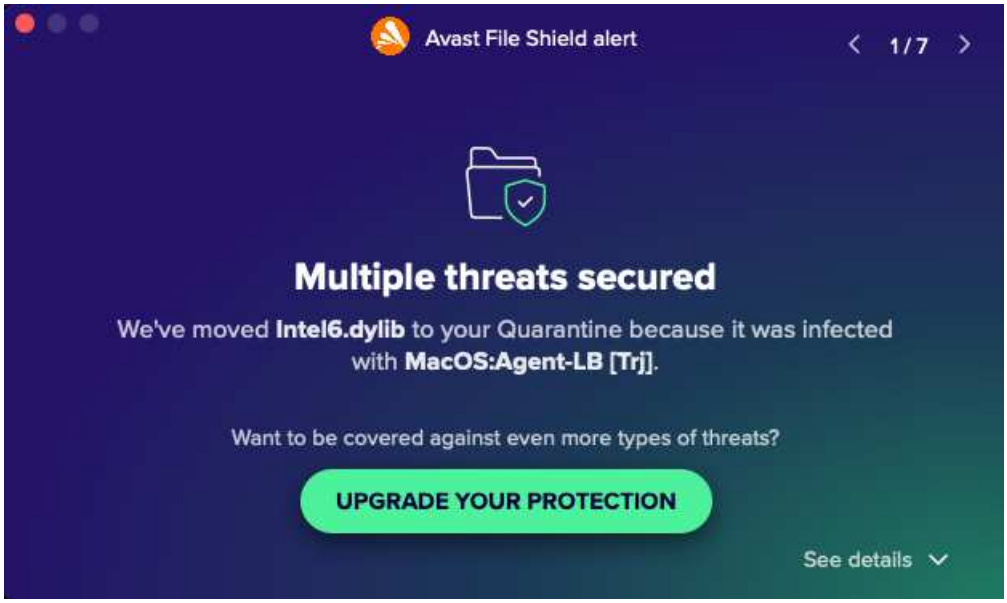
Finding essential features

Status, **default scan, scan options**, and **quarantine** are all found on the home page of the main program window. **Settings** (*Preferences*) can be opened from the menu in the top right-hand corner, or the macOS menu bar. **Subscription information** is not applicable, as the program is free. **Updates** can be run by clicking *Preferences, General* (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.

Alerts

When we disabled Avast's real-time protection, the alert below was shown in the main program window. We were able to reactivate the protection by clicking *Turn ON*, and then setting all the slider buttons on the *Core Shields* page to *ON*.

When malware was detected in our functionality check, Avast displayed the alert shown below. No user action was required. The alert persisted until we closed it. We noted that it's possible to browse through the alerts using the arrows in the top right-hand corner. They can be closed individually by clicking *Got it*, or all at once using the macOS close button in the top left-hand corner.



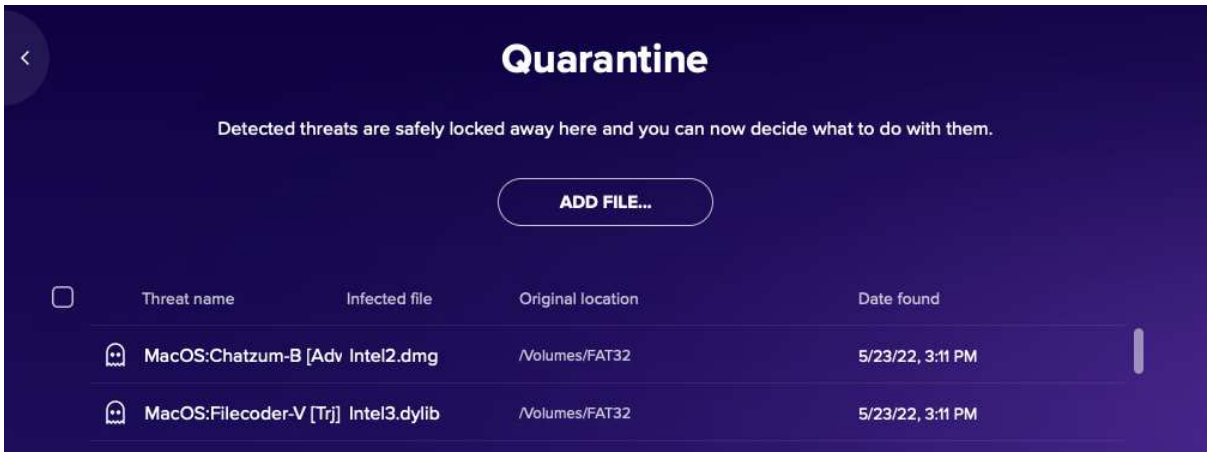
Malware detection scenarios

We found Avast Security for Mac to have highly sensitive and reliable on-access detection of malware. Malicious files that we downloaded or copied to the system were instantly detected and quarantined in all cases. When we tried to copy malware from a network share or external drive to the system, Avast not only prevented the files from being copied, but deleted the source malware on the network share or external drive as well.

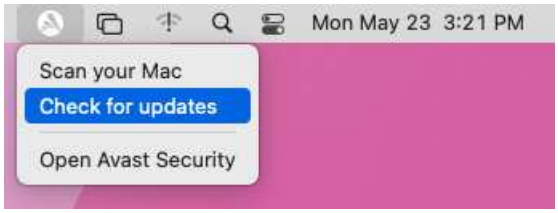
By default, Avast does not automatically scan USB drives when they are connected, but this can be enabled in the program options. When we scanned a flash drive containing malware samples, Avast presented a list of the threats found; we just had to click *Resolve Selected* to quarantine them. We had to enter the macOS administrator password in order to allow the quarantine process to complete.

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



Advanced options

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

- Disable protection features (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 any of these tasks, which we regard as optimal.

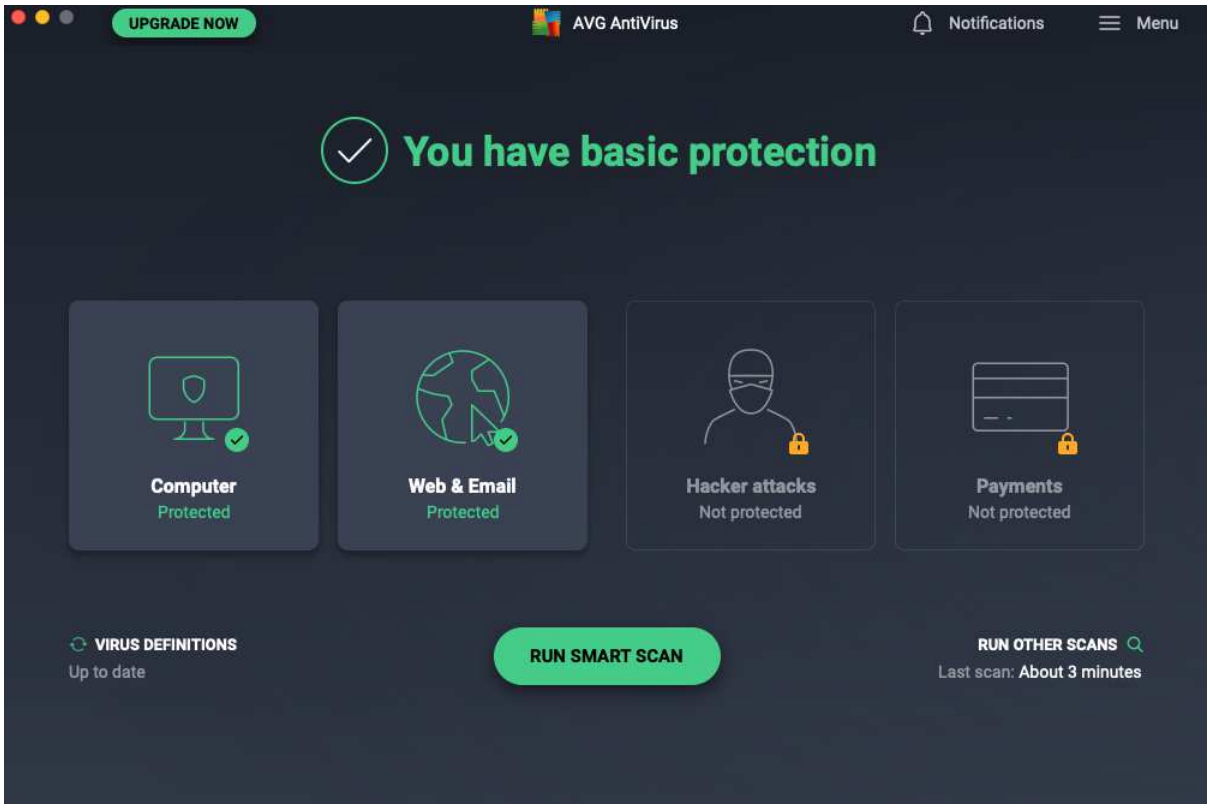
Help

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

Advertising

The *Smart Scan* feature promotes Avast's paid security suite, *Premium Security*. At the end of the scan, it will display 3 "advanced issues", namely vulnerability to ransomware, network threats and fake websites. If you click on *Resolve All* here, a purchase prompt for Avast Premium Security will be displayed. We also saw a pop-up alert with the same function.

AVG AntiVirus FREE for Mac



Summary

AVG AntiVirus FREE for Mac is, as its name suggests, a free antivirus program. The program is very simple to install, and most common features are easy to find in the clean, well-laid out GUI. AVG AntiVirus has highly effective on-access protection, which instantly detects and deletes malicious files when they are copied or downloaded. Alerts are clear and persistent, giving you time to read them. Standard user accounts cannot take any risky actions. The program is well suited to non-expert users due to its ease of use.

Installation

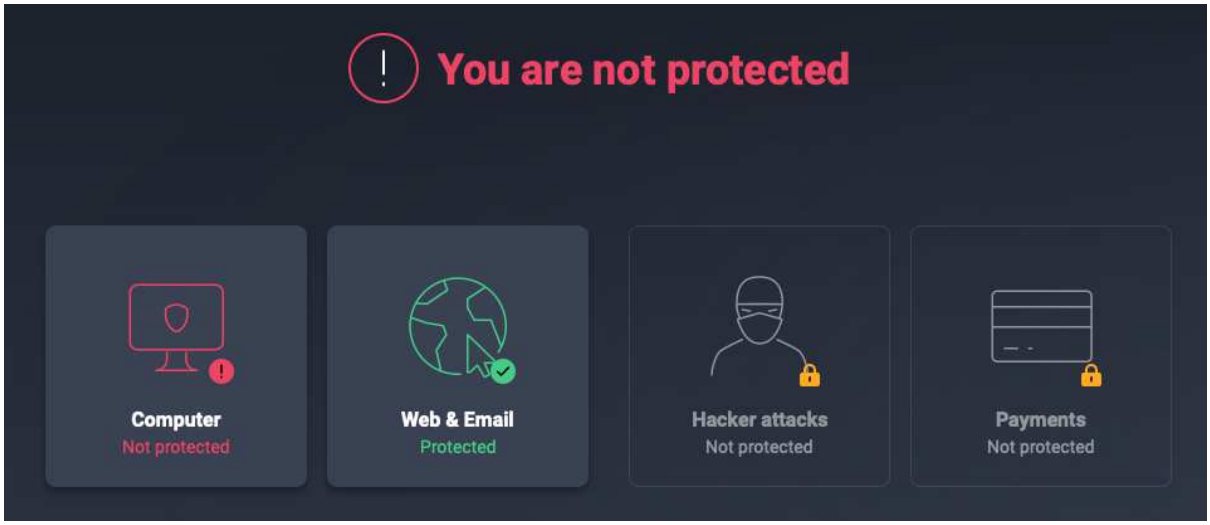
To set up AVG AntiVirus on your Mac, you just download and run the installer file, then double-click *AVG AntiVirus*. You can uninstall the program by clicking *AVG AntiVirus* in the macOS menu bar, then *Uninstall AVG AntiVirus*.

Finding essential features

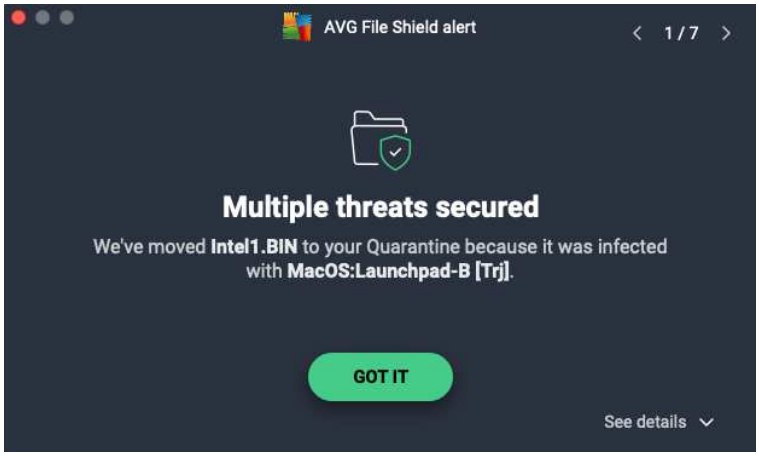
Status, **default scan, scan options** and **updates** are all found on the home page of the main program window. **Settings** (*Preferences*) can be opened from the menu in the top right-hand corner of the program window, or the macOS menu bar. **Quarantine** is found by clicking the *Computer* tile on the home page. **Subscription information** is not applicable, as the program is free. You can **scan a drive, folder or** file from the Finder context menu, by clicking *Scan with AVG*. The **help** page is accessible from the *Help* menu in the Mac menu bar.

Alerts

When we disabled AVG's real-time protection, the alert below was shown in the main program window. We were able to reactivate the protection by clicking *Computer*, and then setting the slider button for *File Shield* to the "on" position.



When malware was detected in our functionality check, AVG displayed the alert shown below. No user action was required. The alert persisted until we closed it. We note that it's possible to browse through multiple alerts using the arrows in the top right-hand corner. They can be closed individually by clicking *Got it*, or all at once using the macOS close button top right.



Malware detection scenarios

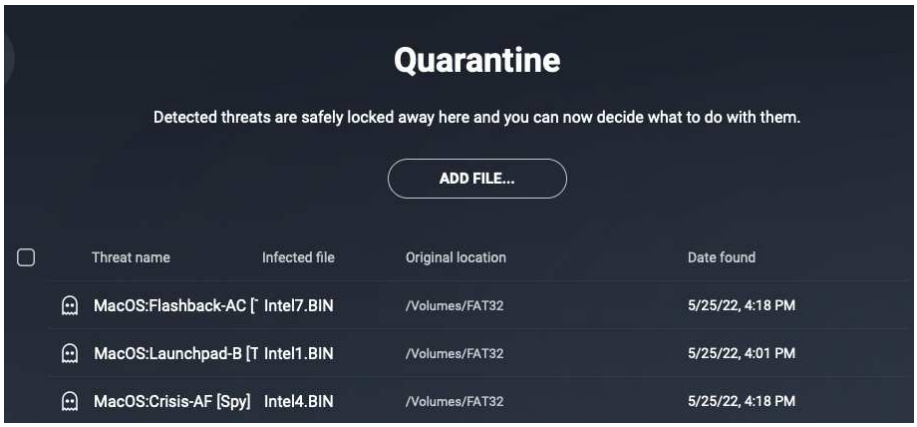
We found AVG AntiVirus FREE for Mac to have highly sensitive and reliable on-access detection of malware. Malicious files that we downloaded or copied to the system were instantly detected and quarantined in all cases. When we tried to copy malware from an external drive to the system, AVG not only prevented the files from being copied, but deleted the source malware on the external drive as well.

By default, AVG does not automatically scan USB drives when they are connected. However, you can activate a setting in the program's preferences that will prompt you to scan external drives upon connection to your Mac.

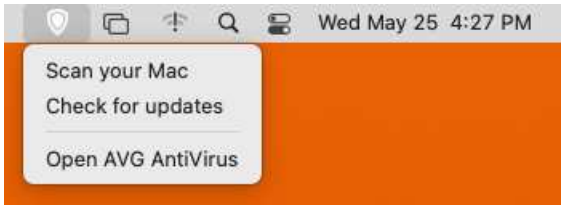
When we scanned a flash drive containing malware samples, AVG presented a list of the threats found; we just had to click *Resolve Selected* to quarantine them.

Quarantine and Logs

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



System Tray menu



Advanced options

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

- Disable protection features (under *Computer\File Shield*)
- Uninstall the program
- Restore items from quarantine

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

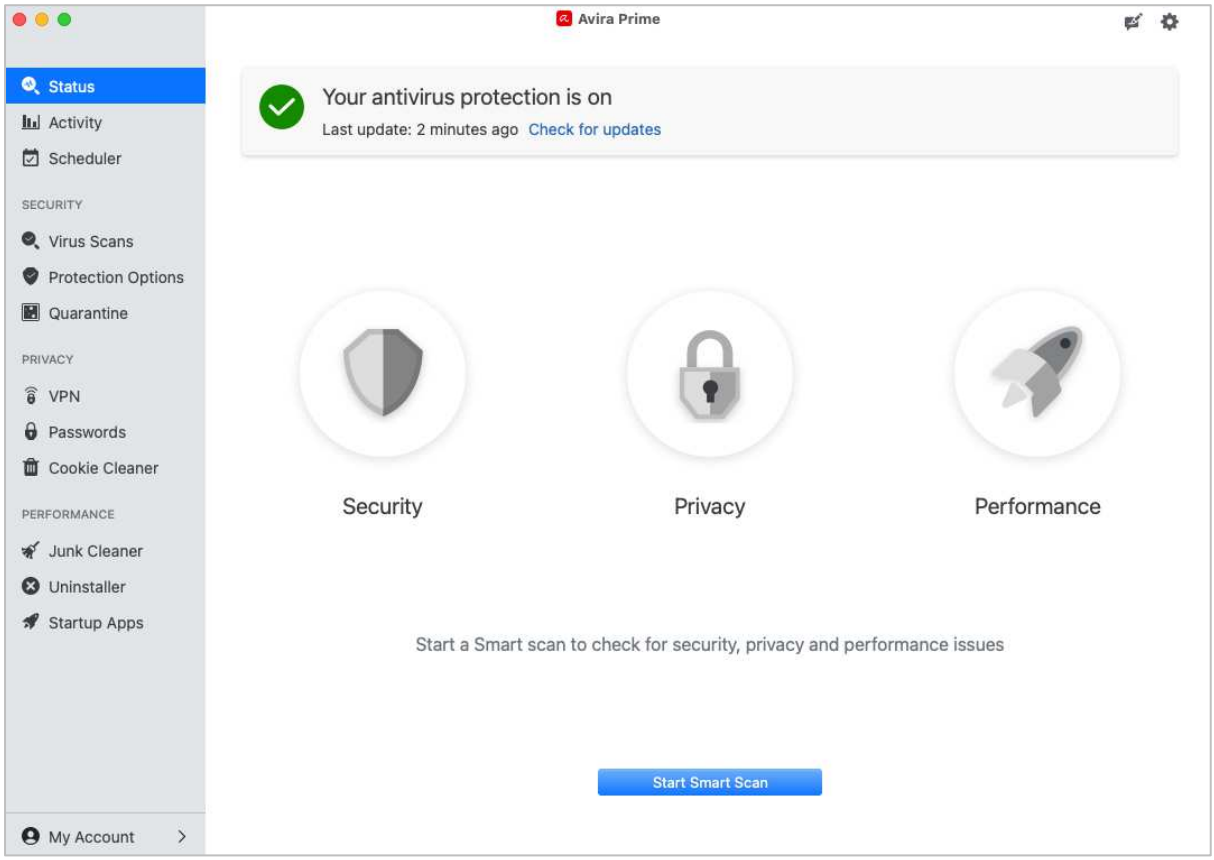
Help

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

Advertising

The *Smart Scan* feature promotes AVG's paid-for Mac security suite, *Internet Security*. At the end of the scan, it will display 3 "advanced issues", namely vulnerability to ransomware, network threats and fake websites. If you click on *Resolve All* here, a purchase prompt for AVG Internet Security will be displayed.

Avira Antivirus Pro for Mac



Summary

Avira Antivirus Pro for Mac is a straightforward, paid-for antivirus program with a data-limited VPN feature. It is very simple to install, and all the available features are easy to find in the neat interface. In our functionality check, we found it to have very sensitive and reliable on-access protection against malware. Detection alerts do not require any user action, and standard user accounts cannot take any risky actions. The simplicity of the program makes it an excellent choice for non-expert users.

Installation

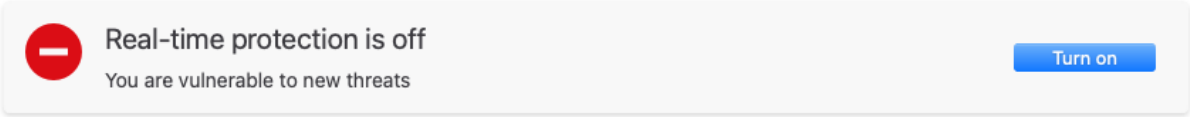
To set up Avira Antivirus Pro for Mac, you need to log in to your Avira account. You then download and run the installer, double-click the Avira icon, then click *Accept and install*. There are no options or decisions to make. When the program window first opens, you are prompted to run a *Smart Scan*. The program can be uninstalled by deleting it from the macOS Applications folder.

Finding essential features

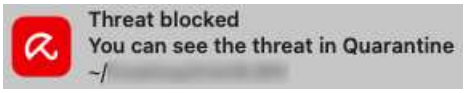
Status, **updates**, **default scan**, **scheduled scan**, **scan options**, **quarantine** and **subscription information** can all be accessed from the main program window (screenshot above). You can also scan a drive, folder or file from the Finder context menu. The **help** feature is found in the *Help* menu in the Mac menu bar. *Protection Options* in the left-hand menu panel lets you activate or deactivate real-time protection and automatic scans of USB devices. Other settings (*Preferences*) can be accessed from the cogwheel icon in the top right-hand corner of the window.

Alerts

When we disabled Avira's real-time protection, the alert below was shown in the main program window. We were able to easily reactivate the protection by clicking *Turn on*.



When malware was detected in our functionality check, Avira displayed a pop-up alert (shown below). No user action was required. The alert closed automatically after 5 seconds.



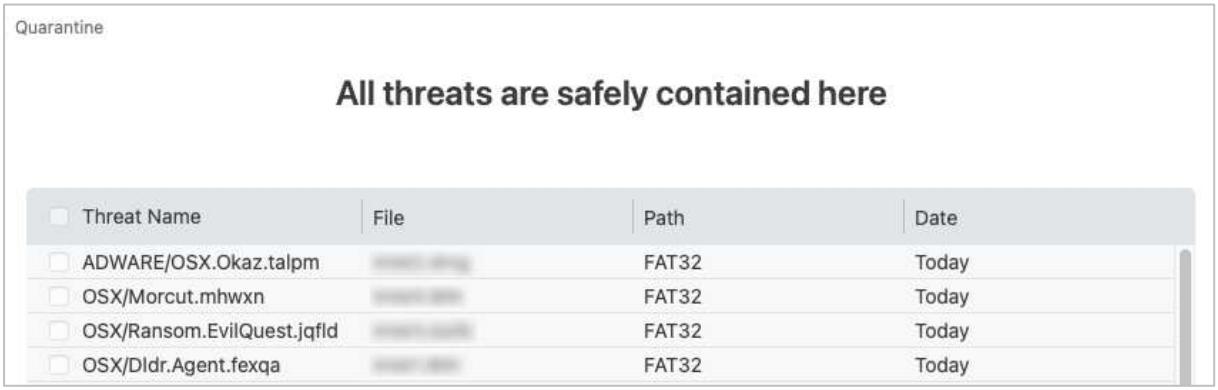
Malware detection scenarios

In our functionality check, we found Avira Antivirus Pro to have very sensitive and reliable on-access detection of malware. Malicious files that we downloaded or copied to the system were instantly detected and quarantined in all cases. When we tried to copy malware from an external drive to the system, Avira not only prevented the copy process, but also deleted the source malware on the external drive.

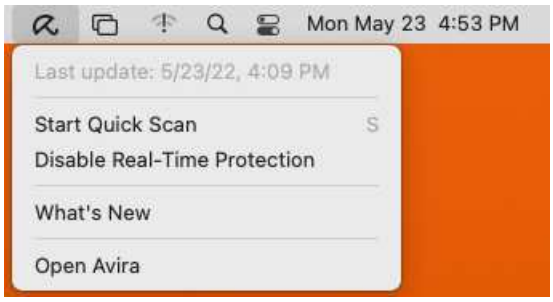
When we connected a USB flash drive to our Mac, Avira briefly displayed a prompt to scan it. We did this, and Avira automatically quarantined the malicious files without the need for any user action. A summary of the malware found, and action taken, was displayed in the main program window. We note that the scan prompt closed after 5 seconds, so you have to be quick to make use of it.

Quarantine and Logs

The *Quarantine* page of the program (screenshot below) shows you all the items that have been quarantined, along with the date when this happened. There are options to delete and restore any of the detected files (you have to enter administrator credentials to take either action).



System Tray menu



Advanced options

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

- Disable protection features (*Protection Options* page or System Tray menu)
- Restore items from quarantine
- Uninstall the program

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

Help

Avira Help (in the *Help* menu in the macOS menu bar) opens the product's support page in a browser. This consists of simple text instructions for everyday tasks, some illustrated with screenshots. There is also a video to explain installation of the product.

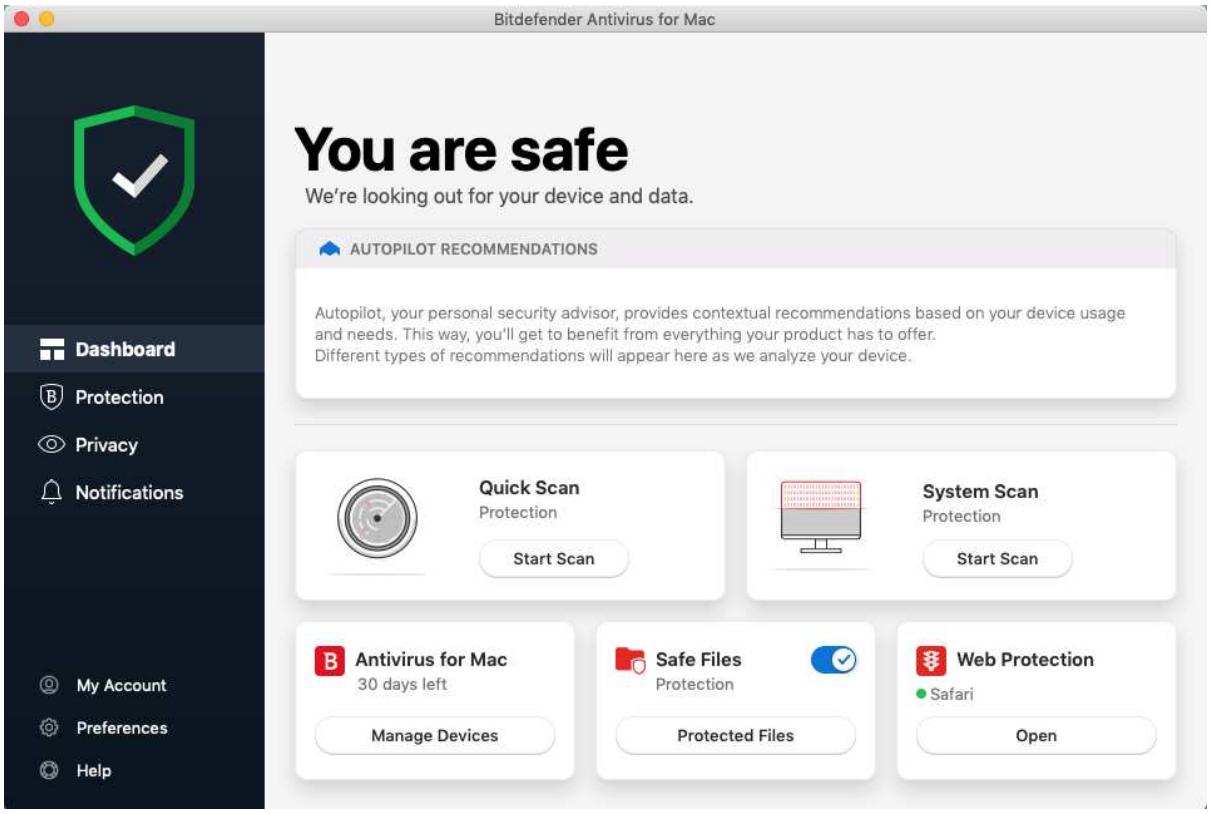
Advertising

Antivirus Pro advertises Avira's *Prime* service, via the *Get Prime* button in the menu panel.

Other points of interest

The program's main window has both dark and light modes, which co-ordinate with the dark- and light-mode settings of macOS.

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/Chrome/Firefox. 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

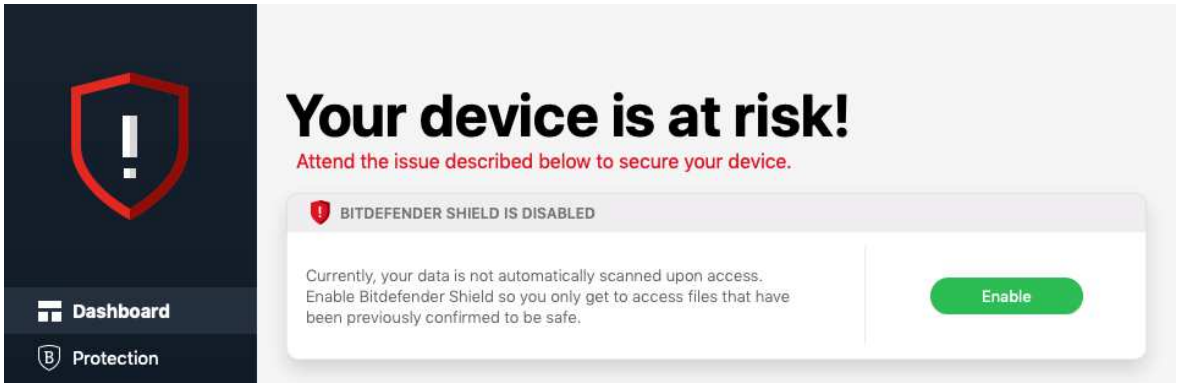
After downloading and starting the installer file, you just need to double-click the setup package icon to start the setup wizard. You do not need to make any decisions, though you can change the interface language. When setup is complete, you need to create a Bitdefender account and sign in. An optional 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. You can uninstall the program using its own uninstaller. This is found in the Bitdefender folder in the Finder Applications window.

Finding essential features

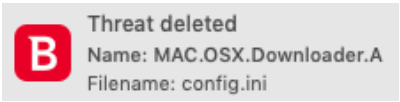
Status, **quick** and **full scans**, **subscription information**, **settings** and **help** are all directly accessible from the program's *Dashboard* (home page). You can find **custom scan**, **quarantine** and **scan exceptions** under *Protection*. **Update** is in the *Actions* menu in the Mac 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*.

Alerts

When we disabled Bitdefender's real-time protection, the alert below was shown in the main program window. We were able to reactivate the protection easily by clicking *Enable*.



When malware was detected in our functionality check, Bitdefender displayed the alert below. No user action was required, and the alert closed after 5 seconds.

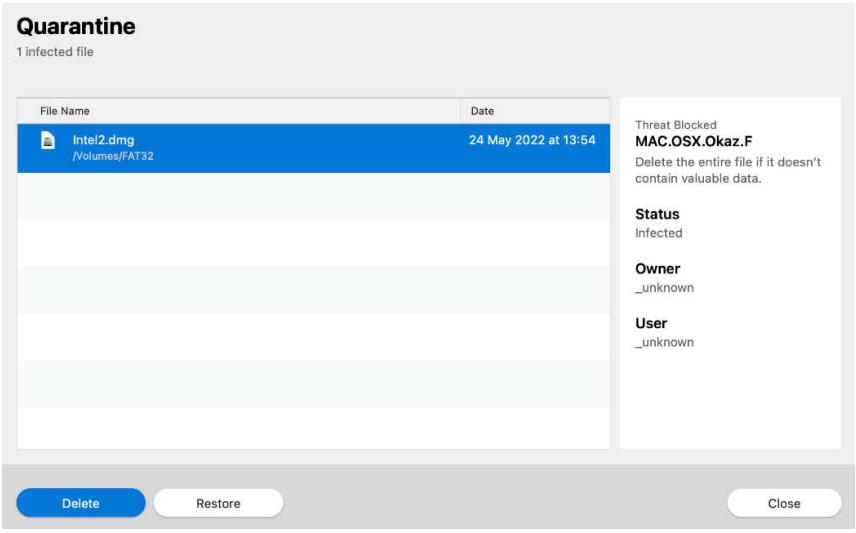


Malware detection scenarios

In our functionality check, we found Bitdefender to have very sensitive and reliable on-access detection of malware. Malicious files that we downloaded or copied to the system were instantly detected and quarantined in all cases. When we connected a USB flash drive containing malware samples to our Mac, Bitdefender automatically scanned the drive and deleted the malware without any user action being required.

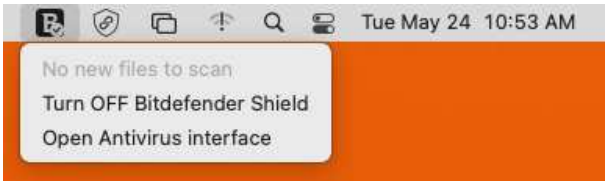
Quarantine and Logs

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. *Notifications* is the log feature. It displays events such as updates, component activation, and malware detections. These can be displayed all together, or filtered by importance (*Critical, Warning, Information*).

System Tray menu



Help

Antivirus for Mac Help in the macOS 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):

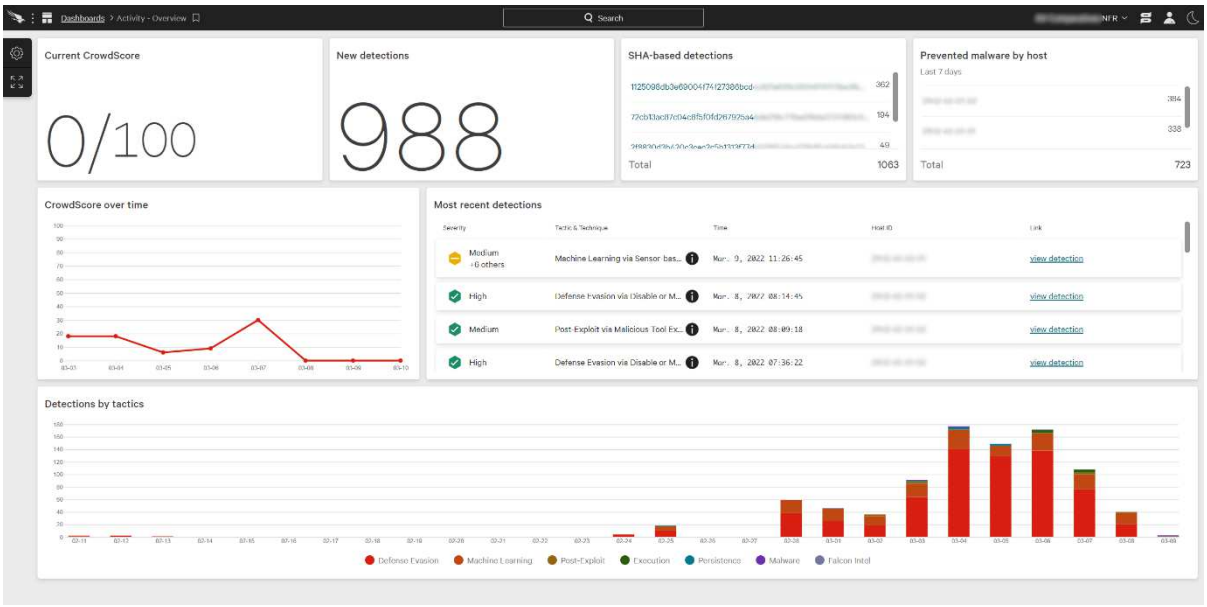
- Disable protection features (under *Preferences*)
- Restore items from quarantine
- Uninstall the program

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 Pro



About the product

CrowdStrike Falcon Pro is a security package for business networks. It provides a cloud-based console for managing the endpoint protection software. Details of the management console described here are applicable to all supported operating systems. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. It can manage networks with thousands of devices. We note that CrowdStrike Falcon Pro is available as a fully managed service for organisations that desire a more hands-off solution to endpoint protection. CrowdStrike tell us that they have datacentres in the USA and EU, in order to comply with the respective data protection regulations.

Advantages

- Investigative functions
- Comprehensive search facilities
- Clickable interface provides easy access to details pages
- Encyclopaedia of known cybercriminal groups
- Suitable for medium- to large-sized enterprises

Management Console

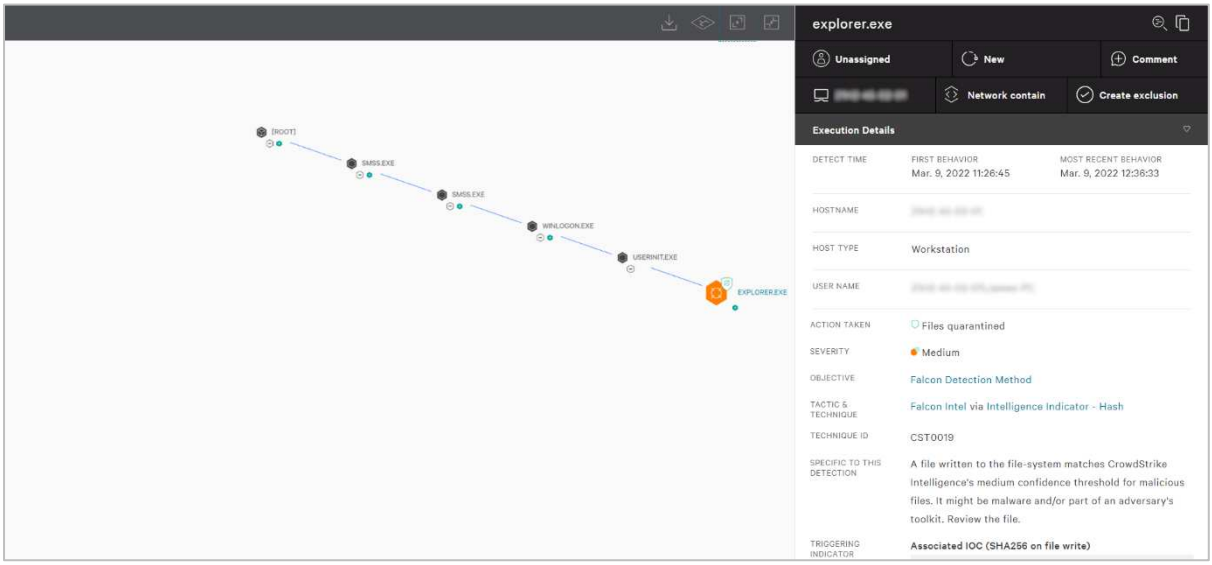
The console is navigated from the Falcon menu in the top left-hand corner of the console. This lists individual pages under headings such as *Activity*, *Investigate*, *Hosts*, *Configuration*, *Dashboards* and *Users*. You can easily bookmark any page of the console (using the bookmark symbol in the top left-hand corner of the page), and then go directly to that page using the *Bookmarks* section of the menu.

Activity\Dashboard page

This is the page you see when you first log on to the console (screenshot above). It shows various status items in large panels. There is a list of most recent detections, with a graphical severity rating. You can also see a graph of detections by tactic (e.g. *Machine learning, Defense Evasion*) over the past month. Terms from the MITRE ATT&CK Framework are used to show attack stages here. Some of the panels are linked to details pages. Thus, you can click on the *New detections* panel to open up the *Detections* details page.

Activity\Detections page

Here you can search a list of threat detections using a wide range of criteria. These include severity, malware tactics, detection technique, date and time, affected device, and logged-on user. For each detection, you can see full details, including a process tree view (screenshot below). You can assign a console user for remediation.



Activity\Quarantined Files page

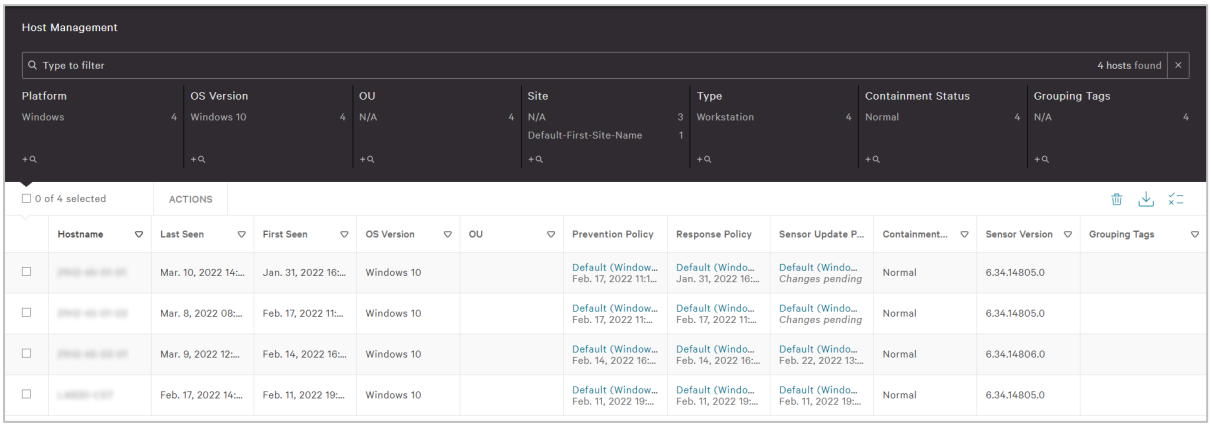
As you would expect, this page lets you see files that have been quarantined by the system. You can see the filename, device name, number of detections counted on the network, user involved, status, and of course date and time of detection. Quarantined files can be released or deleted. Clicking the entry of a quarantined file opens a details panel with additional information. This includes file path for the location where it was detected, file hashes, file size, file version number, detection method and severity. There is a search function and a variety of filters you can use to find specific files within the quarantine repository.

Configuration\Prevention Policies page

Here you can create and edit the protection policies for endpoints. You can define behaviour for a number of different types of attack-related behaviour, such as ransomware, exploitation, and lateral movement. Some sensor components, such as *Cloud Machine Learning* and *Sensor Machine Learning,* have separate configurable levels for detection and prevention. 5 different levels of sensitivity can be set, ranging from *Disabled* to *Extra Aggressive*. Custom Indicators of Attack (IOA) can also be created and assigned here, and there's an option to perform automated remediation of IOA detections.

Policies can be assigned to devices automatically by means of a naming system. For example, any device with "Win" in its name can be automatically put into a specific group of Windows computers, to which a particular policy is assigned. Devices/groups can be assigned more than one policy, whereby a policy hierarchy determines which one takes precedence.

Hosts\Host Management page



The *Hosts/Host Management* page lists all the installed devices. You can immediately see which ones are online. Additional information includes operating system, policy, security status and sensor version. Clicking on a device's entry opens up a details panel for that device. Here you can find additional information, such as device manufacturer, MAC address, IP addresses and serial number.

Intelligence\Actors page

This page provides details of known cybercriminal groups. You can see the nations and industries that each one has targeted, along with technical details of the attack methods used. CrowdStrike tell us that this information is also available in *Detection* details when a detection is associated with a specific actor.

Investigate\Host Search page

The *Investigate* menu provides an extremely comprehensive search facility. It lets you search for devices, hashes, users, IP addresses, domains and events. On the *Host Search* page, you can look for specific devices. A separate menu bar allows you to look for specific aspects, such as *Activity* (including detections), *Vulnerabilities* and *Custom Alerts*.

macOS Endpoint Protection Client

Deployment

Installer files for the *sensor* (endpoint protection client) can be downloaded in .pkg format from *Hosts\Sensor Downloads* page. Half a dozen older versions of the sensor are available if you want. Local installation requires the use of the macOS Terminal – instructions are provided in the documentation.

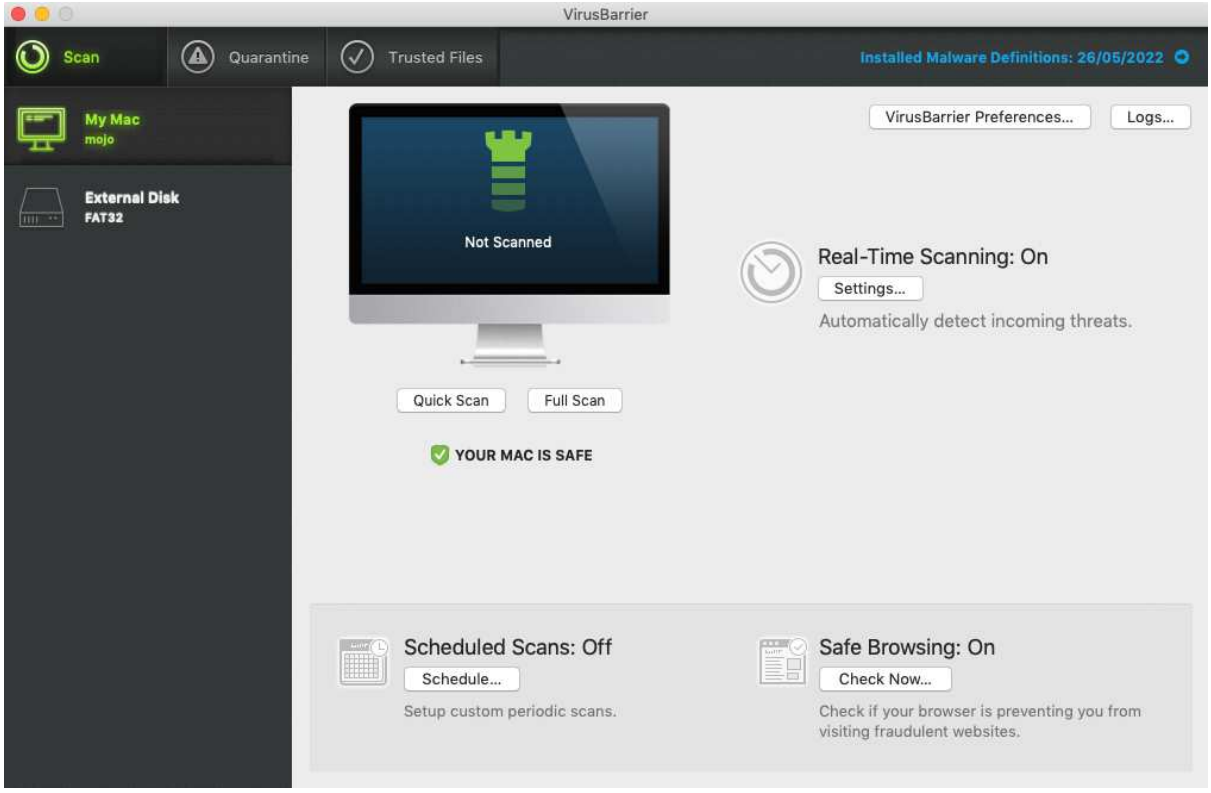
User interface on macOS client

With the settings used for this test, no graphical user interface is provided, so users cannot interact with the program at all. Administrators can use a command-line interface (*falconctl*) via the macOS Terminal. Detected files are not deleted, but quarantined in situ.

Malware detection scenarios

In our functionality check, we found CrowdStrike Falcon Pro for macOS to have sensitive and reliable on-access detection of malware. Malware that we downloaded or copied to the system was instantly detected and quarantined in all cases.

Intego Mac Internet Security X9



Summary

Intego Mac Internet Security X9 is a paid-for security suite. In addition to anti-malware features, it also includes a firewall. This is a separate application within the bundle, called *NetBarrier*. In this review, we have focused on the antivirus application, *VirusBarrier*.

The program's interface makes the most important functions easy to find and use. We found Mac Internet Security X9 to have sensitive on-access protection against malware. Standard user accounts cannot take any risky actions. Overall, the program is straightforward in use.

Installation

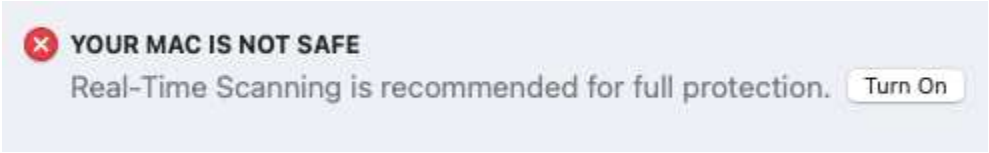
To set up Mac Internet Security X9, you just need to download and run the installer, then select *Double Click to Install*. The first page of the installer includes convenient links to the *Getting Started* user guide, and the uninstaller. The setup wizard is very straightforward, though you have to restart your Mac at the end of it. When you first open the program after the restart, you will be prompted to allow the program Full Disk Access in the macOS settings. The program can be uninstalled by re-running the installer file and double-clicking *Uninstall*.

Finding essential features

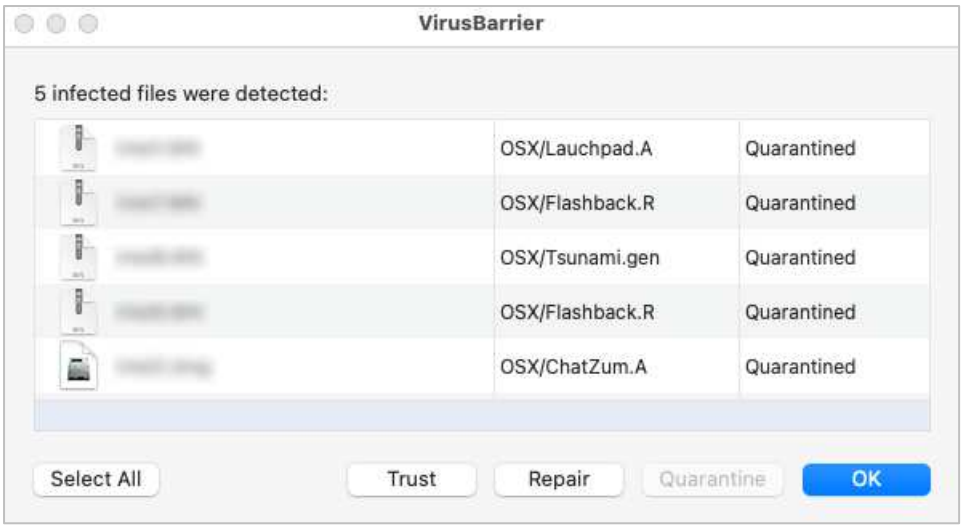
Status, **quick/full/scheduled scans, settings** (*Preferences*)**, logs** and **quarantine** are all found on the program's home page. You can scan a file, folder or drive using Finder's right-click menu. The **update, custom scan** and **help** features are found in the Mac menu bar. The *About* box (*VirusBarrier* menu) shows the licence key and registered email address, but does not state when the licence expires.

Alerts

When we disabled Intego's real-time protection, the alert below was shown in the main program window. We were able to reactivate the protection easily by clicking *Turn On*.



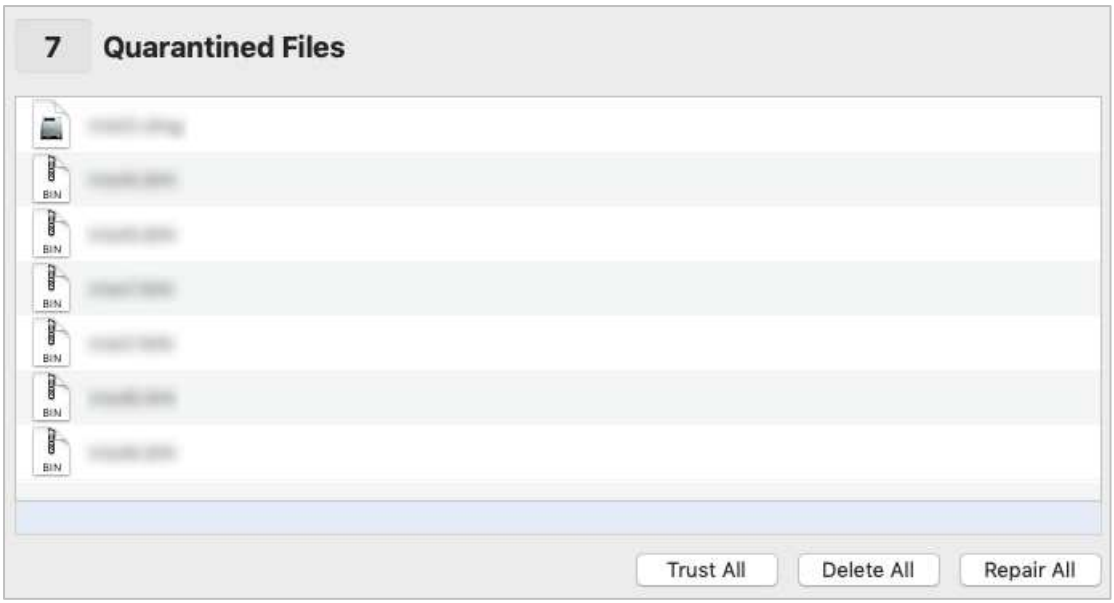
When malware was detected in our functionality check, Intego displayed the alert shown below. No user action was required. The alert persisted until we closed it.



Malware detection scenarios

In our functionality check, we found Intego to have sensitive on-access detection of malware. Malicious files that we downloaded or copied to the system were immediately detected and quarantined in situ. When we connected a USB flash drive containing malicious files to our Mac, Intego prompted us to scan it. We did this, and Intego automatically quarantined the malware. An alert like the one above was shown.

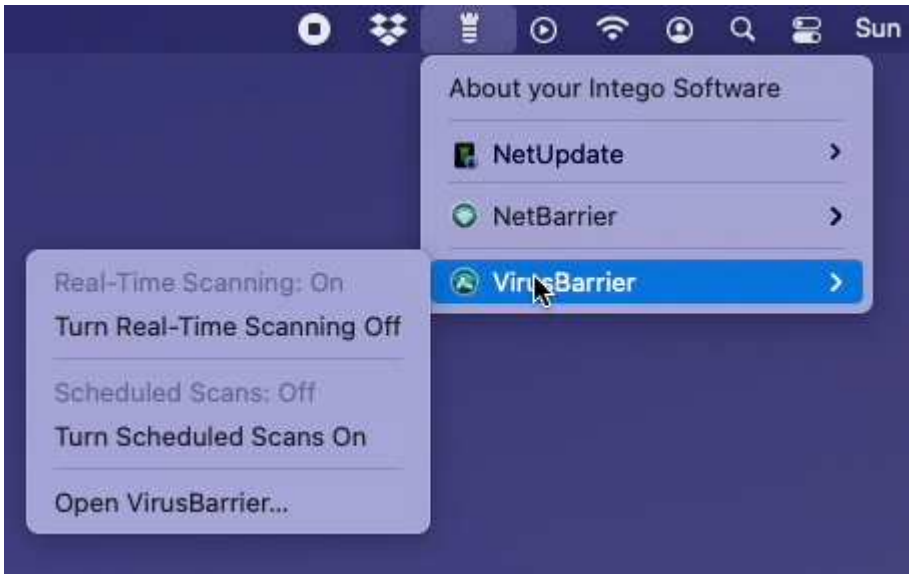
Quarantine and Logs



The quarantine feature is shown above. There are options to delete, repair or restore the quarantined files. If you click on an individual quarantined item, the path to its location will be shown in the status bar at the bottom.

Logs displays a list of all system events, including updates, scans and real-time detections, enabling/disabling real-time protection, and items added to or deleted from quarantine. The applicable date and time are shown, along with a traffic-light colour-coding system for each item. Malware finds are thus shown as red, quarantine actions as yellow, and enabling real-time protection as green.

System Tray menu



Help

There are 2 help items in the Mac menu bar. *Show Basic Help* displays an overlay that explains the principal features in the main program window. *VirusBarrier Help* opens a comprehensive online manual

that covers installation, configuration and use of the program. It is generously illustrated with screenshots.

Advanced options

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

- Disable protection features
- Restore items from quarantine
- Uninstall the program

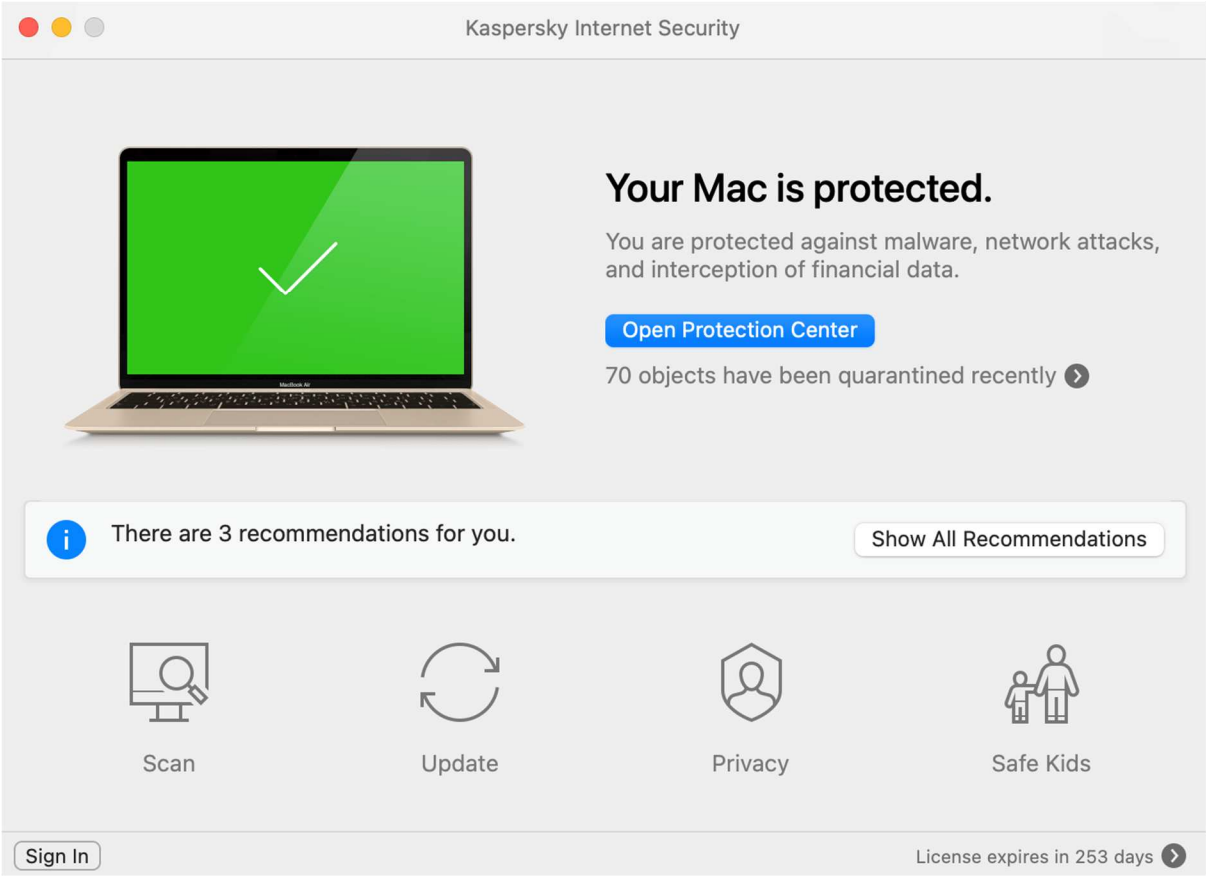
Standard macOS users (i.e. accounts without administrator rights) cannot perform any of the above tasks, which we regard as ideal.

Other points of interest

Whilst running our functionality check, we saw a notification from Intego that the contents of an attached USB flash drive had changed, along with a prompt to rescan the device.

VirusBarrier uses Intego's own detection engine to detect macOS malware, but makes use of the Avira engine to detect Windows malware.

Kaspersky Internet Security for Mac



Summary

Kaspersky Internet Security for Mac is a paid-for security suite with browser add-ons, parental controls and a data-limited VPN. We found it very straightforward to use, with all the features easily accessible from the main program window or macOS menu bar. Effective on-access detection quarantines any malware downloaded or copied to the system. Users without administrator rights cannot disable the protection or uninstall the program. Overall, the product is well designed and reliable in operation.

Installation

Having downloaded and run the installer, you need to double-click *Install Kaspersky Internet Security\Download and Install*. The only technical options are whether to install network protection, encrypted web traffic inspection, and browser extension(s). The latter are provided for Safari, Google Chrome and Mozilla Firefox, and can be selected independently of each other. The program can be uninstalled by clicking *Support\Uninstall* in the *Help* menu of the macOS menu bar.

Finding essential features

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

Alerts

When we disabled Kaspersky's real-time protection, the alert below was shown in the main program window. We were able to reactivate the protection easily by clicking *Enable*.

Malware alerts

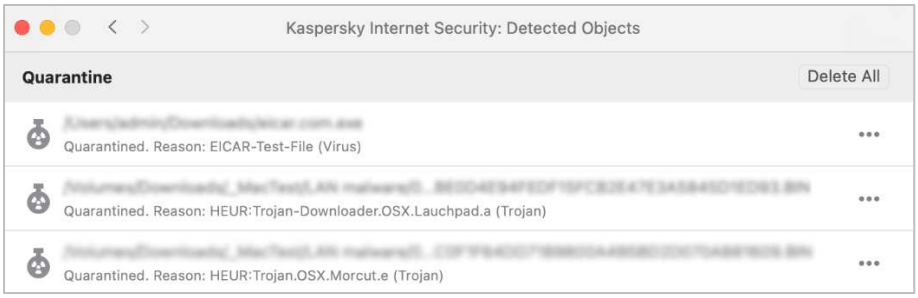
In our functionality check, Kaspersky detected malware silently, i.e. without any visual or audio alerts being shown.

Malware detection scenarios

In our functionality check, we found Kaspersky Internet Security for Mac to have reliable on-access detection of malware. Malicious files that we downloaded or copied to the system were detected and quarantined in all scenarios. When we tried to copy malware from a USB drive or network share, Kaspersky deleted not only the copied files on the Mac Desktop, but also the source malware on the USB drive or share. We noted a short delay, typically between 10 and 20 seconds, between the copy/download process completing and the files being detected by Kaspersky.

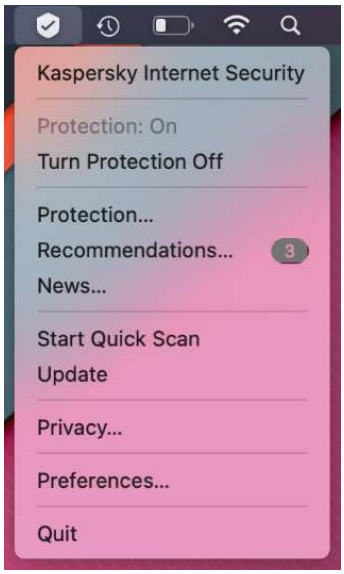
When we connected a USB flash drive containing malware samples to our Mac, Kaspersky prompted us to scan it. We did this, and Kaspersky automatically deleted the malicious files on it, with no user action required. However, no alert was shown. We note that the scan prompt closed after 5 seconds, so a user would have to be quick to make use of it.

Quarantine and Logs



The *Detected Objects* page shows quarantined items. By clicking on the "..." symbol at the end of each line, you can delete or restore individual items. You can delete all quarantined items using the *Delete All* button. The *Reports* page shows the location of detected objects, action taken, threat type, threat name, and date/time of detection.

System Tray menu



Help

Kaspersky Internet Security Help is found in the *Help* menu in the macOS menu bar. It opens the product's support page on the Kaspersky website, which 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
- Restore items from quarantine
- Uninstall the program

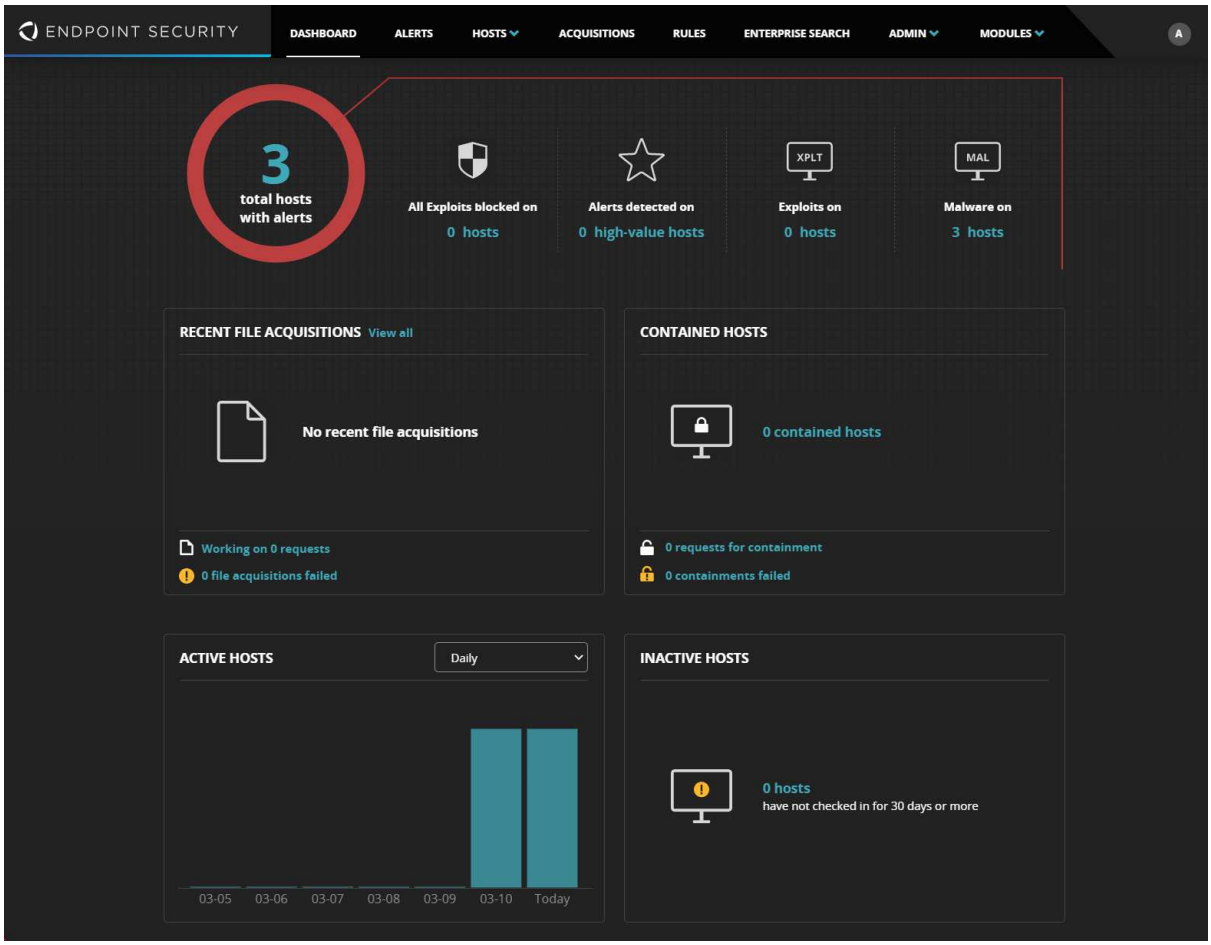
Standard macOS users (i.e. accounts without administrator rights) cannot disable protection or uninstall the program, which we regard as ideal. Non-admin users can restore items from quarantine, although restored malware files are immediately re-detected and re-quarantined by default.

Other points of interest

Kaspersky Internet Security for Mac uses graphics in the program window that could be described as "intelligent". The program detects whether it is installed on a Mac laptop or desktop system, and accordingly shows either a desktop or a laptop graphic. The Update and Scan icons animate when in use.

In our functionality check, we found that Kaspersky Internet Security for Mac did not display any alerts when malware was detected, even though notifications were enabled in both the application itself and the macOS settings for it. This did not affect detection/protection, however.

Trellix Endpoint Security (HX)



About the product

Trellix Endpoint Security (HX) is a security package for business networks. It provides a cloud-based console for managing the endpoint protection software. Details of the management console described here are applicable to all supported operating systems. A variety of console types is available. These include cloud-based, hardware appliance, virtual appliance, and Amazon-hosted. We describe the cloud-based console in this review. As well as malware protection, the product includes investigative functions for analysing and remediating attacks. The product is designed to handle very large organizations, with support for up to 100,000 endpoints per appliance.

Advantages

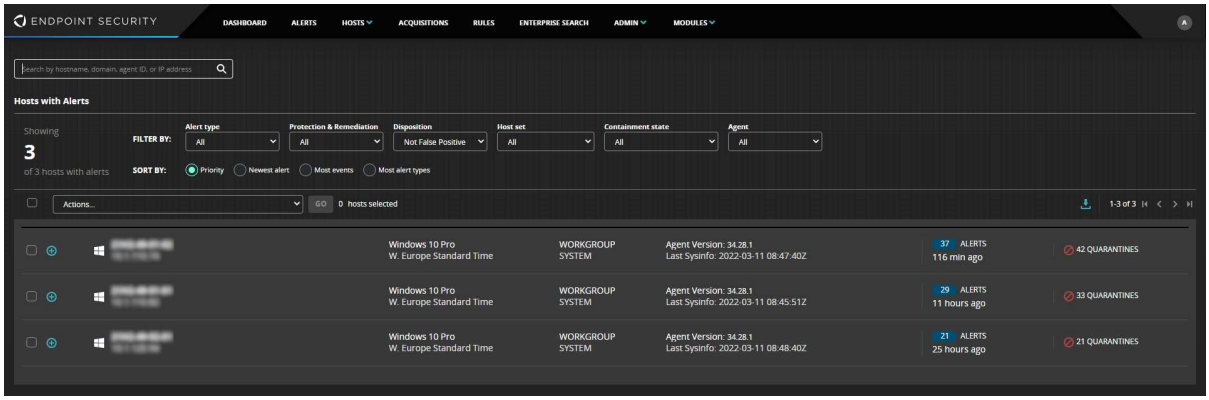
- Attack investigation features
- Variety of console types available
- Suitable for medium- to large-sized enterprises
- Comprehensive search feature
- Containment feature lets you isolate infected devices

Management console

Dashboard

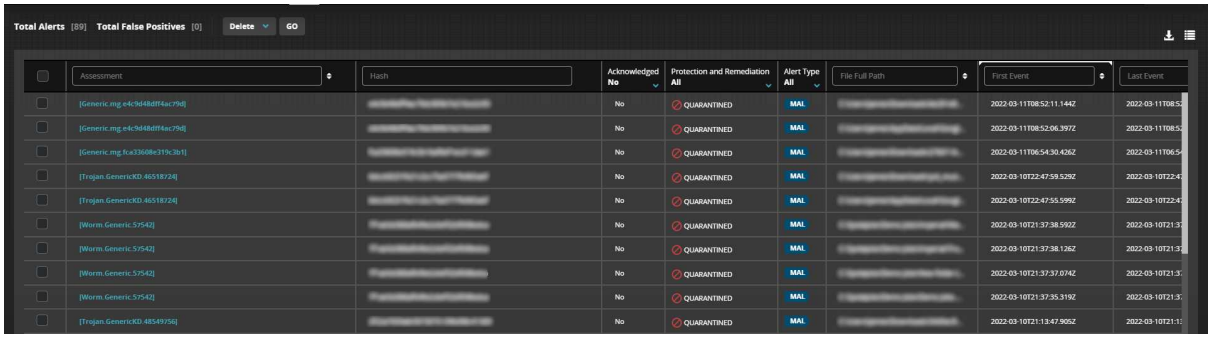
When you open the console, you will see an overview of key status items (screenshot above). These include the total number of hosts with alerts, with a breakdown by exploits and malware. Clicking on the *Total hosts with alerts* button opens the *Hosts with Alerts* page, shown below.

Hosts with alerts



As the name suggests, this page displays details of protected devices with alerts that have not yet been dealt with. If you click on the plus sign for a device, you can see a list of alerts for that device, in chronological order. With malware alerts, a wealth of detail is provided for each one. This includes status (e.g. quarantined), file path, MD5 and SHA1 hashes (but not SHA256), file size, last modified and last accessed times, process path, username of logged-on user, detection name, threat type, and times of first and last alerts for the item. Each threat can be acknowledged (marked as "read"), or marked as a false positive. You can also add comments to the threat details, for future investigation.

Alerts

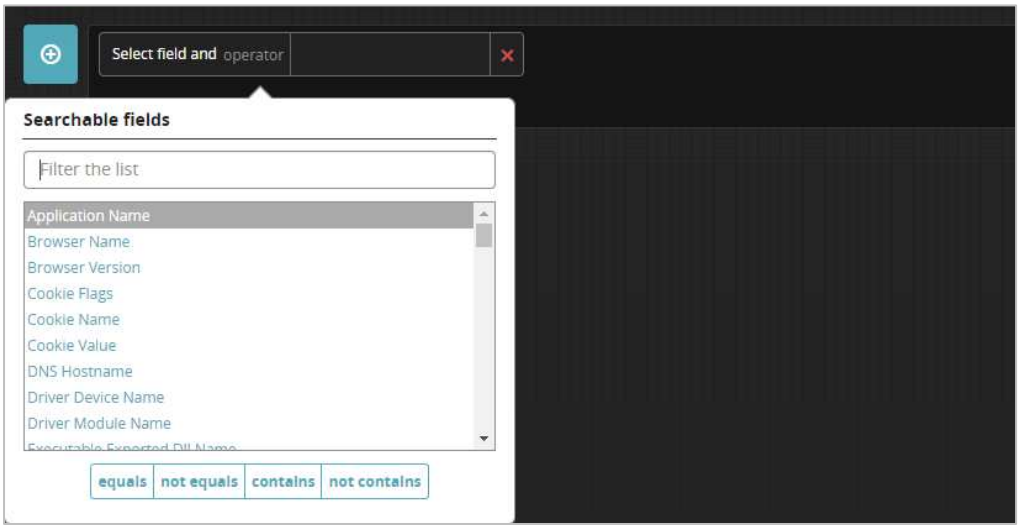


For a threat-centric rather than a device-centric view, you can go to the *Alerts* page. Here you can sort threats by name, file path, first or last detections, and hostname or IP address of the respective device. The options *Acknowledge*, *Mark False Positive* and *Add Comment* are provided here too.

Acquisitions

From the *Hosts* page, you can acquire a file or various items of diagnostic data from an individual device. The *Acquisitions* menu lets you download files that have been acquired from hosts, in order to analyse them.

Enterprise Search



This feature allows you to search the network for a very wide variety of items. These include application name, browser version, hostname, various executables, file names/hashes/paths, IP address, port, process name, registry key, service name/status/type/mode, timestamp, URL, username and Windows Event Message.

Admin\Policies

Here you can configure numerous different aspects of the client protection policy. Examples are scans, whether to show alerts on the client, logging, malware scan settings, polling frequency, tamper protection, scan exclusions, management server address and malware detection settings. Scans can be set to run on a schedule, or after a signature update or device boot.

Admin\Host Sets

These are simply groups of computers. They can be defined according to a wide variety of criteria, or simply by dragging and dropping from the list of all devices. These groups are used to apply different protection policies.

Admin\Agent Versions

This lets you download current and older versions of the endpoint agent for Windows and Mac systems. The admin can thus e.g. avoid compatibility problems with a particular agent version on specific systems.

Admin\Appliance Settings

This page allows you to change settings for the management console itself. There are controls for date and time, user accounts, notifications, network settings and licences, and more.

macOS Endpoint Protection Client

Deployment

Installer files in .dmg format can be downloaded from the Admin menu, Agent Versions. As the name suggests, the current and earlier versions of the client are provided. The installer file can be run manually, or via a systems management product such as Jamf. If you install the product manually, you will need to remember to give the agent full disk access in the macOS settings. This is a necessary action to enable the product to work properly.

After installation, the Trellix agent takes some minutes to download the protection engine. Protection will not be enabled until this is complete.

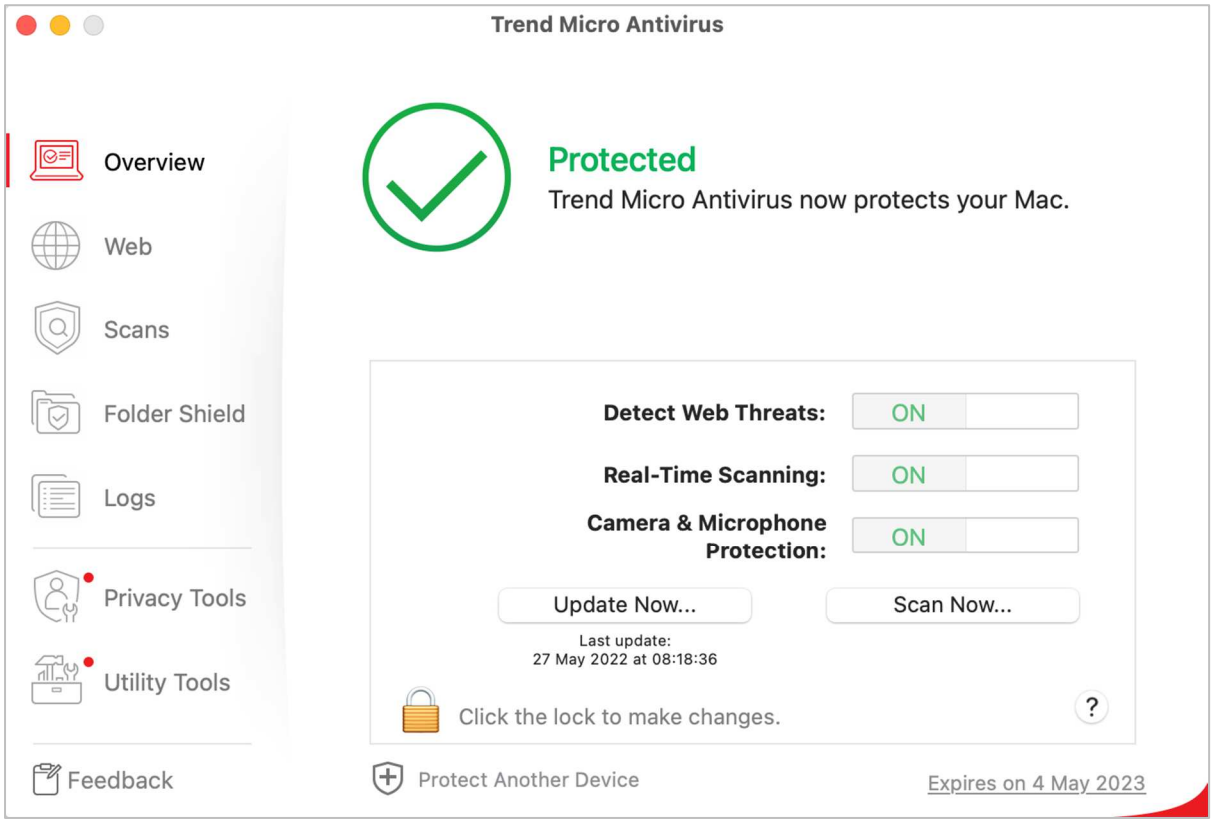
User interface on macOS client

The user interface is completely hidden, and users cannot interact with the program at all. No detection alerts are shown.

Malware detection scenarios

In our functionality check, we found Trellix Endpoint Security for macOS to have very sensitive and reliable on-access detection of malware. Malware that we downloaded or copied to the system was instantly detected and quarantined in all cases. When we tried to copy malware from a USB drive to the system, Trellix not only prevented the malware copy process, but also deleted the source malware on the USB drive.

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. We were particularly impressed with the very effective 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. For advanced users, a resizable quarantine window would be appreciated. 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 links to the following pages on the vendor's website: *System Requirements*, *Known Issues*, and *Quick Start Guide*. There is also an uninstaller, with which you can later quickly and easily remove the program, should you need to.

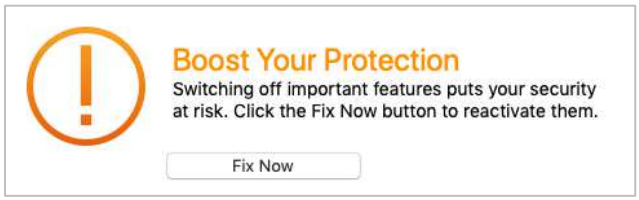
The setup wizard is very straightforward. Aside from choosing whether to enter a licence key or use the trial version, there are no decisions to make. When it comes to the process of authorising Trend Micro extensions and permissions, the setup wizard provides a convenient "Verify" button, which checks whether you have successfully granted the necessary permissions. A Trend Micro Safari Extension is installed, and will be activated if you authorise this. 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 both found 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.

Alerts

When we disabled real-time protection, the alert below was shown in the main window. We were able to reactivate the protection easily by clicking *Fix Now*.



When malware was detected in our functionality check, Trend Micro displayed an alert in the main window (shown below). No user action was required. The alert persisted until we closed it.

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.

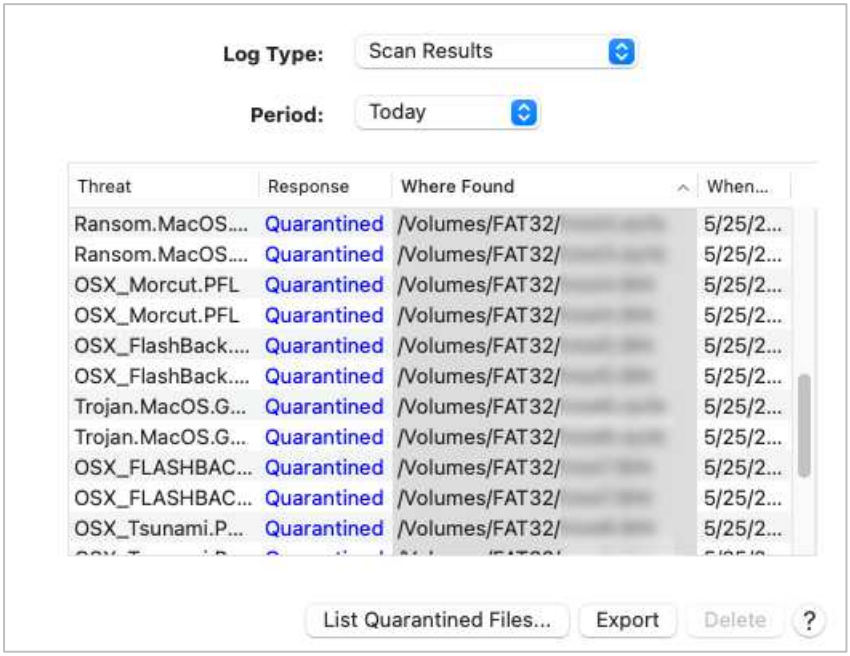
Malware detection scenarios

In our functionality check, we found Trend Micro Antivirus for Mac to have exceptionally sensitive on-access detection of malware. Malware that we downloaded or copied to the system was instantly detected and quarantined in all cases. When we tried to copy malware from a network share or USB drive to the system, Trend Micro not only prevented the malware copy process, but also deleted the source malware on the USB drive or network share.

When we scanned a flash drive containing malware samples, Trend Micro automatically quarantined the malicious files without the need for any user action. At the end of the scan, a message box is displayed, showing a summary of the scan results. There is a button you can click on to see further details.

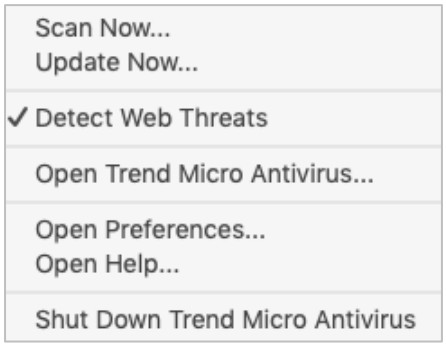
Quarantine and Logs

The quarantine and log functions are both accessed via the *Logs* page. Quarantine functionality, including options to restore or clean quarantined items, is reached by clicking *List Quarantined Files* on the *Logs* page. From here, you can view and delete or (with a macOS Administrator Account) restore any or all of the quarantined items.



As noted in previous years, the quarantine and log data is displayed in panels within small windows that cannot be resized or maximised. It is necessary to resize the columns is required to see all the content, and then scroll to the left to see all the data for one entry. We found this very inconvenient. However, it is possible to export the log as a .CSV file.

System Tray menu



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)
- 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.

Help

Clicking the *?* icon in the bottom right-hand corner of 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.

Advertising

Trend Micro Antivirus for Mac advertises its vendor's freemium Cleaner One Pro program. There is a link to this in the *More Tools* page of the program window. Also, running a *Smart Scan* will find "junk files", and prompt the user to get Cleaner One Pro to remove these.

Other points of interest

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

In our functionality check, we discovered that the link to the *Quick Start Guide* in the installer misdirected to a different page. We informed Trend Micro of this, and they have since fixed the issue.

Featurelist security for macOS Monterey (as of June 2022)										
Product name:	Acronis Cyber Protect Cloud with Advanced Security pack	Avast Security Free for Mac	AVG AntiVirus FREE for Mac	Avira Antivirus Pro for Mac	Bitdefender Antivirus for Mac	Crowdstrike Falcon Pro for Mac	Intego Mac Internet Security X9	Kaspersky Internet Security for Mac	Trellix Endpoint Security HX	Trend Micro Antivirus for Mac
Supported Program languages:	English	English, German, Czech, Spanish, Finnish, French, Italian, Dutch, Polish, Korean, Portuguese, Russian, Swedish, Norwegian	English, German, Czech, Spanish, Finnish, French, Italian, Dutch, Polish, Korean, Portuguese, Russian, Swedish, Norwegian	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, French, German, Japanese, Spanish	English, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish, Czech, Arabic, Thai, Vietnamese	English, Spanish, German, French, Italian, Japanese, Korean, Polish, Portuguese, Russian, Chinese	English, German, French, Spanish, Chinese
Third-party scan engine used (in addition to it's own)	Bitdefender	proprietary	Avast	proprietary	proprietary	proprietary	proprietary	proprietary	Bitdefender	proprietary
Free Trial version available? (how many days?)	n/a (enterprise)	Freemium	Freemium	Freemium	30 days	n/a (enterprise)	30 days	30 days	n/a (enterprise)	30 days
Protection										
Real-Time protection	●	●	●	●	●	●	●	●	●	●
Prevents access to malicious and phishing web sites		●	●	●	●			●		●
On-demand scanner (can be run by the user from the client)	●	●	●	●	●		●	●		●
Quarantine	●	●	●	●	●	●	●	●	●	●
Detects also Mac PUA (>75%)	●	●	●	●	●	●	●	●	●	●
Detects also Windows threats on Mac systems (>75%)	●	●	●	●	●	●	●	●	●	●
Whitelisting for specific files/folders	●	●	●		●	●	●	●	●	●
Firewall / Network attack protection / Home network security		●	●	●			●	●		
Webcam protection								●		●
Folder Shield / Safe Files					●					●
Device Control	●									●
Additional features (we limited this to max. 2 relevant features)				USB Scanner, Ads & Tracking Blocker	VPN, Time Machine Protection	Enterprise investigative features		Private browsing, Secured browser for online banking	Enterprise investigative features	Parental Control
Support										
Online Help and/or User Forum	●	●	●	●	●	●	●	●	●	●
Email and/or Phone Support				●	●	●	●	●	●	●
User manual (PDF)					●	●	●	●	●	●
Online Chat					●		●	●	●	●
Supported languages (of support)	English	English, German, Spanish, French, Italian, Portuguese, Russian, Czech	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, French, Japanese	English, Arabic, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English, Japanese, French, Italian, Spanish, Portuguese, Arabic, Turkish, Hebrew	English, German, French, Spanish, Chinese
List Price (without discount etc.)										
List Price 1 Mac / 1 year USD/EUR	n/a (enterprise)	FREE	FREE	USD 45 / 35 EUR	USD 40 / 40 EUR	n/a (enterprise)	USD 50 / 50 EUR	USD 40 / 40 EUR	n/a (enterprise)	USD 40 / 50 EUR
Auto-renew (not available; opt in; opt out; obligatory)	n/a	n/a	n/a	Obligatory / Obligatory	Obligatory / Opt-out	n/a	Obligatory / Obligatory	Obligatory / Opt-out	n/a	Obligatory / Opt-out

Copyright and Disclaimer

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

AV-Comparatives
(June 2022)