

Independent Tests of Anti-Virus Software



Mac Security Test & Review

TEST PERIOD: MAY 2023

LAST REVISION: 15TH JUNE 2023

WWW.AV-COMPARATIVES.ORG

Content

MACS AND SECURITY SOFTWARE	3
SECURITY SOFTWARE FOR MACOS VENTURA	5
MALWARE PROTECTION TEST	6
RESULTS	7
SUMMARY	8
AV-COMPARATIVES' MAC CERTIFICATION REQUIREMENTS	9
REVIEW FORMAT	10
AVAST SECURITY FREE FOR MAC	11
AVG ANTIVIRUS FREE FOR MAC	14
AVIRA PRIME FOR MAC	17
BITDEFENDER ANTIVIRUS FOR MAC	19
CROWDSTRIKE FALCON PRO FOR MAC	22
INTEGO MAC INTERNET SECURITY X9	25
KASPERSKY PLUS FOR MAC	28
TRELLIX ENDPOINT SECURITY (HX) FOR MAC	30
TREND MICRO ANTIVIRUS FOR MAC	34
APPENDIX – FEATURE LIST	37
COPYRIGHT AND DISCLAIMER	38

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 getting into the wild¹. Moreover, Apple Mac security needs to be considered in the wider context of other types of attacks².

Apple ships some anti-malware capabilities within macOS: *Gatekeeper*, which warns when apps without a digital signature (i.e., not certified by Apple) are run, and *XProtect Remediator*, which checks files against known-malware signatures and remediates infections if malware makes its way onto the Mac. 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.

macOS includes other features which secure and harden the system. For example, *Sandboxing* isolates apps from critical system components, user data, and other apps. Sandboxed apps (e.g., downloaded from the Apple App Store) run in an isolated context where they cannot access areas outside of it and thus cause damage. This does not protect you from malware but limits what it can do.

Since macOS 10.15 (Catalina), apps require *explicit permission* to access user files and other sensitive information (e.g., camera, microphone, logs). Additionally, macOS system files and user data are stored on *separate disk volumes* which makes it more challenging for malware to cause problems with the system.

The effectiveness of Apple's built-in anti-malware features have been questioned³, however, and some security experts recommend strengthening the defences by adding in a third-party antivirus solution. 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 AV programs designed for macOS can also detect malware aimed at other operating systems (e.g., Windows, Android). In a scenario, where malware is inadvertently passed on from one operating system (e.g., Windows) to another (e.g., macOS) using a USB stick, even if the latter machine is not at risk, you might well benefit from effectively handling such threats.

Additional browser extensions and network monitoring functions can identify potential phishing websites. Readers should note that Mac users are just as vulnerable to phishing attacks as e.g., Windows users, as phishing sites deceive the user rather than alter the operating system.

Other programs 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 the integrity of the connection is uncertain. You might also opt to utilize third-party tools for parental control instead of relying solely on macOS' built-in features, if you believe this is more appropriate to your family needs.

¹ <https://www.macworld.com/article/672879/list-of-mac-viruses-malware-and-security-flaws.html>

² <https://blog.cyble.com/2023/04/26/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/>

³ <https://www.macworld.com/article/670537/do-macs-need-antivirus.html>

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.

In general, there are only a limited number of anti-malware products for macOS available on the market. As already mentioned above, the reason being that the threat landscape of macOS is very tiny compared to that of Windows and, therefore, Windows users are more likely to be attacked than Mac users.

Through our yearly Mac testing, we have found that the vendors being evaluated demonstrate a commendable commitment to threat research and continuous product improvement. Their efforts are focused on providing effective security solutions that safeguard Mac users against the ever-changing and potentially rapidly evolving Mac threat landscape. We strongly encourage other security vendors to actively participate in third-party tests to ensure their products meet the current standards and expectations.

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:

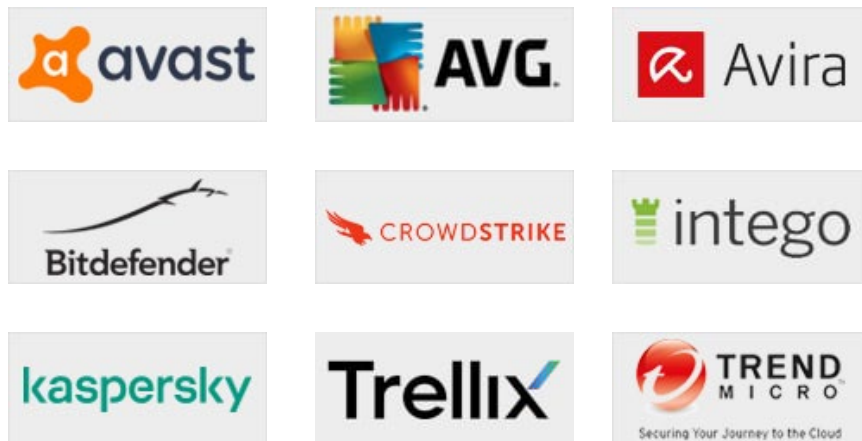
1. Do not use an administrator account for day-to-day computing
2. Use secure passwords (iCloud Keychain) or passkeys (biometric identification such as Touch/Face ID) and enforce multi-factor authentication wherever possible
3. Deactivate any services such as Airport, Bluetooth, or IPv6 that you don't use
4. Be careful about which programs you install and where you download them from
5. Pay attention when granting programs permissions to sensitive system areas or information
6. Be wary of opening any links that you receive via e.g., email
7. Keep your macOS and third-party software up to date with the latest patches

Security Software for macOS Ventura

We have reviewed and tested the following products⁴ for this report, using the newest version⁵ available at time of testing (May 2023):

- **Avast Security Free for Mac 15.6**
<https://www.avast.com/free-mac-security>
- **AVG AntiVirus Free for Mac 20.4**
<https://www.avg.com/en-us/avg-antivirus-for-mac>
- **Avira Prime for Mac 1.15**
<https://www.avira.com/en/prime>
- **Bitdefender Antivirus for Mac 9.3**
<http://www.bitdefender.com/solutions/antivirus-for-mac.html>
- **CrowdStrike Falcon Pro for Mac 6.54**
<https://www.crowdstrike.com/products/bundles/falcon-pro/>
- **Intego Mac Internet Security X9 10.9**
<https://www.intego.com/antivirus-mac-internet-security>
- **Kaspersky Plus for Mac 23.0**
<https://www.kaspersky.com/mac-security>
- **Trellix Endpoint Security (HX) for Mac 35.31**
<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: **Trellix** uses 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 Ventura system against malicious apps. The test took place in May 2023, and used macOS malware that had appeared in the preceding few months. We used a total of 309 recent and representative malicious Mac samples.

In the first half of 2023, 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 really new variants, of true Mac malware seen in 2023. Some of these will only run on certain macOS versions. After careful consideration, we ended up with 309 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.

To prepare for the test, the macOS systems were updated and imaged, with no further OS updates applied afterward. Each security product was installed on a fresh image of the machine, and its definitions were updated to May 16, 2023. Throughout the test, the Mac systems remained connected to the Internet, enabling the use of cloud services. To begin, a USB flash drive containing the malware samples was inserted into the test computer. Some antivirus programs recognized some of the samples at this stage. We then performed a scan of the flash drive, either from the context menu or the main program window, and any detected samples were removed. Samples that were not detected by the real-time protection or scan were copied to the Mac's system disk and executed, providing the security product with a final opportunity to detect them. Along with testing for Mac malware samples, we evaluated the products for false positives by testing a set of clean Mac programs, and none of the programs produced any false alarms.

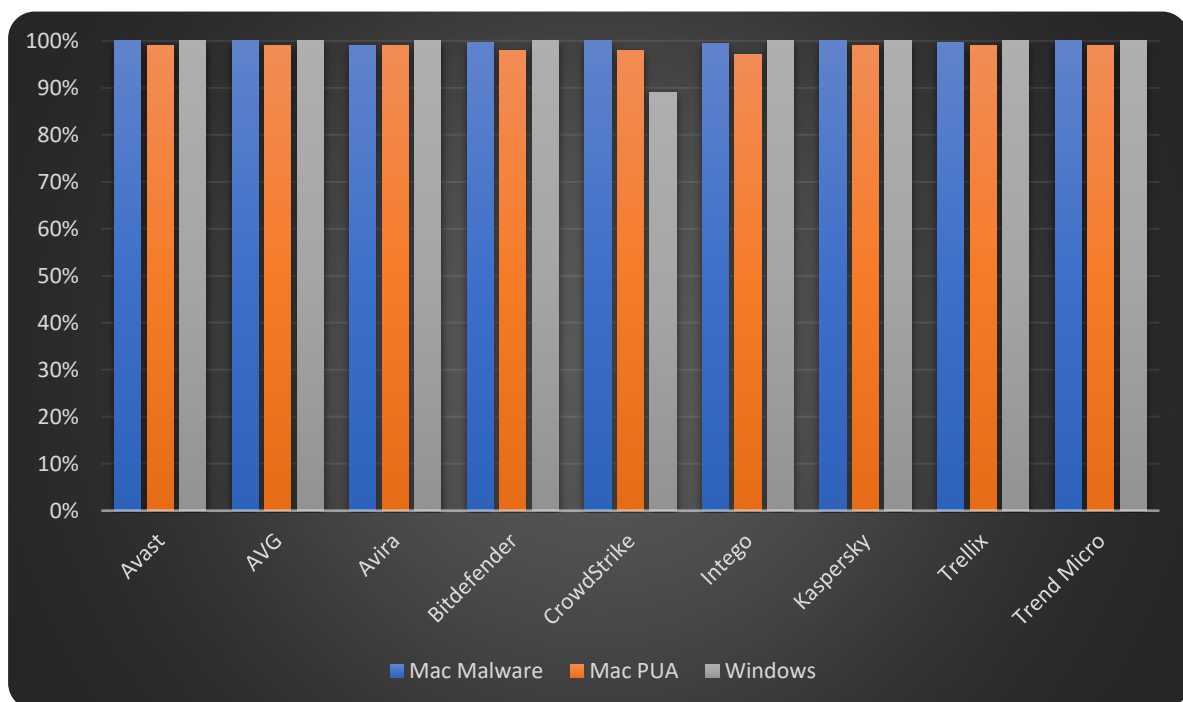
To address the rising number of potentially unwanted applications (PUAs) on Mac systems, we conducted an additional test to evaluate the detection capabilities of the products. Specifically, we assessed the detection of 712 Mac PUAs using the same testing methodology described for malware detection.

Many Mac security products assert that they can identify both Mac and Windows malware to prevent the user's computer from transmitting harmful programs to Windows PCs. To test this claim, we evaluated if the Mac antivirus products can detect prevalent and current Windows malware samples. We used 500 samples and followed the same procedure used for Mac malware detection, excluding any undetected samples since Windows programs cannot be executed under macOS.

Results

The table below shows the protection results⁶ of the tested products.

Product	Mac Malware Protection	Mac PUA Protection	Windows Malware Detection on macOS ⁷
	309 recent Mac Malware samples	712 prevalent Mac PUA samples	500 prevalent Windows malware samples
Avast Free Security for Mac	100%	99%	100%
AVG AntiVirus Free for Mac	100%	99%	100%
Avira Prime for Mac	99.0%	99%	100%
Bitdefender Antivirus for Mac	99.7%	98%	100%
CrowdStrike Falcon Pro for Mac	100%	98%	89%
Intego Mac Internet Security X9	99.4%	97%	100%
Kaspersky Plus for Mac	100%	99%	100%
Trellix Endpoint Security (HX) for Mac	99.7%	99%	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.

Summary

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

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.



Avast Security Free for Mac is a free, fully-featured, and user-friendly antivirus program. It provides clear and persistent alerts when malware is detected.

AVG AntiVirus Free for Mac is a free antivirus program with a full range of anti-malware features. Its tiled user interface enables simple navigation, and malware detection alerts are clear and persistent.

Avira Prime for Mac is a paid-for antivirus product that offers essential anti-malware features. Its simple and user-friendly interface ensures effortless navigation, and malware detection alerts are clearly displayed.

Bitdefender Antivirus for Mac is a paid-for antivirus product that includes a data-limited VPN and ransomware protection in addition to anti-malware features. The interface is simple and well designed.

CrowdStrike Falcon Pro for Mac is designed for large enterprise networks as part of an endpoint protection package. It has a command-line interface on the client machine and is managed using a web-based console.

Intego Mac Internet Security X9 is a paid-for security suite that combines malware protection with a firewall. The minimalistic user interface provides access to all functions, and malware detection alerts are clear and persistent.

Kaspersky Plus for Mac is a comprehensive paid-for security suite with a well-organized and neat user interface, offering a wide range of anti-malware features. Malware detection alerts are clearly displayed.

Trellix Endpoint Security (HX) for Mac is part of an endpoint protection package for large enterprise networks. The client machine does not have a GUI and management is performed via a web-based console.

Trend Micro Antivirus for Mac is a paid-for security suite with camera and microphone protection, as well as an anti-ransomware feature. All features are easily accessible from a well-designed user interface, and malware detection alerts are clear and persistent.

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 rates⁸ (under 85% for Mac PUA⁹) 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.

⁸ For consumer products, the PUA detection threshold must be reached using default settings.

⁹ What is "potentially unwanted" might be debatable, and some 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 structure of the following product reviews for each of the consumer programs in this test. For the enterprise products we have used a slightly different review format which includes a brief product summary and sections about the cloud-based management console (e.g., dashboard, host management, detections, policies, investigation) as well as the endpoint protection client (e.g., deployment, general handling, alerts).

Summary: We briefly describe the nature of the product and list a number of selected key aspects, including whether it is free or paid, important security features, and 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, Setup & Deinstallation: We describe how to get the product up and running on your Mac, starting with downloading the installer, and finishing with any post-setup tasks needed. These might include installing and enabling 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 Ventura (which was used for the tests and reviews), it is necessary to go into the System Settings 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.

General Handling & Essential Features: We consider how easy it is to find the most important functionality: protection status, different scan options, protection features, quarantine, subscription information (not applicable to free programs), update, settings, and help.

Protection: We describe the available scan options, including smart/full/custom scan, external storage scan, and scheduled scans, how and where to trigger them, and briefly mention any special detection settings that are enabled by default, e.g., detection of PUA or stalkerware. We might also give additional information about third-party detection engines and other, relevant malware protection features (e.g., browser/email/ransomware protection).

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

Quarantine & Logs: We check the functionality that shows you which malicious items have been found, what information is provided about them, and what the actions are for dealing with them (e.g., delete, restore). If available from the program interface, we will also note the types of events being logged by the program.

Advanced Options: We check whether only users with a macOS Administrator account can disable the protection features, uninstall the program, or restore/delete items from quarantine. We regard it as ideal if only administrators (not standard macOS users) can perform at least the first two tasks.

Avast Security Free for Mac



Summary

Avast Security Free for Mac is a free antivirus program and well suited to non-expert users. Some of its key aspects are:

- easy and straightforward installation and setup of core features
- most common features displayed in a clean and well-laid-out GUI
- different scan options and comprehensive settings, including scheduled scans
- clear and persistent alerts
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

To set up Avast Security on your Mac, you just download and run the installer file from the vendor's website. The initial setup is straightforward as the program guides you through step by step and provides brief explanations. You can uninstall the program by clicking *Avast Security* > *Uninstall Avast Security* in the macOS menu bar or opening the *Avast Security Uninstaller* directly from the macOS Applications folder.

General Handling & Essential Features

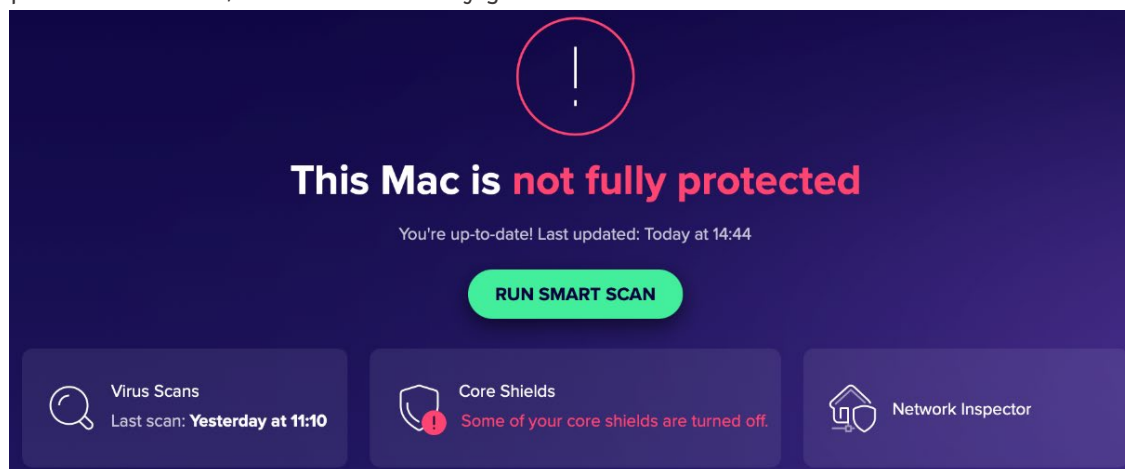
Protection status, smart scan, scan options (*Virus Scans*), **protection features** (*Core Shields*), and **quarantine** are all found on the home page of the main program window. **Settings** (*Preferences*) can be opened from the program menu in the top right-hand corner or the macOS menu bar. **Subscription information** is not applicable, as the program is free. A manual **update** can be triggered by clicking *Check for Updates* from the system tray icon or *Avast Security* in the macOS menu bar. The online **help** is accessible from the *Help* menu in the program menu which opens the support page in the default browser.

Protection

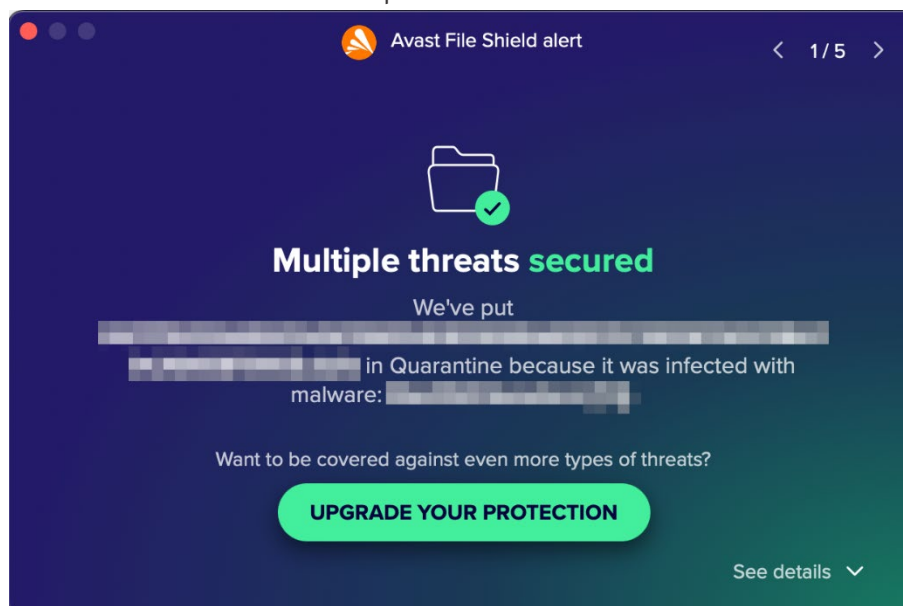
From *Virus Scans* on the home page, you can start a **smart scan**, **deep scan** of all drives and the system memory, **external storage scan** of connected storage devices, or **targeted scan** of specific files or folders. The latter can also be run from e.g., the Finder context menu. **Scheduled scans** can be configured as well. The detection behaviour and settings of the different scan types can be changed from *Preferences*. The detection of PUA is enabled by default. The *Email Guardian* scans emails of provided mail accounts and flags any that seem suspicious. In the free version, only mail apps installed on the Mac are supported (e.g., Apple Mail, Outlook).

Alerts

When we disabled Avast's real-time protection (*File Shield*) or web protection (*Web Shield*) under *Core Shields* on the home page, an alert was shown in the main program window. To reactivate either protection feature, we had to manually go into *Core Shields* and turn it back on.

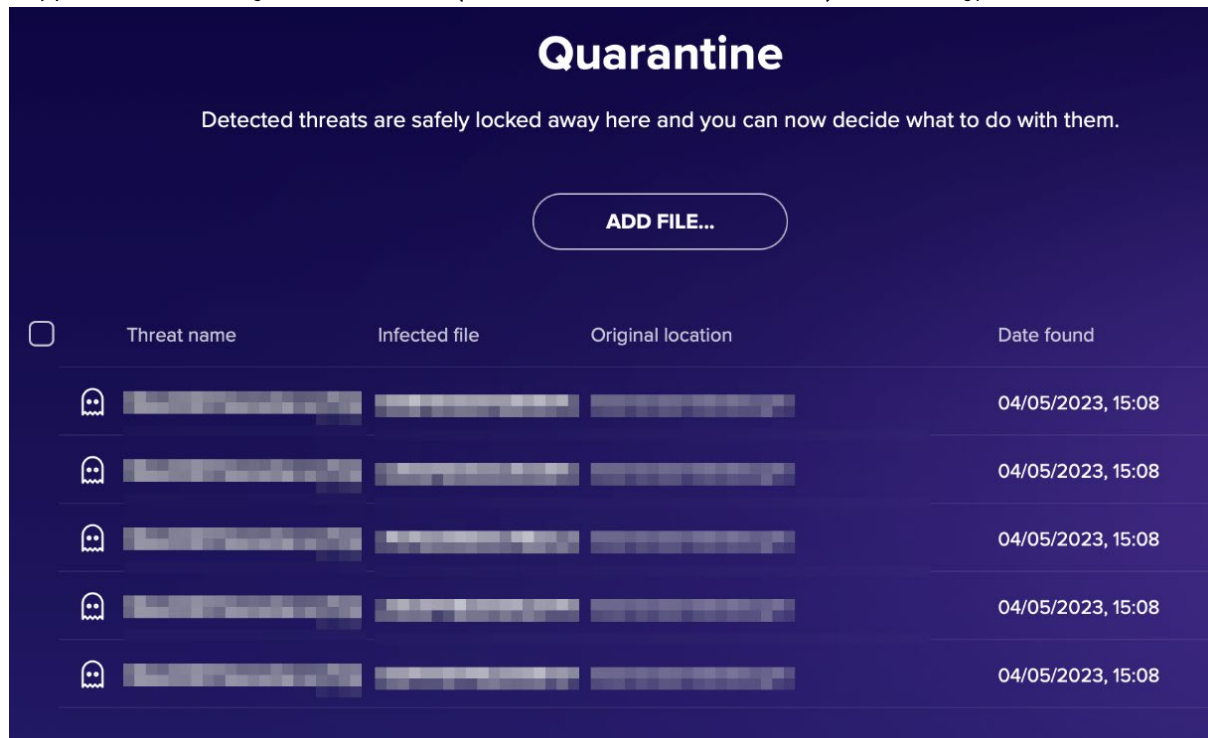


When malware was detected in our protection test, the program displayed the alert shown below. No user action was required, and the alert persisted until we closed it using the macOS close button in the top left-hand corner. We noted that multiple detections are combined into one single alert which you can browse through using the arrows in the top right-hand corner. Further details about the threat, such as the threat name, severity, file name/path, and process, are shown if the details section at the bottom of the alert is expanded.



Quarantine & Logs

The quarantine is directly accessible from the home page of the main program window and lists files that have been quarantined, along with the threat name, file name, file path, and date when this happened. It allows you to delete or (with an administrator account) restore any/all items.



Advanced Options

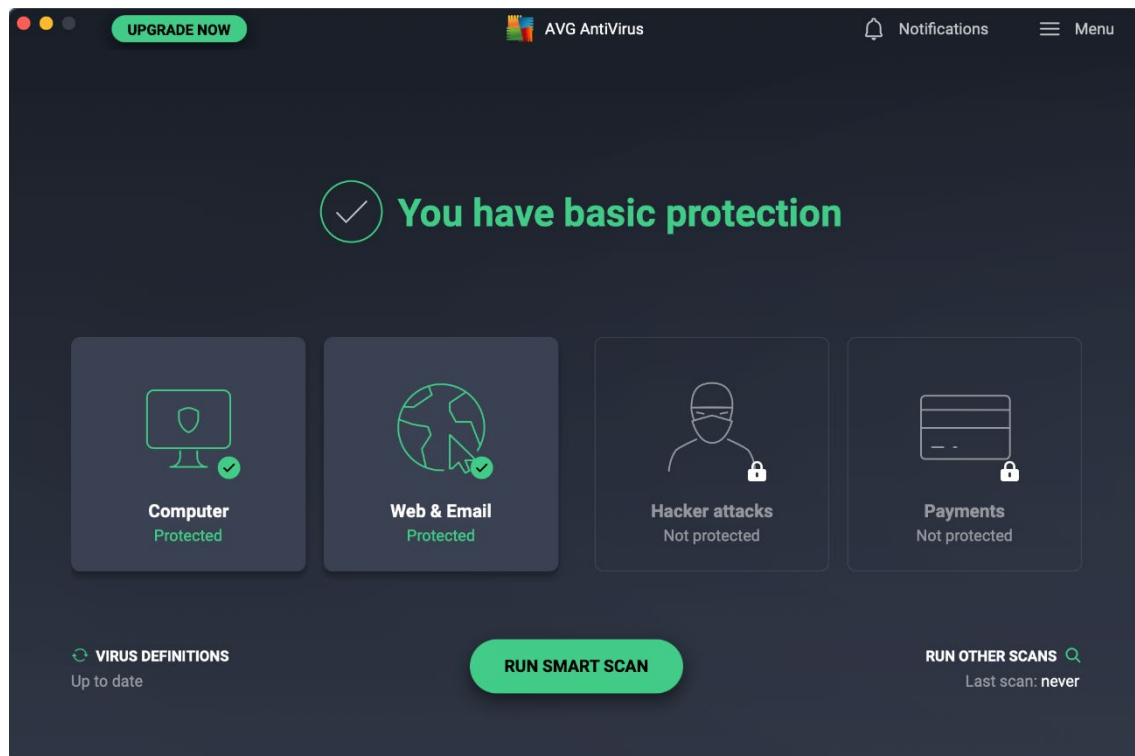
Only users with a macOS Administrator account can perform the following tasks (caution is advised):

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

Advertising

The *Smart Scan* feature promotes Avast's paid-for security suites, *Premium* and *Ultimate*. 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. After dismissing the prompt, a second prompt appears offering a 60-day trial for Avast Ultimate. Clicking the *Go Premium* button on pages of other program features or the *Upgrade your protection* button of a detection alert leads to the same behaviour.

AVG AntiVirus Free for Mac



Summary

AVG AntiVirus Free for Mac is a free antivirus program and well suited to non-expert users. Some of its key aspects are:

- easy and straightforward installation and guided setup of core features
- most common features displayed in a clean and well-laid-out GUI
- different scan options and comprehensive settings, including scheduled scans
- clear and persistent alerts
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

To set up AVG AntiVirus on your Mac, you just download and run the installer file from the vendor's website. The initial setup is straightforward as the program guides you through step by step and provides brief explanations. You can uninstall the program by clicking *AVG AntiVirus > Uninstall AVG AntiVirus* in the macOS menu bar or opening the *AVG AntiVirus Uninstaller* directly from the macOS Applications folder.

General Handling & Essential Features

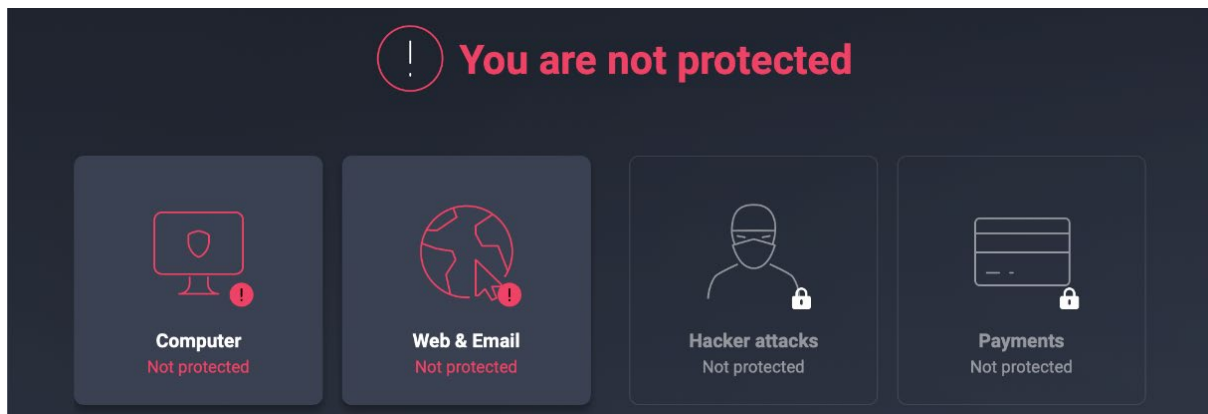
Protection status, smart scan, scan options (*Run Other Scans*), and **protection features** (*Computer, Web & Email*) are all found on the home page of the main program window. The **quarantine** is accessible from the *Computer* tile on the home page. **Settings** (*Preferences*) can be opened from the program menu in the top right-hand corner or the macOS menu bar. **Subscription information** is not applicable, as the program is free. A manual **update** can be triggered by clicking *Virus Definitions* on the home page, or clicking *Check for Updates* from the system tray icon or *Avast Security* in the macOS menu bar. The online **help** is accessible from the *Help* menu in the program menu which opens the support page in the default browser.

Protection

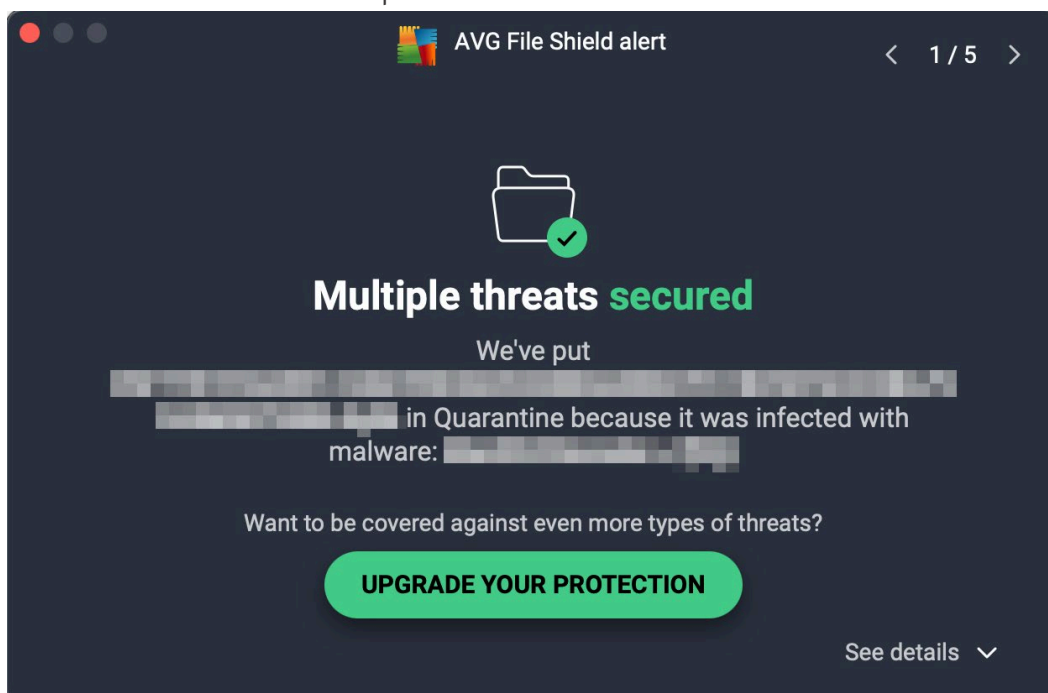
From *Run Other Scans* on the home page, you can start a **smart scan**, **deep scan** of all drives and the system memory, **external storage scan** of connected storage devices, or **targeted scan** of specific files or folders. The latter can also be run from e.g., the Finder context menu. **Scheduled scans** can be configured as well. The detection behaviour and settings of the different scan types can be changed from *Preferences*. The detection of PUA is enabled by default.

Alerts

When we disabled AVG's real-time protection (*File Shield*) under *Computer*, web protection (*Web Shield*) or email protection (*Email Shield*) under *Web & Email* on the home page, an alert was shown in the main program window. To reactivate either protection feature, we had to manually go into the mentioned menu tiles and turn it back on.

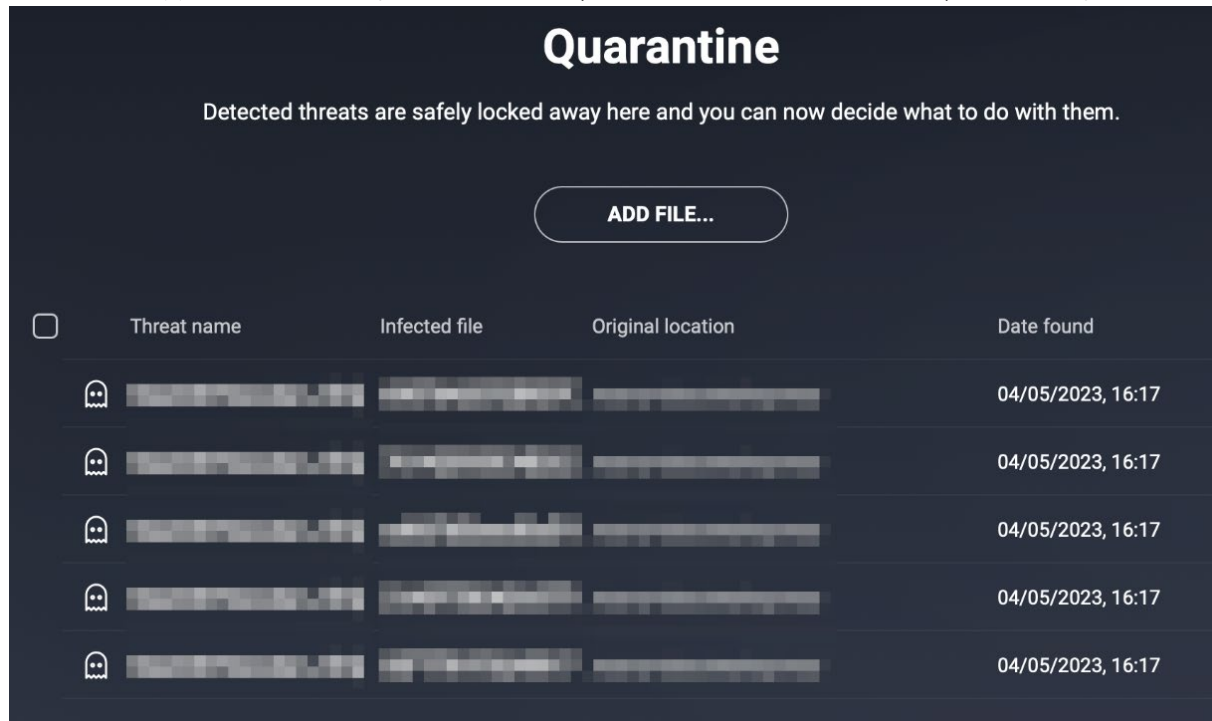


When malware was detected in our protection test, the program displayed the alert shown below. No user action was required, and the alert persisted until we closed it using the macOS close button in the top left-hand corner. We noted that multiple detections are combined into one single alert which you can browse through using the arrows in the top right-hand corner. Further details about the threat, such as the threat name, severity, file name/path, and process, are shown if the details section at the bottom of the alert is expanded.



Quarantine & Logs

The quarantine is quickly accessible from *Computer* on the home page of the main program window and lists files that have been quarantined, along with the threat name, file name, file path, and date when this happened. It allows you to delete or (with an administrator account) restore any/all items.



Advanced Options

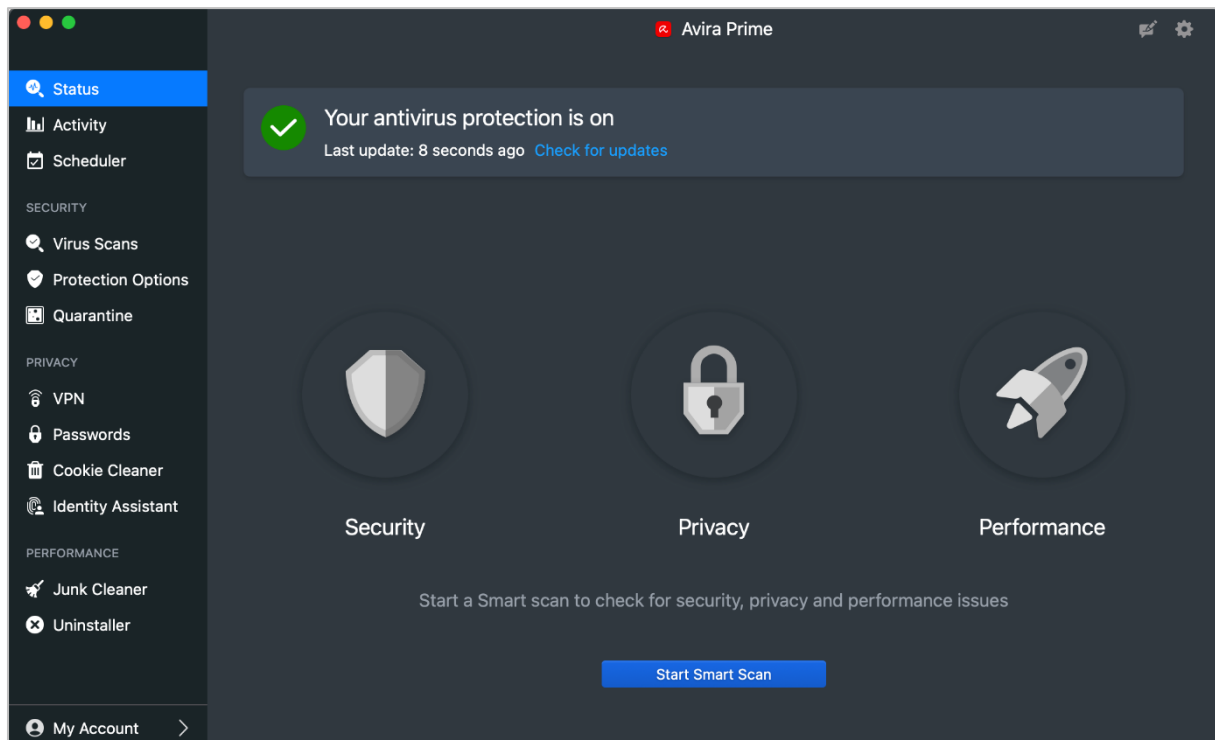
Only users with a macOS Administrator account can perform the following tasks (caution is advised):

- Disable protection features (under *Computer* and *Web & Emails*)
- Uninstall the program
- Restore items from the quarantine

Advertising

The *Smart Scan* feature promotes AVG's paid-for 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. After dismissing the prompt, a second prompt appears offering a 60-day trial for it. Clicking the *Go Premium* button on pages of other program features or the *Upgrade Your Protection* button of a detection alert leads to the same behaviour.

Avira Prime for Mac



Summary

Avira Prime for Mac is a paid-for antivirus program and an excellent choice for non-expert users. Some of its key aspects are:

- simple and straightforward installation and guided setup of core features
- all available features displayed in a well-organized and neat interface
- different scan options and many settings, including scheduled scans and automatic USB scan
- clear alerts
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

To set up Avira Prime for Mac, you need to log in to your Avira account, download and run the installer. The initial setup is straightforward as the program guides you through step by step and provides brief explanations. When the program window opens for the first time, you are prompted to run a Smart Scan. The program can be uninstalled by deleting it from the macOS Applications folder. The program's window has both dark and light modes, which co-ordinate with the dark- and light-mode settings of macOS.

General Handling & Essential Features

Protection status, smart scan, scan options (*Virus Scans*), **protection features** (*Protection Options*), **quarantine**, and **subscription information** (*My Account*) can all be accessed from the main program window. **Settings** can be accessed from the cogwheel icon in the top right-hand corner of the window or the macOS menu bar. A manual **update** can be triggered by clicking *Check for updates* on the main program window. The online **help** is found in the *Help* menu in the macOS menu bar which opens the support page in the default browser.

Protection

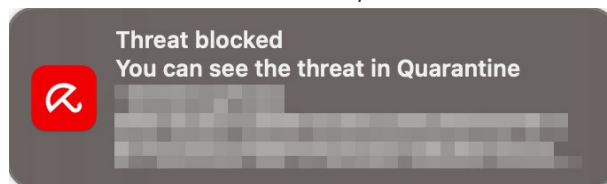
From *Virus Scans*, you can start a **quick scan** of the most vulnerable device areas, **full scan** of the entire file system, or **custom scan** of selected files or folders. The latter can also be run from e.g., the Finder context menu. The *Scheduler* lets you define individual schedules of all the available scan options to run them regularly. The **automatic scan of USB devices** can be activated or deactivated from the *Protection Options*. From *Settings*, the detection behaviour and different scan settings can be changed.

Alerts

When we disabled Avira's real-time protection or download protection under *Protection Options*, the alert below was shown in the main program window. The real-time protection can also be turned off via the system tray icon in the macOS menu bar. We were able to easily reactivate the protection by clicking *Turn on*.



When malware was detected in our protection test, the program displayed an alert in the form of a system notification shown below, including the file path where the threat was found and the action taken. No user action was required, and the alert closed automatically after a few seconds.



Quarantine & Logs

The *Quarantine* page of the program (screenshot below) shows you all the items that have been quarantined, along with the threat name, file name, file path, and 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).

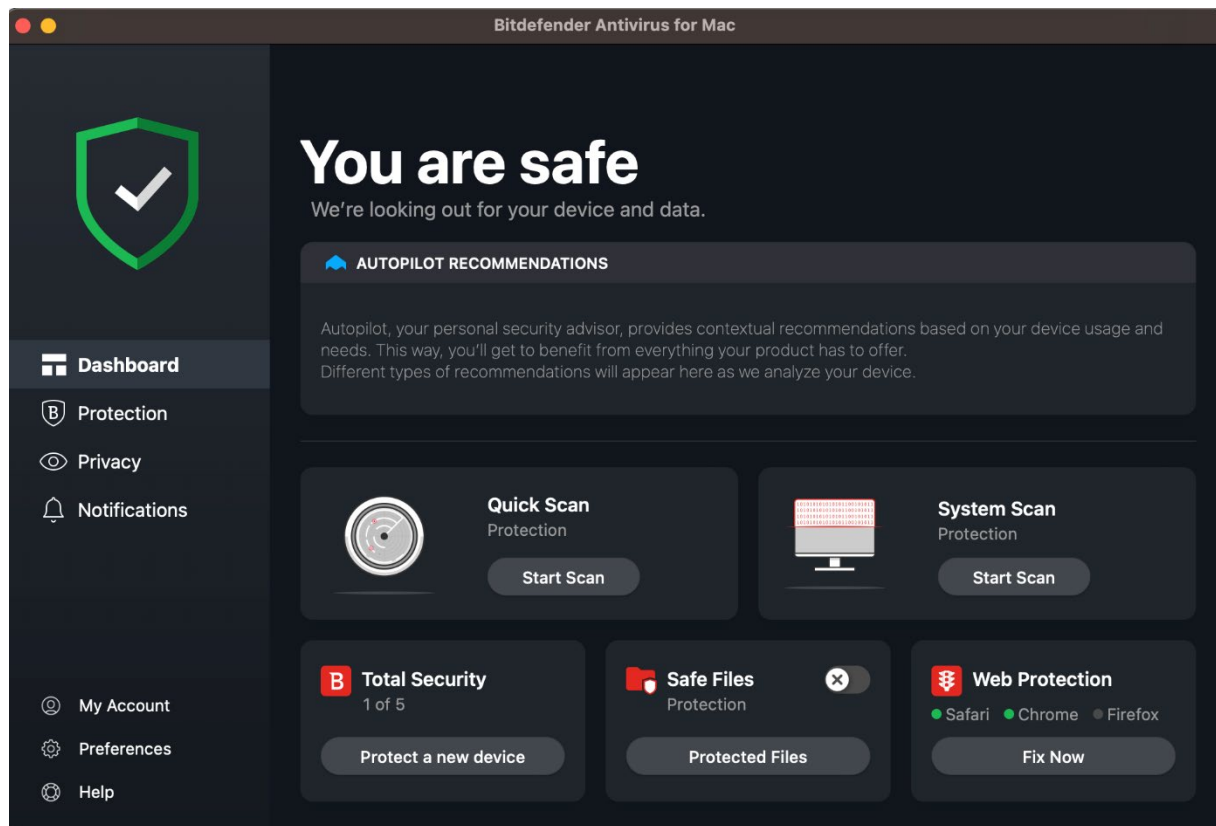
Threat Name	File	Path	Date
[blurred]	[blurred] ⓘ	[blurred]	Today
[blurred]	[blurred] ⓘ	[blurred]	Today
[blurred]	[blurred] ⓘ	[blurred]	Today
[blurred]	[blurred] ⓘ	[blurred]	Today
[blurred]	[blurred] ⓘ	[blurred]	Today

Advanced options

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

- Disable protection features (under *Protection Options* or system tray icon)
- Uninstall the program
- Delete and restore items from quarantine

Bitdefender Antivirus for Mac



Summary

Bitdefender Antivirus for Mac is a paid-for antivirus program which both expert and non-expert users should find suitable for their needs. Some of its key aspects are:

- simple and straightforward installation and guided setup of core features
- all available features displayed in a very well-designed interface
- different scan options, ransomware protection, data-limited VPN, browsing-protection add-ins
- clear in-program alerts but none shown in case of a malware detection
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

After downloading and running the installer from the vendor's website, the setup wizard guides you through each installation and configuration step. When setup is complete, you need to create a Bitdefender account and sign in. An optional introductory tour then starts, after which the program window displays several recommendations, such as installing the browser extension for Safari/Chrome/Firefox (*Traffic Light*), configuring the ransomware protection feature (*Safe Files*), setting up *Time Machine Protection*, and running a system scan. The program can be uninstalled by opening the *Bitdefender Uninstaller*, which is found inside the Bitdefender folder of the macOS Applications folder. The program's window has both dark and light modes, which co-ordinate with the dark- and light-mode settings of macOS.

General Handling & Essential Features

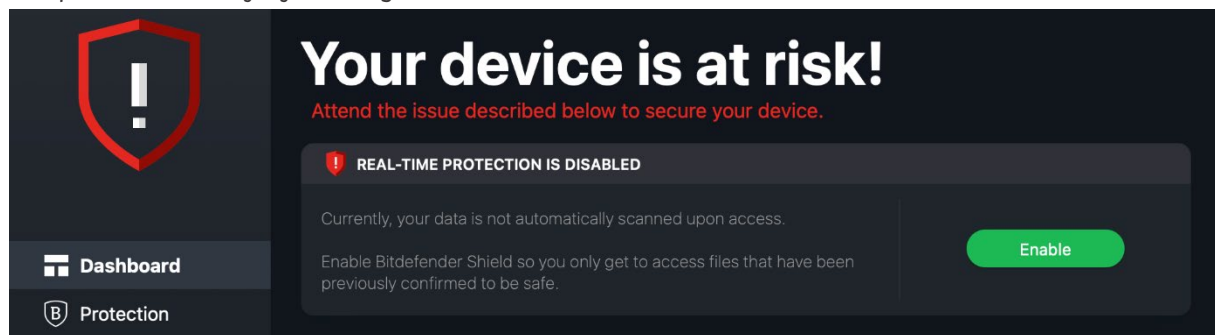
Protection status, **scan options** (quick and system scan), **protection features**, **settings** (*Preferences*), **subscription information** (*My Account*), and **help** are all directly accessible from the program's *Dashboard*. The **quarantine** and list of **scan exceptions** can be found under *Protection*. A manual **update** can be triggered from the *Actions* menu in the macOS menu bar. The data-limited *Bitdefender VPN* as well as additional *Anti-tracker* browser extensions are available under *Privacy*. From *Help*, you can open a very comprehensive manual in PDF format or the support page in the default browser.

Protection

From *Protection*, you can start a **quick scan** of critical areas, **system scan** of all files and directories, or **custom scan** of specific files or folders. The latter can also be run from e.g., the Finder context menu. Settings for the ransomware protection are available as well. The program's protection and detection behaviour can be changed from *Preferences*. If you install the *Traffic Light* browser extension, safety ratings (indicated by coloured symbols) are added to Google search results.

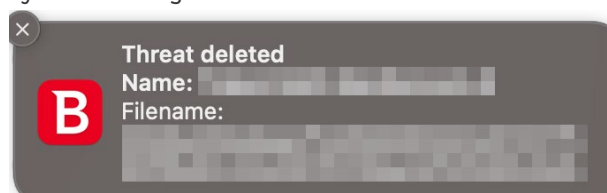
Alerts

When we disabled Bitdefender's real-time protection via *Preferences* or the system tray icon in the macOS menu bar, the alert below was shown in the main program window. We were able to reactivate the protection easily by clicking *Enable*.



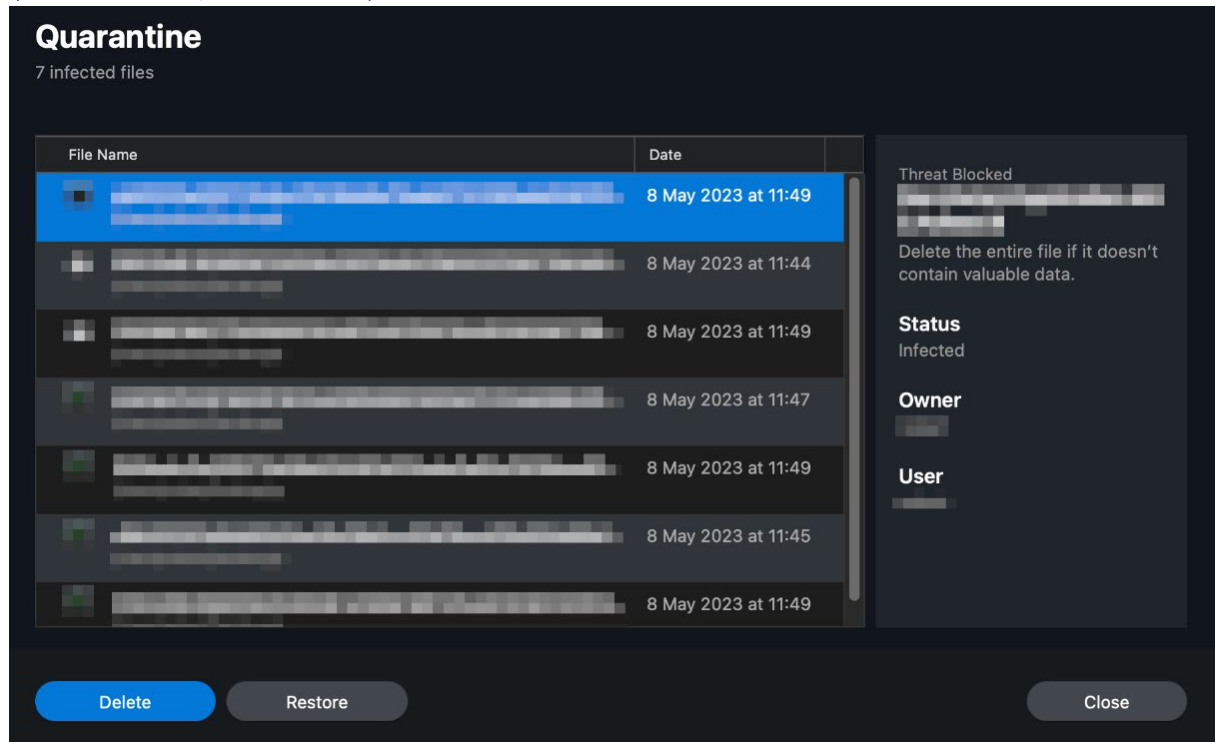
When malware was detected in our protection test, the program silently took action on the threat (e.g., immediately deleted it) as the system tray icon briefly changed upon detection. After manually opening the main program window, the detections appeared on the *Notifications* page. Apart from that, no clear detection alerts were shown.

When verifying the *Notifications* permission in the macOS system settings, we noticed that the notifications were allowed for *Bitdefender Antivirus for Mac* but the option was set to *None* by default. After changing it to *Banners* and re-running the protection test, the program displayed an alert in the form of a system notification shown below, including the threat name, file name, and action taken. No user action was required, and the alert closed automatically after a few seconds. However, the program did not give any hint during installation or usage about enabling notifications in the macOS system settings.



Quarantine & Logs

The *Quarantine* page of the program (screenshot below) lets you view all the items that have been quarantined, along with the threat name, file name, and 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). *Notifications* is the log feature which displays events such as updates, component activation, and malware detections. These can be displayed all together, or filtered by importance (*Critical, Warning, Information*).

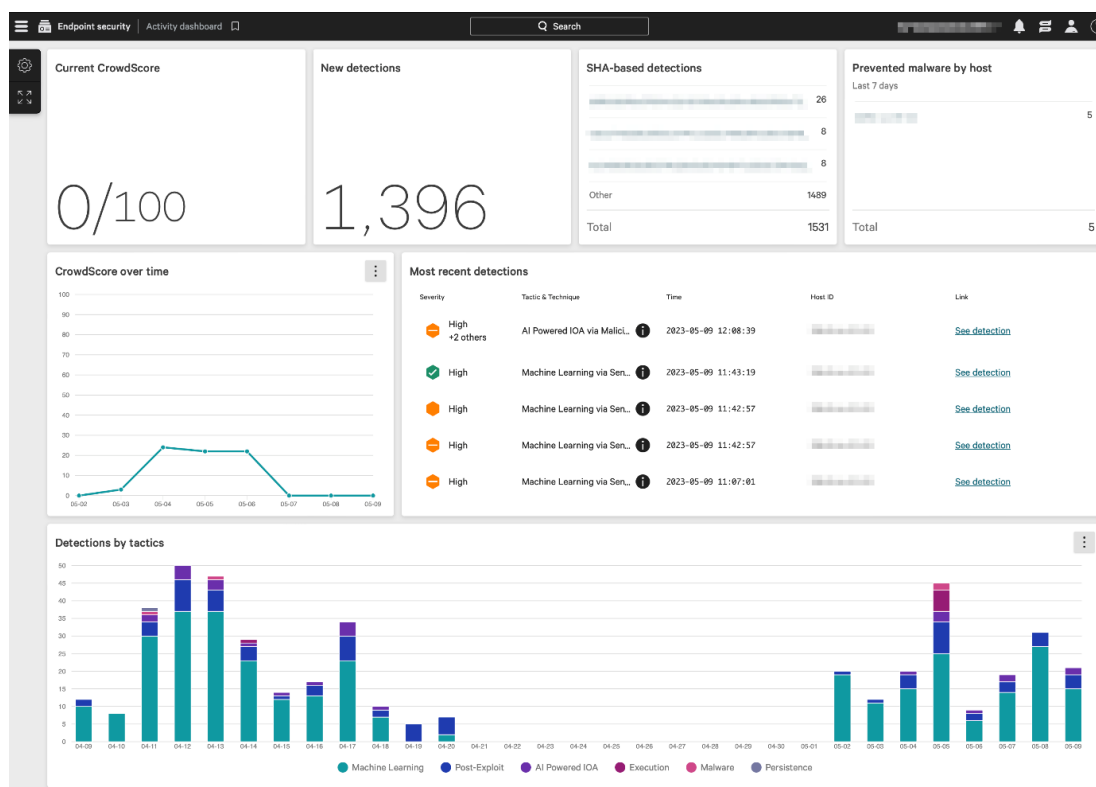


Advanced Options

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

- Disable protection features (under *Preferences*)
- Uninstall the program
- Delete and restore items from quarantine

CrowdStrike Falcon Pro for Mac



Summary

CrowdStrike Falcon Pro is a security package suitable for medium- to large-sized enterprise networks and provides a cloud-based console for managing the endpoint protection software. Some of its key aspects are:

- investigative functions for analysing and remediating attacks
- comprehensive search facilities
- well-organized cloud-based console with easy access to details pages
- encyclopaedia of known cybercriminal groups
- clear alerts at endpoint

Management Console

The console is navigated from the menu in the top left-hand corner of the console. This lists different sections, such as *Endpoint security*, *Threat intelligence*, *Investigate*, *Dashboards and reports*, and *Host setup and management*, which group the individual pages. We will describe the most relevant sections and pages below. You can easily bookmark any page (using the bookmark symbol next to the page title at the top of the page), and then go directly to that page using the *Bookmarks* section of the menu.

Endpoint security > Activity dashboard page

This is the page you see when you first log on to the console. It shows various status items in large panels (screenshot above). 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. The *New detections*, *SHA-based detections*, and *Prevented malware by host* panels redirect to the *Endpoint detections* details page with the respective filters applied.

Endpoint security > Endpoint 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 host, and logged-on user. For each detection, you can see full details, including a process tree view (screenshot below), and assign a console user for remediation.

The screenshot displays a process tree on the left and a detailed execution panel on the right. The process tree shows a sequence of processes: LAUNCHD, TERMINAL, LOGIN, ZSH, and PYTHON. The PYTHON process is highlighted with a red stop sign icon, indicating it was blocked. The execution details panel on the right provides the following information:

- Unassigned** (status)
- New** (action)
- Comment** (action)
- Roberts-Mac.local** (hostname)
- Network contain** (action)
- Create ML exclusion** (action)
- Execution Details** (panel title)
- DETECT TIME**: 2023-05-23 10:43:14
- HOSTNAME**: [redacted]
- HOST TYPE**: Workstation
- USER NAME**: robert
- ACTIONS TAKEN**:
 - Process blocked (checked)
 - File quarantined (unchecked)
- SEVERITY**: High
- OBJECTIVE**: Falcon Detection Method
- TACTIC & TECHNIQUE**: Machine Learning via Cloud-based ML
- TECHNIQUE ID**: CST0008
- SPECIFIC TO THIS DETECTION**: This file meets the File Attribute ML algorithm's high-confidence threshold for malware.
- TRIGGERING INDICATOR**: Associated IOC (SHA256 on library/DLL loaded)
- GLOBAL PREVALENCE**: Low
- LOCAL PREVALENCE**: Unique
- IOC MANAGEMENT ACTION**: None
- Associated File**: [redacted]
- GROUPING TAGS**: None
- LOCAL PROCESS ID**: 1606

Endpoint security > Quarantined files page

This page lets you see files that have been quarantined by the endpoint protection client. For each item, you can see the date and time when it was quarantined, file name, device name, number of AV detections, logged-on user, and its status. Quarantined files can be released, deleted, or downloaded in a password-protected archive. Clicking the entry of a quarantined file opens a panel with additional information, such as the file path, file hashes, file size, file type, detection method, and severity. There is a search function and a variety of filters you can apply to find specific files within the quarantine repository.

Endpoint security > Prevention policies page

Here you can create and edit the prevention policies for the supported OS endpoints. You can define the capabilities of the endpoint protection client for different types of attack-, detection-, and protection-related behaviour. In the case of Mac policies, you can configure components such as *Enhanced Visibility*, *Quarantine*, *Execution Blocking*, *Unauthorized Remote Access*, and *Credential Dumping*. Some sensor components, such as *Cloud Machine Learning* and *Sensor Machine Learning*, have separate configurable sensitivity levels for detection and prevention, ranging from *Disabled* to *Extra Aggressive*. Custom Indicators of Attack (IOA) can be created and assigned too. Policies can be assigned to devices automatically by means of a naming system, whereby a policy hierarchy determines which one takes precedence. For example, any device with "Mac" in its name can be automatically put into a specific group of Mac computers, to which one or more policies are assigned.

Host setup and management > Host management page

This page lists all the registered devices/hosts along with the host status, operating system, policy assignments, containment status, sensor version, and first/last seen date. Clicking on an entry opens a panel with additional details, such as device manufacturer, MAC address, IP addresses, and serial number. Like in other details pages, you can apply many different filters and search for specific hosts.

Platform	OS Version	OU	Site	Type	Containment Status	Grouping Tags
Windows	571 Ventura (13)	1 N/A	1 N/A	1 Workstation	1 Normal	1 N/A
Mac	1					

Hostname	Last Seen	First Seen	OS Version	OU	Prevention Policy	Response Policy	Sensor Update P...	Containment ...	Sensor Version	Grouping Tags
	2023-05-09 13:2...	2023-04-26 13:51...	Ventura (13)		Default (Mac)	Default (Mac)	Default (Mac)	Normal	6.54.16702.0	

Threat 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 told us that this information is also available in *Endpoint detections* details when a detection is associated with a specific actor.

Investigate section

The *Investigate* section provides an extremely comprehensive search facility. It lets you *search* for specific aspects (e.g., hosts, hashes, users, IP addresses, domains, events), *hunt* for activities related to detections, files, or executables, view *timelines* of hosts, processes, and users, check *reports* about remote access, network logon, and geo location activities, and look for *custom alerts* and *vulnerabilities* (e.g., HiveNightmare, Log4Shell).

Endpoint Protection Client

Deployment

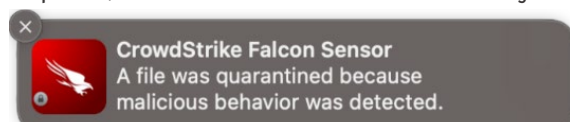
Installer files for the endpoint protection client (*Sensor*) can be downloaded from *Host setup and management > Sensor downloads*. Half a dozen older versions of the sensor are also available. Local installation requires the use of the macOS Terminal – instructions are provided in the documentation (*Support and resources > Documentation*).

General Handling

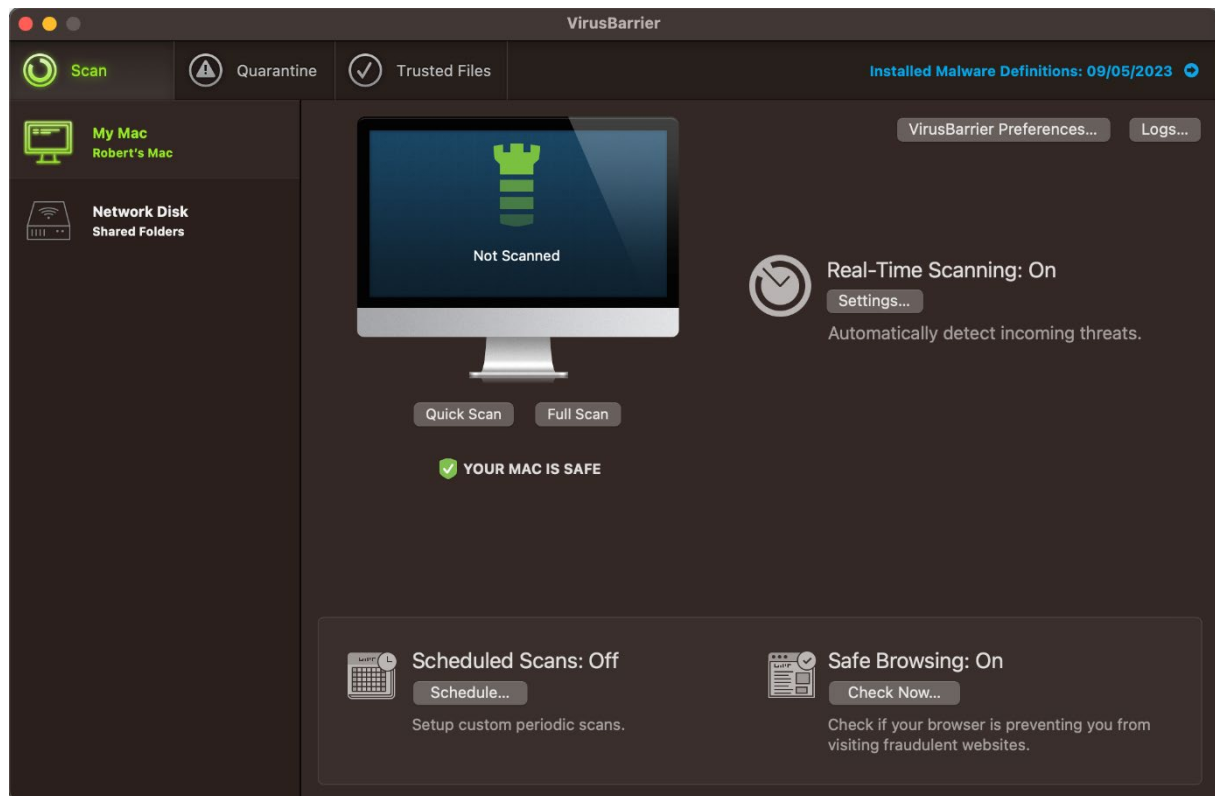
No graphical user interface is provided. Only users with a macOS Administrator account can interact with the sensor using its command-line interface (*falconctl*) via the macOS Terminal. For example, you can output sensor information and statistics (*falconctl stats*), load/unload the sensor (*falconctl load / falconctl unload*), and uninstall the sensor (*falconctl uninstall*). With the settings used for this test, detected files are not deleted but quarantined in situ.

Alerts

When malware was detected in our protection test, the sensor displayed an alert in the form of a system notification shown below, without further details about the threat. No user action was required, and the alert closed automatically after a few seconds.



Intego Mac Internet Security X9



Summary

Intego Mac Internet Security X9 is a paid-for antivirus program and a good choice for non-expert users. In addition to anti-malware features, it also includes a separate firewall application, called *NetBarrier*. In this review though, we have focused on the antivirus application, *VirusBarrier*. Some of its key aspects are:

- simple and straightforward installation and setup of core features
- all available features displayed in a clean GUI
- different scan options, including scheduled scans and scans of mounted volumes
- clear and persistent alerts
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

To set up Mac Internet Security X9, you just need to download and run the installer from the vendor's website. The setup wizard is straightforward however, you have to manually open the program after installation. After that, you will be prompted to activate the product and allow the program *Full Disk Access* in the macOS system settings. The program can be uninstalled by re-running the installer and double-clicking *Uninstall*, or by deleting the Intego folder from the macOS Applications folder. The program's window has both dark and light modes, which co-ordinate with the dark- and light-mode settings of macOS.

General Handling & Essential Features

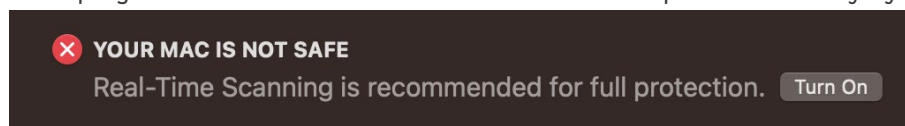
Protection status, **scan options** (quick, full, scheduled scan), **quarantine**, list of **scan exceptions** (*Trusted Files*), and **settings** are all found on the *Scan* page of the main program window. A manual **update** can be triggered by clicking on the *Malware Definitions* link on the *Scan* page, or by selecting *Check for Updates* under the *VirusBarrier* menu or the system tray icon in the macOS menu bar. In all cases, the *NetUpdate* application opens which displays the update status, along with the days after which the protection expires, and related settings. The **subscription information** can be viewed in the About box of the *VirusBarrier* menu. The online **help** is found in the *Help* menu in the macOS menu bar which opens the support page in the default browser. Additionally, a basic help displays an overlay that explains the principal features in the main program window.

Protection

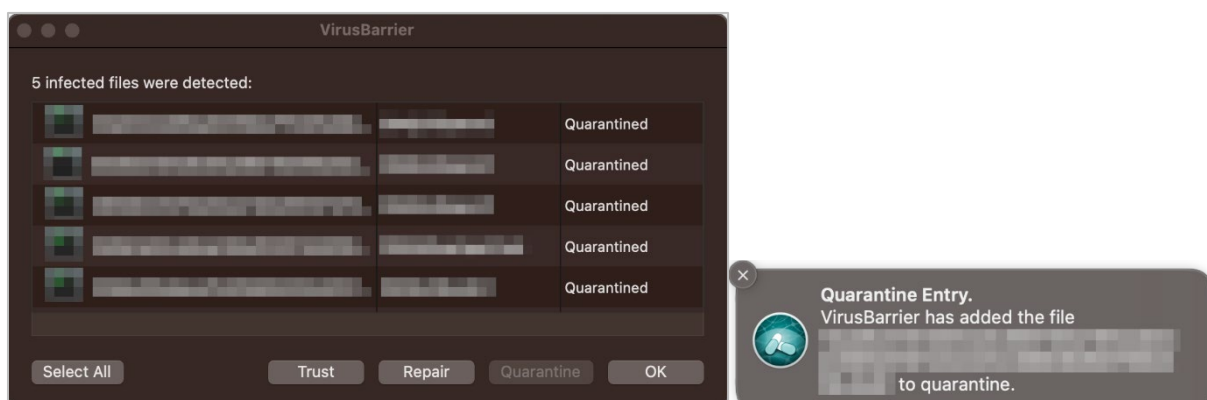
From the *Scan* page of the main program window or the *File* menu in the macOS menu bar, you can start a **quick scan**, **full scan**, or **custom scan** of specific files or folders. The latter can also be run from e.g., the Finder context menu. The **automatic scan of volumes** when they are mounted can be activated in *Settings*. On the *Scan* page, you can also configure **scheduled scans** (*Schedule*) as well as the program's protection and detection behaviour (*VirusBarrier Preferences*). The program checks if the safe browsing feature of supported browsers (Safari, Chrome, Firefox) is enabled and warns you in case it is turned off. *VirusBarrier* uses Intego's own detection engine to detect macOS malware but makes use of the Avira engine to detect Windows malware.

Alerts

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

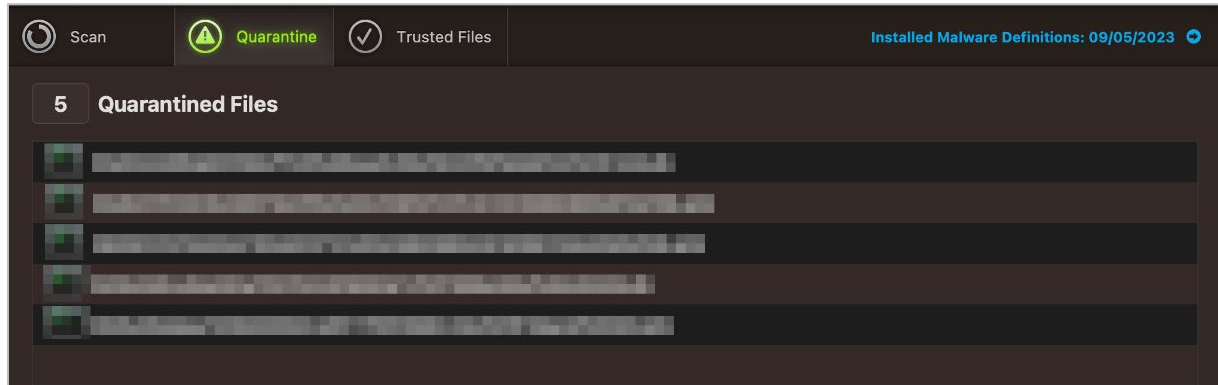


When malware was detected in our protection test, the program showed the dialog and an alert in the form of a system notification, including the file name and action taken, shown below. No user action was required. The dialog persisted until we closed it and the alert closed automatically after a few seconds.



Quarantine & Logs

The *Quarantine* page of the program (screenshot below) shows you all the items that have been quarantined. There are options to delete, repair, or restore (*trust*) a single or all the quarantined files. If you click on an individual item, the path to its location will be shown in the status bar at the bottom.



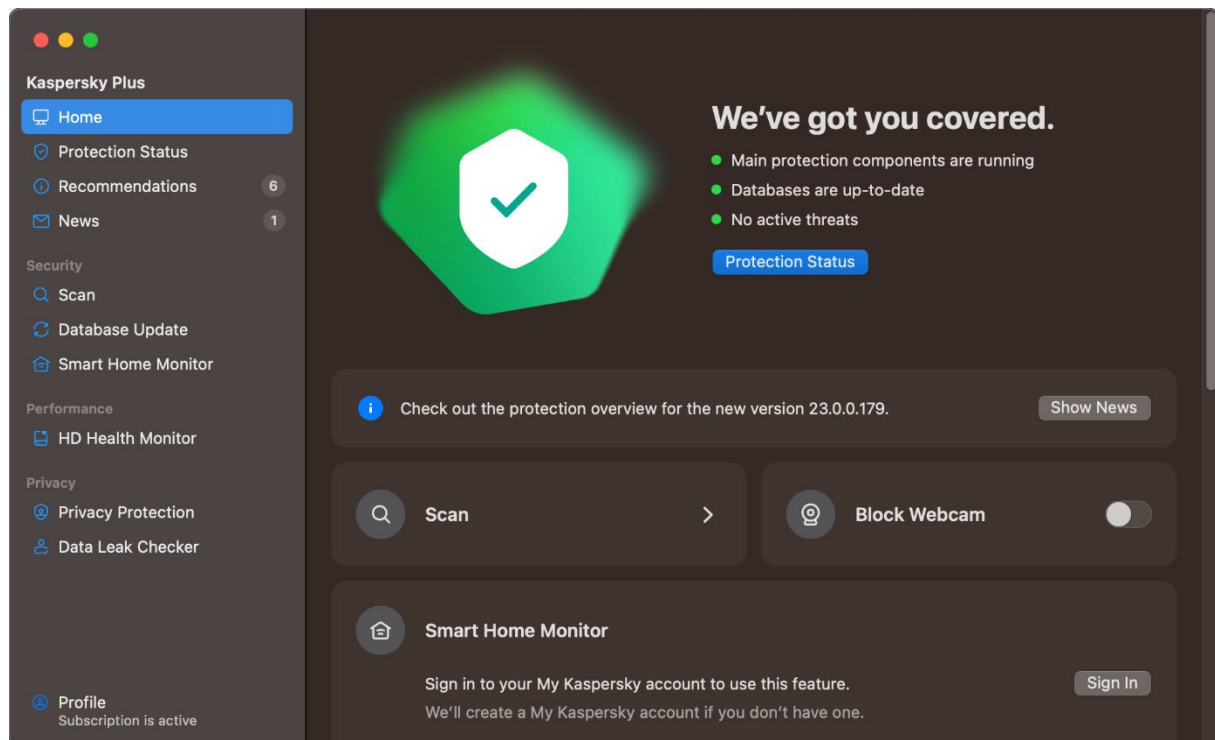
Logs on the *Scan* page displays a list of all system events, including updates, scan and real-time detections, real-time protection status, and items added to or deleted from quarantine. The applicable date and time are shown, along with a traffic-light colour-coding system for each item. Malware finds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

Advanced Options

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

- Disable protection features (under *Scan* page, *Settings*, or system tray icon)
- Uninstall the program

Kaspersky Plus for Mac



Summary

Kaspersky Plus for Mac is a paid-for antivirus program and an excellent choice for non-expert users. Some of its key aspects are:

- simple and straightforward installation and guided setup of core features
- all available features displayed in a well-organized and neat interface
- different scan options and many settings, including scheduled scans and automatic USB scan
- clear alerts
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

You can set up Kaspersky Plus for Mac by downloading and running the installer from the vendor's website. The initial setup is straightforward as the program guides you through step by step and provides brief explanations. During that, you can enable additional protection features, such as Wi-Fi network protection and browser extensions for Safari/Chrome/Firefox. When setup is complete, the main program window displays several recommendations, such as activating automatic macOS updates, signing into My Kaspersky account, and installing missing browser extensions, the Kaspersky VPN or Password Manager apps. The program can be uninstalled by clicking *Support > Uninstall* in the *Help* menu of the macOS menu bar or by deleting it from the macOS Applications folder.

General Handling & Essential Features

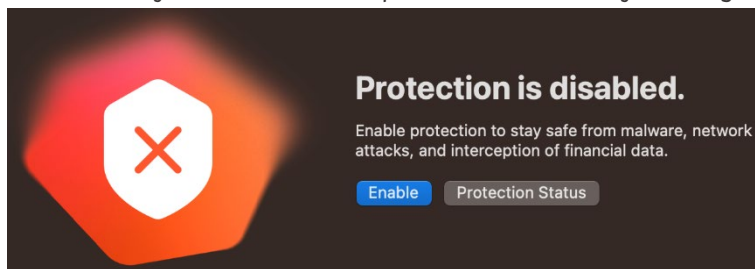
Protection status, **scan options** (*Scan*), and **subscription information** (*Profile*) can all be accessed from the main program window. **Settings**, including all the **protection features** and list of **scan exclusions** (*Trusted Zone*), **quarantine** (*Detected Objects*), and **help**, which shows the support page in the default browser, are all in the macOS menu bar. A manual **update** can be triggered from *Database Update* in the main program window or by clicking *Update Databases* from the system tray icon.

Protection

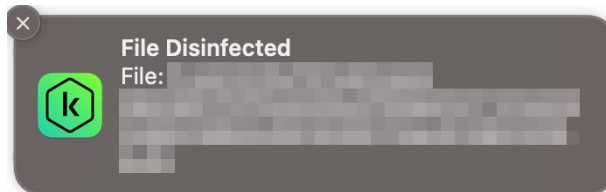
From *Scan*, you can start a **quick scan**, **full scan**, or **custom scan** of selected files or folders. The latter can also be run from e.g., the Finder context menu. **Scans can be scheduled** from the cogwheel icon in the top right-hand corner and the settings. In addition to modifying the program's detection behaviour and the named scan options, the **external disk scan** can be configured from the settings. The detection of stalkerware is enabled by default.

Alerts

When we disabled Kaspersky's real-time protection or any other protection feature under *Settings > Protection*, a notification appeared, and an alert similar to the one below was shown in the main program window. The real-time protection can also be turned off via the system tray icon. We were able to easily reactivate either protection feature by clicking *Enable*.

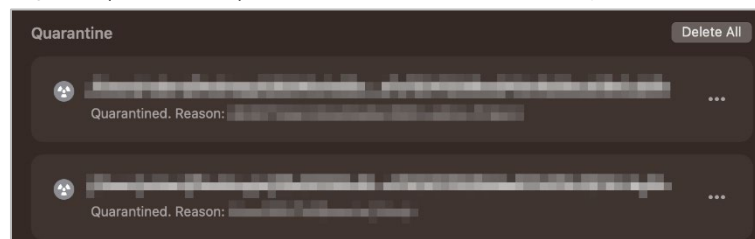


When malware was detected in our protection test, the program displayed an alert in the form of a system notification shown below, including the file path, where the threat was found, and the action taken. No user action was required, and the alert closed automatically after a few seconds. Additionally, a link to the quarantine is shown on the home page of the main program window.



Quarantine & Logs

The *Detected Objects* page shows quarantined items, along with the threat name and file path. 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* window shows processed objects (detections) as well as activities about updates, scans, and the different protection features.

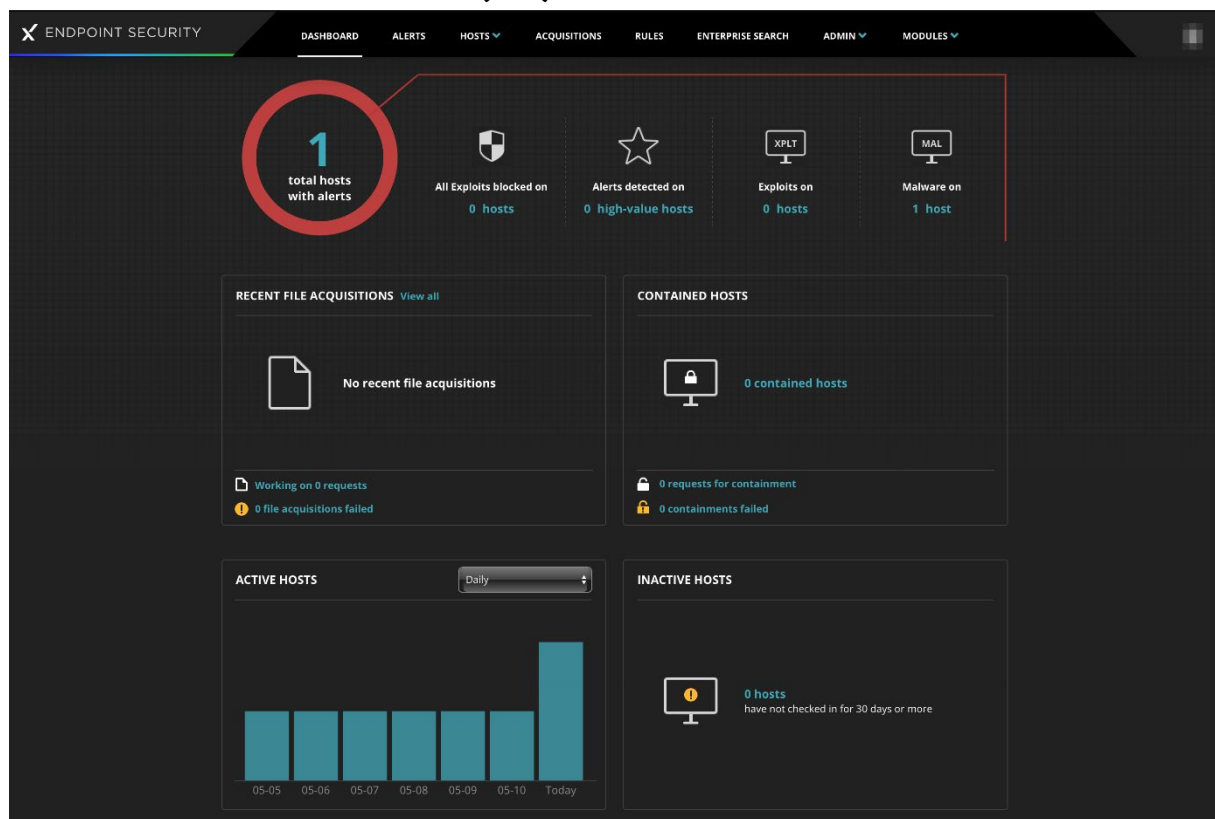


Advanced Options

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

- Disable protection features (under *Settings* or system tray icon)
- Uninstall the program

Trellix Endpoint Security (HX) for Mac



Summary

Trellix Endpoint Security (HX) is a security package suitable for large-sized enterprise networks (up to 100,000 endpoints per appliance) and provides a cloud-based console for managing the endpoint protection software. Some of its key aspects are:

- investigative functions for analysing and remediating attacks
- comprehensive search facilities
- variety of console types (cloud-based, hardware/virtual appliance, Amazon-hosted)
- well-organized cloud-based console with easy access to details pages
- containment feature to isolate infected devices

Management Console

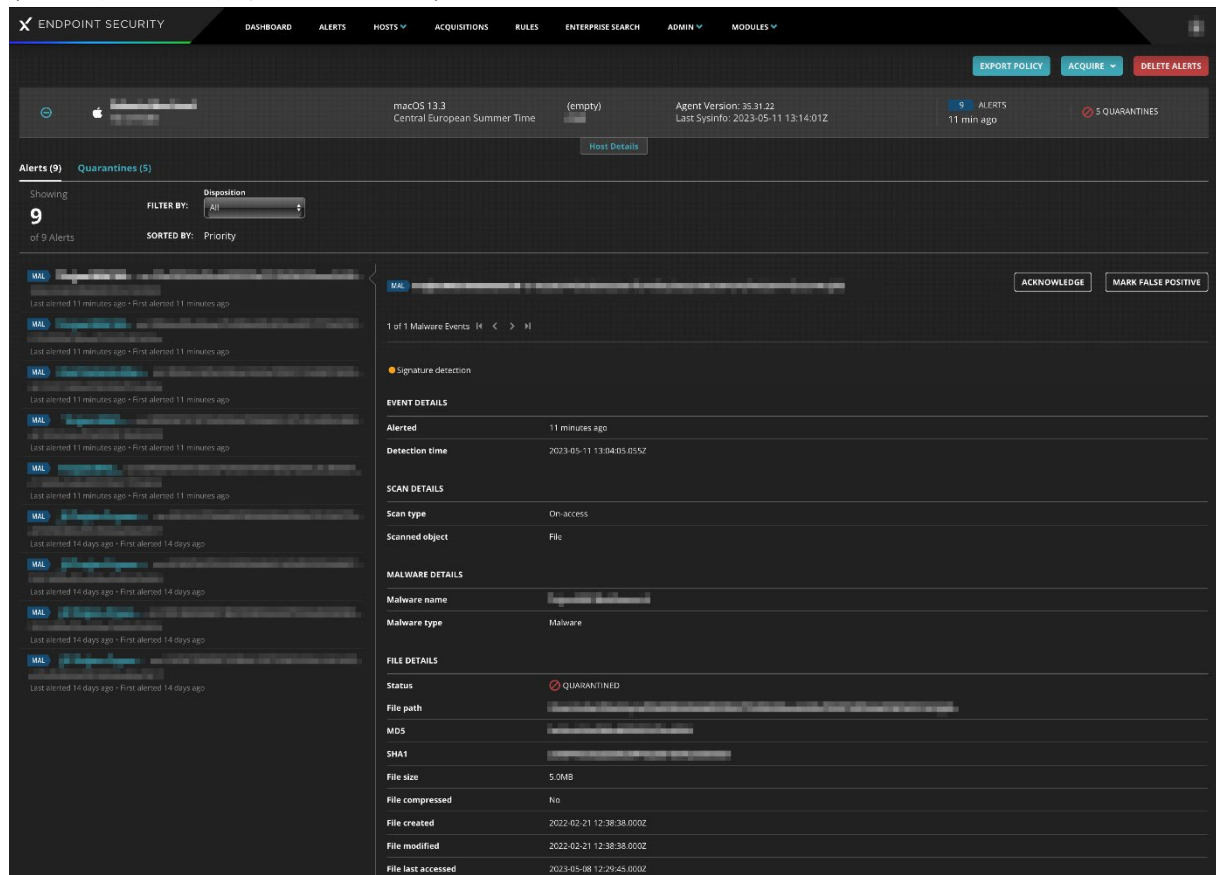
The console is navigated from the menu at the top of the page. This lists different sections and pages, such as *Dashboard*, *Alerts*, *Hosts*, *Acquisitions*, *Rules*, *Enterprise Search*, and *Admin*. We will describe the most relevant sections and pages below.

Dashboard

When you login to 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, *recent file acquisitions*, and *contained/active/inactive hosts*. Clicking on the *Total hosts with alerts* button opens the *Hosts with Alerts* page.

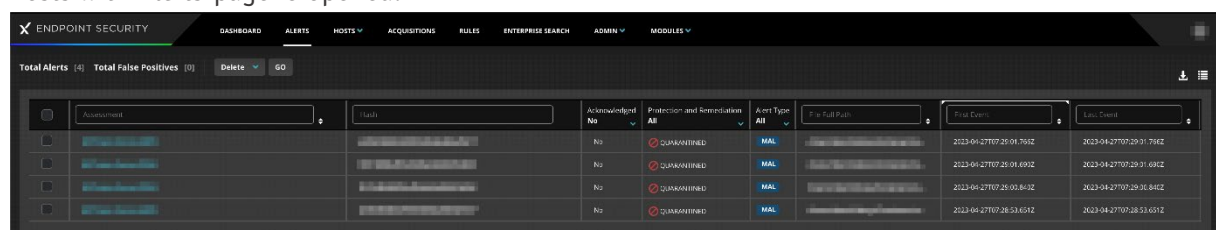
Hosts > Hosts with Alerts page

This page displays details of protected devices/hosts with alerts that have not yet been resolved. If you click on the plus sign for a host, you can view the list of its alerts, in chronological order and with a wealth of details. This includes detection type (e.g., signature detection), alert/detection times, scan type (e.g., on-access, on-demand), malware name/type, file status (e.g., quarantined), file metadata (e.g., path, MD5/SHA1 hash, size, last modified/accessed times), process path, username of logged-on user, and content version (signature). Each threat can be acknowledged (marked as “read”), or marked as false positive. You can also add comments for future investigation. From *Quarantines*, you can restore, delete, or acquire individual quarantined files for further analysis (see *Acquisitions* page shown below).



Alerts page

For a threat-centric rather than a device-centric view, you can go to the *Alerts* page. It shows a list of detected threats which you can sort or filter by name, file path, first/last event time, host name, or host IP address. Besides deleting alerts, options for *Acknowledge*, *Mark False Positive*, and *Add Comment* are provided here too. If you click on the threat name of a list item, the details view of the *Hosts with Alerts* page is opened.



Hosts > Host Management page

This page lists all the registered devices/hosts along with different attributes shown in filterable and sortable columns. The visibility of each column can be changed from a separate menu in the top right-hand corner. The attributes include, e.g., host name, online status, operating system information, username of logged-on user, containment status, installed agent version/signature, active protection/detection capabilities, and last seen date. Clicking on an entry reveals a panel with all the available device information.

Acquisitions page

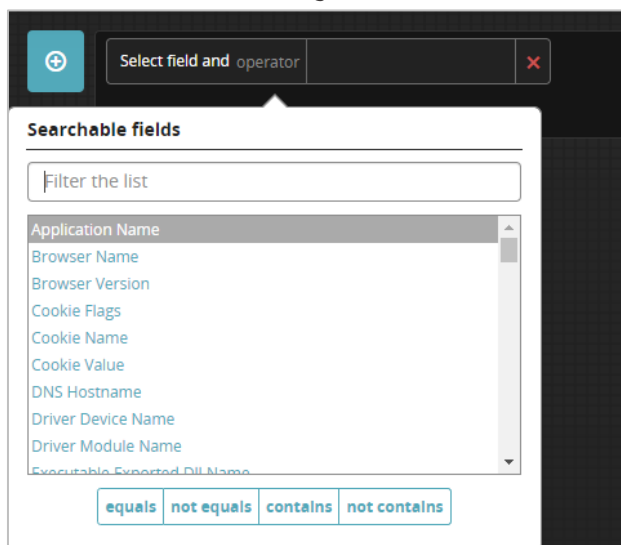
This page lets you download files that have been acquired from hosts in order to analyse them. You can acquire files or various items of diagnostic data from an individual host on the *Hosts with Alerts* page.

Rules page

This page contains rules matching indicators of compromise (IOCs), exploit detections, or false positives in order to help identifying specific threats or suspicious behaviours on an endpoint. This rule collection is primarily maintained by Trellix's *Dynamic Threat Intelligence* (DTI) cloud, but you can add your own enterprise-specific rules with individual conditions as well.

Enterprise Search page

On this page, you can extensively search the network for a wide variety of items. These include application name, browser version, host name, 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 section

On the *Policies* page, you can add custom endpoint protection policies and configure numerous different aspects of existing ones. Examples of configurable categories are malware protection (e.g., detection options, definition updates, exclusions, quarantine actions), malware scans (e.g., scheduled scan), whether to show alerts on the host, event logging (e.g., information level, age), polling frequency, removal and tamper protection, resource usage, and management server address. On the *Host Sets* page, groups of hosts can be defined according to a wide variety of criteria, or simply by dragging and dropping from the list of all hosts. Different protection policies can be applied to each host set.

Endpoint Protection Client

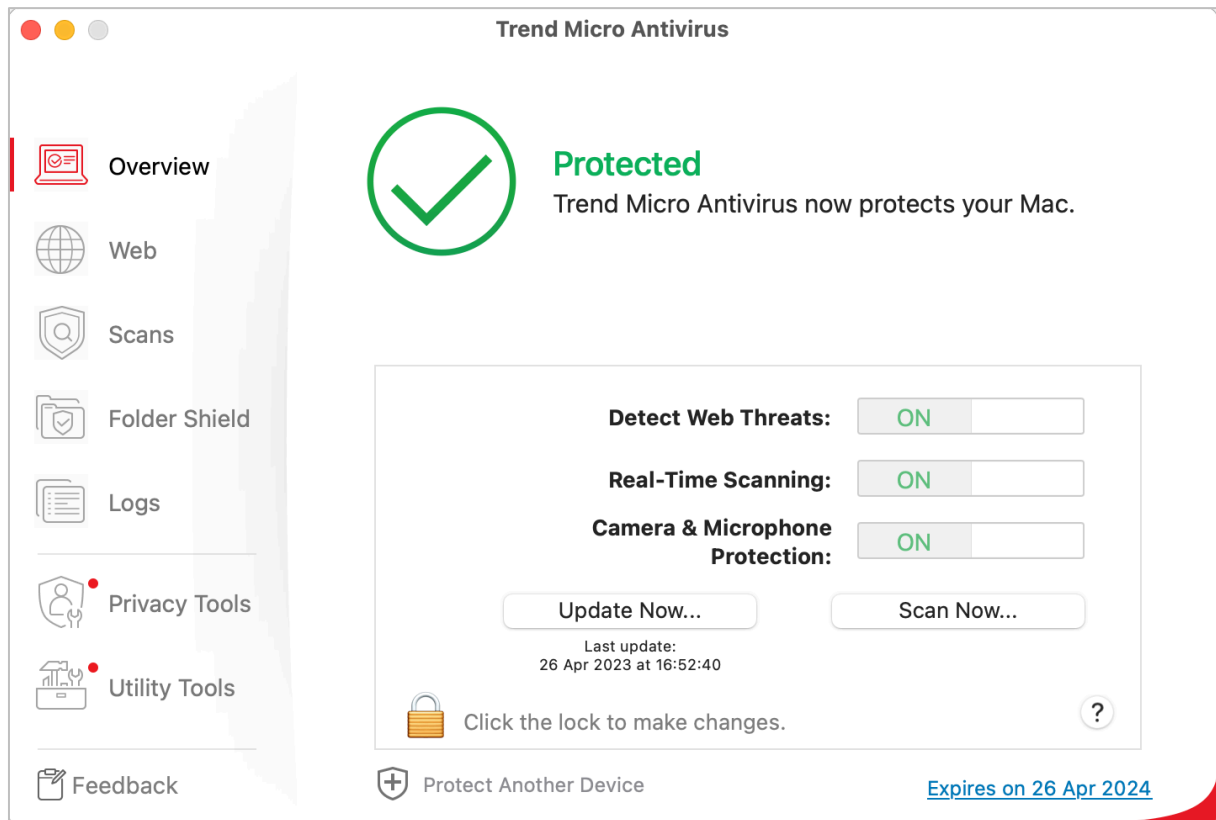
Deployment

Current and older versions of the endpoint protection client (*Agent*) for Windows, macOS, and Linux systems can be downloaded from the *Admin > Agent Versions* page. The installer file can be run manually, or via a systems management product such as *Jamf*. In the former case, you will need to remember to give the agent *Full Disk Access* in the macOS system settings which is necessary for the product to work properly. After installation, the agent takes some minutes to download the protection engine before protection will be finally active.

General Handling & Alerts

With the settings used in this test, no user or command-line interface is provided in order to interact with the program on the host. When malware was detected in our protection test, no detection alerts were shown on the host.

Trend Micro Antivirus for Mac



Summary

Trend Micro Antivirus for Mac is a paid-for antivirus program and well suited to non-experts. Some of its key aspects are:

- simple and straightforward installation and guided setup of core features
- all available features displayed in a well-thought-out user interface
- different scan options including scheduled scans; ransomware protection, browsing-protection add-ins
- clear and persistent alerts
- normal user accounts cannot take risky actions (e.g., disable protection, uninstall program)

Installation, Setup & Deinstallation

After downloading and running the installer from the vendor's website, the setup wizard guides you through each installation and configuration step. Aside from choosing whether to enter a licence key or use the trial version, there are no decisions to make. When you first open the program, it prompts you to set up *Camera and Microphone Protection* and ransomware protection (*Folder Shield*). For the latter, you can easily customise the default list of folders to be protected. Additionally, the Safari extension *Trend Micro Toolbar for Mac* is installed and will be activated if you authorise this. The program can be uninstalled by using the uninstaller located inside the Trend Micro folder of the macOS Applications folder. The Trend Micro folder also contains a diagnostic toolkit used for troubleshooting and other problem-mitigating tasks (requires a macOS administrator account).

General Handling & Essential Features

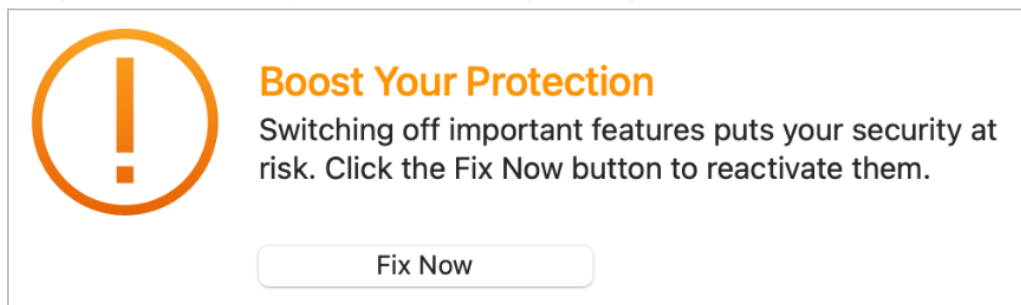
Protection status, **smart scan** (*Scan Now*), **scan options** (*Scans*), **protection features**, and **subscription information** can all be accessed from the *Overview* page of the main program window. **Quarantine** can be found under *Logs > List Quarantined Files*. **Settings** provide access to a list of **scan exclusions** (*Files Not Scanned*) and the quarantine and are located under *Trend Micro Antivirus* in the macOS menu bar or the system tray icon. A manual **update** can be triggered directly from the *Overview* page, *Protection* menu in the macOS menu bar, or the system tray icon. The online **help** opens the support page in the default browser and is found in either the *Help* menu in the macOS menu bar, the system tray icon, or when clicking the ? icon located on several pages of the main program window.

Protection

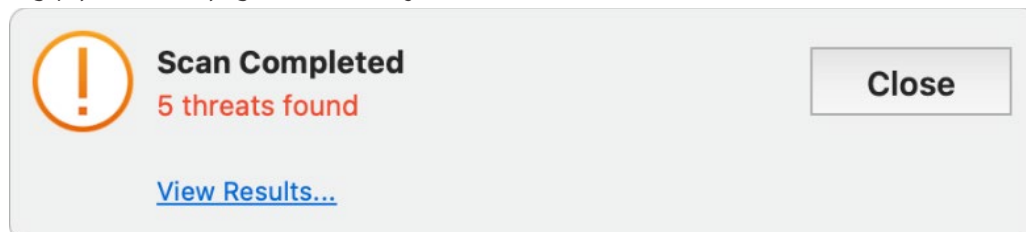
From *Scans*, you can start a **smart scan** of the most critical areas, **full scan** of every file on the system, or **custom scan** of selected files or folders. **Scheduled scans** as well as the detection behaviour and scan options can be configured in the *Scans* page of the settings. The web protection and anti-ransomware feature can be modified from its respective subpage of the main program window. If you install the Trend Micro browser extension, safety ratings (indicated by coloured symbols) are added to Google, Bing, and Yahoo search results as well as web-based email services from Gmail and Yahoo. A *Website Filter* blocks access to selected websites based on rating scores, pre-defined filters (e.g., child, teenager, adult) or a user-defined blacklist.

Alerts

When we disabled Trend Micro's real-time protection or web threat protection on the *Overview* page or from the *Protection* menu in the macOS menu bar, the alert below was shown in the main program window. The real-time protection can also be turned off via the system tray icon. We were able to easily reactivate either protection feature by clicking *Fix Now*.

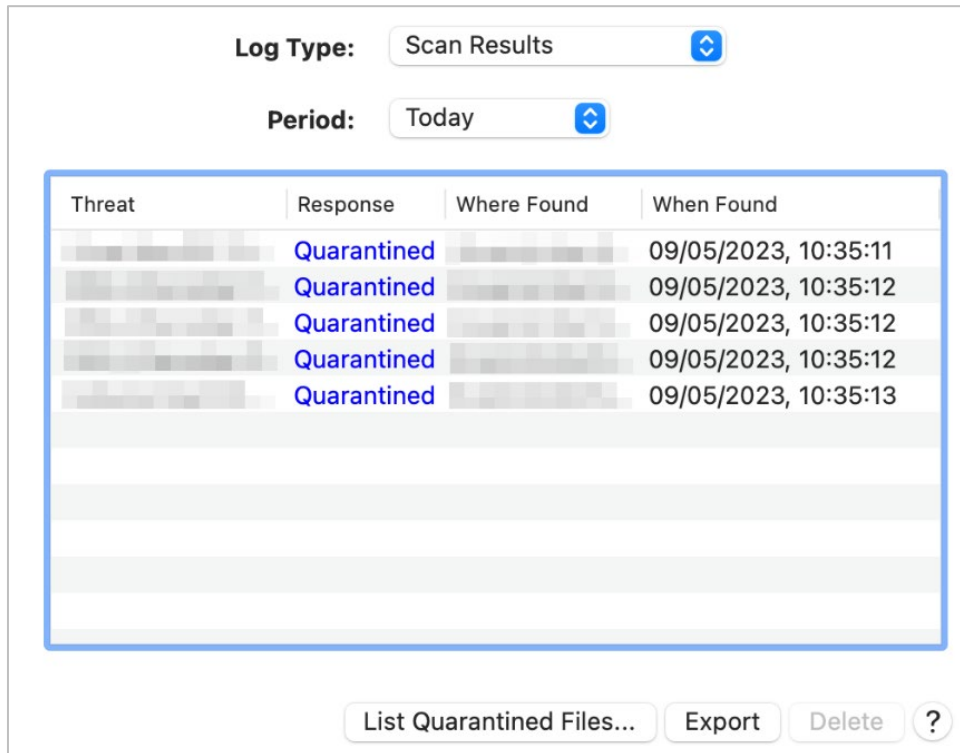


When malware was detected in our protection test, the program displayed the alert shown below. No user action was required, and the alert persisted until we closed it. Clicking on *View Results* opens the logs/quarantine page and shows you what's been detected.



Quarantine & Logs

The *Logs* page lists all the threats that have been detected, along with the threat name, file path, date when this happened, and action taken, under the log type *Scan Results*. Quarantine functionality, including options to delete, restore, or clean quarantined items (you have to enter administrator credentials to take either action), is reached by clicking *List Quarantined Files*.



Threat	Response	Where Found	When Found
[Redacted]	Quarantined	[Redacted]	09/05/2023, 10:35:11
[Redacted]	Quarantined	[Redacted]	09/05/2023, 10:35:12
[Redacted]	Quarantined	[Redacted]	09/05/2023, 10:35:12
[Redacted]	Quarantined	[Redacted]	09/05/2023, 10:35:12
[Redacted]	Quarantined	[Redacted]	09/05/2023, 10:35:13

As noted in previous years, the quarantine and log data are displayed in panels within small windows that cannot be resized or maximised. It is necessary to resize the columns 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.

Advanced Options

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

- Disable protection features (under *Overview*)
- Uninstall the program
- Delete and restore items from quarantine

Advertising

The program advertises Trend Micro's freemium Cleaner One Pro program. Running a *Smart Scan* will find "junk files" and prompt the user to get Cleaner One Pro to remove these. Additional freemium software is promoted on the pages *Privacy Tools* and *Utility Tools* of the main program window.

Featurelist security for macOS Ventura (as of June 2023)									
Product name:	Avast Security Free for Mac	AVG AntiVirus Free for Mac	Avira Prime for Mac	Bitdefender Antivirus for Mac	CrowdStrike Falcon Pro for Mac	Intego Mac Internet Security X9	Kaspersky Plus for Mac	Trellix Endpoint Security (HX) for Mac	Trend Micro Antivirus for Mac
Supported Program languages:	English, Bulgarian, Chinese, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Slovak, Thai, Turkish, Ukrainian, Vietnamese	English, Bulgarian, Chinese, Czech, Danish, Dutch, Finnish, French, German, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Slovak, Turkish	English, Chinese, Dutch, French, German, Italian, Japanese, Portuguese, Russian	English, Czech, Dutch, French, German, Greek, Hungarian, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Thai, Vietnamese	English	English, French, German, Japanese, Spanish	English, Arabic, Bulgarian, Chinese, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Lithuanian, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Spanish, Swedish, Thai, Turkish, Ukrainian, Vietnamese	English, Chinese, French, German, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish	English, Chinese, French, German, Spanish
Third-party scan engine used (in addition to it's own)	proprietary	Avast	proprietary	proprietary	proprietary	Avira	proprietary	Bitdefender	proprietary
Free Trial version available? (how many days?)	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 (>85%)	●	●	●	●	●	●	●	●	●
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									●
Additional features (we limited this to max. 2 relevant features)	Email Scanner, Traffic Monitor	Email Scanner	USB Scanner, Ads & Tracking Blocker	VPN, Time Machine Protection	Enterprise investigative features		Data Leak Checker, Private Browsing	Enterprise investigative features	Parental Control, Device Control
Support									
Online Help and/or User Forum	●	●	●	●	●	●	●	●	●
Email and/or Phone Support	●	●	●	●	●	●	●	●	●
User manual (PDF)				●	●	●	●	●	●
Online Chat				●		●	●	●	●
Supported languages (of support)	English, Czech, French, German, Italian, Portuguese, Russian, Spanish	English, Czech, French, German, Italian, Portuguese, Russian, Spanish	English, French, German, Italian, Portuguese	English, Czech, Dutch, French, German, Greek, Italian, Japanese, Korean, Portuguese, Romanian, Spanish, Turkish	English	English, French, Japanese	English, Arabic, Chinese, Danish, Dutch, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Turkish	English, Arabic, French, Hebrew, Italian, Japanese, Portuguese, Spanish, Turkish	English, Chinese, French, German, Spanish
List Price (without discount etc.)									
List Price 1 Mac / 1 year USD/EUR	FREE	FREE	USD 108 / 100 EUR	USD 40 / 40 EUR	n/a (enterprise)	USD 55 / 50 EUR	USD 58 / 54 EUR	n/a (enterprise)	USD 40 / 50 EUR
Auto-renew (not available; opt in; opt out; obligatory)	n/a	n/a	Obligatory / Obligatory	Obligatory / Opt-out	n/a	Obligatory / Obligatory	Obligatory / Opt-out	n/a	Obligatory / Opt-out

Copyright and Disclaimer

This publication is Copyright © 2023 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(June 2023)