When you purchase through links in our articles, we may earn a small commission. This doesn't affect our editorial independence.

REVIEWS

macOS Gatekeeper review: How well does Apple's free antivirus defend a Mac from malware

Apple's security layers fight the good fight, but malware and suspect applications can still be installed if warnings are ignored.

By Chris Barylick
Contributor, Macworld | SEP 24, 2025 3:02 AM PDT

Image: Foundry

TABLE OF CONTENTS

Should you rely on Apple's Gatekeeper antivirus protection?

At a glance

Macworld EDITORS' CHOICE

Expert's Rating

★★★★☆

Pros

- macOS' Gatekeeper and XProtect functions work well together to block or quarantine the most obvious malware and throw up multiple warning prompts before harmful software can be installed.
- Good automatic cleanup, and in many cases, the Gatekeeper function quarantines and deletes suspect software, and even uninstalls fake copies of Adobe Flash Player.

Cons

- With enough determination—or carelessness—users can override warnings and install malware that compromises core system functions.
- Questionable applications can be installed in the Applications folder with no warnings whatsoever.
- Risk to sensitive systems, such as your webcam, microphone, keystroke data, and other functions, should all warnings be ignored, and you continue to plow ahead and install malware.

Our Verdict

macOS's Gatekeeper and XProtect functions provide a strong baseline for security and block the vast majority of malware and questionable apps. Still, determined or careless users can bypass protections and grant dangerous levels of access to malware, placing your Mac's data and functions at risk. For most users, these safeguards are enough, but a third-party security suite can also offer peace of mind.

With the rise of third-party antiviral and anti-malware applications for the Mac, the question of how macOS defends against malware on its own has surfaced. To this end, is it safe to use macOS on its own and rely exclusively on macOS and security updates from Apple, or are you better off using a well-reviewed antiviral/anti-malware suite in conjunction with the native macOS layers of protection?

Being somewhere between brave, curious, and outright idiotic, I backed up everything on my MacBook Pro as a Time Machine volume on my external hard drive, removed all third-party protection software, and then proceeded to run all of the Objective-See Mac Malware Collection across my operating system, throwing more than 130 chunks of questionable software at macOS 15.6.1 to see how things would hold up. The results were surprising.

At the heart of the macOS security layer is its Gatekeeper system, which collaborates with its Xprotect feature to ensure that only certain applications have permission to run and/or install background functions on macOS. These security layers can be altered to allow for software that's been signed by developers or approved by the Mac App Store, macOS offering warnings galore through its Privacy and Security preference pane.

For the most part, this works well; macOS often deletes suspect malware and moves it to the trash before it can be installed as the system scans it, along with throwing up warning messages after warning messages not to install the software, which it deems to be questionable. This is the good part, and the safeguards are in place, but the developers and the operating system also know they can't completely stand in the way of the users' goals and that suspect software occasionally has to be installed and tested. As such, it's still possible to bypass the warnings, execute questionable software, and install chunks of malware deep within macOS to become login items, background functions, and override core elements such as your web browser's search engine and start page.

It got heady from there.

Going through the malware archive and ignoring/bypassing protection screens, I was able to install third-party software that requested access to my microphone, webcam, keystrokes, and other system functions. During testing, I was allowed to install the NRKIH88 background function, which functions as a trojan; the infamous MacSecurity suite was installed and created background functions, and the LamePyre malware created a mock Discord app that requested permission to record audio and video data. By the end, my Safari start page had been compromised and switched to a website offering Viagra for sale.

Recommended For You

Apple confirms: The new iPhones have a camera problem
Macworld

Apple reportedly has TEN more products ready to launch in the coming months
Macworld

People in Ashburn are Loving Martha Stewart's Meal Kit
Sponsored | Marley Spoon

Powered by Taboola

Although macOS works to keep malware from being installed and throws up warning message after warning message to try to prevent this from happening, it's the native applications that the operating system allows to be installed in the Applications folder without batting an eye that can be disturbing.

Apple attempts to verify if an app is safe.

Image: Foundry

In addition to two fake copies of Adobe Flash Player that were allowed to be installed (but, to macOS' credit, automatically uninstalled later), the operating system allowed questionable software to be installed, such as MixPad, Free Download Manager, Wondershare, Movavi Screen Recorder (which allows full access to your photo libraries), Spedal, VideoPad, and borderline BitTorrent clients such as Vuze and Bigly BT. Granted, many of these applications have undergone updates over the years that took them out of consideration as malware, but the Gatekeeper system still allowed them to be copied into the Applications folder with no warning whatsoever.

So what's the result of this? By the end of my testing, the MacSecurity suite was flashing notifications of viral infection and demanding to be registered, I had granted permission over core system functions to several questionable applications, and after seeing that my search engine and start page preferences had been altered, I was hesitant to log into anything sensitive, such as online banking or health insurance, and entirely glad that I had backed everything up so I could boot my MacBook Pro into Recovery Mode, wipe the drive several times, reinstall macOS Sequoia, reimport my data from Time Machine, and start over again.

Apple warns you when an app wants to access areas of your Mac.

Image: Foundry

macOS' Gatekeeper and XProtect systems fight the good fight and put up considerable resistance to malware infection, but it's still entirely possible to bypass these protections and put some extremely questionable software on your Mac; it just takes a fair amount of effort to do so. Like deciding you're going to head to Home Depot, take off your shoes and socks as you walk over to the construction materials section, and then proceed to drop cinder blocks onto your bare feet over and over again for fun and amusement, it's entirely possible to completely infect your Mac with dangerous malware provided you ignore all the warning signs and press ahead.

EXPLORE FREQUENTLY ASKED QUESTIONS

- What security benefits come from installing apps from the Mac App Store?
- How does Apple's XProtect antivirus function on macOS?
- What happens when bypassing macOS Gatekeeper warnings?
- How frequently does Apple's XProtect update malware definitions?
- How does macOS Lockdown Mode protect against cyberattacks?

Ask your own question... A.I. Search

The system will warn you about what an app tries to access.

Image: Foundry

This, coupled with how easy it is to install some questionable applications with no warning, gives one a bit of pause, but the native protection layer within macOS still holds its own, provided you heed the warnings and veer away from questionable software.

In conclusion, macOS' Gatekeeper function does its job, and does it well with a few exceptions, but there's nothing that can completely keep you from installing some of the worst software on the planet, designed by some of the most sociopathic developers on the planet to line their pockets, if your heart's set on it.

That being said, I'm REALLY glad I made that backup.

Should you rely on Apple's Gatekeeper antivirus protection?

You can't argue with something that's free and part of macOS, and if you're the kind of Mac user who mostly sticks to the Mac App Store, trusted developer downloads, and pays attention to Apple's warning prompts, macOS' built-in protections are generally enough to keep you safe. There are safeguards in place that honestly do a great job of blocking or quarantining the most obvious malware and raising red flags before shady software can do real harm.

Still, nothing's entirely bulletproof, and in the face of an idiot-proof system, nature always finds a way to craft a greater idiot. You can still override every warning and offer over your camera, microphone, keystroke data, and core system settings to some of the sketchiest malware on Earth, and if you handle sensitive data, then a well-reviewed third-party antiviral or anti-malware tool can provide the safety net you're looking for, even if you have to pay for it.

Finally, Time Machine is free. Hook up an external drive, use it, and it may just be the ticket back from the crash or viral infection that could have annihilated your work and driven you crazy.

Author: Chris Barylick, Contributor, Macworld

Chris Barylick is a D.C.-based technology journalist, loves writing about emerging technologies, video games, DIY projects, hardware, utilities, politics, and upgrades, and has written for Macworld since 2007. He is the owner of East Bay Mac Menders, SnarkFish T-Shirts, the Mistakes Were Made Dinocast, and has masters degrees in both Business Administration (George Washington University '05) and Journalism (The University of Maryland '23), and inadvertently wound up in the Guinness Book of World Records for being the "4 AM Guy" at the first Apple Store opening in 2001. He has accidentally set two hard drives on fire to date.

Recent stories by Chris Barylick:

- Norton 360 review: Solid performance on the Mac, but with some tradeoffs
- 5 Mac antivirus apps that beat Apple's built-in security
- Best Mac Cleaner software: Reclaim disk space with a Mac cleaner app

Costco Shoppers Say This Fat-Burning Patch Triggers Weight Loss "Unlike Any Other"

Health Advice Today | Sponsored

Lara Green's Final Collection Stuns Virginia

Artisan Weekly | Sponsored

Learn More

You Can See People Wearing This 250th Anniversary Hat Everywhere

Giosrity | Sponsored

Learn More

Neuropathy is not from Low Vitamin B. Meet the Real Enemy of Neuropathy (Stop Doing This)

FootRenew | Sponsored

Warren Buffett, Elon Musk and other moguls all use the 5-hour rule. Here's what I learned from...

Blinkist Magazine | Sponsored

Learn More

A Lifetime of Bags, One Final Sale — Up to 80% Off

Junie Boutique | Sponsored

Read More

A New Option For Choking Emergencies When Help Is Minutes Away.

Heroic Daily | Sponsored

Learn More

Just Add 1 Drop Of This Household Item To Any Dark Spot (Starts Working Instantly)

skincaresecrets.us | Sponsored

Replace Your Entire Roof in as Little as 1 Day!

Metal Roofing Innovations | Sponsored

Learn More

Here's What a New Metal Roof Should Cost You in 2025!

Metal Roofing Innovations | Sponsored

Get Quote

Copyright © 2025 FoundryCo, Inc.