App security overview

Archived: 2026-04-05 18:45:38 UTC

Today, apps are among the most critical elements of a security architecture. Even as apps provide productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly.

Because of this, Apple provides layers of protection to help ensure that apps are free of known malware and haven't been tampered with. Additional protections enforce that access from apps to user data is carefully mediated. These security controls provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps for iOS, iPadOS, macOS, tvOS, visionOS, and watchOS—all without impacting system integrity. And users can access these apps on their Apple devices without undue fear of viruses, malware, or unauthorized attacks.

On iPad and iPhone, the design principle focuses on centralized distribution, code signing, and strict sandboxing to provide the tightest controls. To reflect the Digital Market Act's requirements, users in the European Union (EU) can install apps from alternative app marketplaces and directly from an authorized developer's website, which introduces additional risks. Apple introduced protections, including (but not limited to):

- Notarization for apps
- An authorization for marketplace developers
- Disclosures on alternative payments
- Install confirmations that provide the user Apple-verified information about the app

These help to reduce risks and deliver the best, most secure experience possible for users in the EU. Even with these safeguards in place, many risks remain including a greater prevalence of malware, fraud and scams, illicit and harmful content, and other privacy and security threats. For more information, see Update on apps distributed in the European Union on the Apple Developer website.

On Mac, many apps are obtained from the App Store, but Mac users also download and use apps from the internet. To safely support internet downloading, macOS layers additional controls. First, by default in macOS 10.15 or later, all Mac apps need to be notarized by Apple to launch. This requirement helps ensure that these apps are free of known malware, without requiring that the apps be provided through the App Store. Second, macOS includes state-of-the-art antivirus protection to block—and if necessary remove—malware.

As an additional control across platforms, sandboxing helps protect user data from unauthorized access by apps. And in macOS, data in critical areas is itself protected—which helps ensure that users remain in control of access

to files in Desktop, Documents, Downloads, and other areas from all apps, whether the apps attempting access are themselves sandboxed or not.

Native capability	**Third-party equivalent**
App notarization	Built into macOS
Kext exclude list	Built into macOS
Mandatory Access Controls	Built into macOS
Mandatory app code signing	Built into macOS
System Integrity Protection	Built into macOS
Gatekeeper	Endpoint protection; enforces code signing on apps to help ensure that only trusted software runs
Application firewall	Endpoint protection; firewalling
eficheck (Necessary for a Mac without an Apple T2 Security Chip)	Endpoint protection; rootkit detection
Packet Filter (pf)	Firewall solutions
File Quarantine	Virus/Malware definitions
Plug-in unapproved list, Safari extension unapproved list	Virus/Malware definitions

Native capability	Third-party equivalent
XProtect/YARA signatures	Virus/Malware definitions; endpoint protection

Please don’t include any personal information in your comment.

Maximum character limit is 250.

Thanks for your feedback.
