Contents

Word Count:1486

A high-level description

List of some security features of macOS:

1. **FileVault -** Full disk encryption that protects data on macOS devices.[10]
2. **Gatekeeper -** Protects against malware and prevents the installation of unauthorized apps. [13]
3. **SIP (System Integrity Protection) -** Prevents unauthorized access, modification, and deletion of system files and directories.[14]
4. **XProtect -** Protects against known malware by verifying files against a database of known malicious software. [9]
5. **TCC (Transparency, Consent, and Control) -** Gives users control over which apps can access sensitive data and system features.
6. **APFS (Apple File System) -** Offers built-in encryption and other security features, such as snapshots and crash protection.
7. **Touch ID and Face ID -** Biometric authentication methods that can be used to unlock devices and authorize transactions.
8. **Keychain Access -** Securely stores passwords, credit card information, and other sensitive data.[15]
9. **Secure Boot -** Ensures that only trusted software can run during the boot process.
10. **Code Signing -** Ensures that software comes from a trusted source and hasn't been tampered with.[16]
11. **Quarantine -** Isolates downloaded files and apps until they have been scanned for malware.
12. **Sandbox -** Restricts the access that apps have to system resources, limiting the potential impact of any security breaches. [13]
13. **Firewall -** Monitors incoming and outgoing network traffic and blocks unauthorized connections.
14. **Time Machine -** Provides automatic backup of files and data regularly.
15. **iCloud Keychain -** Syncs passwords and other sensitive data across devices with end-to-end encryption.

16. **MDM (Mobile Device Management) -** Allows administrators to remotely manage and secure macOS devices.[17]
17. **Secure Enclave -** A separate, secure processor that stores encryption keys and other sensitive data.
18. **Password Policy -** Allows organizations to enforce password complexity requirements and other security policies.
19. **File Sharing Restrictions -** Allows administrators to control access to shared files and folders.
20. **Disk Utility -** Offers tools for formatting, partitioning, repairing disks, and wiping data securely.

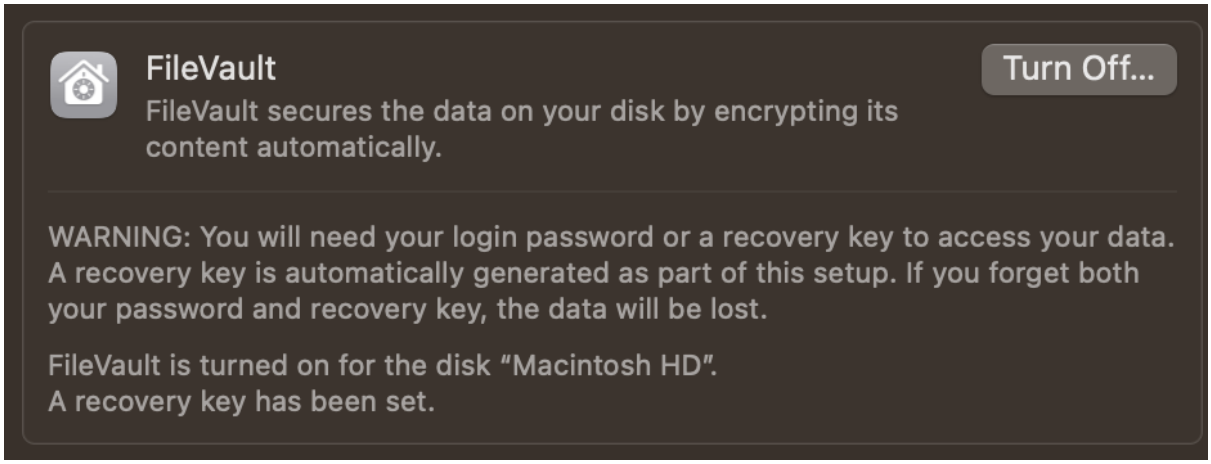
Security Features of macOS File System

The macOS file system is built on top of the HFS+ file system, which was introduced in 1998. Apple introduced the Apple File System (APFS) to replace HFS+. APFS is a modern file system designed to be more secure, reliable, and efficient [1].
Some of the security features in more detail of the macOS file system are:

2.1 FileVault

FileVault is a built-in encryption feature in macOS that encrypts the entire hard drive. When FileVault is enabled, all data on the hard drive is encrypted, including the operating system, applications, and user data [10]. This protects unauthorized access to data, even if the computer is lost or stolen.

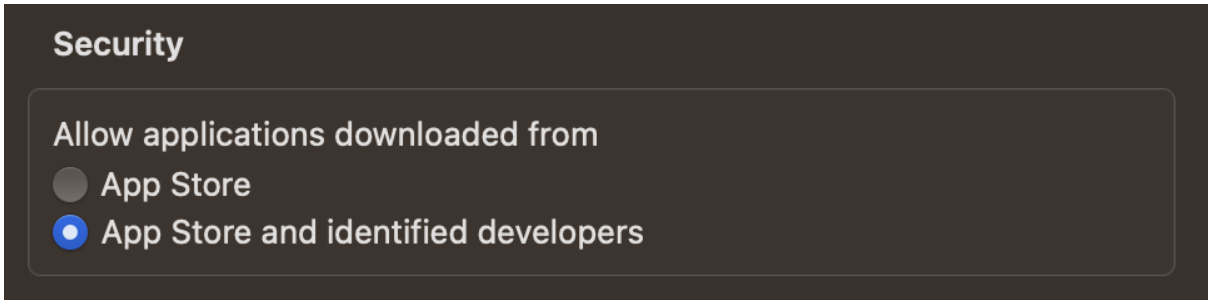
FileVault is in the settings app under Privacy & Security. You can also turn this feature off. Here is a screenshot of FileVault from a MAC system.



2.2. Gatekeeper

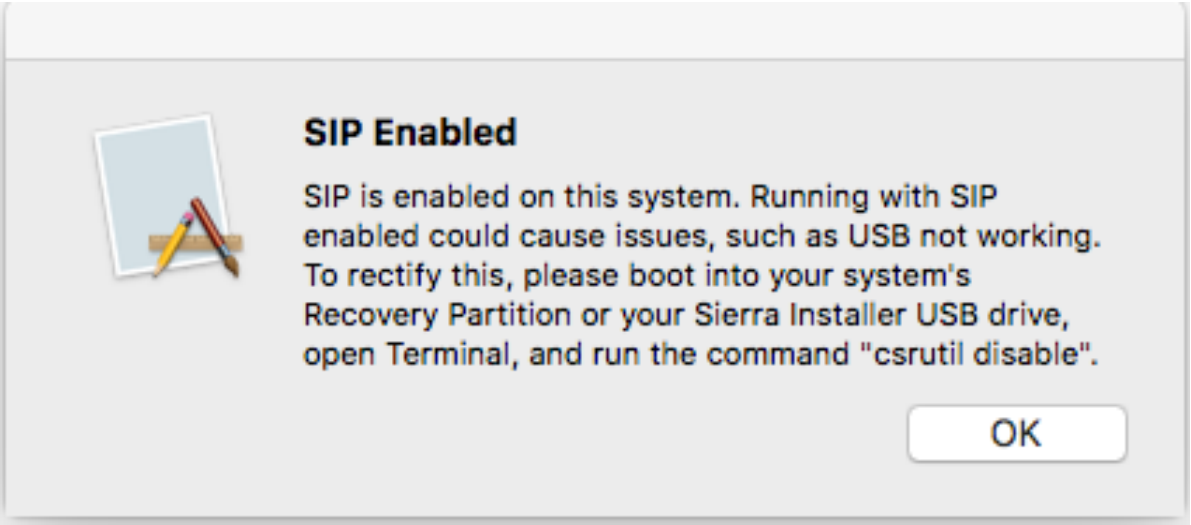
Gatekeeper is a security feature in macOS that helps to protect the computer against malicious software. Gatekeeper ensures that only software from trusted developers can be installed on the computer [18]&[3]. It does this by verifying the digital signature of the software before allowing it to be installed.

There are two options that the gatekeeper provides. One allows download applications from the app store only, and the other to download them from the App store and identified developers. The shown part from the Privacy & Security section of the setting app is known as Gatekeeper.



2.3. SIP (System Integrity Protection)

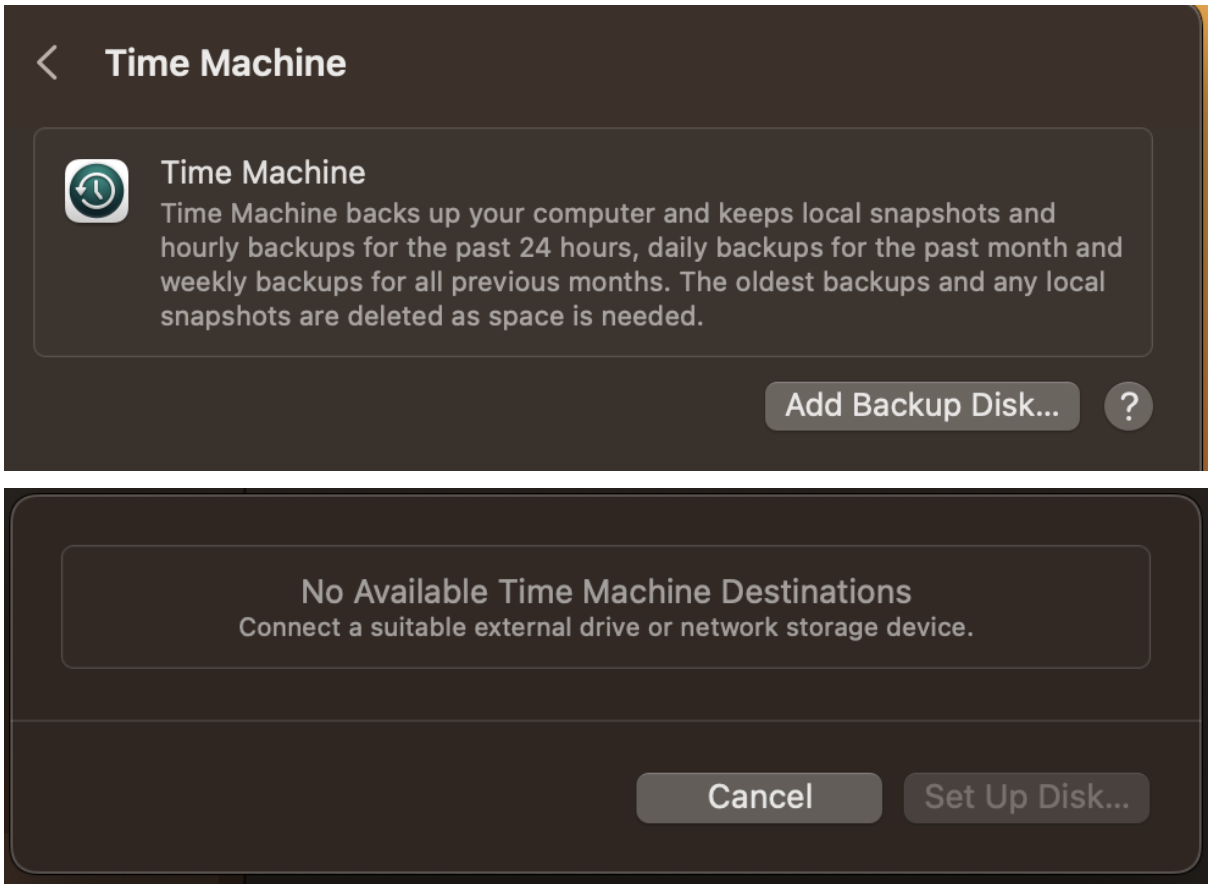
SIP is a security feature in macOS that protects system files and directories from being modified by unauthorized users or software. When SIP is enabled, specific critical system files and directories are protected from modification, even by the root user.



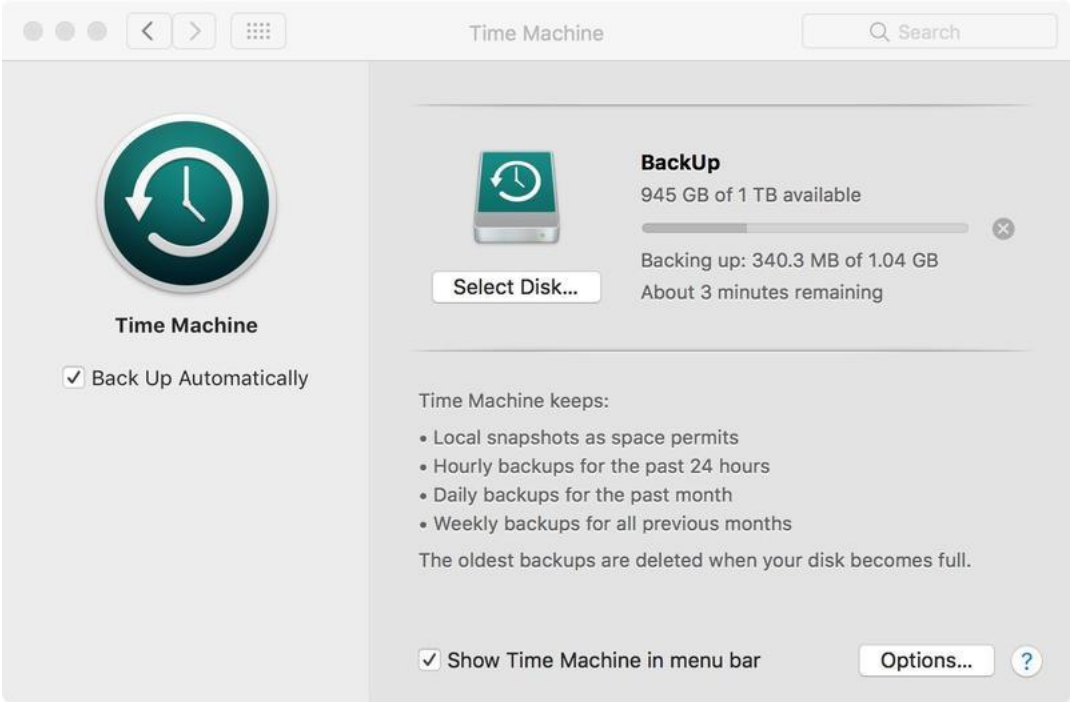
2.4. Time Machine

Time Machine is a backup feature in macOS that automatically backs up the entire system, including user data and applications. Time Machine provides a simple and easy-to-use backup solution that can be used to recover data in case of data loss due to hardware failure or other issues [3]&[19].

If you haven’t set up Time Machine on your Mac, a prompt like this will appear:

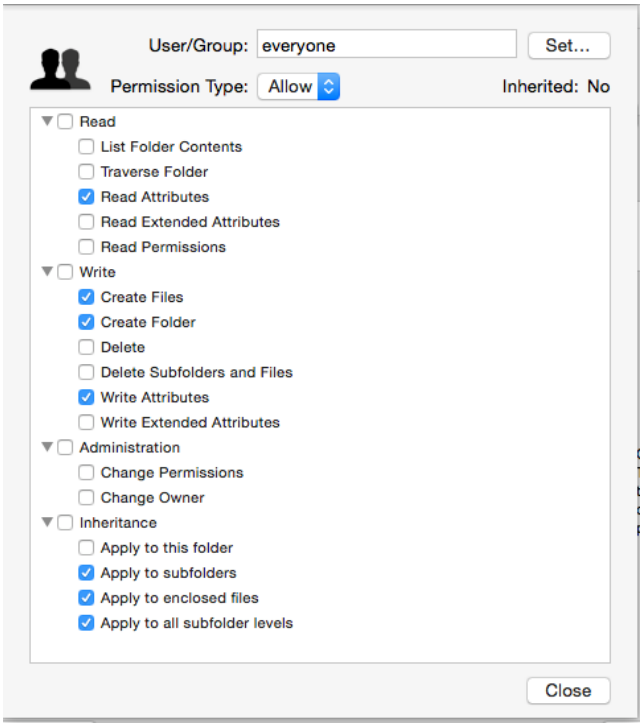


You must add an external drive to back up data using Time Machine. Once the setup is done and your device is backing up, the wizard will look like this:



2.5. Access Control Lists (ACLs)

ACLs are a security feature in macOS that provides fine-grained control over file and folder permissions. They allow administrators to set permissions for individual users or groups of users, giving them either read, write, or execute access to specific files and folders. This helps to ensure that sensitive files and data are only accessible to authorized users and can prevent unauthorized access or modification of critical system files. ACLs can be managed using the Terminal or through the graphical interface in Finder [3] &[20]



How macOS Provides Security Features

macOS provides the above security features through various mechanisms. For example, FileVault is enabled through the System Preferences panel, where users can turn on encryption for their hard drives [3]. Gatekeeper is enabled by default and can be configured in the Security & Privacy preferences panel. SIP is a system-level protection feature always encouraged, and users cannot disable it. Time Machine can be configured through the Time Machine preferences panel, and it automatically backs up the system at regular intervals.

The timeline for these features is as follows:

- FileVault was introduced in Mac OS X 10.3 (Panther) in 2003, and it has been available in all subsequent macOS versions.
- Time Machine was introduced in OS X 10.5 (Leopard) in 2007 and has been available in all subsequent macOS versions.
- Gatekeeper was introduced in OS X 10.8 (Lion) in 2012 and has been available in all subsequent macOS versions.

- SIP was introduced in OS X 10.11 (El Capitan) in 2015 and has been available in all subsequent macOS versions.

Comparison with Windows OS

Security Feature	macOS	Windows
FileVault	Encrypts user data on the hard drive	BitLocker encrypts user data on the hard drive
Gatekeeper	Verifies digital signature of apps before allowing installation	Windows Defender SmartScreen verifies apps and blocks potentially malicious downloads [5]&[21]
SIP	Protects critical system files and processes from unauthorized access	User Account Control (UAC) restricts system-level access and prompts the user for permission before making changes
Time Machine	Creates automatic backups of user's files and data	File History creates automatic backups of user's files and data
ACLs	Provides fine-grained control over file and folder permissions	ACLs provide fine-grained control over file and folder permissions [8]

Both macOS and Windows have security features that protect against unauthorized access, malicious software, and data loss. FileVault and BitLocker encrypt user data on the hard drive, Gatekeeper and Windows Defender SmartScreen verify app downloads, SIP and UAC restrict system-level access, and Time Machine and File History create automatic backups of user data. Both operating systems use ACLs to provide fine-grained control over file and folder permissions.

However, there are some differences between macOS and Windows security features. For example, macOS has built-in protection against adware and malware, while Windows has Windows Defender Antivirus [5]. Additionally, macOS has a built-in firewall, while Windows Firewall is a separate feature that needs to be enabled. Both macOS and Windows

have robust security features, and the choice between the two operating systems will depend on the user's specific security needs and preferences.

Effects on Application Developers

The security features in macOS file systems significantly impact application developers. Developers must be aware of these features and design their applications to work within the security constraints of the operating system. For example, Gatekeeper may prevent users from installing unsigned or untrusted applications, which can impact the distribution of applications. Developers must ensure that Apple properly signs and verifies their applications to distribute them through the Mac App Store or other channels.

Similarly, SIP can restrict access to specific system files and directories, impacting the behaviour of applications that rely on these files or directories. Developers must ensure that their applications are properly designed to work within the constraints of SIP.

Conclusion and Recommendations

In conclusion, macOS provides a variety of security features that help ensure the file system's security. These features include encryption, access control, and backup solutions. These features are critical to protecting data integrity, confidentiality, and availability. However, as the threat landscape evolves, Apple must improve these features and stay ahead of emerging threats.

One recommendation for improving the security of the macOS file system would be to provide more granular control over SIP. This would allow users to enable or disable certain protections based on their needs selectively. Another recommendation would be to provide better support for third-party backup solutions, giving users more flexibility in backing up their data.

macOS provides robust security features for the file system, and these features have a significant impact on application developers. As the threat landscape continues to evolve, Apple needs to improve these features and provide better support for third-party solutions.

References

1. Apple (2017) In-app purchased content is not deployed to managed devices, Apple Support. Available at: https: //support.apple.com/en-us/HT202996 (Accessed: March 3,2023)

2. Apple (2021) MacOS Ventura, Apple. Available at: https://www.apple.com/macos/big-sur/ (Accessed: March 3,2023)

3. Apple (2023) MacOS release notes, Apple Developer Documentation. Available at: https://developer.apple.com/documentation/macos-release-notes (Accessed: March 3,2023)

4. Apple (2021) Documentation archive, Apple Developer. Available at: https://developer.apple.com/library/archive/navigation/ (Accessed: March 3,2023)

5. Dansimp (2023) Windows Threat Protection, Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows/security/threat-protection/ (Accessed: March 3,2023)

6. Microsoft Corporation (2023) Windows 10, version 21H2, Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows/release-health/status-windows-10-21h2 (Accessed: March 3,2023)

7. Microsoft Support (2023) Microsoft, Microsoft Support. Available at: https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963 (Accessed: March 3,2023)

8. Vinaypamnani-Msft (2023) System guard secure launch and SMM protection (windows 10), (Windows 10) | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-system-guard/system-guard-secure-launch-and-smm-protection (Accessed: March 3,2023)

9. Apple Support. (n.d.). *Protecting against malware in macOS*. [online] Available at: https://support.apple.com/en-gb/guide/security/sec469d47bd8/web. (Accessed: March 3,2023)

10. Apple Support. (n.d.). *How does FileVault encryption work on a Mac?* [online] Available at: https://support.apple.com/en-gb/guide/mac-help/flvlt001/mac#:~:text=FileVault%20encodes%20the%20information%20stored (Accessed: March 3,2023)

11) MUO. (2021). *5 Important Security Features Built Into Your Mac*. [online] Available at: https://www.makeuseof.com/security-features-built-into-mac/. (Accessed: March 3,2023)

12) www.rainforestqa.com. (n.d.). *A deep dive into macOS TCC.db | Rainforest QA*. [online] Available at: https://www.rainforestqa.com/blog/macos-tcc-db-deep-dive (Accessed: March 3,2023)

13) Anon, (2022). *10 macOS Security Features You Need to Know - GizmoGrind*. [online] Available at: https://www.gizmogrind.com/blog/10-macos-security-features/. (Accessed: March 3,2023)

14) Apple Support. (n.d.). *About System Integrity Protection on your Mac*. [online] Available at: https://support.apple.com/en-gb/HT204899. (Accessed: March 3,2023)

15) Apple Support. (n.d.). *What is Keychain Access on Mac?* [online] Available at: https://support.apple.com/en-gb/guide/keychain-access/kyca1083/mac (Accessed: March 3,2023)

16) developer.apple.com. (n.d.). *Code Signing - Support - Apple Developer*. [online] Available at: https://developer.apple.com/support/code-signing/. (Accessed: March 3,2023)

17) Apple Support. (n.d.). *Intro to mobile device management profiles*. [online] Available at: https://support.apple.com/en-gb/guide/deployment/depc0aadd3fe/web#:~:text=MDM%20lets%20you%20securely%20and (Accessed: March 3,2023)

18) Apple Support. (n.d.). *Gatekeeper and runtime protection in macOS*. [online] Available at: https://support.apple.com/en-gb/guide/security/sec5599b66df/web. (Accessed: March 3,2023)

19) Apple Support. (n.d.). *Back up your Mac with Time Machine*. [online] Available at: https://support.apple.com/en-gb/HT201250.

20) developer.apple.com. (n.d.). *Access Control Lists*. [online] Available at: https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPFileSystem/Articles/ACLs.html (Accessed: March 3,2023)

21) vinaypamnani-msft (n.d.). *Microsoft Defender SmartScreen overview - Windows security*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview (Accessed: March 3,2023)

Github: https://github.com/ibby2002/secureos