FileVault Encryption for Mac Computers (macOS)

Mac computers include FileVault, a built-in encryption system that secures all data at rest using AES-XTS encryption.

How It Works

On Apple Silicon and T2 Macs:

- FileVault uses Data Protection Class C with a volume key
- Encryption leverages the Secure Enclave and AES engine hardware
- User credentials required at boot after enabling FileVault

Important: On older Macs (pre-T2), non-original internal storage, or external drives: Files created before enabling FileVault aren't encrypted and may be recoverable with forensic tools.

Internal Storage Security

FileVault Enabled

When FileVault is on, volumes remain encrypted even if the physical drive is removed. Without valid credentials or a recovery key, the data is inaccessible.

Encryption covers:

- macOS 10.15: Both system and data volumes
- macOS 11+: Data volume (system volume protected by signed system volume feature)

Key Management Apple Silicon and T2 Macs use a hierarchical key system that:

- Requires user password for decryption
- Protects against brute-force attacks on removed storage
- Enables instant secure data wiping
- Allows password changes without full reencryption

All key operations occur within the Secure Enclave—encryption keys never reach the CPU. Each APFS volume has a volume encryption key (VEK) that encrypts contents and metadata. The VEK is wrapped by a key encryption key (KEK), which is protected by both the user password and hardware UID.

FileVault Disabled

Even without FileVault, Apple Silicon and T2 Macs still encrypt volumes—but the VEK is protected only by the hardware UID. Enabling FileVault later is instant (data already encrypted) and adds an anti-replay mechanism to prevent the old hardware-only key from being used.

Secure Deletion

Deleting a volume triggers the Secure Enclave to securely erase its VEK, preventing future access. Additionally, all VEKs are wrapped with a media key. Erasing the media key (via MDM commands, for example) makes the volume cryptographically inaccessible.

External Storage

Removable drives don't use Secure Enclave capabilities—they're encrypted the same way as Intel Macs without T2 chips.

Revision #3
Created 7 November 2025 15:36:11 by Josh
Updated 7 November 2025 15:39:44 by Josh