Apple at Work

Platform Security

Secure by design.

At Apple, we care deeply about security—both for the user and for protecting corporate data. We've built advanced security into our products from the ground up, making them secure by design. And we've done this in a way that's in balance with a great user experience, giving users the freedom to work the way they want. Only Apple can provide this comprehensive approach to security, because we create products with integrated hardware, software, and services.

Hardware security

Secure software requires a foundation of security built into hardware. That's why Apple devices—running iOS, iPadOS, macOS, tvOS, or watchOS—have security capabilities designed into silicon.

These include custom CPU capabilities that power system security features and silicon dedicated to security functions. The most critical component is the Secure Enclave coprocessor in modern iOS, iPadOS, watchOS, and tvOS devices and in all Mac computers with the Apple T2 Security Chip. The Secure Enclave provides the foundation for encrypting data at rest, secure boot in macOS, and biometrics.

All modern iPhone, iPad, and Mac computers with a T2 chip include a dedicated AES hardware engine to power line-speed encryption as files are written or read. This ensures that Data Protection and FileVault protect users' files without exposing long-lived encryption keys to the CPU or operating system.

Secure boot of Apple devices ensures that the lowest levels of software aren't tampered with and that only trusted operating system software from Apple loads at startup. In iOS and iPadOS devices, security begins in immutable code called the Boot ROM, which is laid down during chip fabrication and known as the hardware root of trust. On Mac computers with a T2 chip, trust for secure boot begins with the Secure Enclave itself.

The Secure Enclave enables Touch ID and Face ID in Apple devices to provide secure authentication while keeping user biometric data private and secure. This enables users to enjoy the security of longer and more complex passcodes and passwords with, in many situations, the convenience of quickly authenticating.

The security features of Apple devices are made possible by the combination of silicon design, hardware, software, and services available only from Apple.

System security

Building on the unique capabilities of Apple hardware, system security is designed to maximize the security of the operating systems on Apple devices without compromising usability. System security encompasses the boot process, software updates, and the ongoing operation of the operating system.

Secure boot begins in hardware and builds a chain of trust through software, where each step ensures that the next is functioning properly before handing over control. This security model supports not only the default boot of Apple devices but also the various modes for recovery and updating iOS, iPadOS, and macOS devices.

The most recent versions of iOS, iPadOS, and macOS are the most secure. The software update mechanism not only provides timely updates to Apple devices—it also delivers only trusted software from Apple. The update system can even prevent downgrade attacks, so devices can't be rolled back to an earlier version of the operating system as a method of stealing user data.

Finally, Apple devices include boot and runtime protections so that they maintain their integrity during ongoing operation. These protections vary significantly between iOS, iPadOS, and macOS devices based on the very different sets of capabilities they support and the attacks they must therefore thwart.

To accomplish this level of protection, iOS and iPadOS use Kernel Integrity Protection, System Coprocessor Integrity, Pointer Authentication Codes, and Page Protection Layer, while macOS uses Unified Extensible Firmware Interface security, System Management Mode, Direct Memory Access protections, and peripheral firmware security.

Encryption and Data Protection

Apple devices have encryption features to safeguard user data and enable remote wipe in the case of device theft or loss.

The secure boot chain, system security, and app security capabilities all help to ensure that only trusted code and apps run on a device. Apple devices have additional encryption features to safeguard user data, even when other parts of the security infrastructure have been compromised–for example, if a device is lost or is running untrusted code. All of these features benefit both users and IT administrators, protecting personal and corporate information at all times and providing methods for instant and complete remote wipe in the case of device theft or loss.

iOS and iPadOS devices use a file encryption methodology called Data Protection, while the data on Mac computers is protected with a volume encryption technology called FileVault. Both models similarly root their key management hierarchies in the dedicated silicon of the Secure Enclave on devices that include a SEP. Both models also leverage a dedicated AES engine to support line-speed encryption and to ensure that long-lived encryption keys never need to be provided to the kernel OS or CPU, where they might be compromised.

App security

Apps are among the most critical elements of a modern security architecture. While apps provide amazing productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly. Apple provides layers of protection to ensure that apps are free of known malware and haven't been tampered with. Additional protections enforce the access of any user data from apps and carefully mediate that process.

Built-in security controls provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps for iOS, iPadOS, and macOS—all without impacting system integrity. And users can access these apps on their Apple devices with controls in place to help protect against viruses, malware, or unauthorized attacks.

On iPhone, iPad, and iPod touch, all apps are obtained from the App Store—and all apps are sandboxed—to provide the tightest controls. 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 on macOS 10.15 or later, all Mac apps need to be notarized by Apple to launch. This requirement ensures that these apps are free of known malware without requiring that the apps be provided through the App Store. In addition, macOS includes industry-standard 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 sandboxed—which ensures 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.

Services security

Apple has built a robust set of services to help users get even more utility and productivity out of their devices. These services include Apple ID, iCloud, Sign in with Apple, Apple Pay, iMessage, FaceTime, Siri, and Find My. These services provide powerful capabilities for cloud storage and sync, authentication, payment, messaging, communications, and more, all while protecting users' privacy and the security of their data.

Partner ecosystem

Apple devices work with common corporate security tools and services, ensuring the compliance of devices and the data that resides on them. Each platform supports standard protocols for VPN and secure Wi-Fi to protect network traffic, and securely connect to common enterprise infrastructure.

Apple's partnership with Cisco provides enhanced security and productivity when paired together. Cisco networks provide enhanced security via the Cisco Security Connector and grant priority to business applications on Cisco networks.

Find out more about security with Apple devices.

apple.com/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/security