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 its 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, as well as additional silicon that's dedicated to security functions. Security-focused hardware follows the principle of supporting limited and discretely defined functions in order to minimize attack surface. Such components include a boot ROM, which forms a hardware root of trust for secure boot, dedicated AES engines for efficient and secure encryption and decryption, and a Secure Enclave.

The Secure Enclave is a system on chip (SoC) that is included on all recent generation iPhone, iPad, Apple Watch, Apple TV, and HomePod devices and on a Mac with Apple silicon as well as those with the Apple T2 Security Chip. The Secure Enclave follows the same principle of design as the SoC does, containing its own discrete boot ROM and AES engine. The Secure Enclave also provides the foundation for the secure generation and storage of the keys necessary for encrypting data at rest, and it protects and evaluates the biometric data for Touch ID and Face ID.

Storage encryption must be fast and efficient. At the same time, it can't expose the data (or keying material) it uses to establish cryptographic keying relationships. The AES hardware engine solves this problem by performing fast in-line encryption and decryption as files are written or read. A special channel from the Secure Enclave provides necessary keying material to the AES engine without exposing this information to the application processor (or CPU) or overall

operating system. This ensures that the Apple Data Protection and FileVault technologies protect users' files without exposing long-lived encryption keys.

Apple has designed secure boot to protect the lowest levels of software against tampering and to allow only trusted operating system software from Apple to load at startup. Secure boot begins in immutable code called the Boot ROM, which is laid down during Apple SoC fabrication and is known as the hardware root of trust. On Mac computers with a T2 chip, trust for macOS secure boot begins with the T2. (Both the T2 chip and the Secure Enclave also execute their own secure boot processes using their own separate boot ROM—this is an exact analogue to how the A-series and M1 chips boot securely.)

The Secure Enclave also processes fingerprint and face data from Touch ID and Face ID sensors in Apple devices. This provides secure authentication while keeping user biometric data private and secure. It also enables users to benefit from the security of longer and more complex passcodes and passwords with, in many situations, the convenience of swift authentication for access or purchases.

These Apple device security features 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 responsible for controlling access to system resources in Apple devices without compromising usability. System security encompasses the boot-up process, software updates, and protection of computer system resources such as CPU, memory, disk, software programs, and stored data.

The most recent versions of Apple operating systems are the most secure. An important part of Apple security is secure boot, which protects the system from malware infection at boot time. 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 timely updates on Apple devices. Subcomponents like the T2 chip and the Secure Enclave also perform their own secure boot to help ensure they only boot known-good code from Apple. The update system can even prevent downgrade attacks, so that devices can't be rolled back to an older version of the operating system (which an attacker knows how to compromise) as a method of stealing user data.

Apple devices also include boot and runtime protections so that they maintain their integrity during ongoing operation. Apple-designed silicon on iPhone, iPad, Apple Watch, Apple TV, and HomePod, and a Mac with Apple silicon, provide a common architecture for protecting operating system integrity. macOS also features an expanded and configurable set of protection capabilities in support of its differing computing model, as well as capabilities supported on all Mac hardware platforms.

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 verify 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 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, whereas the data on an Intel-based Mac is protected with a volume encryption technology called FileVault. A Mac with Apple silicon uses a hybrid model that supports Data Protection, with two caveats: The lowest protection level (Class D) isn't supported, and the default level (Class C) uses a volume key and acts just like the FileVault on an Intel-based Mac. In all cases, key management hierarchies are rooted in the dedicated silicon of the Secure Enclave, and a dedicated AES engine supports line-speed encryption and helps ensure that long-lived encryption keys aren't exposed to the kernel operating system or CPU (where they might be compromised). (An Intel-based Mac with a T1 chip or lacking a Secure Enclave doesn't use dedicated silicon to protect its FileVault encryption keys.)

Besides using Data Protection and FileVault to prevent unauthorized access to data, Apple operating system kernels enforce protection and security. The kernel uses access controls to sandbox apps (which restricts what data an app can access) and a mechanism called a Data Vault (which restricts access to the data of an app from all other requesting apps rather than restricting the calls an app can make).

App security

Apps are among the most critical elements of a security architecture. Even as 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.

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, and macOS—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 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 in macOS 10.15 or later, all Mac apps need to be notarized by Apple to launch. This requirement helps to ensure that these apps are free of known malware without requiring that the apps be provided through the App Store. In addition, 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.

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 provide powerful capabilities for cloud storage, sync, password storage, authentication, payment, messaging, communications, and more, all while protecting users' privacy and the security of their data.

These services include iCloud, Sign in with Apple, Apple Pay, iMessage, Business Chat, FaceTime, Find My, and Continuity and may require an Apple ID or Managed Apple ID. In some cases, a Managed Apple ID can't be used with a specific service like Apple Pay.

Note: Not all Apple services and content are available in all countries or regions.

Network security overview

In addition to the built-in safeguards Apple uses to protect data stored on Apple devices, there are many measures organizations can take to keep information secure as it travels to and from a device. All of these safeguards and measures fall under network security.

Users must be able to access corporate networks from anywhere in the world, so it's important to ensure that they are authorized and that their data is protected during transmission. To accomplish these security objectives, iOS, iPadOS, and macOS integrate proven technologies and the latest standards for both Wi-Fi and cellular data network connections. That's why our operating systems use—and provide developer access to—standard networking protocols for authenticated, authorized, and encrypted communications.

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—including per account VPN connections on iOS and iPadOS 14—and secure Wi-Fi to protect network traffic, and securely connects to common enterprise infrastructure.

Apple's partnership with Cisco provides enhanced security and productivity when paired together. Cisco networks provide enhanced security through 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