iOS Security Overview

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 to make them secure by design. And we've done this in a way that's in balance with a great user experience, allowing individuals 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.

Secure by design

iOS devices include advanced features to protect the entire system, secure all apps running on the platform, and ensure that corporate and personal data is encrypted and managed seamlessly. These features provide comprehensive security right out of the box.

System security. iOS is designed so both software and hardware are secure across all core components of every iOS device.

- From the moment a device is turned on, iOS ensures a secure startup process. The system is further verified through device activation.
- iOS makes it easy for IT to manage system software updates to address security concerns. All software updates are authorized to ensure that only software provided by Apple is installed.
- Extensive system safeguards are available, including strong passcode policies and innovative features such as Touch ID and Face ID so that only authorized users can access the device.

Data security. iOS provides robust and powerful methods for managing and protecting data at all times.

- iOS devices come with a dedicated hardware processor and use AES-256 encryption enabled out of the box.
- File-level data protection uses strong encryption keys derived from the user's unique passcode.
- iOS uses proven technologies to connect to corporate networks seamlessly and securely, protecting data during transmission.

App security. A complete security model for iOS apps protects against malware, malicious code, and concerns that data or privacy could be unknowingly compromised.

- Apple verifies the identity of all developers before they can participate in an Apple developer program.
- Apps in the App Store are reviewed by Apple to ensure that they don't contain significant bugs, don't compromise user privacy, and operate according to clear guidelines.
- In-house apps must be signed and provisioned with a certificate provided by Apple through the Apple Developer Enterprise Program.
- With runtime protection, sandboxing, and entitlements built into iOS, users can download, install, and run apps knowing that they're accessing data only in authorized ways.

Freedom to work

Comprehensive security is built into iOS devices, giving employees the freedom to work. Users can personalize their devices to help them be even more productive. And iOS preserves user privacy while seamlessly protecting and separating work and personal data.

Personalization. iOS makes it easy for users to set up their own devices through a simple, streamlined process that can be further automated using Apple's Device Enrollment Program (DEP) and mobile device management (MDM) tools.

- With iOS Setup Assistant, users can activate their devices, configure basic settings, and start working right away.
- Users can log in with their own Apple ID for a personalized experience; enterprise data doesn't back up content to iCloud, but personal data does; and locate a missing device using Find My iPhone.

Separation. iOS and MDM solutions provide smart ways to manage corporate data and apps discretely, while seamlessly separating work and personal data.

- There's no need for containers or dual workspaces that frustrate users and degrade the user experience.
- Corporate accounts, apps, content, settings and contacts that are installed via an MDM solution are considered "managed" by iOS and can be removed by IT at any time, without impacting personal data.
- Networking features such as Per App VPN ensure that traffic from corporate apps goes through the corporate network and that personal traffic goes through the public network.
- Features such as Managed Open In can be used to control the flow of corporate data between apps and prevent documents from being saved to the user's personal apps or cloud services. This also applies to document provider extensions.

Privacy. Enterprise data remains within IT's control, and personal data—like messages, location data, photos, and iCloud data—remains private.

- Apple builds extensive safeguards into apps, Internet services, and iOS so that strong privacy measures are constantly at work protecting corporate information.
- Developers can leverage tools such as Touch ID APIs, 256-bit encryption, and app transport security to build secure apps. Apple also requires developers to ask for permission before accessing personal information like contacts.

Additional Resources: iOS Security Paper | Face ID Security Guide | Privacy Webpage