Apple at Work

平台安全性

講求安全性的設計。

Apple 高度重視安全性，不僅從使用者的角度，也兼顧對企業資料的保護。從產品設計之初，我們已將先進安全功能內建其中，打造講求安全性的設計。同時，我們也不忘兼顧安全性與絕佳使用者體驗之間的平衡，讓使用者享有高度自由，以想要的方式來工作。只有 Apple，才能提供如此全面的安全防護措施，因為我們所打造的產品，皆是硬體、軟體與服務高度整合的結晶。

硬體安全性

安全的軟體，需以硬體內建的安全性基礎為後盾。也因此每部 Apple 裝置，不論搭載的是 iOS、iPadOS、macOS、tvOS 或 watchOS，都將安全功能設計整合於晶片之中。

其中包括自訂 CPU 功能，可支援系統安全功能和安全功能專用的晶片。最重要的元件是安全隔離區協同處理器，已建置於較新款的 iOS、iPadOS、watchOS 和 tvOS 裝置，以及配備 Apple T2 安全晶片的所有 Mac 電腦之中。安全隔離區提供基礎，可為儲存資料、macOS 中安全開機，以及生物辨識資料進行加密。

所有較新款的 iPhone、iPad 和配備 T2 晶片的 Mac 電腦都包含專用的 AES 硬體引擎，可在寫入或讀取檔案時提供線速加密。如此一來就能確保「資料保護」和「檔案保險箱」充分保護使用者的檔案，又不會將可長效使用的加密密鑰暴露給 CPU 或作業系統。

Apple 裝置的安全開機功能，則可確保底層軟體不會遭到篡改，且只有 Apple 推出的受信任作業系統軟體才能在開機時載入。iOS 和 iPadOS 裝置的安全性，始於晶片製造階段即已鋪設的不可變更程式碼 Boot ROM，也稱為硬體信任根。在配備 T2 晶片的 Mac 電腦上，安全隔離區本身就是安全開機信任鏈的開端。

安全隔離區讓 Apple 裝置中的 Touch ID 和 Face ID 得以提供安全認證，同時讓使用者生物辨識資料保持私密且安全。因此，使用者得以享有更長、更複雜的密碼帶來的安全性，還能在很多狀況下享受快速認證的便利性。

Apple 獨家提供的晶片設計、硬體、軟體與服務相輔相成，成就了 Apple 裝置固若金湯的安全功能。

系統安全性

系統安全性以 Apple 硬體獨特的功能性為建置基礎，最大化提升 Apple 裝置作業系統的安全性，且不影響其易用性。系統安全性包含開機程序、軟體更新，以及作業系統的持續運作。

安全開機從硬體開始，然後透過軟體建立信任鏈，每個步驟都先確保下一步運作正常，再交出控制權。這種安全模式不但支援 Apple 裝置的預設開機，也支援各種恢復模式與 iOS、iPadOS 和 macOS 裝置的更新。

最新版本的 iOS、iPadOS 和 macOS 最為安全。軟體更新機制不但為 Apple 裝置提供適時的更新，而且只遞送來自 Apple 的受信任軟體。更新系統還可以防止降級攻擊，讓裝置無法退回到舊版作業系統，以免有心人藉此竊取使用者資料。

最後，Apple 裝置包含開機和執行階段保護，因而能在持續運作期間維持完整性。這些保護在 iOS、iPadOS 與 macOS 裝置之間，根據所支援的不同功能組合，以及必須因應與阻擋的攻擊，而有相當大的差異。

為達到這種層級的保護，iOS 與 iPadOS 運用核心完整性保護 (Kernel Integrity Protection)、系統協同處理器完整性 (System Coprocessor Integrity)、指標認證碼 (Pointer Authentication Codes) 以及頁面保護層 (Page Protection Layer)，而 macOS 則是運用統一可延伸韌體介面 (Unified Extensible Firmware Interface) 安全性、系統管理模式 (System Management Mode)、直接記憶體存取 (Direct Memory Access) 保護，以及周邊裝置韌體安全性。

加密與資料保護

Apple 裝置具備加密功能，可保護使用者資料安全，並能在裝置遭竊或遺失時進行遠端清除。

安全開機鏈、系統安全性和 app 安全功能，皆有助於確保唯有受信任的程式碼和 app 可在裝置上執行。Apple 裝置具有額外的加密功能，可保護使用者資料安全，即使安全基礎設施其他部分遭入侵，如裝置遺失或執行不受信任的程式碼，還是能保護資料。這些功能都可讓使用者和 IT 管理者受益、隨時保護個人和公司資訊，並在裝置遭竊或遺失時，提供多種方法可即時完整地進行遠端清除。

iOS 和 iPadOS 裝置使用稱為「資料保護」的檔案加密方法，而 Mac 電腦上的資料則是使用稱為「檔案保險箱」的卷宗加密技術來進行保護。這兩種模式頗為相似，都是讓密鑰管理階層架構，以包含 SEP 的裝置上安全隔離區的專用晶片為其根基。兩種模式也都以專用的 AES 引擎來支援線速加密，並確保不需將可長效使用的加密密鑰提供給核心 OS 或 CPU，藉此避免密鑰遭到洩露。

App 安全性

App 是現代化安全架構中，最重要的元素之一。雖然 app 能提供使用者驚人的生產力助益，但是如果處理不當，也可能會對系統安全性、穩定性及使用者資料造成負面衝擊。Apple 提供多層保護來確保 app 不會遭受已知惡意軟體攻擊，而且未曾遭到篡改。從 app 存取使用者資料時則由額外的保護機制負責執行，並謹慎小心地居中調解整個流程。

內建安全控制項目為 app 提供穩定安全的平台，讓數以千計的開發者遞交成千上萬適用於 iOS、iPadOS 和 macOS 的 app，完全不會影響到系統完整性。使用者也可以在 Apple 裝置上存取這些 app，並有控管機制來協助保護，免於遭受病毒、惡意軟體或未經授權來源的攻擊。

在 iPhone、iPad 和 iPod touch 上，所有 app 都能從 App Store 取得，而且所有 app 都進行沙箱處理，以提供最嚴密的控管。在 Mac 上，有許多 app 是從 App Store 取得，但 Mac 使用者也會從 Internet 下載並使用各種 app。為了安全地支援 Internet 下載，macOS 設置了多層額外控制。首先，在 macOS 10.15 或後續版本中，已預設所有 Mac app 都必須經過 Apple 公證才能啟動。這個必要條件確保這些 app 沒有任何已知惡意軟體，而且並未要求這些 app 須源自 App Store 所提供。此外，macOS 內含業界標準的防毒保護，能阻擋並在需要時移除惡意軟體。

此外，在跨平台的額外控制當中，沙箱處理有助保護使用者資料，避免遭 app 未經授權存取。而且在 macOS 中，重要區域內的資料本身就已經過沙箱處理，可確保從所有 app 存取桌面、文件、下載項目及其他區域中的檔案，使用者仍保有完整的控制權，不論試圖存取的 app 本身是否經過沙箱處理。

服務安全性

Apple 建立了一系列可靠的服務，幫助使用者更充分發揮裝置的工具程式和生產力功能。這些服務包括 Apple ID、iCloud、使用 Apple 登入、Apple Pay、iMessage、FaceTime、Siri，以及「尋找」功能。這些服務提供強大的功能性，可進行雲端儲存和同步、認證、付款、傳訊、通訊等運作，同時也都能保護使用者的隱私權與資料的安全。

合作夥伴生態系統

Apple 裝置能與業界常用的公司安全工具和服務搭配運作，確保裝置及其中儲存的資料都能合乎規範。每個平台都支援 VPN 與安全 Wi-Fi 的標準通訊協定，以保護網路流量，並安全地連線到共通的企業基礎設施。

Apple 與 Cisco 建立的合作夥伴關係，相輔相成提供更高的安全性和生產力。Cisco 網路透過 Cisco Security Connector，提供更強大的安全性，並授予 Cisco 網路上的商務應用程式優先權。

進一步了解 Apple 裝置的安全性。

apple.com/tw/business/it

apple.com/tw/macos/security

apple.com/tw/privacy/features

https://support.apple.com/zh-tw/guide/security/welcome/web