Apple at Work

平台安全

安全，从设计做起。

在 Apple，我们非常关注安全性，既为了确保用户安全，也为了保护企业数据。我们在产品中全面内置了高级安全功能，从设计上保证它们的安全性。在实现这一点的同时，我们还兼顾了出色的用户体验，使用户能够按照他们期望的方式自由地工作。只有 Apple 能够提供这种全方位的安全保护方案，因为我们制造的产品将硬件、软件和服务融为一体。

硬件安全

要确保软件的安全，就要先在硬件中内置强大的安全基础。因此，运行 iOS、iPadOS、macOS、或 watchOS 的 Apple 设备从芯片设计开始就考虑了安全功能。

其中包括可支持系统安全功能的自定义 CPU 功能，以及专为安全功能设计的芯片。在新款 iOS、iPadOS、watchOS 以及配备 Apple T2 安全芯片的所有 Mac 电脑中，最关键的组件就是安全隔区协处理器。安全隔区为加密静态数据、在 macOS 中安全启动以及生物识别技术提供了坚实基础。

所有新款 iPhone、iPad 和采用 T2 芯片的 Mac 电脑都配备了专用 AES 硬件引擎，可在写入或读取文件时执行线速加密。这样能够确保“数据保护”和文件保险箱会保护用户的文件，避免了将长期加密密钥暴露给 CPU 或操作系统。

Apple 设备的安全启动可以确保最底层软件不会被篡改，而且只有来自 Apple 的受信任操作系统软件才能在开机时加载。在 iOS 和 iPadOS 设备中，安全性源自名为 Boot ROM 的不可变代码，它是在制造芯片时写入的，被称为硬件信任根。在配备 T2 芯片的 Mac 电脑上，对安全启动的保障则源自安全隔区自身。

安全隔区使得 Apple 设备中的触控 ID 和面容 ID 在提供安全验证的同时，确保用户生物特征数据的私密和安全。它所提供的安全性与更长、更复杂的口令和密码相当，同时，用户在很多情况下可以方便快捷地进行身份验证。

Apple 设备的安全功能是通过 Apple 独有的芯片设计、硬件、软件和服务共同结合来实现的。

系统安全

系统安全建立在 Apple 硬件的独特功能基础之上，能够在不降低易用性的前提下，最大限度地提高 Apple 设备操作系统的安全性。系统安全包括启动过程、软件更新以及操作系统持续运行时的安全。

安全启动从硬件开始，通过软件建立信任链，其中每一步都会在确保下一步可以正常执行后才会移交控制权。这一安全模式不仅支持 Apple 设备的默认启动，还支持用于恢复和更新 iOS、iPadOS 和 macOS 设备的各种模式。

最新版本的 iOS、iPadOS 和 macOS 的安全性非常出众。软件更新机制不仅为 Apple 设备提供及时更新，而且仅提供来自 Apple 的受信任软件。更新系统甚至可以防止降级攻击，这样，设备就不会被恢复到更早版本的操作系统，以防通过这种方式来窃取用户数据。

最后，Apple 设备还配置了启动和运行时保护机制，可在持续运行期间确保其完整性。iOS、iPadOS 和 macOS 设备支持的功能各有不同，要阻挡的攻击也不同，因此他们的保护机制之间存在显著差异。

为了实现这种级别的保护，iOS 和 iPadOS 使用了内核完整性保护、系统协处理器完整性、指针验证码和页面保护层，而 macOS 则使用了统一可扩展固件接口安全性、系统管理模式、直接内存访问保护和外围固件安全。

加密和数据保护

Apple 设备配有加密功能来保护用户数据，在设备丢失或被盗的情况下可以进行远程擦除。

安全启动链、系统安全和 app 安全功能都有助于确保设备上只运行受信任的代码和 app。Apple 设备还配有其他加密功能来保护用户数据，即使在安全基础架构的其他部分已经遭到攻击的情况下 (例如设备丢失或正在运行不受信任的代码) 仍能保护数据。所有这些功能都为用户和 IT 管理员带来了益处，随时保护个人和企业信息，并在设备被盗或丢失的情况下提供多种方法来进行即时、彻底的远程擦除。

iOS 和 iPadOS 设备使用名为“数据保护”的文件加密方法，而 Mac 电脑上的数据则采用名为“文件保险箱”的宗卷加密技术进行保护。这两种模式都同样将它们的密钥管理层次结构根植于带有 SEP 的设备上的安全隔区专用芯片。这两种模式还利用了专用的 AES 引擎支持线速加密，并确保永远不需要向操作系统内核或 CPU 提供长期加密密钥，以免在这些位置遭到入侵。

App 安全

App 是现代安全架构最关键的要素之一。尽管 app 可显著提高用户的工作效率，但如果处理不当，也可能会对系统安全、稳定性和用户数据产生负面影响。Apple 提供的保护层可确保 app 没有感染任何已知恶意软件，而且没有遭到篡改。访问 app 中任意用户数据时会执行其他保护措施，而且这些措施会谨慎调解该过程。

内置安全控制为 app 提供了安全稳定的平台，使得成千上万的开发者能够为 iOS、iPadOS 和 macOS 提供数十万款 app，而不会影响系统完整性。用户可以在他们的 Apple 设备上访问这些 app，并通过设置好的控制措施来保护他们免受病毒、恶意软件或未经授权的攻击。

在 iPhone、iPad 和 iPod touch 上，所有 app 都要从 App Store 中获取，而且所有 app 都已经过沙箱化处理，以实现严格的控制。在 Mac 上，许多 app 都要从 App Store 获取，但 Mac 用户仍可以从互联网上下载并使用 app。为了确保互联网下载的安全性，macOS 将其他控制措施进行了分层。首先，在 macOS 10.15 或更新版本中，所有 Mac app 都默认需要获得 Apple 公证后才能启动。这一要求可确保这些 app 没有感染已知的恶意软件，而且也不要求通过 App Store 提供这些 app。此外，macOS 中包含符合行业标准的防病毒保护机制，可阻止和删除 (如有必要) 恶意软件。

作为跨平台的一项额外控制手段，沙箱技术有助于防止未经授权的 app 访问用户数据。在 macOS 中，关键位置的数据本身都已进行沙箱化处理，这样，无论要尝试访问的 app 本身是否已经完成沙箱化处理，都能确保用户仍然可以控制所有 app 对“桌面”、“文稿”、“下载”及其他位置的文件的访问。

服务安全

Apple 开发了一系列功能强大的服务，可帮助用户更充分地使用设备并提高工作效率。这些服务包括 Apple ID、iCloud、使用 Apple 登录、Apple Pay、iMessage 信息、FaceTime 通话、Siri 和查找。这些服务提供了强大功能以实现云存储和同步、身份验证、付款、信息、通信等等，同时也保护了用户的隐私及其数据的安全。

合作伙伴生态系统

Apple 设备与通用企业安全工具和服务配合使用，确保设备及存储在设备中的数据符合规定。每个平台都支持 VPN 和安全 Wi-Fi 标准协议，以保护网络流量并安全地连接到通用企业基础架构。

在配合运行时，Apple 与 Cisco 的合作关系可以增强安全性并提升效率。Cisco 网络通过 Cisco Security Connector 增强安全性，并对 Cisco 网络上的商务应用程序给予优先权。

进一步了解 Apple 设备的安全性。

www.apple.com.cn/business/it/

www.apple.com.cn/macos/security/

www.apple.com.cn/privacy/features/

support.apple.com/zh-cn/guide/security/welcome/web