JAMF software
企业概要

苹果本机安全

以少胜多

面对不断演变的威胁，保障企业资料安全是一场永不止息的战斗。攻击者手法层出不穷，攻击媒介亦在不断进化。企业经常添置新的装置设备，威胁亦随日而增。要解决这安全挑战的一个方法就是使用苹果装置平台，充分利用苹果本机的安全框架。对于现代化、流动性高的办公团体，这个方法能在不影响用户体验下全面保卫装置的安全。

流动装置安全的四大支柱

保卫流动电脑（不管是笔记本电脑、智能手机还是平板电脑）都需要认真注意以下四个关键领域：

1. 静态数据—保护装置上的数据安全
2. 传送中的数据—保护以络传输数据到装置时的安全
3. 应用程式安全—从安全的来源安装可信的软件
4. 修补—不断更新软件以避免漏洞

要透彻可靠地保障组织讯息科技安全，另外还有有三个方面至关重要：

- 装置管理—部署、应用、分发、执行安全策略
- 报告—所有装置的库存及其设置
- 审核与补救—审核是否符合安全标准与在需要时用以补救的工具

苹果如何确保流动装置安全

JAMF software
企业概要

硬件加密

VPN

苹果App Store
生态系统

本机软件修补
工具

若无需要，何必再添一层防护？

系统越复杂，系统安全越难保障。每添加一层复习性都会导致新故障、新漏洞及潜在冲突的出现，让攻击者有机可乘的。在 IT 领域，复杂性经常以附加软件层次的形式出现。IT 安全软件行业为装置安全的四大支柱提供了许多解决方案，但这些方案往往非常复杂。拥有本机安全控制的电脑系统通常是较容易管理，而且本身亦更安全。通过整合安全框架跟操作系统，更新便变得简单轻松，复杂性也能降至最低。

苹果的本机安全一路领先

苹果公司在设计及直观功能上引领全行，但不太为人所知的是苹果为 iOS 和 OS X 作业系统设置的本机安全框架。过去数年，苹果大大提高了Mac电脑、iPad 及 iPhone 的保密门槛。今时今日，若论苹易用性、隐私控制及资讯科技安全，没有任何桌上或流动系统平台的能与苹果匹敌。

苹果科技如何巩固四大支柱

苹果的 OS X (Mac) 及 iOS (iPhone, iPad) 作业系统内含针对以上四大支柱而设的本机安全控制：

1. 静态数据 — iPhone 和 iPad 内有为静态数据而设的预设启动硬件加密技术。至于Mac装置，全磁盘加密系统 FileVault（OS X的一个本机功能）能在不影响系统表现或电池寿命的情况下保护数据。
2. 传送中的数据 — 苹果装置可以通过 VPN（虚拟专用网络）保卫传送中的数据安全。要使用这个安全功能不需要加装任何软件，一旦配置便能轻易使用 。
3. 应用程式安全 — 苹果公司对IT安全领域其中一个最大的贡献就是其 App Store 生态系统。 苹果会审查所有提交到 App Store 的软件并剔除恶意软件。每个软件包都被加密签署，以防止文件遭篡改。 OS X 和 iOS 作业系统会拒绝任何没有加密签署的软件。IT 人员亦可可以登录自己的软件包，加以利用此应用安全层。
4. 修补—自电脑的出现，所有软件都包含一定数量的缺陷或漏洞。这些缺陷有些可以被恶意攻击者利用窃取信息。保卫资讯科技安全的最佳办法是确保所有的软件获得更新，在发现安全漏洞时将之消除。 苹果内置OS本机软件修补工具令这工作变得简单。IT人员可在企业网络上安装 Apple Software Update Server（苹果软件更新服务器）加快修补。

本机安全管理好

苹果本机安全控制使用方便，一经配置用户便不需操心，非常适合个人或小企业使用。就大型组织而言，流动装置管理工具是配置、部署和审核安全配置不可或缺的。 JAMF Software的卡斯帕套件专为苹果平台而设，能融合所有苹果本机安全控制。它具有一套完整的部署和配置工具、动态库存集和审核及修复能力。

总结

确保组织信息科技安全不一定是个复杂繁琐的工序。在过去十年，苹果构建了一个集装置、软件和服务于一身的丰富生态系统，为个人电脑用家提供了最佳的用户体验。同时，苹果作业系统内含的本机安全控制能够提供一个企业级安全框架，配以苹果科技为中心的管理工具卡斯帕套件，苹果的生态系统即能为最终用户和资讯科技安全人员送上最佳的体验。

想了解更多有关苹果本机安全控制及卡斯帕套件的资料，请浏览
www.jamfsoftware.com/zh

想进一步体验卡斯帕套件？欢迎申请试用

jamfsoftware.com/zh/request-trial

Level 12, Infinitus Plaza,
199 Des Voeux Road Central
Sheung Wan, Hong Kong

电话：+852 3008-5865
www.jamfsoftware.com/zh
asia.enquiries@jamfsoftware.com