jamf

白皮书

有关企业中 Apple 设备的安全注意事项。

本白皮书讨论了常见的安全问题，并解释了组织机构需要了解的、有关 Apple 平台的各项信息，以便其内部团队在向工作环境中添置 Apple 设备之前，充分了解有关安全的最佳实践。

其中涵盖以下主题：

- Apple 设备管理方法
- Apple 设备的专属安全特性
- 添加新 Apple 设备时需要考虑的事项
- 可通过哪些 Apple 集成内容来利用您的现有资源

Apple 生态系统的结构

我们应该如何进行 Apple 设备管理?

Apple 公司采用集成方式设计了 iOS 和 macOS 平台的硬件、软件和服务，并在设计方案中确保了上述产品的安全性，使 IT 团队可以轻松进行配置、部署和管理。员工们在工作中使用 iPhone、iPad 和 Mac 时能够获得始终如一的使用体验；同样，IT 人员在为员工管理这两个平台时也会获得类似的体验。

Apple 可通过特定的企业程序简化设备的部署过程并优化其安全性，从而为用户提供开箱即用型体验。Apple 将其设备注册程序 (DEP) 和批量购买方案 (VPP) 与移动设备管理 (MDM) 相结合，可为 Mac、iPad、iPhone 和 Apple TV 设备提供始终如一的管理和防护。

许多组织机构都在寻求用一种工具来满足 Apple、Microsoft 和 Google 设备的全部需求。这使得组织机构在管理、用户体验和安全性方面存在缺口。使用单一的管理工具来管理多个平台时，各个安全特性将无法正常发挥作用，同时 Apple 设备专属功能的优势也将消失。

Apple 框架

为了阐明 Apple 所采用的安全措施，我们必须先来了解一下 Apple 框架的基础知识。

Apple 设备管理与 Microsoft 设备管理的区别

Apple 与传统的 Microsoft 端点管理有何不同

Apple 设备易于使用的关键在于其内置的管理框架，即移动设备管理 (MDM)。IT 人员可通过 MDM 构建相关配置文件，用来定义操作系统内部的各项设置。这些配置文件可通过 Apple 推送通知服务 (APN) 进行 OTA 传输。APN 可保证与 Apple 设备之间的稳定连接，为 IT 人员省去繁琐的连接操作。传统的 Windows 管理员仅能通过绑定或组策略对象 (GPO) 来实现 MDM 所支持的管理功能。

APN 会影响我们的安全状况吗?

APN 是一种用来向 iOS、watchOS、tvOS 和 macOS 设备传播信息的服务，既安全又高效。APN 是实现 Apple 部署程序和其他安全特性（如远程锁定和远程擦除）的关键一环。如果事实如此，则 Apple 相关程序（如 DEP、VPP 或 MDM）在没有 APN 的情况下将无法正常工作，原因是这些程序无法通过代理连接加以利用。您必须通过 Apple 设备的直接通道（即 APN）访问这些程序。

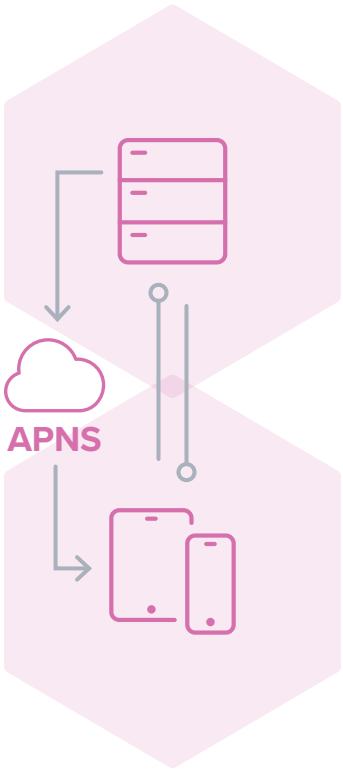
以下是 APN 的其他优势:

- 提高了管理企业 Apple 资产的安全等级。APN 支持对丢失/被盗/受损设备进行 OTA 远程锁定/擦除操作。
- MDM 依靠 APN 发送软件安装或库存更新等关键命令。
- 尽管您可以将 MDM 配置文件负载“离线”传送至 macOS, 但此方法所产生的间接费用要高于 OTA 方法。
- APN 会触发每台设备, 使其自动检入 MDM 服务器。

这种独特技术看似对安全性提出了挑战，实则会为您带来诸多好处。
如今，Google 和 Microsoft 的许多服务开始要求提供与 APN 相同的信任级别和直接连接。Cisco 面向 iOS 设备的 VOIP 解决方案要依靠 APN 来推送消息和 Callkit。APN 对设备安全和用户体验而言至关重要。App Store、iCloud 身份验证和 Internet 恢复等服务在没有 APN 的情况下将部分（或完全）无法运行。如果您按照 Apple 设备的规格开放端口，则一切都将回归正常。

详细信息请参阅 Apple 的网站: https://help.apple.com/deployment/macos/#/ior9d28751c0.

Apple 推送通知服务器架构



Apple 是否需要第三方安全软件

不同于 Windows 或 Android 的是，Apple 设备不常使用额外的安全层或第三方附加工具。

以 Windows 为中心的传统安全公司往往落后于 Apple 设备的开发周期，这可能会减慢应用新操作系统和新安全特性的速度。事实上，对 Apple 平台另眼相待通常会对员工的工作效率造成影响，并破坏 Apple 设备引以为傲的人性化用户体验。另外，在 Apple 设备上应用 Windows 版本的软件将导致代码执行不畅、内存占用以及基于内核扩展 (KEXT) 的种种隐患，从而引发大量 IT 和安全问题。

Apple 设备内置了加密和防病毒功能，这使得许多组织机构可以在没有第三方介入的情况下运行设备，但仍有一些组织机构在寻找相应方案，以解决公司的数据泄露问题。我们可以通过 MDM 来监控企业数据泄漏情况，并利用 Cisco Security Connector 等工具在网络端提供额外保护。

2018 年 2 月，Cisco、Apple、Aon 和 Allianz 推出了首个企业网络风险管理解决方案，其中包括来自 Aon 的网络弹性评估服务、来自 Cisco 和 Apple 的最安全的技术、以及来自 Allianz 的增强型网络保险选项。有关此次合作的详细信息，请阅读 Apple 网站上的完整公告。

管理 Apple 设备时的体验如何?

一直以来，传统的 IT 思维模式始终是“我们用来管理 Apple 设备的工具不具备 Windows 设备管理工具的品质。”这种看法，加上 Apple 设备比其他平台更难以管理的错误观念，让许多组织机构对 Apple 望而却步。

然而，相关调查显示，Apple 实际上比其他平台更容易管理。Dimensional Research 发起的一项调查表明，66% 的受访者表示 Mac 比 PC 的安全系数更高，而 90% 的受访者表示 iOS 比其他平台的安全系数更高。当被问及 Apple 设备是否易于部署、配置和支持时，受访者也给出了相同的答案。

行业巨头 IBM 正是诸多决定提供 Apple 平台员工选择计划的企业之一。事实上，IBM 现任首席信息官 Fletcher Previn 已经证实，IBM 所选用的每台 Mac 都比 PC 要更节省成本。

这种情况也表明，企业渴望获得一致性部署和用户体验。而 Apple 将这种一致性和安全性变为了现实。

66%

的组织机构认为 Mac 比 PC 更加安全

90%

的组织机构认为 iOS 比其他平台更加安全

Apple 生态系统的专属安全特性

macOS 内置了哪些安全特性?
macOS 的基础由集成式安全软件构成。

以下是内置的 macOS 系统安全特性:

- FileVault 是 macOS 内置的一个额外的加密层, 可在设备丢失或被盗时保护用户数据。
- Apple 直接提供软件更新及其数字签名, 方便组织机构和 IT 人员将其判断为可信信息。
- 系统完整性保护 (SIP) 可用于保护核心的操作系统文件, 否则这些文件可能成为用户和应用程序访问的利用目标。
- IT 人员可以通过 Gatekeeper 定义用户下载应用程序的路径。Gatekeeper 可以防止未签名的应用程序 (或恶意软件) 运行, 并搭配 XProtect 迅速阻止恶意软件的传播。
- XProtect 是一款自动化的反恶意软件实用程序, 由 Apple 持续更新。该程序可以防止在 Mac 上运行恶意软件和/或易受攻击的插件 (通常是 Java 和 Flash 等过期的插件。
- 恶意软件清除工具。Apple 可以清除准备侵入系统的恶意软件。
- Apple 始终负责审核 App Store 中的可下载应用程序, 且资源只有在得到 Apple 批准后方可供用户使用。Apple 有权随时撤销应用程序的可用性, 并废除开发人员的相关凭证。
- “应用程序沙盒”(App Sandboxing) 可确保应用程序不会共享 (或窃取) 来自系统或其他应用程序的数据。
- 隐私控制可供用户和 IT 人员定义一个透明流程, 让用户知道何时使用位置服务、哪些应用程序可以访问联系人或日历, 以及正在与 Apple 和/或应用程序开发人员共享哪些信息。

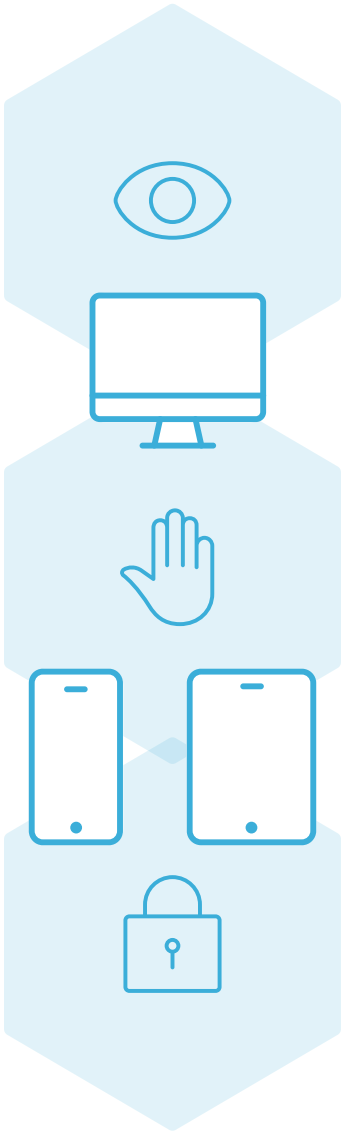
有关 Mac 安全特性的完整列表，请访问: https://www.apple.com/macos/security/.

为什么我们应该利用 FileVault 进行磁盘加密?
FileVault 是 macOS 内置的磁盘加密措施，这意味着 IT 人员无需添加任何附加软件即可实现对驱动器的加密。该措施可通过手动方式启用，也可由 IT 人员针对所有 Mac 电脑进行远程启用。加密密钥支持集中管理，因此 IT 人员可以在员工离开公司或忘记密码后帮助其登录设备并访问必要的数据。此外还可轻松循环加密密钥，从而提高信息安全性。

iOS 内置了哪些安全特性?
Mac 有许多同样适用于 iPad 和 iPhone 的核心安全功能，从而在整个 Apple 生态系统中实现了一致且安全的用户体验:

- 系统安全涵盖安全启动、软件授权、安全区域等技术，可确保操作系统不受到危害。此外，IT 人员还可清空整个 iOS 操作系统并重新开始。
- 指纹识别功能/面部识别功能 (Touch ID/Face ID) 可利用指纹感应和面部识别来简化登录过程，并确保只有授权用户才能访问设备。
- 加密和数据保护可确保个人和公司数据不受损坏，即使在其他数据因设备被盗或丢失而被擦除的情况下也是如此。
- 监管是一组附加功能，可供 IT 人员在更为受控的环境中获取额外的管理功能。

有关 iOS 安全特性的完整列表，请访问: https://www.apple.com/business/docs/iOS_Security_Guide.pdf.



添加新 Apple 设备时需要考虑的事项

我们要如何展示 Apple 设备的安全性?
创建配置文件的能力是 Apple 设备管理的基础。IT 人员可通过 Jamf Pro 等移动设备管理解决方案来构建配置文件，以执行密码、限制设置、定义网络协议、配置 VPN 设置和邮件帐户等等。随后，IT 人员即可将上述任一设置部署到托管设备中。

为什么我们不需要使用应用程序容器?
我们可利用 Jamf Pro 等一些以 Apple 为中心的管理工具将经过批准的应用程序部署到设备上，并防止未经批准的应用程序进入设备。目前 iOS 已支持使用原生应用程序，通过 Jamf Pro 等解决方案来管理企业应用程序。此种管理方法将企业数据与个人数据分开，并可在不使用容器应用程序的情况下管理数据流，从而避免了因使用此类程序导致的性能降低以及与各版本操作系统间的冲突.

Mac 在 MDM 框架以外存在哪些安全控制?
对 macOS 而言，Jamf Pro 等解决方案超越了 Jamf Agent 的基本设备管理。Jamf Agent 是在 Mac 注册管理后安装的二进制文件。IT 人员可通过该文件创建隐藏的管理员帐户，以授予所有受控 Mac 计算机的远程根目录访问权限。

安装 Jamf Agent 后，IT 人员即可运行更高级的策略和脚本，以及安装 App Store 之外的软件（如 Adobe）等等。该文件可扩大设备的自定义范围并扩展相关的管理功能，而这已超出了 MDM 的能力范围。

我们应如何验证、执行和报告 Apple 设备在工作环境中的合规性?
对于受到高度监管的行业而言，审计工作可能频繁而乏味；因此，证明设备确实处于受控的安全状态对于证明其合规性来说十分重要。

收集库存信息是满足监管和企业安全要求的关键。了解企业环境中有多少设备、谁拥有哪些设备、软件更新状态如何、为每台设备分配了哪些配置文件和设置、当前的加密状态如何，以及应用了哪些限制和配置，对于任何健康和安全的环境而言都是至关重要的。

IT 人员可通过 Jamf Pro 等解决方案运行几乎无尽的库存类别报告，帮助企业制定更为合适的决策并展示设备的合规性。如果设备不合规，则可将配置文件部署到相应设备以强制恢复其合规性。

如果存在多台不合规设备，或必须针对整个环境运行检查，则可利用 Jamf Pro 创建动态设备智能分组。“智能分组”基于 IT 人员定义的高级库存条件，并可根据库存报告触发自动化管理措施。

我们要如何处理对第三方 macOS 软件的修补?
软件可能很快就会过期，而一旦软件过期，设备、数据和网络就可能容易受到内部和外部威胁的影响。利用修补程序管理可以快速、高效地弥补这些漏洞。

您的 MDM 修补程序管理功能应允许 IT 人员在存在可更新的第三方软件版本时接收修补程序警报，使用适当的修补程序（更新的软件版本）创建软件包，将修补程序分发到相应的设备，然后通过库存管理接收修补程序报告，以确保修补程序安装正确。

目前企业纷纷采取主动的安全工作流方法，迅速了解哪些应用程序和软件已经过期，然后迅速采取相应措施，以确保安装最新且安全的软件版本。

为什么我们不应该将 Apple 设备绑定到 Active Directory?
在部署方面，Mac 有别于传统的一对一部署。Jamf Pro, Enterprise Connect 和 NoMAD, 等工具的出现，使得绑定成为历史。如果某个组织机构未将其域控制器暴露在外，则绑定不仅会使 DEP 工作流更加复杂，而且采用绑定的组织机构也会失去将新设备移交给远程用户控制的能力。尽管绑定也是一种选择，但使用 Jamf Pro 等解决方案的组织机构同样可以管理本地帐户，在实现相同的密码复杂性和过期要求的同时，不必担心连接或与 AD 不同步等问题。这意味着最终用户需要执行的密码提示操作更少，且 IT 帮助台接到的求助电话也会减少。

云服务如何与 Apple 设备配合使用?
当前的云端化趋势愈演愈烈。不同于您网络中服务器上的数据库，在使用云托管时，数据库的访问权限会受到限制。数十年来，组织机构一直在他们的公司外围构建“防护墙”，利用网络边界作为第一道防线。随着工作空间的移动性日益增强，仅凭防火墙将无法继续确保数据的安全；因此组织机构必须向着更为现代化的、基于身份的安全模式迈进。

Microsoft 正在使用 Azure Active Directory 将企业数据转移到云端。为确保只有受信任设备上的受信任用户才能使用受信任应用程序访问位于云端的上述公司数据，Microsoft 和 Jamf 提供了独家集成内容，以实现无代理的条件访问。

请单击此处阅读更多内容：https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/.

移动工作模式转变以及对云端的依赖比以往任何时候都要显著。

85%
的组织机构会在云中保存高度机密信息

80%
的员工使用未经批准的 SaaS 应用程序来开展工作。

41%
的员工表示，移动业务应用程序改变了他们的工作方式。

我们要如何执行行业安全标准?
执行方式要取决于安全标准是什么，以及必须符合哪些合规性标准。SOC 2 不同于 HIPAA，且 PCI 不同于 CIS。知道需要坚持哪些标准是重要的第一步。

Jamf Pro 提供了一个灵活的框架，以帮助您遵从众多的常规监管标准。IT 人员仅需确定适用的标准，构建相应的配置文件和策略并予以应用即可。其中可能包括限制 iCloud Drive 等消费者功能、强制 Gatekeeper 仅下载安全应用程序、强制 FileVault 加密 Mac，或在所有托管 Apple 设备上搜索受限应用程序（甚至 macOS），并在查找到此类应用程序后将其删除，以此限制应用程序。IT 人员仅需确定设置内容，并使用该信息构建相关的配置文件和策略，并将其应用于设备即可。

请查看本白皮书，以了解如何遵循互联网安全中心 (CIS) 指南：https://www.jamf.com/resources/white-papers/macos-security-checklist/.

我们为什么要使用 Apple 部署程序?

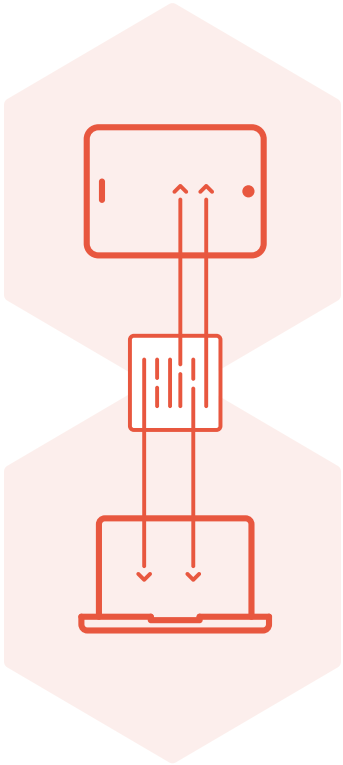
DEP 和 VPP 均为 Apple 的免费企业部署程序，且为 Apple 独家所有。上述程序不仅可以使设备安全性达到更高级别，还允许 IT 人员进行大规模的自动化和个性化设备设置。

- DEP 是 Apple 所推荐的、将组织机构的 Apple 设备置于安全受控状态的首选方法。DEP 支持零接触部署，这意味着传统的成像过程以及通过 IT 人员进行手动配置和设置的需求不复存在。用户可以快速、无缝地注册到环境中，从而最大限度减少了上手时间，且仅需点击几个按键即可完成对端点的保护。直接从 Apple 或其授权经销商处订购的设备有资格使用 DEP，并将于初始设置期间自动完成管理注册。
- 对于 macOS、iOS 和 tvOS 设备，DEP 可实施额外的管控手段，并授予更深层次的管理权限。
- 在与移动设备管理或 MDM（Apple 的内置管理框架）结合使用时，系统会根据用户的需求，通过动态方法将终端状态传递给用户，而不是炮制千人一面的方案。
- IT 人员可通过 VPP 为 App Store 中的应用程序授予相应权限，并将软件分发至个人或设备。如果直接将软件分发至设备，则无需提供 Apple ID。Apple ID 用于识别用户身份，并授予其访问 iCloud、iTunes 和 App Store 等 Apple 服务的权限。
- IT 人员可以管理已购买的 VPP 应用程序，并在员工离职或不再需要某应用程序的情况下将其收回并进行重新分配。

“并非所有 Apple 设备管理解决方案都支持 Apple 的程序和服务。请联系您的供应商，确保他们支持这些程序以及渐进式变更。”

可通过哪些 Apple 集成内容来利用您的现有资源

Apple（和 Jamf）是如何与我们现有的 IT 技术堆栈集成的?
组织机构、IT 人员和员工并非存在于虚幻当中。Apple 与 Cisco 等技术型公司展开合作，以提供现代化且安全的企业服务，从而兑现了他们对广大企业的郑重承诺。



有许多公司需要 Apple 生态系统以外的服务。组织机构可借助安全和具有兼容性的集成内容，充分利用其环境中的各方面优势，并积极通过大量服务推动业务发展。

相关示例如下：

- Jamf 的应用程序编程接口 (API), 具有利用现有 IT 工具构建集成内容的灵活性。
- Microsoft EMS 与 Jamf 的集成, 可为 Mac 上的条件访问提供独家免代理集成内容。
- Cisco ISE, 可为连接到公司网络的设备创建和实施安全和访问策略。
- Cisco Fast Lane, 可通过应用程序优先排序和服务质量自动配置来节省网络带宽。
- ServiceNow, 用于实现运营管理业务流程和 IT 流程自动化。

随着现代化组织机构转而使用 Cisco 等企业工具，在 Mac 管理的过程中加入 Jamf 即可获得全面集成的解决方案，其性能在任何受支持的平台上均不打折扣。

另外，身份管理公司 Okta Inc. 在其近期的安全数据报告中公布了几项调查结果，重点关注网络安全应用程序在企业中的日益普及。今年，Jamf 等安全工具首次跻身于增长最快的前 15 个应用程序行列当中。

Apple + Jamf 可实现无与伦比的设备管理效果和安全性

最安全的平台需要借助最强大的管理解决方案，以确保所有可用的安全特性都得到执行和安装。除了 Jamf，没有哪家移动设备管理公司能够更好地集成 Apple 设备及服务，也没有哪家提供商更能确保 Apple 取得成功。

这也是具有安全意识的组织机构（包括美国十大银行以及排名前十的科技企业中的 9 家）都选择 Jamf 来管理其 Apple 环境的原因。

凭借对 Apple 旗下所有操作系统和相关特性的无时差支持，Jamf 产品获得了广大 Apple 设备应用企业及员工的信赖和支持。

Jamf 可提供必要的工具，以保障 100 – 100,000 台 Apple 设备的安全，让组织机构可以更加专注于战略性任务，从而帮助其节省时间、改善用户体验并使其业务获得长足发展。

Jamf 有 96% 的客户都在年复一年地续签合同。要了解 Jamf Pro 如何影响您的 Apple 设备管理，请访问 jamf.com/zh/products/jamf-pro.

要了解有关 Jamf Pro 如何影响 Mac 和 iOS 管理的详细信息， 请访问
jamf.com/zh/products/jamf-pro