



开启移动办公的无限可能

通过革新移动设备，改变员工的工作方式。

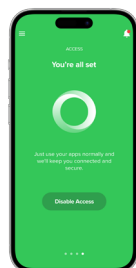
利用移动设备做更多事情

寻求流程创新的组织通常会采用集成移动设备的工作流程。然而，由于各种移动使用案例的要求错综复杂，设备要想充分发挥其潜能具有挑战性。很多时候，组织将不同的工具与其主要（通常是 UEM）工具一起使用，从而导致用户体验碎片化和项目停滞不前。

有了 [Jamf for Mobile](#)，企业就能获得在工作中释放移动能力所需的所有功能 -- 让移动团队满足安全性和合规性要求，同时改善用户体验。

Jamf for Mobile 使移动团队能够：

- 在员工工作的任何地方都能安全访问关键应用程序，从而扩展工作流程。
- 为移动和安全团队提供可视性和控制能力，在保护设备的同时保留原生移动体验。
- 同时支持“一人一机”和“设备共享”两种分配模式及应用场景。
- 建立基准以确保符合组织和监管框架的要求。



规划、部署和扩展工作流程的关键能力



设备管理

零接触式部署可自动配置和定制设备，使您的团队能够更高效地工作，并提高用户生产力。可在任何移动设备上轻松部署、更新和自定义应用程序。



端点合规

建立安全基线，验证每台移动设备是否符合监管要求。监控易受攻击的应用程序版本、应用程序风险级别、过时的操作系统，以及阻止或隐藏未经授权的应用程序等。



以移动端为先的用户体验

借助专为 Apple 框架打造的解决方案，为用户提供他们所期待的原生体验。Jamf 提供扩展支持，以解决跨平台难题，并安全地管理主流操作系统、所有权模式和设备形态。



网络保护

利用先进的网络保护功能，保护用户免受在线威胁（如网络钓鱼），并执行组织的“可接受使用政策”。通过“数据上限”管理蜂窝数据消耗，并通过“内容过滤”控制受限内容的访问，确保在所有应用程序和浏览器上安全、合规地浏览。



威胁检测和响应

通过实时检测和快速响应保护贵组织的数据。使用数据流将关键威胁事件、网络流量、设备数据和应用洞察直接发送到 SIEM，并使用威胁风险信号迅速修复新出现的移动威胁。



安全应用程序访问

通过在员工需要时为其提供对关键应用程序的无缝访问，使员工能够随时随地高效工作。“零信任网络访问（ZTNA）”与身份自动化集成确保只有使用经批准设备的可信用户才能访问工作资源。



Jamf +1's

优化并提升您的 Apple 及移动设备工作流程。由 Jamf 构建的应用程序支持独特的行业工作流，能够为任何用户或使用场景（尤其是共享设备）进行设备配置、自定义和更新。深入了解设备使用情况，并为一线员工提供量身定制的原生体验。



主要行业

Jamf 与各行业领先企业合作，在医疗保健、零售、制造业、安全帽行业和航空业部署 Apple 设备。



行业专家、服务和合作伙伴

Jamf 的移动管理与 Apple 专家将与您的团队通力合作，为您量身定制最适合您需求的解决方案。我们的 [Marketplace](#) 合作伙伴通过预构建的解决方案增强了 Jamf 的功能，而 Jamf 专业服务则能加速贵组织对 Jamf 的采用。



www.jamf.com/zh-cn/

© 2026 Jamf, LLC. 保留所有权利。

Jamf for Mobile 已在 AWS 和 Microsoft Marketplace 上架，并符合预承诺云支出计划的条件。

如需了解更多信息，请联系您的 Jamf 客户代表或[申请试用](#)。