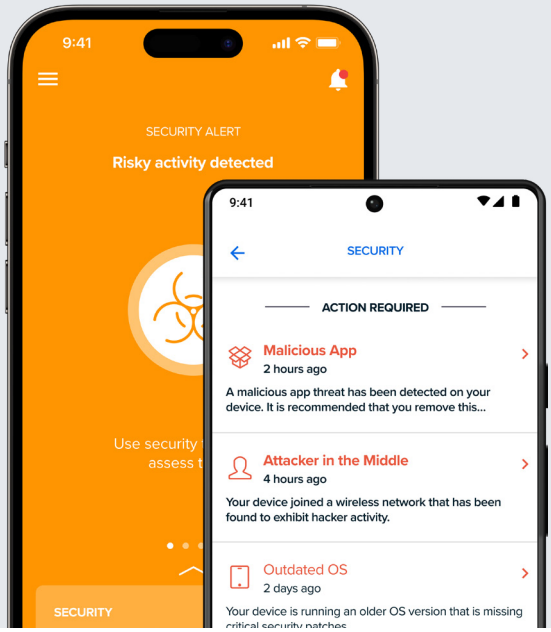
jamf

保护移动端点
抵御现代威胁。

预防网络攻击，维护端点合规，
识别主动威胁并做出响应。



现代劳动力对混合和远程工作环境的适应能力极强。

由于灵活性的提高，越来越多的工作是在移动设备上完成的。这些设备存储了大量的工作和个人数据，并始终与互联网相连，因此成为网络攻击者的最佳目标。移动体验往往使用户更难发现可疑的攻击，因此额外的保护措施对保证用户和工作信息的安全至关重要。

进入 Jamf 移动安全

专门设计的移动安全解决方案，可抵御移动攻击，执行可接受使用或数据上限策略，提供设备合规性的清晰可见性，并为任何应用程序提供实时条件访问。确保工作中使用的所有移动设备（无论是个人还是公司所有）的安全，以确保工作资源的安全。

解决保护移动设备安全的独特挑战

Jamf 移动安全结合了多层安全保护，通过以下功能保护用户、终端和网络：

移动端点安全
对各种端点安全检查点进行持续监控，确保移动设备达到所需的安全基线。

网络钓鱼防护
先进的机器学习功能可在设备受到影响前实时阻止已知和新型网络钓鱼攻击、加密劫持以及风险或恶意域。

网络内容过滤
基于类别的内容过滤可执行可接受使用策略，防止用户访问违禁或有风险的内容。

越狱检测
通过高级扫描确定移动设备是否被终端用户或恶意行为者 root 或修改。

操作系统漏洞报告
轻松报告在 iOS 和 iPadOS 上检测到的操作系统漏洞。运行易受攻击操作系统的设备会被标记为高风险状态。

应用风险监控
监控侧载应用程序、可疑开发人员配置文件、恶意代码模式、危险动态行为和危险权限。

公共 Wi-Fi 安全
防止攻击者截获可能危及公司敏感信息的互联网流量。

网络威胁流
通过将 iPhone、iPad 和 Android 设备上的各种安全数据流传输到 Jamf 或直接传输到 SIEM，获得全新的可视性。

数据封顶和报告
管理移动设备的蜂窝数据消耗。防止用户在国内或漫游时使用过量数据，以控制成本并防止意外超额。

风险信号
全面的移动安全数据可为每台设备的个人风险评分提供信息，该评分可用于为使用 Jamf 和其他零信任网络访问 (ZTNA) 解决方案的零信任访问决策提供信息。

简单部署
Jamf Trust 应用程序可通过 **Jamf Pro** 或任何现代移动设备管理 (MDM) 解决方案进行部署和配置，使任何组织都能获得全面的移动端点安全。

连续条件访问
Jamf 采用风险感知访问策略和按应用程序连接，提供零信任访问工作应用程序和数据，满足员工在移动设备上提高工作效率的需要。

Jamf 移动安全由 Jamf 威胁实验室（Jamf Threat Labs）提供支持：该实验室由经验丰富的威胁研究人员、网络安全专家和数据科学家组成，他们调查未来的安全威胁，不断增强 Jamf 产品的安全能力。

jamf

www.jamf.com/zh-cn/

Updated 01/2025.

申请试用，了解 有关使用 Jamf 保护移动端点安全的更多信息。

或者联系您的首选经销商。