jamf

# 移动安全购买指南

## 确保所有端点都受到保护

## 移动员工面临着不断变化的威胁

### 成功的移动部署需要敏锐的可视性和果断的行动。

员工越来越多地离开办公桌或公司办公室，使用移动设备工作。要防御这些分散的现代端点是一项挑战，尤其是当用户面临新的威胁载体时。

网络威胁并非只在我们的电脑上。

移动设备面临的风险也是真实存在的。

- **40%**的工作移动设备存在已知漏洞。
- 工人在移动设备上遭受网络钓鱼攻击的几率比笔记本电脑高 **50%** 。
- **1%** 的移动工作者受到恶意软件的影响，但高级持续威胁 (APT) 使攻击者能够非常精确地锁定目标用户

因此， **移动安全** 对于保护您的移动员工、设备和数据至关重要。强大的移动安全计划包括

- 防止安全配置错误
- 阻止攻击
- 通过强大的取证和事件响应功能检测入侵行为

## 主要功能

那么，您应该考虑为部分或全部移动机队实施哪些安全功能呢？

### 安全配置管理

**移动设备加固**

- 建立良好的安全意识
- 执行合规性审计
- 监控配置漏洞

**补丁管理**

- 利用详细的漏洞报告确定打补丁的优先次序
- 减少操作系统和应用程序漏洞

**数据丢失防护**

- 控制应用程序之间的业务数据流
- 根据用户或设备状态限制应用程序访问权限

**可接受使用政策**

- 利用基于类别的动态策略限制网络使用
- 按用户、组、区域或全局配置执行 AUP

### 攻击预防

**恶意软件和其他应用程序风险**

- 阻止恶意软件
- 识别易受攻击和有风险的应用程序
- 防止应用程序中的敏感数据泄露
- 监控替代应用程序市场的使用情况

**中间对抗者**

- 识别恶意热点和协议攻击
- 利用加密隧道缓解中间对抗

**网络威胁**

- 防止网络钓鱼，包括零时差攻击
- 阻止恶意网络流量，包括 C2 和数据外渗
- 消除加密劫持、垃圾邮件和其他网络威胁

### 安全访问

**保护传输中的数据**

- 为关键业务应用程序和数据建立加密隧道

**审计关键应用程序的使用情况**

- 报告移动工作人员访问的所有应用程序

**执行实时访问策略**

- 建立包含用户详细信息和设备状态检查的访问策略

### 威胁检测与响应

**收集丰富的遥测数据**

- 收集详细日志，进行离线分析

**检测异常**

- 启用威胁狩猎功能，搜索显示恶意活动的异常情况
- 将入侵迹象和新的知识纳入威胁情报，以改进未来的检测工作

**修复威胁**

- 检测到入侵时拒绝访问关键应用程序和工作负载
- 清除恶意软件，使用户恢复生产状态

## 使用 Jamf 实现可信访问结果

Jamf 帮助企业保护其最宝贵的资产，确保只有经过授权的用户才能使用符合企业安全要求的注册设备访问敏感的业务应用程序。

## 明智选择移动安全功能

威胁形势和我们的工作方法都在不断变化。昨天的充分保护并不能保证今天的安全。以下是选择移动安全解决方案时的一些注意事项。

### 调查解决方案的功能。

重要的是要检查解决方案的实际功能——仅仅声称具有 "移动安全 "功能是不够的。您的解决方案应考虑到移动设备所面临的独特威胁，而不仅仅是将计算机安全概念应用于移动设备。

### 安全需要设备管理。

单一的安全解决方案可能无法满足您的所有要求，仅靠安全软件也是不够的。设备管理对安全至关重要；毕竟，看不到的东西是无法确保安全的。您的管理软件可帮助您保持设备合规并修复潜在问题。

### 用户体验非常重要。

员工使用移动设备是因为其移动性有助于他们保持工作效率。过多阻碍设备功能的安全策略对用户没有帮助，他们可能会找到未经批准的变通方法来规避这些安全策略。

移动设备已发展成为用户赖以提高工作效率的重要工作工具。当设备发生策略动作时，必须建立工作流程，让用户尽快恢复工作。

并非所有设备都需要相同的安全工具。在应用工具和策略配置之前，考虑部署方案和用例。例如:

- 考虑员工如何使用他们的设备。他们的角色影响着他们的风险。例如：
  一名可以访问一些敏感数据和网络的普通员工，需要防范常见的威胁。他们的设备应保持合规，并防止网络钓鱼和恶意软件。内容过滤、威胁防御和零信任网络访问可进一步确保它们的安全。
- 无桌办公员工（如零售业）可从内容过滤和应用程序安全中获益。如果他们的设备无法访问浏览器，网络钓鱼的风险就会降低。
- 能够访问更多关键数据的高管和角色往往会成为攻击目标。它们需要额外的保护，而且往往需要满足监管要求。


©2002-2025 Jamf, LLC. 保留所有权利。

最先进的移动保护和连接解决方案，旨在保护贵组织的移动机群。免费试用 Jamf。