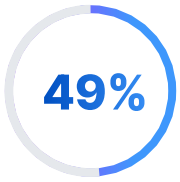
为什么选择 Jamf for Mac

企业 IT 领导者需要确保设备正常运行时间，提升终端用户的工作效率和满意度，同时降低风险暴露并缓解任何网络威胁。

随着越来越多的员工选择使用 Mac，IT 团队需要在既定预算范围内，为用户提供无缝的使用体验和企业级安全保障，且不做任何妥协。这就是 Jamf 发挥作用的地方。

IT 团队在日 IT 任务上花费了过多的时间。

现代 IT 环境对速度提出了更高要求，但过时的流程、孤立的工具，以及缺乏实时数据迫使团队不得不花费大量时间来拼凑解决方案。它不具备可扩展性。

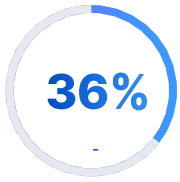


的组织表示，他们在关键时刻无法及时获取信息 [1]

由于无法实时监控设备状态，IT 团队不得不花费大量时间通过临时解决方案和手动 API 调用拼凑数据，仅仅为了生成基本的报告。缺乏实时数据对设备安全构成更大的风险。

的 IT 领导者表示，集成挑战阻碍了数字化转型计划的推进。 [2]

缺乏清晰的文档、原生构建的集成或支持无缝集成的政策框架，IT 团队不得不花费大量时间来确保其工具能够顺畅协作。



的 Mac 电脑被发现未启用 FileVault 功能 [3]

的 Mac 电脑被发现防火墙处于关闭状态 [3]

IT 团队花费过多时间手动强化和修复设备以符合合规基线。其他供应商提供的合规模板并不完整，或未能反映 macOS 安全合规项目中的合规基线。这给 IT 团队带来了更多工作量。

每年 Apple 环境中的风险都会增加。

Mac 在企业中的普及度提高是一把双刃剑：黑客们现在认为，破解 Apple 设备虽然难度较大，但值得一试。

缺乏针对 Apple 特定威胁的保护只会增加风险暴露。缺乏 Mac 特定事件数据的遥测（即 Gatekeeper 和 XProtect）意味着，在威胁行为者触发其他安全控制措施之前，您将无法获得全面的可见性。如果没有专门针对 Apple 的威胁追踪团队，大多数安全供应商都难以应对。

违反数据保护法规的平均成本为 1480 万美元。[2]

缺乏全面的日志记录和审计跟踪导致审计准备不足，但与安全信息和事件管理（SIEM）提供商的集成可提供额外的可见性，实现真正的安全统一视图。

39% 的组织至少拥有一台存在已知漏洞的设备；[3] 对 CVE 的可见性有限，且缺乏自动化的软件补丁工作流程，这使您面临使用易受攻击软件的风险。

300

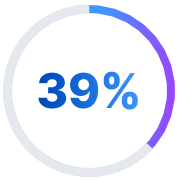
Jamf 威胁实验室监控 macOS 平台上的超过 300 个 恶意软件家族 [3]

21

Jamf 威胁实验室在2023 年就发现了21个新的恶意软件家族 [3]

1480万美元

违反数据保护法规的平均成本



的组织至少拥有一台存在已知漏洞的设备 [3]

那么，为什么选择Jamf for Mac?

Jamf 的生产力提升效果是竞争对手的两倍[4]，因为它能够无缝集成到任何 IT 基础设施中。这将减少数据收集、设备停机时间、一级支持以及手动操作所花费的时间。

我们的安全解决方案通过减少针对 Apple 的威胁、缩短响应时间、减少未修补的漏洞并提高合规性准备程度，将风险暴露降低到竞争对手的 2 到 3 倍。

我们通过以下方式实现这一目标：

- 通过专门针对 Apple 的威胁追踪团队，对多个向量进行实时威胁监控
- 全面的库存管理、报告、日志记录和审计功能
- 强大的预置 IT 和信息安全集成方案
- 强大的政策框架，提供自动化、实时执行和最终用户自助服务功能。
- 应用程序的自动化获取、验证、重新打包和部署

我们的支持和服务中心团队堪称传奇。我们还提供 Jamf Nation——全球最大的 Apple 管理员论坛——会员们可以在这里相互分享丰富的专业知识。

“我从朱莉（技术支持工程师）那里获得的出色技术支持，充分证明了选择 Jamf for Mac 管理是明智之举。我可以自信地向我的管理团队证明，Jamf 是一个值得信赖的选择。”

– 政府机构的 IT 分析师

Jamf 的生产力提升效果优于其他解决方案。

Jamf 凭借以下优势超越竞争对手：

- 减少设备停机时间
- 提升 IT 运营效率
- 减少直接对终端用户支持的需求
- 更好的监控和可视化

更快地投入生产

实时访问全面的设备信息和自动化工作流程，减少了对人工报告、审计和工作流程管理的依赖。

具体如下：

- **自动化入职流程**基于角色、部门、用户和位置自动设置配置，可节省 IT 部门时间并让新员工快速投入工作。
- **精准定位**有助于实现故障排除、设备强化及软件更新的自动化，从而节省终端用户和IT团队的时**间。**
- **一级支持**服务不仅涵盖基本用户功能的故障排除，还为用户提供自助服务模式，以便添加生产力应用程序。

Jamf 相比其他解决方案能降低更多风险。

Jamf 的强大策略框架涵盖设备管理框架、基于策略的脚本执行以及网络控制。我们的威胁追踪专家团队运用训练有素的行为分析技术，阻止针对 Apple 的攻击。

借助Jamf，IT领导者可以：

- 阻止已知和新型的 Apple 特定威胁零日攻击
- 通过针对性、实时执行的修复措施， 更快地应对安全风险。
- 通过 CVE 漏洞报告和自动软件及应用程序更新，限制未修复的漏洞。
- 通过针对 Apple 设计的安全连接和针对更多数据点的动态风险评估，降低数据丢失 的可能性
- 通过集成到 macOS 安全合规项目中，实现设备加固的自动化，消除人为错误的风险，并通过详细的日志记录和审计跟踪提升审计准备度。

1.《自动化：趋势、挑战与最佳实践》，IDC，2023
2.《IT 状态报告》，第三版，Salesforce
3.《Jamf 安全 360：2024 年年度趋势报告》，Jamf，2024 年
4.《提高投资回报率：久经考验的 Apple 企业管理解决方案的案例》，Jamf 白皮书，2021 年

Jamf 是您的理想选择。
但别光听我们的一面之词！

G2评测：

“Jamf Pro 仍然是 Apple Mac 卓越的移动设备管理解决方案。”

“供应商提供了大量支持。Jamf 通常会明确地包含在供应商文档 中，因为它是 Apple MDM 的领先产品。”

jamf

试用 Jamf