



补全适用于 Apple 的 Microsoft 技术栈

Jamf 将 Apple 设备管理与安全防护与 Microsoft Sentinel、Entra 及 Intune 统合一体，使 IT 和安全团队**能够随时随地对每一台 Apple 设备拥有全盘可视性。**



在 Microsoft 环境中管理 Apple 设备的组织正面临安全漏洞。身份与访问决策的有效性，完全取决于其背后的设备信号强度；缺乏深度的 Apple 原生合规数据，条件接收便无法在全量设备中全面贯彻零信任原则。

同时管理 Mac、iPhone 和 Windows 设备的安全团队，常常处于信息掌握不全的困境，因为通用型跨平台工具很难捕获 Apple 特有的遥测数据。与此同时，主要针对 Windows 环境打造的工具需要手动变通处理，且部署到 Apple 设备的速度十分缓慢。

通用型管理方式拉高了成本，却未能带来成比例的价值。更糟的是，随着组织扩大 Apple 设备的使用规模，不一致的身份认证或入职配置还会阻碍生产力。

Jamf + Microsoft = 针对 Apple 的单一平台

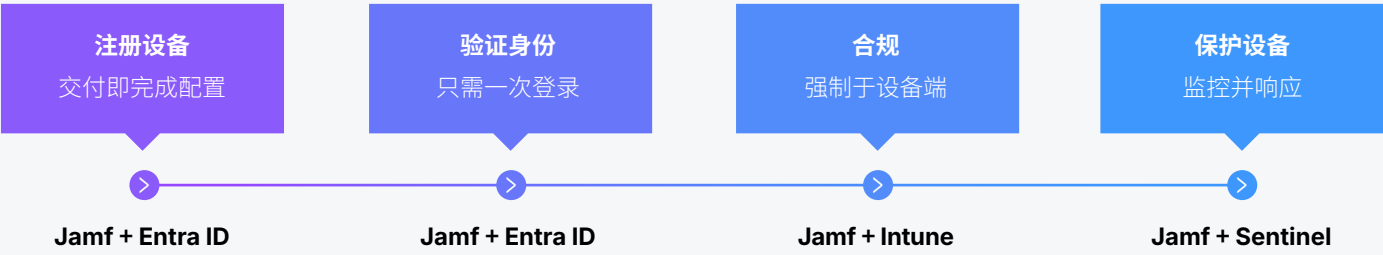
微软与 Jamf 携手为共同客户提供单一、连贯且一体化的技术栈，以支持其全员高效工作。无论身在何处，IT 团队都能获得统一的可视性，安全团队可实现全方位的覆盖，而终端用户在每一台 Apple 设备上都能享受到无缝的入职体验与日常办公体验。

原生协同，天生一对

能力领域	优势简述
规模化部署与管理 Apple 设备	设备开箱即已完成配置、符合安全合规，并可直接投入工作。零触控部署由 Microsoft Entra ID 凭据与 Apple Business Manager 驱动。
与 Entra ID 实现实时合规	Apple 原生合规信号会实时同步至 Microsoft Entra 条件访问，当设备面临风险时自动限制其访问权限。
为每位用户提供无缝的身份认证	用户使用其 Microsoft Entra ID 凭据登录；Jamf 则自动完成账户预配与 FileVault 磁盘加密。
在 Microsoft Sentinel 中实现深度 Apple 环境可视性	Apple 原生遥测数据直接流式传输至 Sentinel，为安全团队提供跨 Mac、移动设备与 Windows 的统一视图。
借助 Security Copilot 实现统一的安全运营	Jamf 插件可将 Apple 设备上下文信息直接呈现在分析师的工作流程中，从而显著提升调查与响应的速度。

客户收益

- 弥补 Microsoft 技术栈中的 Apple 合规与可视性盲区
- 通过零触控部署与自动化策略强制执行，简化 IT 运维流程。
- 在不牺牲安全性的前提下提升员工体验



设备管理集成	说明	产品文档或 市场列表	Jamf 产品	Microsoft 产品	客户反馈
用于查询用户和组的 LDAP	有关组织用户的目录信息（姓名、电子邮件、角色等）可用于确保正确的应用程序和设置被正确的最终用户使用。管理员无需手动重新创建这些信息。	与 LDAP 目录服务集成	Jamf Pro	本地活动目录	
用于查询用户和组的云身份提供商	现在云端 IdP 中可以找到有关组织用户的信息（姓名、电子邮件、角色等），可用于确保将正确的应用程序和设置应用于正确的用户和设备。将这些信息连接到 Jamf Pro 中，管理员就不必手动插入了。	Microsoft Entra ID 集成	Jamf Pro	Microsoft Entra ID 和 Intune（Microsoft 端点管理器）	“Jamf 和 Microsoft 都提供了简单易懂的文档。我参与过的最简单的整合”。 I Borota
仪表板分析报告	免费获取创建和保存无限交互式报告所需的一切。使用 Jamf Pro Power BI 应用程序为您的 Jamf 部署带来更深层次的数据分析。扩展 Jamf Pro 的报告功能，并在 Power BI 架构中进行捕获。 可用数据：计算机和移动设备、详细信息、应用程序、扩展属性和组	Power BI	Jamf Pro	Microsoft Power BI	Power BI 与 Jamf Pro “Power BI 与 Jamf Pro 无缝集成，可提供有关 Jamf Pro 实例各个方面的详细报告。设置 MacOS 版本、病毒定义版本、每栋楼设备数量等报告。我们非常喜欢这个提供数据的工具。” C McBride



身份和访问集成	说明	产品文档或 市场列表	Jamf 产品	Microsoft 产品	客户反馈
适用于 macOS、iOS 和 iPadOS 的设备合规	企业希望在允许可信用户访问公司资料之前，确保他们使用的是符合要求的设备。通过这种集成，Jamf Pro 可以验证设备是否符合标准，并将 "是"/"否" 状态发送给 Microsoft。 *从 Jamf Pro 10.4 开始，它将取代条件访问。	设备合规	Jamf Pro	Microsoft Entra ID 和 Intune	“通过集成，确保符合要求的设备能够访问办公数据。Jamf 与 Microsoft Entra ID 之间的无缝集成有助于我们实现这一安全要求。从安全角度来看，必须实施解决方案”。 Samstar777
云身份的单点登录 (SSO)	这使得企业管理员可以使用他们的 Entra ID 登录到他们的 Jamf Pro 实例、Jamf macOS Security Cloud 和 Jamf Security 门户。	使用 Active Directory 联合服务配置单点登录 Microsoft Entra 单点登录 (SSO) 与 Jamf Pro 集成	Jamf Pro	Microsoft Entra ID 和 Intune	最佳 IDP 集成 “Microsoft Entra ID 与我们所有支持外部身份提供商 (IDP) 的系统无缝集成。Jamf Pro 中用于 SSO 的云身份提供商功能以及 Jamf Protect 的集成功能可将企业身份轻松带入 Jamf 产品和其他第三方服务。” T Ellis
基于云的 Mac 身份识别	这使得组织内的终端用户能够使用其 Entra ID 登录 Mac。	与 Microsoft Entra ID 集成	Jamf Connect	Microsoft Entra ID 和 Intune	"根据给出的说明，实施起来很容易。SSO 改变了生活"。 Tyler Verlato



端点安全集成	说明	产品文档或 市场列表	Jamf 产品	Microsoft 产品	客户报价
适用于 Microsoft Sentinel 的 Jamf Protect	适用于 Microsoft Sentinel 的 Jamf Protect 集成通过简单易行的工作流将详细的事件数据从 macOS 设备发送到 Microsoft Sentinel。通过利用包含由 Jamf Protect 捕获的 警报 和 统一日志 的 Sentinel 工作簿和分析规则，这为安全团队提供了对 Mac 上发生的独特安全事件的可见性。	用于 Microsoft Sentinel 的 Jamf Protect	Jamf Protect	Microsoft Sentinel	"Sentinel Security 与 Jamf 协作。Jamf Protect 的应用和配合可以增加工作流程，简而言之，可以帮助您提高工作效率，深入了解设备群的安全状况，从而赢得 SecOps 的青睐。强烈推荐"。 - Dominic Vasquez
终端遥测数据转发	默认情况下，Mac 会收集有关其性能和应用程序的各种数据。虽然这些信息可能很多，但我们可以通过 Jamf Protect 将其过滤为他们所关心的信息，并将其发送到他们的安全工具上供进一步使用。	将 Jamf Protect 与 Microsoft Sentinel 集成	Jamf Protect	Microsoft Sentinel	"又一个例子说明了 Jamf 和 Azure 的集成效果有多好！" 用户—MrCcStj BF
网络威胁流事件转发	网络流量流使企业能够通过第三方日志聚合器和分析工具，对服务基础设施处理的所有网络活动进行流式处理、记录和审查。事件以通用事件格式（CEF）编码的 Syslog 方式，通过传输层安全性协议（TLS）进行实时发送，以确保数据传输的安全。 威胁事件流可以以通用事件格式（CEF）编码的系统日志或 JSON 编码的 HTTP 事件的形式实时发送事件。这两种数据流都可以集成到 Microsoft Sentinel 中。	网络流量流 威胁事件流	Jamf Protect 和 Jamf Connect	Microsoft Sentinel	"与 Azure 和 Sentinel 的完美集成。与 Jamf Protect 的结合非常有帮助。 Catherine Breese
Security Copilot 插件	借助此插件，安全管理员可以在安全事件发生后以自然语言快速查询 Jamf Pro 设备信息，通过聊天界面接收清单信息，而无需进入 Jamf Pro 控制台。	如何在 Copilot for Security 中进行集成，如何集成Jamf Pro	Jamf Pro	Microsoft Security Copilot	

