Jamf 和 Microsoft - 管理和保护企业中 Apple 设备

随着组织采用现代工作方式，IT 和安全团队正在寻找支持 Apple 用户的最佳方法。

在制定 Apple 战略时，组织通常会面临相同的挑战：

- 如何管理和保护存储敏感数据且可从任何地点访问的设备
- 如何整合工具、少花钱多办事，同时提高管理和安全能力
- 如何支持员工选择计划、移动设备及自带设备（BYOD）

尽管已开发出许多先进技术来应对这些现代挑战，但组织仍难以同时保障用户和数据的安全。

这往往会导致...

- 配置全面安全时不必要的复杂性
- 糟糕的用户体验也会增加管理开销
- 安全漏洞没有扩展到整个基础设施的所有设备
- 缺乏对包括数据等公司敏感资源的一致控制

Microsoft Solutions Partner

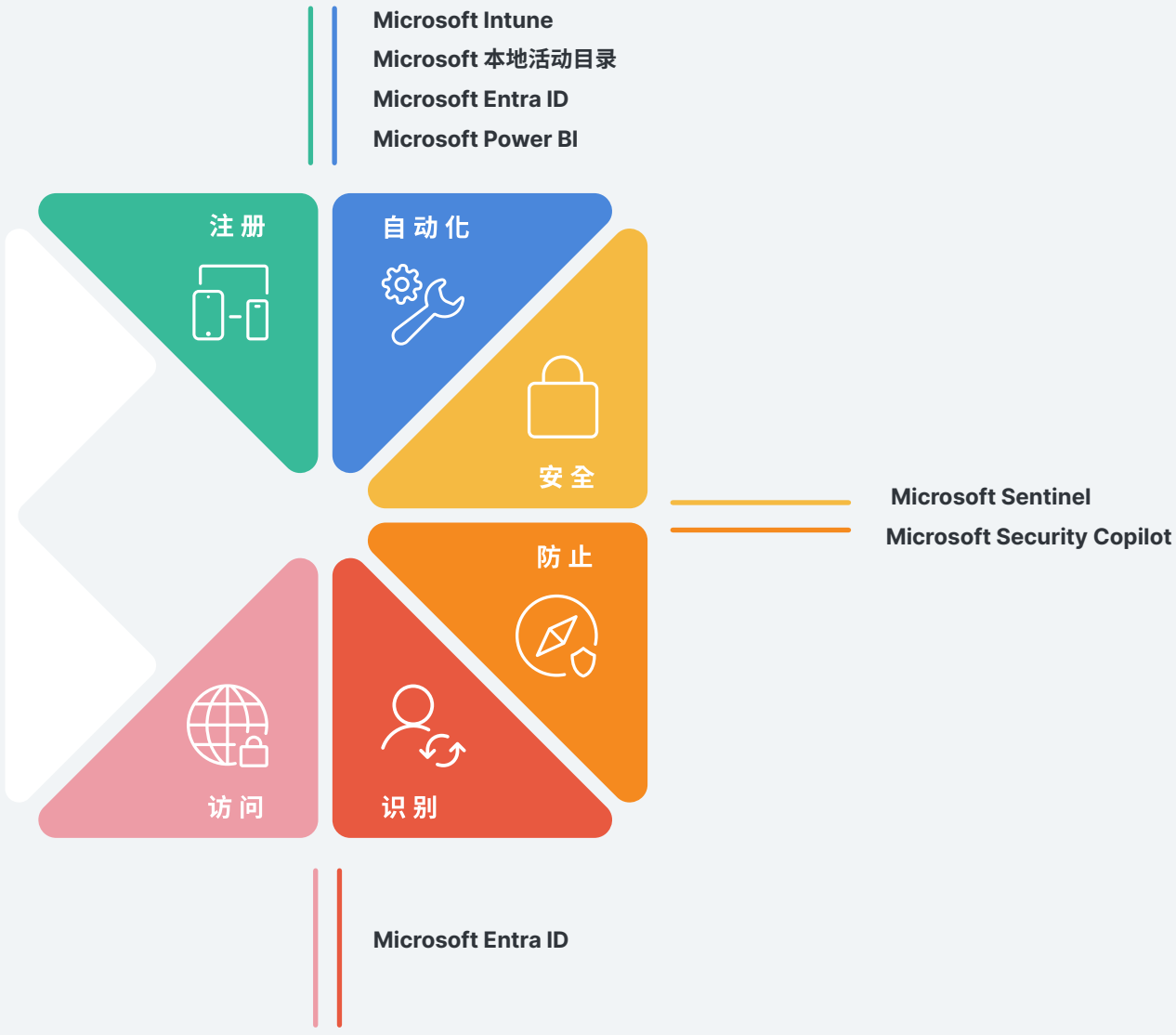
Available on Microsoft Azure Marketplace

Jamf + Microsoft 如何有效支持使用 Microsoft 平台的企业中的 Apple 设备

Jamf 拥有独特的优势，能够将 Apple 设备管理、用户身份和端点保护方面的优势融合在一起，与 Microsoft 携手打造以 Apple 为首的零信任解决方案。这使组织能够确保只有经过授权的用户在已注册且受保护的设备上才能连接到业务应用程序和数据。为了实现这一零信任目标，联合客户通过与云身份提供商（IdP）的集成来实现，这就是为什么 Jamf 和 Microsoft 是绝佳选择。所有注册设备均受到管理和终端保护，所有流量均由零信任网络访问（ZTNA）控制，以实现安全的远程连接 — 旨在适应现代威胁环境，同时纠正传统 VPN 的缺陷。

将 Jamf 与 Microsoft 整合是组织利用 Microsoft 平台推动基础设施发展，成功使用 Apple 产品的关键。

查看 Jamf 与 Microsoft 的集成，简化企业中的 Apple 操作。



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量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 iOS、iPadOS 和 macOS 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（例如：更新操作系统、启用密码）。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 macOS 的条件访问功能。	**设备合规性**	**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）	这样，企业的管理员就可以使用 Azure 凭据登录到他们的 Jamf Pro 实例、Jamf macOS 安全云门户和 Jamf 安全云门户。	**使用 Active Directory 联合服务配置单点登录** **Microsoft Entra 单点登录（SSO）与 Jamf Pro 的集成**	**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	这样，企业的最终用户就可以使用 Azure 凭据登录 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

Member of
Microsoft
Intelligent
Security
Association

Microsoft

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
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 Jam 和 Azure 的集成效果有多好！" 用户—MrCcSti|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）编码的系统日志通过传输层安全（TLS）实时发送，以确保数据的安全传输。 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	

要了解更多关于 Microsoft 与 Jamf 合作的信息，请访问我们的 Microsoft 集成页面。立即开始，申请试用。