jamf

填补空白：macOS 安全

安全需求贯穿于所有操作系统，macOS 也不例外。Apple 投入巨资提供原生隐私和安全功能，但随着 Mac 平台在企业市场的份额增长，攻击的价值也随之提升，使其成为恶意软件、数据泄露和漏洞挖掘更具吸引力的目标。 如今企业通过员工自选计划允许使用 macOS 的情况比以往任何时候都更为普遍。在这样做时，他们意识到，就像任何其他平台一样，需要额外的安全性和可见性。

多家安全厂商提供额外的解决方案来保护 Mac，但其中许多方案采用的是特定于该厂商及其 Windows 产品的安全模型，而非基于 macOS 提供的现代框架进行协作。这使得它很难跟上不断变化的操作系统。 相反，最佳实践是扩展现有的 macOS 安全模型，填补空白，并添加 macOS 特有的功能——这些正是安全团队有效运作所需的能力，以保护组织免受威胁侵害。

Apple 操作系统将隐私和安全作为平台的核心要素，在硬件和软件中直接内置了保护机制。与此同时，Apple 优先考虑直观的用户体验，以支持易用性和生产力。因此，许多功能的设计主要围绕个人用户而非组织的更广泛需求展开，这正是额外的可见性和安全控制措施发挥价值之处。

在我们的白皮书中，我们概述了 macOS 当前的安全状况，并就如何以高效、有效且用户友好的方式增强 Apple 的安全基线提供了指导。

您将学习：

- 可用的内置 Mac 安全功能的详细信息
- Jamf 如何在企业中增强这些功能
- Jamf 如何将威胁检测扩展到签名和内置功能之外
- 扩展 Apple 安全模型以实现高级企业安全的其他途径

macOS 上的应用

Apple 投入了大量精力设计安全功能，以保护用户及其运行的第三方应用程序。本节将介绍其中若干功能，并探讨如何从战略层面增强和扩展这些功能。要深入了解 Apple 的安全功能，请访问 **Apple 全面平台安全指南**。

通过 Gatekeeper 验证信任。

Apple 推荐且最值得信赖的第三方应用安装途径是通过 App Store。此举使 Apple 能够审查并筛选不符合其隐私、安全或用户体验标准的应用程序。然而，Apple 也限制了 App Store 中应用程序的功能，许多关键业务应用程序并不适合这种分发模式。

当无法通过 App Store 分发时，Apple 允许 macOS 开发者直接通过托管下载及其他传统分发方式发布应用程序。为支持这些“临时性”分发，Apple 已在操作系统中引入其他检查机制，以降低软件在 macOS 设备间大规模传播的风险。Gatekeeper 是 Apple 验证检查的核心功能名称。最初在 macOS 中作为一个选项，用于根据程序的风险容忍度来决定是否运行的功能，已经发展成了一套更加严格和全面的要求与防范措施。允许从“App Store” 或 “App Store 及已验证开发者”下载应用的基本接纳机制依然存在，但运行问题代码或风险代码的选项仍处于边缘化状态。

请注意，这些检查仅适用于从互联网下载的应用程序。Apple 通过在下载文件中附加额外的元数据来追踪这些应用程序，该元数据被称为隔离属性。当程序执行时，Gatekeeper 会执行一系列检查，例如验证隔离属性以确定是否允许执行。其中最基础的检查之一是确认应用程序是否由合法开发者签名，或是否通过 App Store 分发——具体取决于先前讨论的设置。

如果应用程序由开发者签名，系统会将证书与已撤销签名数据库进行比对，以确保签名者过去未曾与恶意软件相关联。通过这种方式，Apple 能够迅速撤销证书，阻止恶意软件的大范围传播。

从 macOS Catalina 开始，通过 Gatekeeper 验证还要求应用程序经过 Apple 的公证。要通过审核，应用程序必须上传至 Apple 进行分析。分析成功后，公证数据将与申请关联，以标注其已通过此额外层级的审查。

最终的信任取决于用户。

为了提升易用性，macOS 在许多情况下允许最终用户“覆盖” Gatekeeper。用户只需右键点击应用程序，选择“打开”或“用其他应用打开”。系统不会直接拒绝启动应用程序，而是弹出新提示框警告用户正在启动未知或潜在恶意应用程序，但 Gatekeeper 仍允许其继续操作。 需特别注意：XProtect 已明确识别的恶意软件，用户无法通过任何方式授权其运行。

应用程序首次执行后，隔离组件将自动更新，确保下次打开该应用程序时不再重复执行 Gatekeeper 操作。

⚠ 使用 XProtect 和 MRT 阻止威胁。

Gatekeeper 技术套件还包含 Apple 的签名式检测机制，即 XProtect 和恶意软件清除工具（MRT）。它们能够协同扫描操作系统中的文件，寻找文件中与已知恶意软件相关的特征。XProtect 在应用程序启动时触发，而 MRT 则定期扫描文件系统。

XProtect 通过名为 Yara 的二进制签名扫描引擎运行。Yara 支持灵活而强大的二进制签名定义和高效的执行引擎。为验证应用程序，XProtect 会在初次执行及后续更新时扫描每个可执行文件下载。若检测到任何匹配签名，该程序将被禁止运行。已知的恶意签名文件通过 Apple 对 macOS 的独立更新提供。Apple 根据自身需求定义并提供这些签名，其运作独立于 Yara 执行引擎本身。与 Gatekeeper 类似，此扫描仅在应用程序持有正确的隔离扩展属性时执行，该属性会在应用程序首次成功执行后更新。

另一方面，MRT 则采用定时执行机制而非程序运行时扫描，它会定期扫描文件系统中与历史恶意软件相关的特定文件名及残留物，一旦发现即予以清除。该功能主要旨在发现并修复已在 macOS 用户群体中传播的已知威胁。

⚙ 将 Gatekeeper 扩展至企业。

Gatekeeper 能有效地按其设计目的运行。它阻止未受信任的应用程序启动，并在识别出可疑或恶意应用程序时向用户发出通知。IT 和安全管理员需要能够发现企图在企业设备上运行未经信任软件的行为。更重要的是，他们需要意识到用户选择了右键点击并启动应用程序，这实际上绕过了企业安全控制措施。为满足这些企业需求，Jamf for Mac——凭借其专为 Mac 打造的端点安全解决方案——持续监测 Gatekeeper 操作的迹象，并将结果上报至中央平台，使 IT 和安全团队能够准确评估风险并做出明智决策。

除了提供对 Gatekeeper 活动的可视性外，Jamf 还允许企业通过在企业环境中将额外的签名信息注册为不受信任，从而掌控开发者信任模型。通过 Apple 最新的终端安全 API，Jamf 将主动阻止企业特定阻止列表中任何应用程序的执行。这可以在应用程序级别（应用程序 ID）或供应商级别（开发团队 ID）上进行定义。

此外，macOS 并未针对各类灰色软件（即潜在不需要或未经授权的软件）提供签名或拦截功能，其中包含大量参与不受欢迎且可能具有侵入性行为的广告软件和加密货币挖矿程序。通常，这些程序是由 Apple 开发者合法签名的，用户在安装时同意允许其信息被收集或资源被使用——通常是在不知情的情况下。因此，在许多情况下，Apple 不会干预这些应用程序的运行。

然而，企业中的风险计算方式截然不同，可能需要采取更严格、更具针对性的方法。因此，Jamf 强制执行其自身的受管 Yara 规则、二进制签名和不受信任的开发者证书，用于在进程执行时进行扫描，无论是否存在隔离扩展属性。这确保了当新增签名时，以及企业更新其安全态势时，现有应用程序不仅在首次执行时会被重新扫描，在后续每次执行时也会被重新扫描。

Jamf 基于其对 macOS 威胁的深入研究以及第三方 Mac 威胁数据，精心整理了这份已知针对 Mac 的恶意软件信息流。对于希望对运行在自身环境中的软件实施更精细化管控的组织，可通过自定义二进制哈希值、TeamID 等列表，扩展 Jamf 的默认应用程序屏蔽清单。当在 macOS 10.15（Catalina）或更高版本系统上运行某应用程序时，若其行为或特征与已知恶意软件匹配，Jamf 将阻止该进程执行，隔离违规文件，并记录恶意软件拦截警报。此操作独立于 Gatekeeper/XProtect 操作之外，旨在作为其功能的超集。Jamf 将识别已知的恶意软件，而不受隔离位的影响，从而识别潜在不安全的二进制文件，并维护更广泛的恶意软件知识库。

通过自助服务扩展 App Store 信任模型。

在某些情况下，通过利用预先填充了 IT 部门批准资源的自助式应用商店，限制用户可安装的程序可能是合适的做法。

Jamf Self Service+ 通过赋能 IT 部门创建专属企业应用目录，实现安全即时的资源访问。用户可自主安装应用、更新配置并解决常见问题，无需提交 IT 支持工单。

控制和监控应用程序行为。

通过隐私控制限制并确认应用程序行为。

系统隐私控制功能在 macOS Mojave 中首次推出。这些控制措施要求用户（或企业）为每个应用程序授予对特定操作和文件夹的访问权限。一旦应用程序获得特定操作的访问权限，未来当同一应用程序执行该操作时将不再需要再次授权。此功能确保应用程序必须明确获得许可才能访问操作系统中潜在敏感的组件（如网络摄像头、麦克风、键盘输入、下载内容），并促使用户放慢操作节奏，确认其正在授予应用程序访问私人数据的权限。

超越控制，审计并分析应用程序行为。

尽管隐私控制措施限制了应用程序的授权行为，但用户难免会犯错，授权权限也可能遭到滥用。我们已阐述过 Jamf 如何通过可视化呈现 Apple 内置安全功能的运行状态，并结合传统恶意软件/广告软件防护能力，持续为企业提供安全态势洞察与防护保障。但在 Jamf，我们认为终端保护不应止步于此。Jamf 还提供了传统上仅限于终端检测与响应（EDR）产品的审计和监控功能——但采用以 Apple 设备为优先的策略，并始终关注 macOS 用户所期待的隐私与安全标准。

Jamf for Mac 设备检测技术

Jamf 终端保护的核心是一个轻量级用户模式传感器（无附加文本），该传感器利用了 Apple 自有的逻辑执行引擎 GameplayKit。尽管使用游戏引擎分析安全事件属于非传统做法，但这使 Jamf 能够与 Apple 生态系统保持紧密集成，并在必要收集或报告之前持续分析设备上的数据。游戏引擎还被设计成能够实时处理海量事件，使其成为分析设备上实时活动的理想工具。与之形成鲜明对比的是，许多安全解决方案首先专注于 Windows 平台，随后才作为事后考虑移植到 macOS——或者那些要求所有数据都必须在云端收集和分析的方案。

GameplayKit 的另一项优势在于，它与 Yara 类似，将执行引擎与检测规则分离，使得检测功能能够在无需更新核心代理的情况下进行更新和扩展。检测定义同样基于 Apple 原生技术，采用 NSPredicate——一种强大的逻辑查询机制，支持常规查询语法及正则表达式。Jamf 的数据模型经过专门设计，充分利用了 NSPredicate 的丰富特性，包括调用原生函数和串联数据模型的能力。这解锁了某些功能，这些功能若采用其他更传统的方式实现，会显得杂乱无章或计算成本高昂。

例如，使用 Jamf 的数据模型和 NSPredicate，我们可以：

- 若文件被自行删除，则发出警报——这是掩盖行踪的常见手段。这个看似简单的用例涉及分析被删除的文件及其删除过程，且无需昂贵的连接操作或硬编码检测。
- 若未签名或可疑签名的二进制文件作为启动守护进程持久存在，则发出警报。这涉及解析配置文件，从中提取嵌入的二进制路径，并在分析过程中使用该二进制文件的相关元数据。
- 若 Microsoft Office 应用程序创建了意外子进程，则触发警报以识别 Office 宏利用行为。此示例突显了理解子/父关系的能力，以及揭露应用程序功能被滥用的能力。
- 若发现其他“利用现有资源”的活动被用于攻击行为，请立即发出警报。此类活动需要访问子进程/父进程及进程组关系、命令行参数等信息，以便发现看似无害的活动（如curl、ssh、python等）中的滥用行为。
- 在整个企业范围内追踪 USB 使用情况，并报告写入可移动介质的文件元数据。

为了便于理解这些类型的检测带来的影响，Jamf 将识别到的攻击映射到 MITRE ATT&CK™ 框架（如适用）。目前的覆盖范围包括框架中的多个用例，包括以下类别中的技术检测：

- 持久化
- 初始访问
- 命令与控制
- 防御规避
- 发现
- 权限提升
- 凭证访问

通过 Mac 原生遥测技术增强可见性

随着组织加强其 macOS 安全态势，对系统和用户活动进行更深入的可视化监控变得日益重要。原生 Apple 框架提供了坚实的基础，但安全团队通常需要更丰富、更关联的信号来检测异常行为、调查事件并大规模维持合规性。

Jamf 的遥测功能基于 Apple 的终端安全 API，可从每台设备收集详细的 macOS 特定信号。这使组织能够精确分析系统、用户、应用程序和网络活动，所用数据真实反映 macOS 的运行状态。该遥测系统采用轻量化设计且性能卓越，以保障用户体验；同时具备防篡改特性，确保日志与安全事件记录的可靠性，满足调查与合规需求。

通过关联跨进程、应用程序、身份验证、配置变更和用户操作的事件，Jamf 遥测技术帮助安全团队重建详细的时间线，并识别可能表明滥用或新兴威胁的行为。

借助 Jamf 遥测功能，组织可以：

- 满足监管和内部合规要求，提供准确、高质量的事件数据
- 检测配置漂移、影子 IT 和策略偏差
- 通过分析相关事件和攻击路径来加速事件响应
- 通过丰富的 macOS 专属洞察支持主动威胁狩猎
- 与 SIEM 平台无缝集成，实现集中化可视化管理

这些功能提供了大规模管理和保护 Mac 设备所需的深度和上下文，为高级检测和分析奠定了坚实基础。遥测功能还与 macOS 统一日志系统协同工作，使组织能够同时收集增强的安全信号和针对性日志数据，用于审计、调查和合规性管理。

简易统一的日志采集与报告

大多数安全分析师和 IT 管理员在进行合规性审计或试图弥补其他安全控制措施的漏洞时，对终端日志有着强烈的需求。当 macOS 从 syslog 日志文件转向统一日志系统后，企业层面收集、盘点和检查这些信息变得更加困难。macOS 的 Console.app 应用程序为本地 Mac 上的统一日志基础设施提供了出色的访问和可视化功能，但它无法让组织轻松集中管理这些数据。

借助 Jamf，客户端日志在写入统一日志后即可实时流式传输至记录系统。为确保仅收集目标数据，Jamf 管理员采用与内置 `log stream` 命令行工具相同的谓词过滤语言（NSPredicate）。由此，为 Mac 日志数据建立记录系统变得简单易行，无需逐台设备进行繁琐的收集。例如登录和注销、SSH、AirDrop 以及授权事件。如果数据被记录到统一日志中，Jamf 即可收集这些数据。

符合 Apple 的标准。

发布当日支持

为与 macOS 进行交互并收集安全决策所需的数据，Jamf 利用了 Apple 原生技术。这些技术包括新兴框架，例如 Apple 公司的终端安全 API 和声明式设备管理协议（设备管理框架的演进版本）。通过采用这些机制，Jamf 最大限度地减少了对设备的影响，且不会因补丁或重大操作系统版本更新中引入的 macOS 变更而产生冲突。尽早且频繁地打补丁是最常被推荐的安全协议。严格遵循发布当日支持的安全工具是遵守该协议的核心要素，也是全面深度防御安全策略的关键组成部分。

用户体验作为一项功能

Jamf 持续监控应用程序和用户活动以识别潜在威胁，但刻意不扫描休眠状态或与 Microsoft Windows 相关的恶意软件。对仅存在于文件系统中的文件进行扫描以检测大量恶意软件特征，往往是导致用户体验不佳的主要因素。该方法与 Gatekeeper/XProtect 保持一致，即在威胁可能执行时进行识别，从而最大限度地减少对用户体验和生产力的影响。

声明式设备管理框架

在 WWDC 21 上宣布的声明式设备管理（DDM）是设备管理协议的演变和更新。通过 DDM，设备可以主动应用管理设置、自动报告状态变化，并与 MDM 服务器进行异步通信。这标志着从传统的命令响应模式向更高效、更自主的方法的重大转变。

隐私

Jamf 分析设备上的数据，仅在配置后收集相关信息，通常是在实时检测到潜在恶意或高关注度活动时进行。这在企业需求与用户隐私之间实现了平衡，因为从设备中提取并存储在云端的数据更少。若检测到任何恶意活动，系统将把该活动及其相关数据传递至 Jamf 云控制台或已配置的安全信息与事件管理（SIEM）系统。任何超出上述范围的特定请求数据也会推送到 Jamf 或 SIEM 系统。通过过滤掉所有无关数据，负责监控和调查事件的安全分析师能够获得高质量的适用数据集合。

Apple 安全模型的其他扩展

最佳实践：强化 macOS 安全

尽管 Apple 提供并支持着市场上最安全可靠的操作系统之一，人们仍常会思考：还能采取哪些额外措施，让 macOS 更完美地契合企业环境？

最佳的第一步是开始利用 Apple 的移动设备管理（MDM）框架，实现大规模自动化管理。MDM 不仅能帮助您更好地保护您的组织，还将大大减轻 IT 部门在管理和保障设备安全方面的负担。

随OS X 10.7（“Lion”）推出的 MDM 框架，为定制设备功能以满足组织特定需求提供了海量工作流方案。配置文件和管理命令是利用移动设备管理（MDM）确保团队无论身处何地都能保持安全的两种最常见方式。

通过将 MDM 与 Apple 商务管理的强大功能相结合，将安全防护提升至全新高度。Apple 商务管理是 Apple 为企业提供的免费解决方案，可帮助自动化硬件采购、管理等流程。

从 Apple 开始...

多年来，Apple 以安全至上的理念赢得了声誉，这一点在 macOS 系统中得到了充分体现。每台加入组织环境的新 Mac 设备均可使用原生功能，包括 FileVault 2 加密、双重认证、远程锁定/擦除功能，以及强制执行密码标准的能力。

现代管理与安全平台（如 Jamf）借助 Apple 的最新技术，将这些功能进一步深化，助力用户针对加密等重要安全工具实现定制化部署、强制执行及报告生成。

...通过 Jamf 实现增强。

虽然移动设备管理（MDM）为任何组织提供了坚实的基础，但许多人仍在思考：他们还能采取哪些措施来进一步提升安全态势并强化员工隐私保护？这就是 Jamf 发挥作用的地方。

众所周知，当设备数量达到一定规模时，设备管理工作就会成为团队资源的巨大负担。更多的人意味着更多的硬件，而更多的硬件意味着更高的 IT 开销。

至少，在 Jamf 这类平台出现之前确实如此。

借助蓝图和智能组等专利技术来帮助管理企业设备并自动执行管理功能，IT 团队能够减少耗费在设备管理的琐碎事务上的时间，从而腾出更多精力处理其他日常 IT 任务。智能组将实时监控设备库存，根据设备状态变化自动将设备添加至预定义组或移出该组。

macOS 现代身份管理

现代安全的核心在于身份——为终端用户提供安全且定制化的访问权限。传统 IT 系统依赖本地目录服务作为员工信息的集中存储库，例如姓名和部门信息。随着安全和部署需求的不断演变，企业必须将身份与访问管理纳入其企业战略，并采取全新方法来应对这一挑战。借助完整的云端身份管理平台，企业能够在硬件和软件层面统一身份管理，从而释放功能潜力、实现先进工作流，最终推动业务转型。

基于目录服务的信息，基于云的单点登录（SSO）确保终端用户输入安全凭证即可访问公司资源。

Jamf 扩展了这些常见的身份管理形式。

Jamf 通过无缝认证流程，在所有公司应用和用户的 Mac 设备上实现统一身份管理。终端用户通过单一云身份，能够轻松快速地访问所需资源，从而提升工作效率。

借助 Jamf，组织机构可获得：

- 开箱即用的精简配置与身份验证，全面支持远程及现场员工
- 用户身份与设备凭证的自动化同步
- IT 部门在所有服务和设备上提供完整的身份管理能力
- 零信任网络访问（ZTN）解决方案，旨在取代传统 VPN（虚拟专用网络），满足现代混合企业的需求。

在 Mac 上响应并修复威胁

Jamf 提供仪表板，帮助组织随时掌握其 Mac 设备的状态，并标记需要关注的硬件。通过专利智能群组功能，IT 管理员可精准定位需要更新或打补丁的设备，从而提升其安全防护水平。所有操作均可远程完成并实现自动化，因此 IT 人员无需实际接触设备。

当将 Jamf Protect 与 Jamf Pro 结合使用时，威胁修复能力将更上一层楼。借助这项智能组技术，所有 MDM 和 Jamf 命令均可根据基于活动的警报进行协调执行。这包括自动网络隔离、条件访问失败、用户通知以及其他多种针对性的修复和响应措施。

超越设备管理的安全防护

阅读我们关于 Apple 企业安全现状的报告，该报告调查了1,500名 IT 和信息安全专业人士。其中涵盖当前设备使用情况及相关方法、设备安全面临的挑战以及终端安全的发展前景。

Jamf for Mac

现代组织需要统一的方法来大规模管理和保障 macOS 设备的安全。Jamf for Mac 通过整合 Apple 内置防护功能与先进能力（如身份和权限管理、可移动存储控制及威胁预防）来实现这一目标。这构筑了分层且符合 Apple 安全理念的防护体系，在实时保护设备的同时，不会破坏用户期待的熟悉 macOS 体验。

借助 Jamf for Mac，组织能够更深入地洞察设备活动，更严格地遵循合规基准，并具备实施最小权限原则、管控可移动存储介质以及防范基于网络的威胁的能力。这些功能有助于降低整个 Mac 设备群的风险，同时保持用户生产力并延续流畅的 Apple 体验。

通过将管理、身份验证和终端安全整合到一个以 Apple 设备为核心的解决方案中，Jamf for Mac 使组织能够全面保护 macOS 设备，并在 Mac 部署规模持续扩大的过程中从容应对。

jamf

立即开始，
或联系您首选的经销商，免费试用 Jamf。

www.jamf.com/zh-cn/