



Mac 端点遥测

Apple 专家为您提供 Mac 的实用见解



Telemetry

Telemetry collects system and user event log data and sends it to a SIEM. Telemetry log data helps administrators and security specialists proactively monitor and detect threats on macOS computers in their environments. Telemetry log data also assists with investigations of user activities or malicious events by providing context for the various events that occur on each device.

Create Telemetry

Telemetry – Set 1		Telemetry – Set 2		Telemetry – Set 3	
Acme, Soft: customized telemetry set for meeting CMMC – Level 1.		Acme, Soft: customized telemetry set for meeting NIST-900-171 framework.		Acme, Soft: customized telemetry set for meeting EO 14028 (formerly M-21-31). Acme, Soft, is using telemetry to achieve compliance.	
Usage Overview	Amount	Usage Overview	Amount	Usage Overview	Amount
Plans	0/1	Plans	0/1	Plans	0/1
Edit →		Edit →		Edit →	

Telemetry – Set 4		Telemetry – Set 5	
Acme, Soft: customized telemetry set for meeting the ENISA Framework.		Acme, Soft: customized telemetry set for meeting compliance for NIST 800-53 security baseline.	
Usage Overview	Amount	Usage Overview	Amount
Plans	0/1	Plans	0/1
Edit →		Edit →	

随着 Mac 在工作场所的使用越来越多，不良分子的兴趣和注意力也越来越大。

为了达到与其他平台相同的合规性、安全性和操作标准，Mac 需要量身定制的可视性和防御措施。

来自 Jamf 专为 Mac 打造的端点遥测技术

该遥测技术由 Apple 的端点安全 API 提供支持，并由 Jamf 20 多年的 Apple 专业知识进行策划，可对 macOS 活动进行深入审计。它提供相关的、完全可追溯的洞察力——流向安全团队日常使用的解决方案。

主要优势

- 遵守复杂的监管框架和安全基准
- 通过重建详细的攻击时间表，加快事件响应速度
- 猎杀高级 macOS 威胁，缩短停留时间并增强复原能力
- 与领先的安全供应商建立 SIEM 集成，实现无缝采用

将事件数据转化为行动。



下一代端点遥测技术

专为满足现代合规、安全和 IT 需求而设计

- 直接从 Apple macOS 端点安全 API 获取**高保真遥测数据**
- 与 macOS 安全架构**无缝集成**，提供防篡改、高完整性数据
- **设计轻巧**，在保持用户体验的同时，提供关键端点活动的细粒度可视性



无与伦比的 macOS 可见性

前所未有的深入了解您的 Mac 机群

- **从各个角度** 对流程执行、身份验证、特权操作、用户访问和提升、持久性、内置安全事件**等**活动进行审计
- **以 macOS 为重点的数据模型** 可为 Apple 设备的合规性审计、威胁检测和调查提供量身定制的洞察力
- **量身定制的洞察力**：我们以 macOS 为重点的数据模型可为 Apple 设备的合规性审计、威胁检测和调查提供量身定制的洞察力



加速调查

Apple 专家针对 macOS 威胁构建的遥测技术

- 利用可追溯的流程遗产和全面的遥测相关性**重建事件时间线**
- 利用对异常情况、罕见事件和常用 macOS 攻击技术（如 "离地生存"）的洞察力来**检测攻击者**
- 通过精细化、情景化的遥测技术，**快速做出安全决策**，从而增强快速调查和响应的能力



轻松集成

采用只需几分钟，而不是几周

- 通过对 Splunk、Microsoft Sentinel、Elastic、Google Security Operations 和其他 SIEM 的即插即用支持，从 SIEM 解决方案中**获取更多** 信息
- 利用专门针对 macOS 威胁场景设计的**解析器减轻团队负担**，使遥测数据与 SIEM 的数据模型保持一致
- 为安全和 IT 团队提供大量文档，**确保无缝实施**

使用 Jamf 全面了解您的 Mac 端点。

Mac 端点遥测技术由 [Jamf Threat Labs](#) 提供支持：Jamf Threat Labs 是一个由经验丰富的威胁研究人员、网络安全专家和数据科学家组成的团队，负责调查未来的 Apple 安全威胁。



www.jamf.com/zh-cn

© 2025 Jamf, LLC. 保留所有权利。

要了解更多信息，请联系您的 Jamf 代表。

[申请试用。](#)

或者联系你的首选经销商。