jamf

Jamf Protect
终端安全防护能力

企业采用 Mac 做为工作设备的比例逐步提高，也引起了骇客对攻击 macOS 的兴趣。

jamf PROTECT

设备安全

- 防毒软件
- 行为侦测
- 资料控制
- 自动与自定义修复

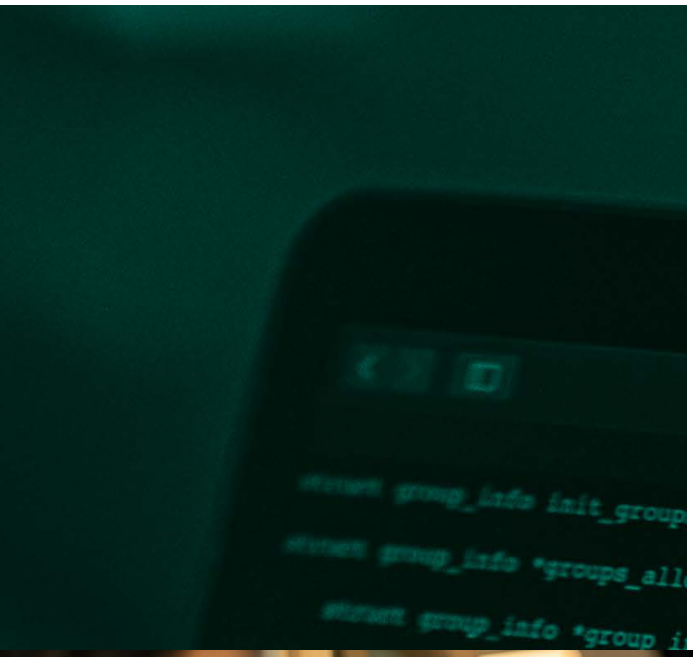
安全操作

- 自定义分析
- macOS 安全能见度
- 威胁猎捕
- CIS 框架
- 日志集中管理
- SIEM 整合
- 设备隔离
- 设备锁定
- 文件修复
- 隔离使用者
- 锁定使用者

信息安全

- 监督文件完整性
- 应用程序控制
- 合规条件监测
- 标准化修复
- 应用程序报告
- 重新部署 macOS

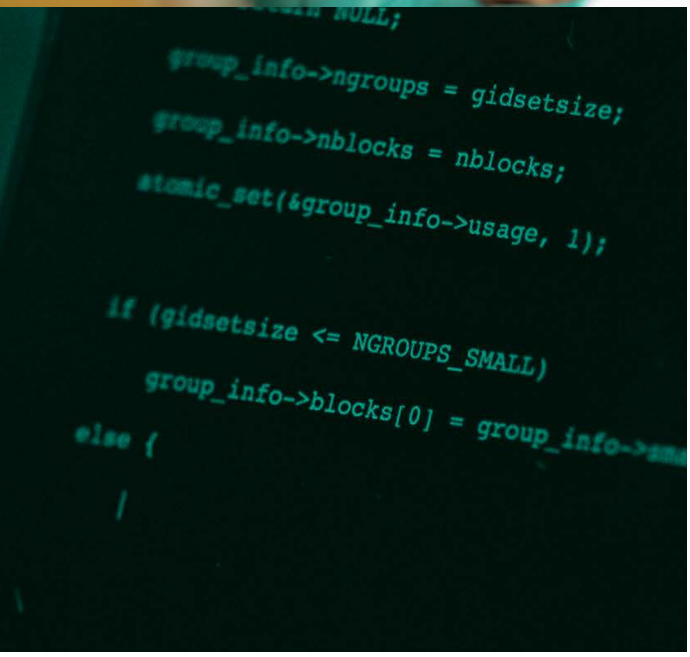
Jamf Protect
Jamf Pro
Jamf Connect



当 macOS 从 Unix 的世界发展出来，其对文件、软件与网络的内部处理方式，使 macOS 成为一个独一无二的操作系统。面对这样的环境，针对于 macOS 的攻击方式，就与攻击 Windows 或其它操作系统的方式不甚相同。然而，多数的安全防护软件公司仅将过往针对 Windows 的系统扫描、防护及修复等功能，移植到 Mac 平台上。

由于现今我们所常见的一体适用信息安全工具并不是为 Mac 所设计，企业很可能会因此忽视了存在于 Mac 架构上的攻击。为了要能面对并强化你的企业信息安全问题，提供专门为 Mac 设计的信息安全平台，到公司目前的安全架构里显得更为重要。

Jamf Protect 是一个专为 Mac 量身订做的终端安全解决方案，持续保障 Mac 设备在公司合规下，聚焦于 macOS 上的恶意程序与威胁，掌握应用程序情报，在最不影响使用者的情况下，侦测并修复针对 Mac 的威胁，维持 Mac 一贯的使用者体验。若同时整合了 Jamf Pro 或 Jamf Connect，Jamf Protect 就能展现出更强大的自动化、调查研究与修复能力，处理 Mac 设备上大大小小的安全风险。



Jamf 建构于 Apple 为 macOS 设计的安全核心框架，并承诺 Apple 同天支持，当每次操作系统更新时，取得更贴近企业的强大防护力、管控力、能见度以及更完善的威胁修复能力。有别于一体适用的信息安全解决方案，通常会在 Apple 发表新版操作系统时存在空窗期。Jamf 则是无缝地与最新版 macOS 衔接，随时保护使用者免于威胁，不受到任何耽误。

专注于 Mac 的防毒软件

防毒软件是大多数组织最基本的安全需求。 Apple 内建的 macOS XProtect、Gatekeeper 与 MRT 技术，提供了最基础的防毒软件机制。然而，这些科技并未提供相关行动的数据资料，更新也较不定期。 Jamf Protect 提供了深度的防毒软件功能，延伸了 macOS 底层的安全科技，能够阻止并隔离 Mac 上的恶意程序，而且远远超过以 Windows 做为基础的防毒软件所能提供的。

- 防毒：避免知名 Mac 恶意程序在设备上运行
- 能见度：提供组织了解 macOS 内建的 XProtect 与 Gatekeeper 运作状况
- 洞悉恶意程序：借助于 Jamf 及其它第三方对 macOS 的恶意程序分析数据，预防常见恶意程序运行
- 隔离：当恶意程序被识别时，自动从使用者环境移除并且隔离作为分析使用
- 使用者体验：Jamf Pro 能确保使用者采取正确措施，尤其在 Jamf Protect 识别到恶意行为时，以防止类似事件再度发生
- 文件捕捉：当威胁被识别时，从 Jamf Pro 取回文件样本

专注于 Mac 上的侦测与响应

传统的终端侦测及响应（ EDR）工具已存在 Mac 市场一段时间，但大多数并未能针对 Mac 打造，使其拥有比较好的效率去侦测威胁。反而，这些工具更倾向于把 Windows 的模式强加于 Mac 设备上。由于 Jamf Protect 仅聚焦在 Mac，因此 Jamf 能显著降低不正确的回报，而且能够大幅提升在 Mac 上的侦测效率。随着与 Jamf Pro 一起使用，Jamf Protect 得以最小化破坏式修复，赋予其远超过于其它 EDR 的平均能力。

- 行为分析：从一系列在设备上的行为分析，侦测未知恶意程序或进阶威胁
- 涵盖多项警示范围：Jamf Protect 能警示 MiTRE ATT&CK 框架事件，包含初始访问时间、运行阶段、持续潜伏、权限提升、防御逃脱、条件式访问、发现、横向移动、收集、渗出与冲击等类别
- 通知：Mac 以即时的方式透过 Jamf Protect 控制台、电子邮件或是你的 SIEM 等触发安全警告
- 通知内容：取得深入完整的信息，了解为何安全警示被触发，省去你在分析上的不必要猜测
- 降低伪阳性反应：在你的环境里任意调整侦测方式，以最小化误判事件
- 自定义侦测：为你的组织自行定义侦测内容，最小化信息安全风险

安全事件响应

当攻击被侦测到时，会启动一连串的机制，包含威胁隔离、移除威胁，或者将使用者或设备移回信任状态。使骇客在组织内缺乏至其它设备的攻击点，也就越不能偷取资料、毁损数据或是伤害企业。大多数的自动化安全事件不会通知终端用户，在某些情况下，会由安全团队决定下一步动作。

- 隔离：避免恶意程序运行并隔离，以降低延伸后果并做为分析使用
- 通知使用者：教育使用者以防止未来类似事件再次发生
- 自动化复原：自动在资安事件发生时，触发 Jamf Pro 修复程序，减少设备停机时间
- 文件取回:与 Jamf Pro 搭配使用，从被标记恶意行为、需调查的设备上取回文件

- 资料收集：当威胁被识别时，由 Jamf Pro 从设备上取回稽查必须的资料
- 隔离设备/使用者：从 Jamf Pro 自动限制设备访问网络资源，或是经由 Jamf Connect 禁止使用者访问资源
- 锁定设备/使用者：当威胁使设备不再受到信任时，自动使用 Jamf Pro 锁定该设备，或是利用 Jamf Connect 锁定使用者
- 重新部署 macOS：Jamf Pro 通过远程重新安装 macOS 操作系统与应用程序，将一个非受信任的设备复原至信任状态
- 引导使用者：当可疑事件被侦测到时，经由 Jamf Pro 重新引导使用者至内部培训教材

控制应用程序以最小化风险

确保使用者不会安装带有对公司或内部资料产生危害的应用程序。Jamf Pro 能让组织提供一系列已信任的应用程式到使用者，而安全部门往往需要更深要求，有了 Jamf Protect，你将能控制：

- 不受信任应用程序：避免不希望的应用程序在公司设备上被运行
- 避免已知威胁：避免执行具备弱点的软件版本
- 不信任的开发者：避免未受信任开发者所开发的程序在设备上执行

监控合规行为与威胁捕捉

成熟的安全团队会从多个安全工具上识别恶意行径与收集多方资料。换句话说，IT 团队经常需要共同分担收集资料的重任，做为合规稽查所用。无论何种情况，有一个持续的流程，能从设备上取回正确资料至中央是非常必要的。

- 行为能见度：以最不影响使用者体验的前提下，在 Mac 上收集文件、程序与认证信息
- 设备日志：导出设备日志资料（从 macOS 的日志纪录） 做为离线分析
- 资料集中：将资料统一收集至 SIEM 或其它能做为交互参考或长期保存的系统

资料控制

当使用者及其设备变得越来越移动化，也越来越分散的同时，保护资料越便成为组织成功的中核心，聚焦于资料是如何被流动与传出更是必要。

- 监控 USB 设备使用：抓取 USB 设备使用量以确保只有信任设备可被使用
- 控制 USB使用：利用 Jamf Pro 限制设备使用 USB 存储设备
- 监控 USB 活动：提供 USB 存储设备上文件异动的能见度
- 监控屏幕截图活动：识别任一个未受允许应用程式尝试进行屏幕截图等行为

保持安全基准线

只要在意信息安全，启动操作系统上的设定以强化设备已是最佳实践。为不同操作系统所发展出的先进安全框架，也常被不同产业间分享与使用。现在，部署与维护这些设定已成过去式。

- 监控指标：监控设备符合 Jamf Pro 所部署的安全设定基准线
- 验证指标变化：快速识别设备里的指标变化
- 重设指标：在设备在使用 Jamf Pro 重设基准线
- 文件完整性验证：监看重要档案变化

更好的用户体验

Mac 用户期待在他们的设备上有一个流畅、稳定及有效率的工作体验。Jamf Protect 将用户放在心上 —— 保护使用者隐私并最小化冲击。

- 原生安全框架：支持苹果终端安全框架（ ESF）减少对终端使用者的影响
- 无需使用 Kernel Extensions（KEXT）：Jamf 应用程式提供使用者最大的稳定度，而且无需使用系统核心组件，而是在有必要时，使用系统扩充功能（System Extension）
- 同天支援：Jamf 产品总是能在 macOS 推出新版本时立即发布支持版本，从未延迟。安全与管理套件不应该成为推迟升级操作系统的借口
- 即时防御与侦测:即时地侦测与防止有害行为。不使用长时间的系统扫描功能影响设备性能。Mac 量身订做：Jamf 只为 Apple 而生。Jamf Protect 能识别在 Mac 设备上的攻击，而不是对 Mac 无作用的 Windows 威胁

生态系整合

很少有组织只在环境内，部署一项安全工具。不同的工具，能够互相在技术上或是程序上整合，才能最大化设备上的安全与效率。

- SIEM：资料与警报可被推送到你自己所拥有的 SIEM
- 自定资料库：资料与警报可被推送到你的 S3 储存库
- 通用第三方支持：资料与警报可被推送到你的 SOAR 及其它用以 HTTPS 接收 JSON 的系统

Jamf 提供工业级安全解决方式至你的 Mac 设备，具有高防御能力及侦测率。我们的解决方案简洁、直观，与 Apple 原生功能高度相容，并让设备在被保护时，仍能为客户带来高效率工作环境。

前所未见的能见度，领先业界的修复能力。
只为 Mac。

jamf

www.jamf.com