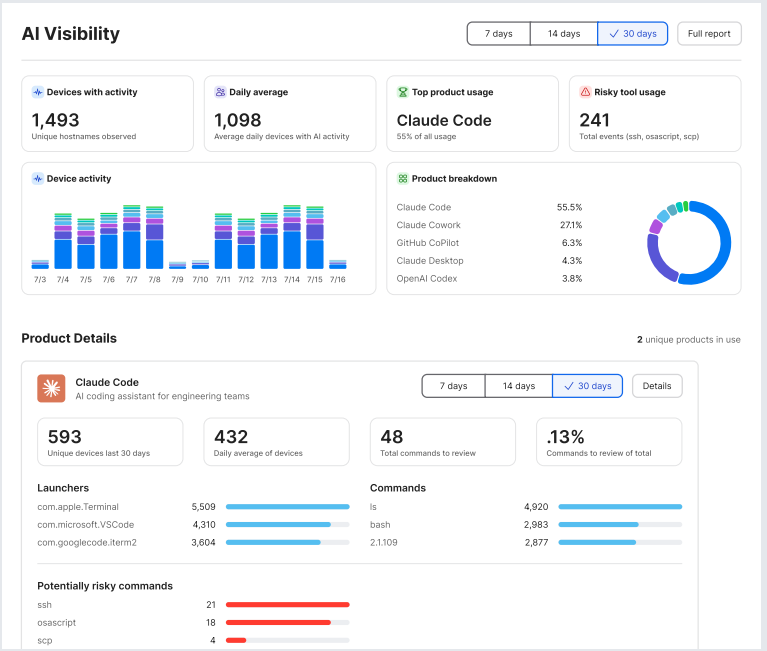
jamf

提高生產力：**安心治理 AI**。

唯一原生 Mac 端點解決方案，能透過您已熟悉的管理平面，大規模偵測、治理與部署 AI 配置。



影子 AI 早已存在於您的組織中。

從第一位員工下載 Claude Code、Cursor 或 Claude Desktop 的那一刻起，AI 工具就已進入您的受管 Mac 裝置群——它們具備正當的強大功能、原生執行，且完全脫離您的治理範圍。IT 能看見裝置本身。卻無法掌握 AI 在裝置上執行的各項操作。

這類工具運作模式不同於傳統軟體。配置狀態、MCP 伺服器連線與代理程式執行階段行為，對現有的裝置管理工具、網路代理伺服器與端點偵測平台而言皆不可見。這些工具內部其實已具備企業級控管機制，包含受管偏好設定、模型限制與網路邊界，但這些機制目前以原始 JSON 格式存在，且隨每次供應商版本更新而變動，無法大規模治理。

最終形成兩個未受治理的使用者群體，以及兩種截然不同的影子 AI 風險面向。執行 Claude Code 與 Cursor 的開發團隊面臨程式碼外洩、無限制存取模型以及自主代理程式不受政策邊界約束等風險。更廣泛的員工則使用個人 AI 帳戶上傳敏感文件，並透過 MCP 連接器查詢業務系統，相關行為無法被監控、無稽核軌跡，也無法向董事會提出具效力佐證。現有工具無法透過單一執行平面同時管控這兩類使用者群體。

AI 治理：Mac 上企業 AI 專屬配置平面

Jamf 為企業組織提供唯一原生的第一方解決方案，能在大規模 Mac 裝置群中檢視、治理與部署符合供應商規範的 AI 工具配置，將未受治理的 AI 轉變為可受稽核、具備佐證效力的合規狀態，無需新增基礎架構，也不影響終端使用者的生產力。AI 治理內建於平台中，部署方式與所有其他裝置政策相同：透過管理平面、於作業系統層級執行，並留存完整稽核軌跡做為佐證。

關鍵功能

AI 應用程式清單盤點	運用跨平台供應商無法複製的第一方端點資料，呈現 Mac 裝置群中運行的所有 AI 工具——由誰啟動、連線至何處，以及哪些工具呼叫具有最高風險。
MCP 伺服器清單盤點	檢視裝置群中運行的所有 MCP 伺服器、其所開放的資源，以及哪些 AI 用戶端與之連線，讓您在制定任何政策規則之前，就先掌握需要治理的對象。
供應商感知政策建置器	無需編輯 JSON 即可配置 Claude Code、Claude Cowork 與 OpenAI Codex。三種精選政策範本：寬鬆、平衡、嚴格——經 Anthropic 驗證，可在單次作業中完成部署
透過 MDM 的防竄改強制執行機制	AI 政策以 Jamf 藍圖形式部署，並於作業系統層級套用，開發人員與終端使用者無法覆寫特定的防竄改設定。
供應商控管追蹤引擎	自動監控 Anthropic 版本發布，並在數天內標記新增或變更的控管項目——政策無需手動審查週期即可保持最新。
治理報告與稽核軌跡	每套配置皆隨附一份 PDF 格式的高階主管 AI 態勢報告，內容包含：核可與未受治理工具的對比分析、完整稽核軌跡，以及歐盟 AI 法案對照表。報告可直接呈報董事會、自動產生，無需額外編寫。

透過您已熟悉的管理平台部署符合供應商規範的 AI 治理——無需新工具，也無需新技能。

- 讓開發人員從第一天起就使用配置正確的最佳 AI 工具，不會被 IT 拖慢速度。
- 免除手動編輯 JSON 配置的作業負擔。 政策建置器會追蹤每一次 Anthropic 版本發布並自動更新。
- 從全面封鎖 AI 轉為精細且由作業系統強制執行的政策，在提升生產力的同時不產生治理缺口。
- 透過您已用於管理 Mac 裝置群的管理平面，自動滿足歐盟 AI 法案的稽核軌跡要求與 SOC 2 義務。
- 為資安長（CISO）與資訊長（CIO）提供可直接呈報董事會的 AI 態勢報告，該報告自動產生且無需額外編寫。

AI 工具早已存在於您的裝置群中。現在即可完整治理。

AI 治理內建於 Jamf for Mac。現有客戶可輕鬆建置具稽核效力的 AI 態勢，難度遠低於預期。

jamf

www.jamf.com/zh-tw/

如需更多資訊，請聯繫您的 Jamf 通路代表。

立即預約試用。

或者聯絡您指定的經銷商。