Apple 裝置不再是例外
企業的隱形風險管理術

klickklack Communications

關於我

郭杰穎（Mouse Kuo）

可立可股份有限公司
執行長暨共同創辦人
<mouse@kkco.com.tw>

社團法人台灣駭客協會
理事
<mouse@hacker.org.tw>

可立可的服務涵蓋：連結 Connectivity、協作 Collaboration、合規 Compliance，以兼具韌性與彈性的服務賦能企業

HITCON 於 2005 年起成立，除每年的資安研討會，亦透過駭客協會，希望替臺灣的資安 產業盡一份心力。

駭客對 iOS 越來越有興趣

越來越頻繁的 iOS 更新 與 越來越多的 CVE 修補

- 2024.12.11（iOS /iPadOS 18.2）https://support.apple.com/zh-tw/121837
  - 41 個 CVE 修補
- 2025.01.27（iOS /iPadOS 18.3）https://support.apple.com/zh-tw/122066
  - 28 個 CVE 修補

- 2025.02.10（iOS /iPadOS 18.3.1）https://support.apple.com/zh-tw/122174
  - CVE-2025-24201 CVSS:6.1
- 2025.03.11（iOS /iPadOS 18.3.2） https://support.apple.com/zh-tw/122281
  - CVE-2025-24201 **CVSS:8.8**

- 2025.03.31（iOS / iPadOS 18.4） https://support.apple.com/zh-tw/122371
  - **62 個 CVE 修補**

CVE（Common Vulnerabilities and Exposures）是一套由美國 MITRE Corporation 維護的 資安漏洞識別編號系統，目的是讓全世界的資安從業人員有一致的方式來辨識與追蹤已知漏洞。

📈 越來越頻繁的 iOS 更新 與 越來越多的 CVE 修補

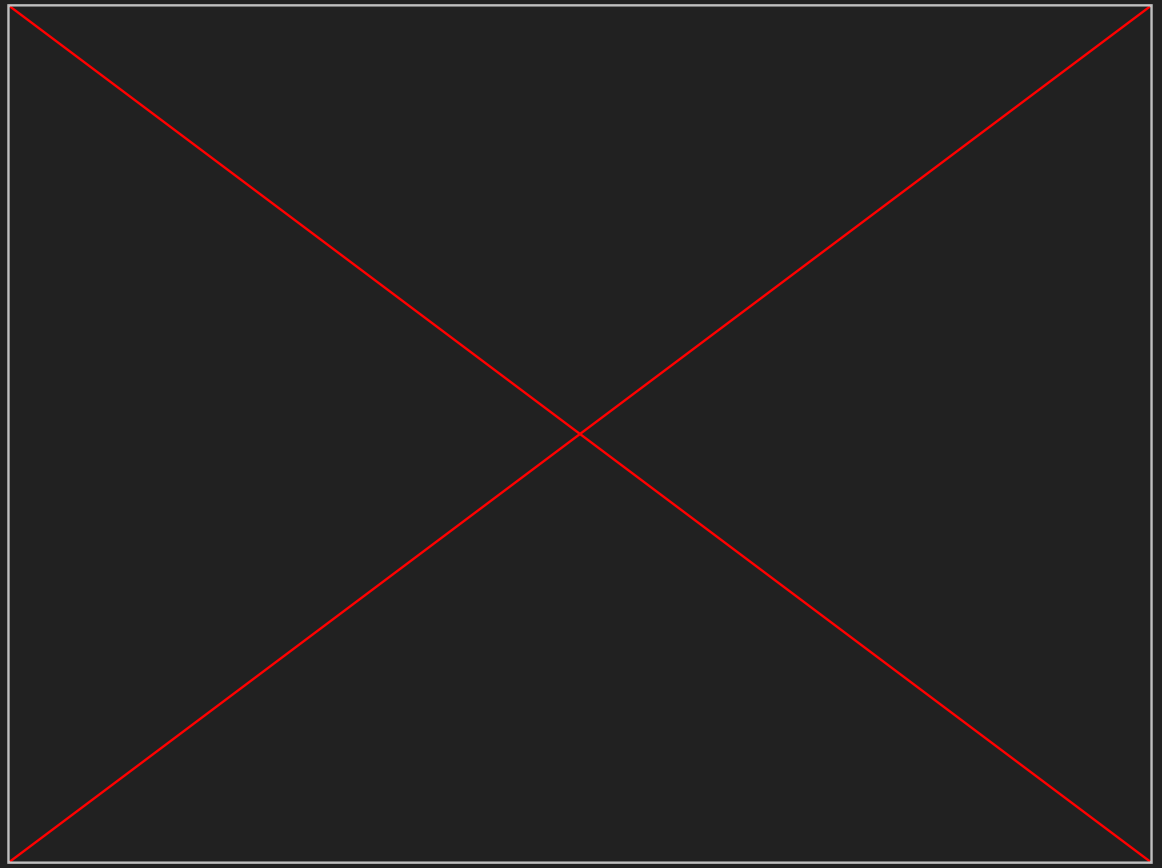
CVSS 分數範圍	嚴重程度標籤	中文說明
0.0	None（無）	無風險或資訊性漏洞
0.1 – 3.9	Low（低）	對系統影響極小
4.0 – 6.9	Medium（中）	有一定風險，但可控
7.0 – 8.9	**High（高）**	**重大漏洞**，建議儘速處理
9.0 – 10.0	**Critical（危急）**	**極重大漏洞**，需立即修補

2025.03.11 發佈更新，你有一週 內就更新嗎？

- 2025.03.11（iOS /iPadOS 18.3.2）https://support.apple.com/zh-tw/122281
  - CVE-2025-24201 **CVSS:8.8**

你真的有更新嗎？

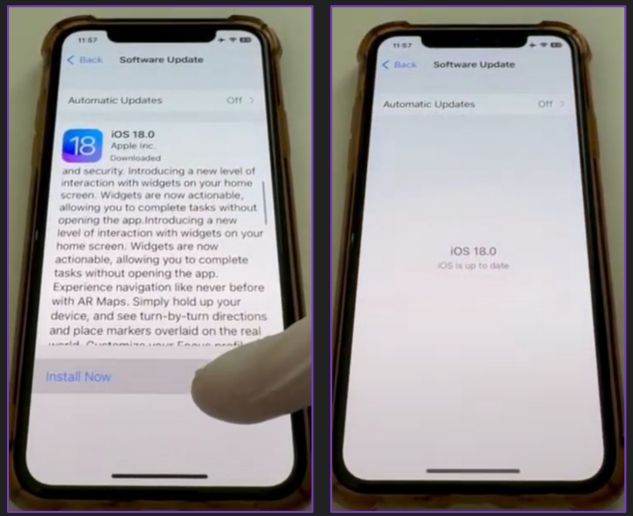
你真的更新了嗎？還是你以為有更新？



Jamf Threat Labs explores how bad actors use fake iOS updates to maintain persistence on compromised devices.
https://www.jamf.com/blog/fake-ios-updates-security/

偽造 iOS 更新畫面攻擊：你真的有更新嗎？

你以為你升級了，實際上是讓惡意程式可以留得更久。



- 攻擊技術核心：假 iOS 系統更新畫面
  - 裝置被入侵後，偽造「系統更新」的畫面。
  - 使用者甚至以為自己已經完成更新。
  - 利用機會隱藏駐留、阻止真實更新。

- 利用 UI 偽裝來操控使用者信任
  - 攻擊者模仿 Apple 官方更新提示、進度條、提示語言等介面細節。
  - 實際上，背後更新的是惡意程式架構，或阻擋裝置與 Apple 官方伺服器溝通。

Apple 設備 ≠ 工具
而是企業的基礎設施

所以，這不只是 IT 的事，而是企業營運的風險控制問題

企業環境有哪些合規要求？（節錄）

根據 ISO/IEC 27001 資訊安全管理系統「控制項設計」建議之資產保護原則：

- A.5.9 使用者端點設備保護（User end-point devices）
  控制目標：組織應實施適當的安全措施，以保護使用者端點設備免受威脅。
  安裝防毒與 EDR 軟體、啟用硬碟加密、設定螢幕閒置自動鎖定、管控裝置遺失風險、強制安裝更新　等。

- A.5.15 存取控制規則（Access control）
  控制目標：確保資訊與系統資源僅由授權人員依職務需求存取。
  建立 角色為本（RBAC）或 職責為本（PBAC）的權限模型、定期審 查權限、禁止共用帳號 等。

- A.5.16 身分認證資訊保護（Identity and credential management）
  控制目標：防止帳號或憑證外洩，確保端點與系統的存取行為可驗證且追蹤。
  複雜密碼原則、多因子認證（ MFA）、使用指紋等身份驗證技術 等。

- A.5.24/A.5.25 資訊安全事件管理準備 與 應對機制
  應具備裝置發生異常行為時的通報與處理機制：快速應對、減少損害並提升應變效率。

企業環境有哪些合規要求？（節錄）

根據 ISO/IEC 27001 資訊安全管理系統「控制項設計」建議之資產保護原則：

項次	項目	控制目標	實做建議
A.5.9	使用者端點設備保護 User end-point devices	組織應實施適當的安全措施，以保護使用者端點設備免受威脅。	安裝防毒與 EDR 軟體、啟用硬碟加密、設定螢幕閒置自動鎖定、管控遺失風險、強制安裝更新 …等組態基準（Configuration Baselines）。
A.5.15	存取控制規則 Access control	確保資訊與系統資源僅由授權人員依職務需求存取。	建立 角色為本（RBAC）或 職責為本（PBAC）的權限模型、定期審 查權限、禁止共用帳號等。
A.5.16	身分認證資訊保護 Identity and credential management	控制目標：防止帳號權限外洩，確保端點與系統的存取行為可驗證且追蹤。	制訂複雜密碼原則、多因子認證（ MFA）、使用指紋等身份驗證技術 等安全機制。
A.5.24 A.5.25	資安事件管理準備 與 資安事件管理應對機制	應具備裝置發生異常行為時的處理與 通報機制。 快速應對、減少損害並提升應變效率。	

Jamf 協助客戶設備合規

Center for Internet Security

Defense Information Security Agency (US)

National Institute of Standards and Technology (US)

National Cyber Security Centre (UK)

jamf

透過 CIS 白皮書達成裝置合規（節錄）

根據 CIS Apple macOS Benchmarks，針對 ISO/IEC 27001 控制項 A.5.9、A.5.15、A.5.16、A.5.24/A.5.25 的建議對應控制項：

項次	項目	CIS 建議控制項（節錄）
A.5.9	使用者端點設備保護 User end-point devices	• CIS 2.6.5 啟用 FileVault（全磁碟加密） • CIS 2.2.1 啟用防火牆 • CIS 2.6.4 啟用 Gatekeeper（僅允許受信任 App）
A.5.15	存取控制規則 Access control	• CIS 2.12.1 停用來賓帳號 • CIS 2.3.3.11 停用 Bluetooth Sharing
A.5.16	身分認證資訊保護 Identity and credential management	• CIS 5.2.3~6 強制密碼需含大小寫、數字、特殊字元 • CIS 2.10.2 睡眠或螢幕保護後要求密碼解鎖 • CIS 2.10.1 設定螢幕保護啟用時間（20 分鐘內）
A.5.24 A.5.25	資安事件管理準備 與 資安事件管理應對機制	• CIS 3.7 稽核軟體清單（透過 Jamf 可視化） • CIS 3.5 控制稽核記錄存取權限

透過 CIS 白皮書達成裝置合規（102項分類）

根據 CIS Apple macOS Benchmarks，針對 ISO/IEC 27001 控制項可依以下分類統計

編號	分類名稱	數量	分類目標描述
1	軟體與安全更新	7	確保系統與應用持續獲得最新的安全修補與更新，降低已知漏洞被利用的風險。
2	系統設定	41	建立穩健的系統預設 值與作業環境限制，防止錯誤配置導致潛在資安弱點。
3	登入驗證與存取安全	10	強化登入機制與裝置存取控制，避免未授權用 戶繞過身份驗證。
4	日誌與稽核	7	確保所有關鍵操作與異常行為皆可追溯與審 查，以利事件調 查與持續改進。
5	網路組態	3	限制不必要的網路服務與協定，減少攻擊面與未經授權的連線可能。
6	檔案系統權限與存取控制	8	維持檔案系統的最小權限原則，避免資料遭未授權使用者讀取或竄改。
7	密碼管理	8	建立符合強度與複雜度要求的密碼政策，阻止簡單或重複密碼被濫用。
8	系統存取、認證及授權	8	管理使用者角色與存取權限，確保只有授權者能操作敏感功能。
9	應用程式	10	控制預設應用行為與隱私設定，保護使用者資料與瀏覽活動不被濫用。

但是並不是所有企業
都會被要求 ISO 27001

有哪些事情建議先採取行動？

- 帳號與權限的管控機制
  目標：確定權限的建立和設定、帳號的發放，以及 **回收機制** 流程。

- 資安威脅有哪些可能性？可能造成的風險有哪些？

- 跟你的 20 美金顧問聊一聊：

GPT 怎麼說？

- 當你們作為一間 15 人的行銷公司，將客戶資料存放在 Google Workspace 時，首要風險是 帳號被盜用，可能來自密碼過弱、未開啟多因素驗證或釣魚攻擊，導致 Gmail 和 Drive 機密資料外洩。

- 其次，若員工使用來路不明的第三方應用程式，可能讓攻擊者存取你們的帳號與資料，成為隱性風險來源。

- 內部疏失也常見，例如文件分享設錯權限、離職員工帳號未關閉，或使用未加密的個人裝置處理工作，都可能造成資料外洩。

- 最後還要留意勒索軟體與供應鏈攻擊，若缺乏裝置管理、資安教育與規範流程，小型團隊一樣容易成為攻擊目標，遺失重要資料甚至影響商譽。

關於可立可

攜手 Jamf，結合 Workplace NaaS，提供從網路到裝置合規管理的整合方案

網路即服務 解決方案

- Workplace NaaS (Network-as-a-Service)
- 提供穩定、遠端維運的 **企業網路**
- 持續監控、即時應變、彈性擴充
- 免除企業自行部署與維護的負擔

X

Apple 生態系的安全與管理

一條龍 Jamf Managed Service

- 顧問導入、部署、代管、資安到合規
- 從 **員工體驗出發** 的裝置生命週期管理
- NaaS + ZTNA 整合部署：從端點到零信任

* ZTNA：零信任網路存取 Zero Trust Network Access
* MSP：託管服務供應商 Managed Service Provider

JAMF MSP

JAMF ELITE Partner

我們發現了什麼？

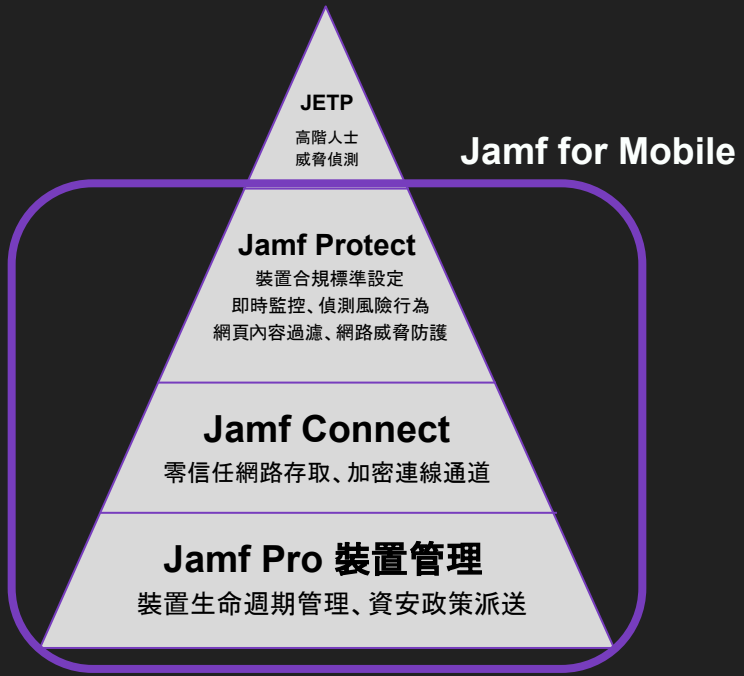
- 內網、外網的邊界越來越模糊：可以連線上網的地方就可以辦公。
  - 辦公室 WiFi 如何高效維運？透過可立可 Workplace NaaS 來達成。

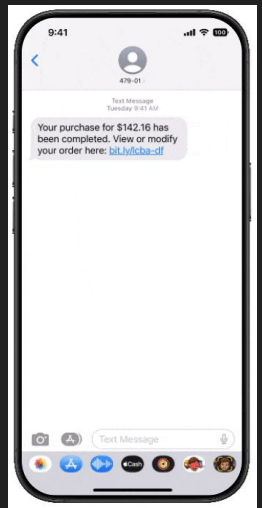
- 行動裝置的上網防禦、提升安全性
  - 隨時都可以連線，如何阻擋釣魚 / 惡意網站，越來越重要。
  - 透過 Jamf for Mobile 讓資安威脅可視化

- Mac 電腦的採用：降低營運管理成本的同時，提升資安等級
  - 站在巨人（Apple）的肩膀上：Apple 有相當完整的資安防禦框架，但沒有能見度
  - 透過 Jamf for Mac 滿足組態合規、落實上網防護、提升資安能見度。

適合全公司的資安防護

企業可以透過 Jamf for Mobile 提供行動裝置的全面防護。





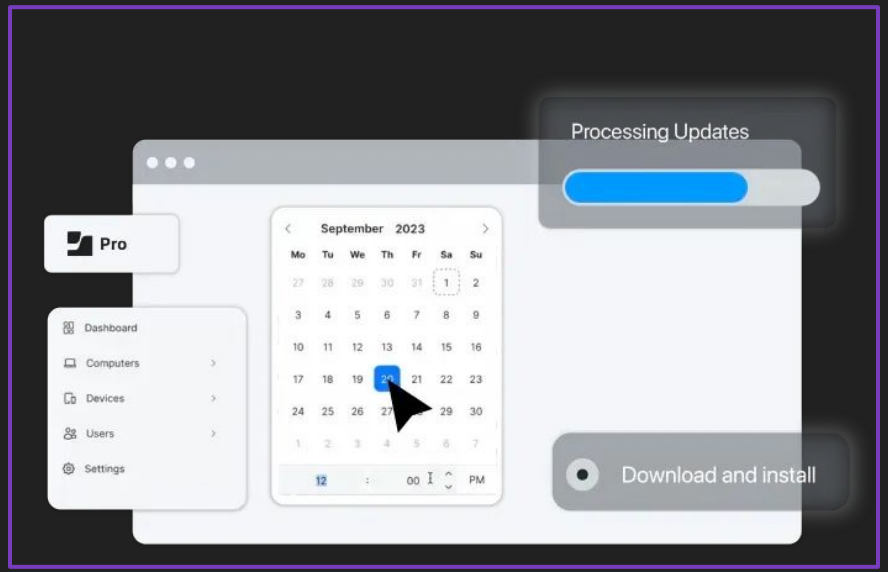
Jamf Protect
網路威脅防護

Jamf for Mac 能做什麼？

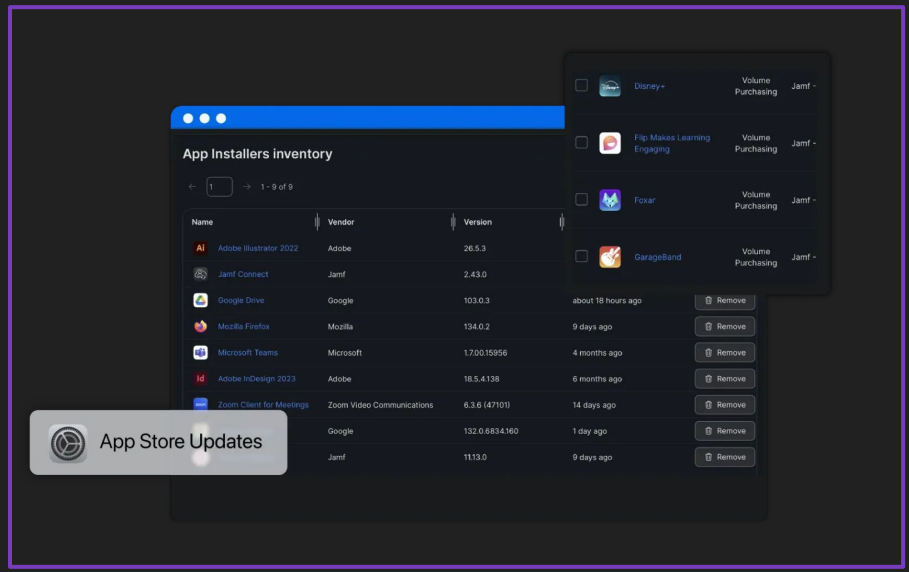
離職&密碼遺失 → 管理員權限回收 → 輕鬆重置密碼並回收裝置

電腦遺失 → 一鍵鎖定並遠端清除

Jamf for Mac 能做什麼？

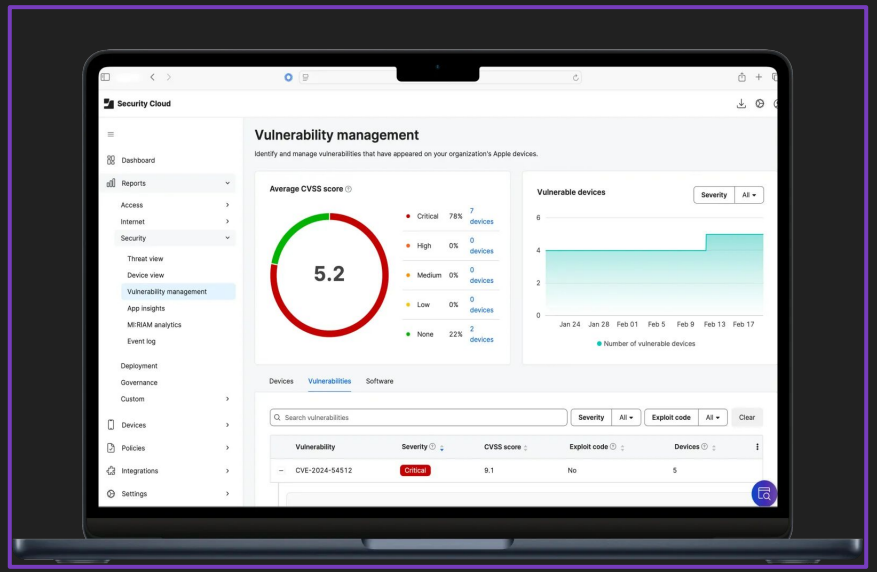


作業系統更新

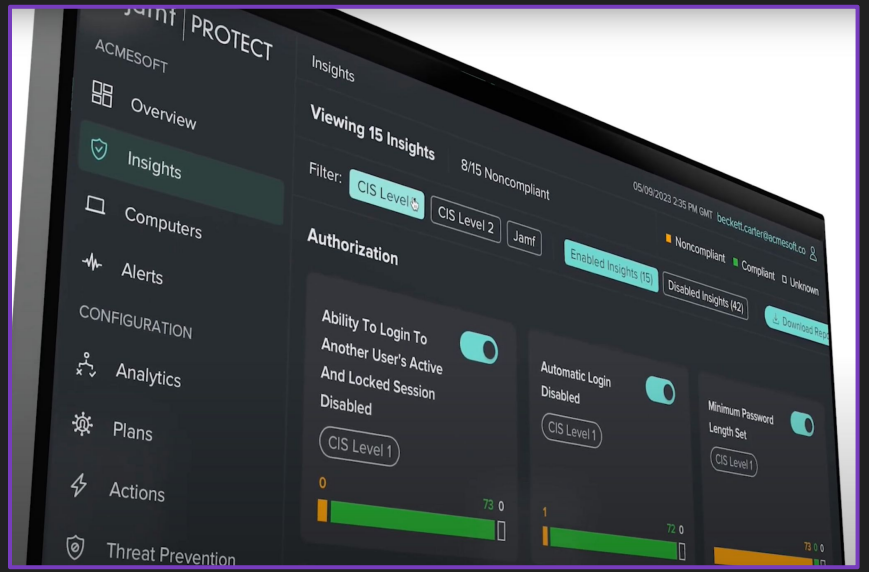


軟體版本更新

Jamf for Mac 能做什麼？

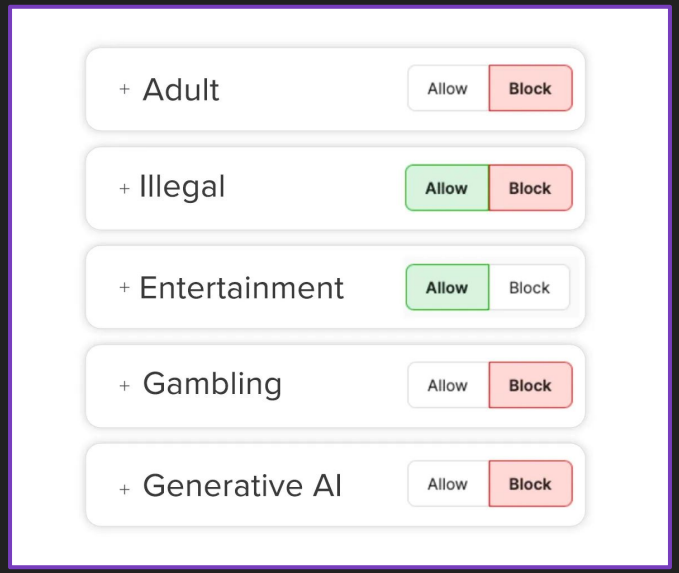


漏洞管理與追蹤

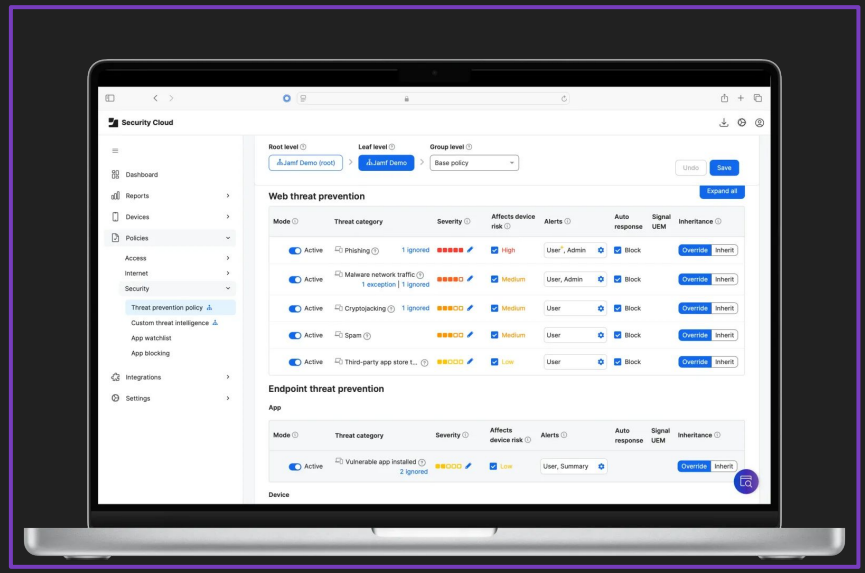


合規政策管理

Jamf for Mac 能做什麼？

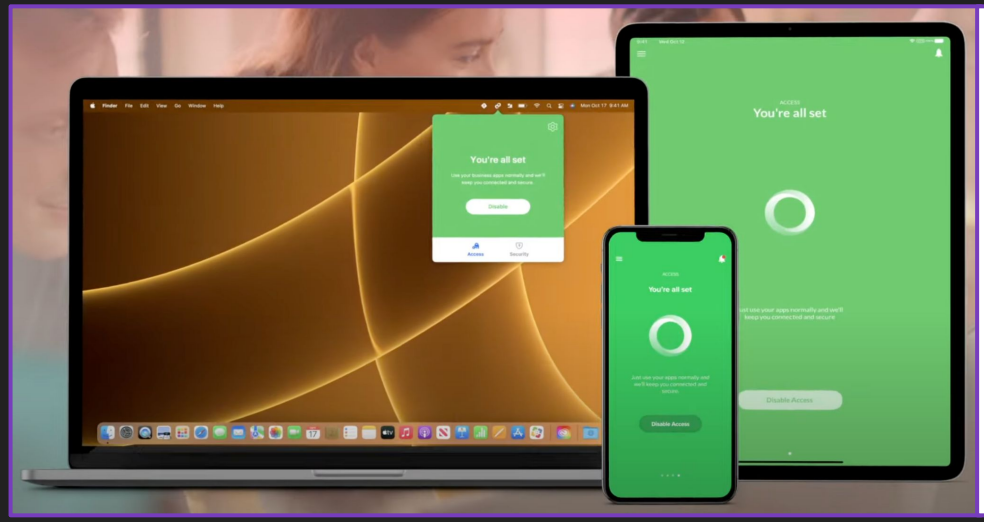


上網過濾政策



網路威脅防禦

Jamf for Mac 能做什麼？



建立安全加密通道:存取地端資源、連接外部　SaaS、實踐零信任網路架構

Key takeaways

1. 不是每個人都會面對合規要求。
2. 先釐清有哪些風險、以及威脅可能帶來的後果。
3. Apple 設備已經成為企業的重要基礎設施。
4. 站在 Apple 的肩膀：運用 Apple 的科技降低管理成本。
5. 我們不是從零開始，而是從 Apple 的安全架構出發，透過 Jamf 讓它變得可管理、可追蹤、可稽核。

可立可股份有限公司

統一編號：52554620
服務專線：02-2375-7775
傳真號碼：02-8978-2161
服務信箱：service@kkco.com.tw
通訊地址：114757 臺北市內湖區新湖一路85號4樓

klickklack Communications