jamf

全方位的 教育資安防護

結合 Jamf Protect 與 Jamf Safe Internet 的雙重防護

從 Mac、手機到平板，確保你的網路與使用者皆安全無虞

新型且複雜、看似來自可信來源的攻擊手法，即便已針對使用者落實嚴密的資安宣導，都還是需要額外的防護層。隨著 校園日益重視個人化學習與學生的獨立自主能力，學校也更容易面臨資安風險，因此更需要確保學生不受網路威脅的侵害。必須部署完善的解決方案，以化解學生與教職員對資安的疑慮。

將 Jamf Safe Internet 和 Jamf Protect 納入您的資安策略，結合頂級的網路威脅防護與龐大的內容篩選資料庫，能有效阻擋不安全內容以及惡意軟體、網路釣魚等攻擊，讓學生無憂無慮地探索學習。

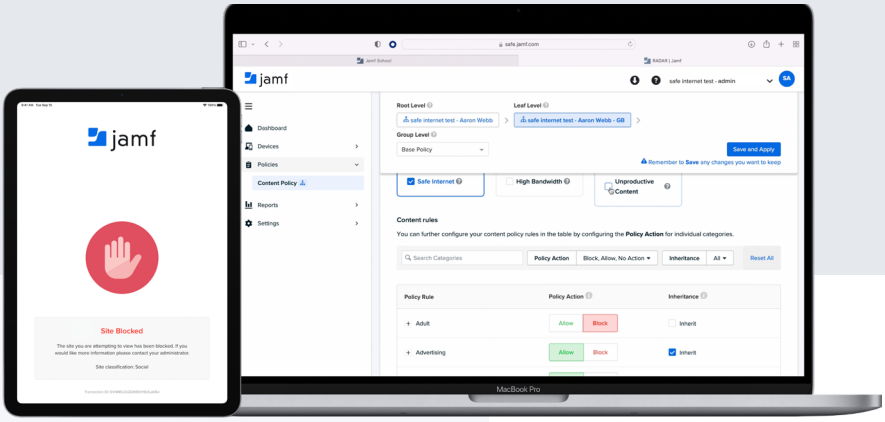
透過 Jamf 來實現完善的安全機制

- 保護終端使用者免受網路釣魚、惡意軟體等威脅攻擊
- 確實執行適當使用原則，而不只是流於形式或紙上談兵
- 在裝置上所有 App 執行強大的「內容篩選」功能
- 確保學生受到 Google 的「安全搜尋」和 YouTube 的「嚴格篩選模式」保護，即使在獨立作業時也不例外
- 提供強化安全性的同時，學生和教職人員不必擔心隱私受到侵犯

確保 Apple 教育裝置的安全

裝置端 **威脅防護**	應用 **程式報告**	**威脅情報**引擎 (MI:RIAM)
裝置端 **內容篩選 (ODCF)**	兼顧隱私 **的防護機制**	**安全搜尋** **與**限制存取

Jamf Protect + Jamf Safe Internet：
您將獲得哪些效益？



適用於 MacBook 與 iPad 的 Jamf Safe Internet：

網路威脅防護

Jamf Safe Internet 利用我們的 MI:RIAM 機器學習引擎，主動預防網路釣魚攻擊中常見的惡意網域等已知威脅。

裝置端功能

裝置端防護透過在網路底層架構執行，能提升安全性，防止使用者透過 VPN 或代理伺服器 (Proxy) 繞過規範；且無論在任何網路環境（包含學生家中）皆能持續運作。

政策排程管理

在校期間執行嚴謹的管控規範，而在家使用裝置時則提供更高的靈活性。透過時段性政策，管理員能輕而易舉地在安全性、合規性與家長的選擇權之間取得平衡。

隱私第一，首選 Apple

利用 Apple 平台上最新的 DoH 技術來防止有害內容，且不會侵犯學生的隱私

內容篩選

依據不同班級需求自訂內容篩選等級，防止學生接觸不當網路內容。

有限的隱私權

以學生隱私為首位，同時賦予學校管理權限。管理員可視需求開啟瀏覽活動的可見度，在不損及隱私的情況下，查看特定對象存取了哪些網站。

一加一大於二

與 Jamf School 和 Jamf Pro 皆可順暢整合，使部署和同步變得輕而易舉。

適用於 MacBooks 的 Jamf Protect：

端點防護

全面偵測並防禦專門針對 Apple 裝置的惡意軟體與攻擊。透過裝置控制功能管理外接儲存裝置，防止資料外洩。

SIEM 相容性

統一日誌與遙測資料 (Telemetry data) 可直接在 Jamf Protect 中查看，或串接至 SIEM/SOAR 系統，實現所有端點與使用者活動的集中化管理與可視化。

合規性與可視性

Jamf Protect 透過可自訂的合規回報機制與詳細的遙測數據，透視資安事件的各個面向，進而幫助機構實現裝置的合規目標。

jamf

www.jamf.com/zh-tw/

如欲了解有關 Jamf 的資安方案等更多資訊 歡迎前往 jamf.com/zh-tw/，也可以立即預約試用或者聯絡您的授權經銷商。