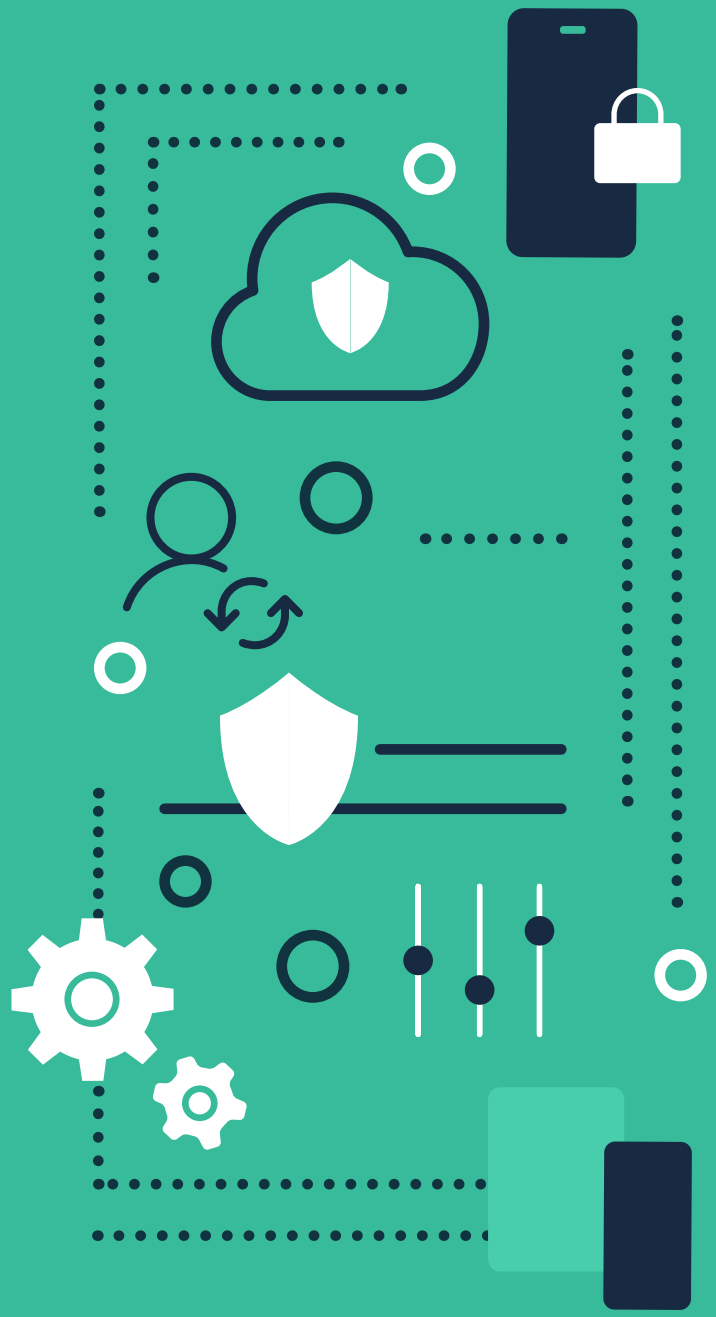


jamf

Mac 端點防護

入門

原生安全性不是終 (點)

毫無疑問，Mac 是市場中最安全的開箱即用裝置。這一點幾十年來一直沒有改變。組織在考慮其團隊組成時，用以保護資料、裝置與使用者的安全性解決方案便顯得至關重要。

在安全措施方面自鳴得意，反而可能導致會帶來損害或代價高昂的安全漏洞問題。憑藉 Mac 專用的端點防護解決方案，IT 與安全團隊不僅可以防範已知的威脅，還可以不斷適應與預測組織將來的安全需求。

無論您是擁有大量 Apple 裝置的企業，還是僅有少數 Mac 裝置的小型企業，Jamf 均可在 Apple 原生功能以外提供延伸的端點防護，相輔相成保護您的 macOS 裝置、組織的資料與端點使用者。

在本指南中，我們將討論以下內容：

- Mac 端點防護涉及
- 為什麼為多個作業系統設計的端點防護不足以保護 Mac

MAC 的端點防護：

將原生安全性優勢延伸至 Apple，並準備好解決未知問題。

隨著 Mac 在企業、小型企業、學校與醫療照護機構中更加普及，確保授權使用者以正確方式、基於正當目的使用裝置與資料，也就變得愈發重要—現在，就來進入 Mac 端點防護的世界吧。

為達成此目標，便要仰賴很多不斷變動的部分，包含身分識別管理、修補、防毒 (AV)、配置、端點偵測與應變，共同支援 IT 與安全性團隊的需求。

如需進一步了解管理企業資源、資料與使用者之資訊，請參閱我們的《身分識別管理入門》(Identity Management for Beginners) 電子書。

身分識別與存取管理

無論是現場還是遠端工作狀態，凡是透過身分識別管理實施的安全措施，都會在員工任職期間影響終端使用者與 IT 部門。零信任網路存取 (ZTNA) 解決方案、虛擬私人網路 (VPN) 與 SaaS App 可將員工連結到企業資源，都可提供加強端點防護的好機會。

隨著人力資源的特性日益靈活機動，有越來越多員工會在不同地點使用不同裝置工作，因此組織必須能管理並保護這些裝置及公司本身的資訊，同時不必被內部部署的 Active Directory 綁住。Jamf Connect 自始至終都為使用者提供支援。使用者在開箱 Mac 並接上電源後，只要使用一組雲端身分識別憑證登入，即可存取所有企業應用程式。組織可憑藉 Jamf Connect 使用對終端使用者體驗影響最小的方式監控身分識別與存取，同時享受一致的裝置與資料安全性優先權。

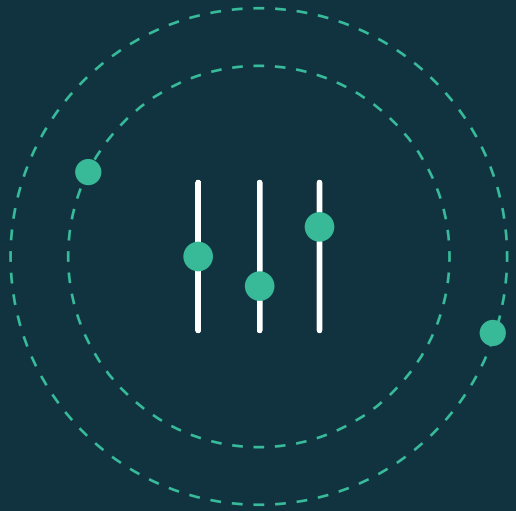
APP 管理

自動化 App 管理可簡化工作，並支援高效、安全的使用者。

確保使用者可透過安全的方法取得正確的 App，比如 Jamf Self Service 或 Mac App Store：

- 可將 App 部署至正確的使用者與裝置
- 在使用者需要時，他們都能使用自訂標題與 App
- IT 部門可以推送更新，並設定保護組織與使用者的要求

在 Apple Business Manager 中整合 Jamf Pro，以指派與管理您組織 App 與軟體的授權。此外，Jamf Pro 可協助進行修補與軟體更新。這也可確保您能更新與管理所有可能存在漏洞的軟體版本，並維持全體 Mac 裝置狀態的可見度。安全性修補應經常進行且可輕鬆完成，以確保能減少所有已知的 App 漏洞。使用 Jamf 可簡化 macOS 維護或更新 App 的必要工作，為其他合規性與相容性提供可見度，同時提供優質的終端使用者體驗。這也表示應在 macOS 最新版本發佈後即採用，以避免因升級延遲導致安全漏洞產生。



不應因安全與管理工具問題，而推遲作業系統更新或升級。只要使用 Jamf，解決方案就不再成為絆腳石，而且只要有新版本的 macOS 發佈，您就能立即獲得支援。您可以自行決定何時升級裝置，不必被我們左右。

防毒 (AV)

乍看之下，AV 是 Mac 的新需求，但時空環境確實也不再相同。隨著 Mac 與 macOS 在企業中更廣泛應用，大眾對其關注也日益增加。

在提供符合基準的安全措施方面，AV 是大多數組織用裝置必須達到的基本要求。Apple 在 macOS 中納入了一個基本 AV 機制，包括 XProtect、Gatekeeper 與 MRT。但這些工具只是偶爾會更新，組織也無法窺知這些工具的運作方式。Jamf Protect 新增了更精細完善的 AV 功能，以防止與隔絕針對 Mac 的惡意軟體，遠超過 macOS 中仍以 Windows 系統為重心的解決方案可提供的功能。

組織不應等待惡意軟體、廣告軟體或其他意外軟體問題出現，才著手解決問題。他們需要的 AV 應能有效識別與修復針對 Mac 的攻擊，而無需將寶貴的資源浪費尋找在 Mac 中針對 Windows 系統的威脅。有效、高效率與全面的 Mac AV 功能，對於安全性與裝置體驗均至關重要。另一方面，任何會干擾終端使用者工作效率的 AV 解決方案，卻會讓所有相關人員不勝其擾。Jamf Protect 旨在保護 macOS 免受惡意軟體損害，同時無需改變終端使用者對 Mac 體驗的期待。

Mac AV 已不再是奢侈品，而是必需品。您不僅需要 AV，還必須擁有 Mac 專用 AV，不受專為跨系統使用而設計之 AV 所造成的限制。

設定

Mac 具備立即可發揮作用的安全防護，仍是業界表現最佳，但隨著當代不斷演進的網路安全威脅，Mac 本身的安全防護仍稍嫌不足。您需要評估與改進您的安全性態勢，以保護您的裝置與資料。如果強化您的安全性很簡單，為什麼不做呢？

安全專家社群中已提供大量知識與程式碼，可用來協助您進行此工作。

利用 Jamf 即可輕鬆實作與執行這些資源，並監控所有試圖修改這些標準的使用者。Jamf 掃除了障礙，讓您可在各裝置中順暢設定符合基準的安全措施。

在定位您的安全性需求與基準方面，FileVault、啟用防火牆與密碼要求、設定螢幕保護程式與鎖定要求都各自發揮了作用。

不知道從何處開始嗎？資訊安全中心 (Center for Information Security，CIS) 提供了產業基準，而 Jamf 也已通過 CIS 認證。因此，有了 Jamf，您可說是已準備萬全，同時我們也有更多資源可用來協助您。

請參閱我們的 macOS 安全性檢查清單，進一步了解 CIS 安全性基準與 Jamf。

以 MAC 為中心的偵測與回應

用於 Mac 的傳統端點偵測與回應 (EDR) 工具已問世多時，但大多數工具並不是為了有效偵測專門針對 Mac 的攻擊而打造。相反的，這些工具往往會強行在 Mac 裝置上套用 Windows 模型。由於 Jamf Protect 是專為 Mac 與 macOS 所打造，因此 Jamf 可最大限度地減少誤報，同時盡量提高在 Mac 中的偵測率。

將 Jamf Protect 與 Jamf Pro 搭配使用後，您就具備了盡可能避免損害的補救能力，表現遠超出一般的 EDR 功能。IT 與安全團隊可藉由 Jamf 設定無縫事件應變方案，以便您的各個團隊可以合作無間。

JAMF 採用端點防護。

具備 Jamf Protect 的 Mac 端點防護可支援端點合規作業、透過防範 macOS 惡意軟體滿足防毒需求、控制與保護組織內的 Mac App，並偵測與修復特別針對 Mac 的威脅，同時將對終端使用者體驗的影響降至最低。

與 Jamf Pro 搭配使用後，Jamf 可解鎖豐富的自動化、調查與補救功能，以減少大大小小的端點安全性風險。

或預約免費試用。

或者，如果您準備好要加強安全防護措施，請聯絡您偏好的 Apple 經銷商。

進一步了解 Jamf 的端點防護功能。