填補資安缺口：macOS 安全性

資安需求橫跨各種作業系統，macOS 也不例外。雖然 Apple 投入大量資源提供內建的隱私與安全功能，但隨著 Mac 在企業市場的佔有率提升，攻擊該平台的獲益也隨之增加，使其成為惡意軟體、資安漏洞與破壞者的熱門目標。現在，更有越來越多公司透過「員工自選計畫」允許員工使用 macOS。在推行過程中，企業也意識到 Mac 就和任何平台一樣，需要額外的安全防護與可視化管理。

市面上有不少資安廠商提供 Mac 的防護解決方案，但其中許多仍沿用自家或 Windows 產品的安全模型，而非真正整合 macOS 所提供的現代化安全框架。
這樣的做法，讓解決方案難以跟上不斷演進的作業系統。相對而言，最佳實務應該是建立在既有的 macOS 安全架構之上，補齊不足之處，並加入符合 macOS 特性的關鍵能力，讓資安團隊能有效運作、全面保護組織。

Apple 作業系統將隱私與安全視為平台基礎，防護機制直接內建於硬體與軟體之中。與此同時，Apple 優先考慮直覺式的體驗，以支援易用性與生產力。因此，許多功能的設計主要是圍繞著個人使用者，而非組織的全面性需求，這正是「額外可視化」與「安全控制」顯現價值之處。

在本白皮書中，我們將概述 macOS 安全性的現況，並指導如何以高效、有效且友善的方式強化 Apple 的安全基準。

您將了解到：

- Mac 內建可用的各項安全功能與其運作細節
- Jamf 如何在企業環境中強化這些安全功能
- Jamf 如何將威脅偵測延伸至簽章與內建機制之外
- 進一步延伸 Apple 安全模型、滿足進階企業 資安需求的其他方式

macOS 上的應用程式

Apple 在設計安全功能上付出了巨大努力，以保護使用者及其執行的第三方應用程式。在此章節中，我們將介紹其中幾項功能，並探討如何透過策略性地強化與延伸。 欲深入了解 Apple 安全功能，請參閱 **Apple 官方完整的平台安全 指南**。

透過 Gatekeeper 驗證信任。

Apple 建議且最信任的第三方應用程式安裝路徑是透過 App Store。這讓 Apple 能夠審核並篩選不符合隱私、安全或使用者體驗標準的程式。然而，Apple 同時也限制了 App Store 中應用程式的權限，且許多對商務至關重要的應用程式並不適合透過此方式發布。

當無法選擇從 App Store 發布時，Apple 允許開發者透過直接下載或其他傳統管道分派應用程式。為了支援這些「點對點」的分派方式，Apple 在作業系統中加入了其他檢查機制，以降低軟體在 macOS 裝置間大規模傳播的風險。Gatekeeper 就是 Apple 驗證檢查機制的核心功能名稱。這項功能最初只是讓使用者依據風險承受度選擇是否執行程式，現在已演變成一套更全面、更嚴格的要求與緩解機制。雖然目前仍保有「App Store」或「App Store 與已識別的開發者」等基本信任層級，但執行有問題或高風險程式碼的空間已越來越小。

請注意，這些檢查僅適用於從網際網路下載的應用程式。Apple 會在下載的檔案附加額外的中繼資料（Metadata）來進行追蹤，這被稱為「隔離屬性」（Quarantine Attribute）。當程式執行時，Gatekeeper 會執行一系列檢查（例如驗證隔離屬性）來判斷是否允許執行。其中最基本的檢查項目之一，就是應用程式是否由合法開發者簽署，或是否來自 App Store。

如果應用程式是由開發者簽署的，系統會比對已撤銷簽章的資料庫，確保該簽署者過去沒有與惡意軟體關聯。透過這種方式，Apple 可以快速撤銷憑證，阻止惡意軟體大規模散布。

從 macOS Catalina 開始，通過 Gatekeeper 驗證還需要應用程式經過 Apple 的「公證」（Notarization）。為了通過檢查，應用程式必須上傳至 Apple 進行分析。分析成功後，公證數據會與該應用程式關聯，註記其已通過這層額外的檢驗。

最終的信任決策權仍在使用者手中。

為了顧及易用性，macOS 在許多情況下允許終端使用者「繞過」（Override）Gatekeeper。使用者只需右鍵點擊應用程式並選擇「打開」，系統不會直接拒絕執行，而是會彈出警告，告知這是一個未知或具潛在威脅的程式，但 Gatekeeper 仍會允許執行。值得注意的是，如果 XProtect 已明確判定為惡意軟體， 使用者就無法授權執行。

一旦應用程式完成首次執行，隔離組件就會更新，下次開啟時就不會再重複 Gatekeeper 的檢查程序。

⚠ 利用 XProtect 與 MRT 阻擋威脅。

Gatekeeper 相關 技術套件還包含了 Apple 基於特徵碼的偵測 機制， 即 XProtect 與惡意軟體移除工具 (MRT)。兩者 協同作業，掃描作業系統中的檔案，尋找與已知惡意軟體相關的特徵。 XProtect 在啟動應用程式時觸發， 而 MRT 則定期 掃描檔案系統。

是使用名為 Yara 的二進位特徵掃描引擎來運作。Yara 支援彈性且強大的二進位特徵定義，並擁有高效的執行引擎。為了驗證應用程式，XProtect 會在初次執行及後續更新後掃描每個下載的執行檔。如果偵測到相符的特徵碼，程式將不被允許執行。已知惡意特徵碼檔案是透過 Apple 獨立的 macOS 更新進行派發。Apple 負責定義並派發這些特徵碼，這與 Yara 執行引擎本身是分開處理的。與 Gatekeeper 類似，這項掃描僅在應用程式帶有隔離擴充屬性時執行，該屬性會在 應用程式首次成功執行後更新。

相對地，MRT 是採排程執行而非在程式啟動時執行，它會掃描檔案系統中與過去惡意軟體相關的特定檔名或跡象，並在發現時將其移除。此功能主要用於發現並補救可能已在大量 macOS 裝置中執行的已知威脅。

⚙ 將 Gatekeeper 延伸至企業環境。

Gatekeeper 確實發揮了其預期效果。它能阻擋不受信任的應用程式啟動，並在辨識出可疑或惡意程式時通知使用者。IT 與資安管理人員需要了解是否有在公司資產上執行不受信任軟體的行為。更重要的是，管理員必須知道使用者是否自行繞過了安全規範（例如透過右鍵強制開啟應用程式）。為了滿足企業需求，Jamf for Mac（專為 Mac 打造的端點安全解決方案）會監控 Gatekeeper 的運作跡象，並將結果回報至中心後台，讓 IT 與資安團隊能精確評估風險並做出正確決策。

除了提供 Gatekeeper 活動的可視化外，Jamf 還允許企業自行掌握開發者信任模型，將特定的簽署資訊列為企業環境中的「不受信任」名單。透過 Apple 最新的端點安全 API，Jamf 會主動禁止執行企業黑名單中的任何應用程式。這可以針對個別應用程式（App ID）或個別開發商（Team ID）來定義。

此外，macOS 並未針對各種「灰色軟體」（潛在不想要或未經授權的軟體）提供特徵碼或阻擋功能，這類軟體包括許多會進行討厭或潛在侵入行為的廣告軟體及挖礦程式。通常這類程式都擁有合法的 Apple 開發者簽署，且使用者在安裝時會同意收集資訊或使用資源——通常使用者是在不知情的狀況下點選同意。因此，在多數情況下，Apple 不會干預這些應用程式的運作。

然而，企業端的風險評估標準不同，通常需要更嚴格且精準的管理方式。因此，Jamf 強制執行自有的 Yara 規則、二進位特徵碼及不受信任的開發者憑證，無論應用程式是否帶有「隔離屬性」，都會在執行時進行掃描。這確保了當新的特徵碼加入或企業更新安全規範時，現有的應用程式在下次執行時會重新接受掃描，而不僅僅是第一次執行時才檢查。

Jamf 根據對 macOS 威脅的深入研究以及第三方威脅數據，整理出一套針對 Mac 惡意軟體的防護情資。對於希望更精細控制環境內軟體的組織，他們可以在 Jamf 阻擋清單中加入自訂的檔案雜湊值（Hashes）、開發者 ID（Team ID）等。在 macOS 10.15 或更新版本上，當應用程式執行時若符合已知惡意軟體的行為或特徵，Jamf 會阻止該程序執行、隔離違規檔案，並發出「已阻止惡意軟體」的警示。此操作獨立於 Gatekeeper/XProtect 之外，其設計功能涵蓋範圍更廣（互補且增強）。Jamf 在辨識已知惡意軟體時不會受限於隔離屬性標記，能精準識別潛在危險的檔案，並保有更廣泛的惡意軟體 知識庫。

透過 Self Service 延伸 App Store 的信任模型。

透過「自助服務」（Self Service）商店提供經 IT 審核過 的軟體資源，是規範使用者安裝程式的最佳方式。

Jamf Self Service 讓 IT 能建立企業專屬的應用程式型錄，讓使用者能安全且即時地自行安裝 App、更新環境設定或排除常見問題，無需提交報修單。

控制並監控應用程式 行為。

透過隱私控制功能來限制與確認應用程式行為。

系統隱私控制功能最初於 macOS Mojave 推出。這些控制項要求使用者（或企業）必須授權各別應用程式存取特定動作與資料夾。一旦授權後，該應用程式未來執行相同動作時就不會再重複詢問。此功能確保應用程式存取作業系統敏感權限（如視訊、麥克風、側錄按鍵、下載資料夾）時必須獲得明確許可，這能促使使用者停下來確認自己正授權存取私有數據。

超越控制：對應用程式行為進行審核與分析。

雖然隱私控制可以限制授權，但使用者仍可能出錯，且授權也有被濫用的風險。我們已經介紹了 Jamf 如何針對 Apple 內建安全功能提供可視化資訊，以及如何透過傳統惡意程式防護來保護企業。但在 Jamf，我們認為端點保護不應止步於此。Jamf 還提供了傳統上只有 EDR（端點偵測與回應）產品才有的審核與監控能力，且採用「Apple 優先」的開發理念，兼顧 macOS 使用者對隱私與安全的高標準。

使用 Jamf for Mac 進行偵測工程

Jamf 端點保護的核心是一個輕量化的使用者模式感應器（Agent），它利用了 Apple 內建的邏輯執行引擎 GameplayKit。雖然使用遊戲引擎來分析安全事件非常規的做法，但這讓 Jamf 能與 Apple 生態系緊密結合，在裝置端直接進行數據分析，僅在必要時才收集或回報。遊戲引擎原本就是為了處理海量的即時事件而設計，因此非常適合用來分析裝置上發生的各項活動。這與許多優先考慮 Windows 平台後才將功能移植到 macOS，或是要求將所有數據上傳雲端分析的解決方案形成了鮮明對比。

GameplayKit 的另一個優點是與 Yara 類似，它將執行引擎與偵測定義分開，讓偵測規則能獨立更新與擴展，無需更動核心 Agent。偵測定義也採用 Apple 原生的 NSPredicate，這是一種強大的邏輯查詢機制，支援一般查詢語法與正規表示式。Jamf 的數據模型經過專門架構，能發揮 NSPredicate 的豐富功能，包含呼叫原生函式與串聯數據模型。這解鎖了許多以傳統方式實作時會顯得雜亂、或耗費大量運算資源的功能。

例如，利用 Jamf 的數據模型與 NSPredicate，我們可以：

- 當檔案「自我刪除」時發出警示（這是常見的掩蓋攻擊痕跡手段）。這個看似簡單的案例，需要同時分析被刪除的檔案與執行刪除的程序，且無需複雜的關聯運算或寫死的偵測規則。
- 當未簽署或簽署異常的二進位檔轉化為持續執行的啟動服務（Launch Daemon）時發出警示。這涉及解析設定檔、從內容中提取嵌入的二進位路徑，並在分析中使用該檔案的元數據。
- 當 Microsoft Office 應用程式產生異常的子程序時發出警示，藉此識別 Office 巨集攻擊。這個案例強調了系統辨識父子程序關係的能力，以及揭發應用程式功能被惡意利用的行為。
- 當出現「就地取材」（Live-off-the-land）式的攻擊行為跡象時發出警示。這類活動需要存取父子程序關係、程序群組關係及指令參數等資訊，才能揭露那些平時看似無害的指令（如 curl、ssh、python 等）是否遭到濫用。
- 追蹤全企業範圍內的 USB 使用情況，並針對寫入至抽取式裝置的文件回傳中繼資料（Metadata）

為了讓您輕鬆了解這類偵測事件的影響，Jamf 會將識別出的攻擊行為對應至 MITRE ATT&CK™ 框架（若適用）。目前的涵蓋範圍包含框架中的各種案例，其中包括偵測以下類別的技術：

- 持續攻擊（Persistence）
- 初始入侵（Initial Access
- 指揮與控制（Command and Control）
- 防禦規避（Defense Evasion）
- 初步了解階段（Discovery）
- 特權提升（Privilege Escalation）
- 憑證存取（Credential Access）

透過 Mac 原生遙測（Telemetry）提升可視性

隨著組織加強其 macOS 安全態勢，深入了解系統與使用者活動變得越來越重要。Apple 原生框架提供了強大的基礎，但資安團隊通常需要更豐富且有關聯性的信號，來偵測異常行為、調查事件，並在大規模環境下維持合規。

Jamf 的遙測功能建立在 Apple 的「端點安全 API」（Endpoint Security API）之上，能從每台裝置收集詳細且針對 macOS 的專屬信號。這讓組織能精準分析系統、使用者、應用程式與網路活動，並使用能反映 macOS 運作方式的數據。遙測功能極為輕量且高效能，能確保不影響使用者體驗，同時具備防竄改特性，確保日誌與安全事件在調查與合規用途上維持可靠。

透過將程序、應用程式、身份驗證、設定變更與使用者操作等事件進行關聯，Jamf 遙測能協助資安團隊重構詳細的時間軸，並識別可能代表濫用或新興威脅的行為。

透過 Jamf 遙測，組織可以：

- 利用準確且高品質的事件數據，符合法規與內部合規要求。
- 偵測設定偏移（Configuration Drift）、影子 IT（Shadow IT）以及政策偏差。
- 透過分析關聯事件與攻擊路徑，加速事件響應（Incident Response）。
- 利用豐富且專為 macOS 設計的洞察，支援主動式威脅獵捕（Threat Hunting）。
- 與 SIEM 平台無縫整合，實現集中化的可視性。

這些功能提供了大規模管理與保護 Mac 裝置所需的深度與情境，為進階偵測與分析奠定了堅實基礎。遙測功能也能與 macOS 統一日誌（Unified Log）系統協同運作，讓組織能同時收集強化後的安全信號以及特定的日誌數據，用於稽核、調查與合規。

簡便的統一日誌（Unified Log）收集與報表功能

大多數資安分析師與 IT 管理員在進行合規稽核或修補資安控制漏洞時，都對端點日誌有強烈需求。當 macOS 從 syslog 文件遷移到統一日誌（Unified Logging）後，要在企業環境中收集、盤點與檢查這些資訊變得更加困難。macOS 的「主控台」(Console.app) 雖然提供了查看本機統一日誌架構的極佳功能，但卻無法讓組織輕鬆地集中管理這些數據資料。

透過 Jamf，用戶端日誌只要寫入統一日誌，就能立即串流至記錄系統（System of Record）。為了確保僅收集目標數據，Jamf 管理員可以使用與內建 log stream 命令列工具相同的述詞過濾語言（NSPredicate）。如此一來，建立 Mac 日誌的記錄系統就變成了簡單的設定工作，而不再需要逐台機器進行繁瑣的收集。範例包括登入與登出、SSH、AirDrop 以及授權事件。只要數據被記錄在統一日誌中，Jamf 就能收集它。

與 Apple 的標準保持一致。

零時差支援（Day-of-release support）

為了與 macOS 銜接並收集安全決策所需的數據，Jamf 利用了 Apple 的原生技術。這些技術包括新興框架，例如 Apple 的端點安全 API 與宣告式裝置管理（Declarative Device Management）協定（即裝置管理框架的演進版）。藉由使用這些機制，Jamf 能將對裝置的影響降至最低，且不會與 macOS 更新或重大作業系統版本中的變更產生衝突。儘早且頻繁修補」是最常見的安全規範建議。堅持「零時差支援」的安全工具是遵循該規範的核心，也是全面深度防禦（Defense-in-depth）策略的關鍵組成部分。

將「使用者體驗」視為一項功能

雖然 Jamf 持續監控應用程式與使用者活動以應對潛在威脅，但我們特意不針對靜態或與 Windows 相關的惡意軟體進行掃描。針對檔案系統中存放的大量惡意軟體特徵碼進行掃描，通常是造成使用者體驗不佳的主要原因。這種方式與 Gatekeeper/XProtect 的理念一致，即在潛在的「執行時」識別威脅，從而將對使用者體驗與生產力的影響降到最低。

宣告式裝置管理（Declarative Device Management）框架

宣告式裝置管理 (DDM) 於 WWDC 21 發布，是裝置管理協定的演進與升級。透過 DDM，裝置可以主動套用管理設定、自主回報狀態變更，並與 MDM 伺服器進行非同步通訊。這象徵著從傳統的「指令-響應」模型向更高效、更自主的模式重大轉變。

隱私權

Jamf 在裝置端分析數據，僅在配置需要時（通常是即時偵測到潛在惡意或高度相關活動時）才收集相關資訊。由於從裝置獲取並存儲在雲端的使用者數據更少，這在企業需求與使用者隱私之間取得了平衡。若識別出任何惡意活動，該活動及相關數據將被傳送到 Jamf 雲端主控台或指定的資安資訊與事件管理 (SIEM) 系統。除此之外，任何特別要求的數據也會被推送到 Jamf 或 SIEM。藉由過濾掉不必要的數據，負責監控與調查事件的資安分析師能獲得高品質且具參考價值的數據集

Apple 安全模型的其他擴充

最佳實踐：強化 macOS 安全性

雖然 Apple 提供了最安全且可靠的作業系統，但企業常見的疑問是：還可以採取哪些額外步驟，讓 macOS 更符合公司環境的需求？

最好的第一步就是開始利用 Apple 的行動裝置管理 (MDM) 框架來進行大規模的自動化管理。MDM 不僅能協助您更好地保護組織，還能減輕 IT 團隊在管理與保護裝置群時的負擔。

自 OS X 10.7 (Lion) 推出以來，MDM 框架啟動了無數的工作流程，可根據組織的特定需求量身打造裝置功能。設定描述檔（Configuration profiles）與管理指令是利用 MDM 確保團隊無論在何處 工作都能保持安全的兩種最常用方式。

將 MDM 與 Apple Business Manager（Apple 為企業提供的免費解決方案）結合使用，可以進一步提升安全性，並協助自動化硬體採購與管理。

從 Apple 開始...

多年來，Apple 建立了「安全第一」的商譽，這點在 macOS 中也表露無遺。原生功能如 FileVault 2 加密、雙重認證、遠端鎖定/抹除功能，以及強制執行密碼標準的能力，在每台加入組織 環境的新 Mac 上都能使用。

現代化的管理與安全平台（如 Jamf）利用 Apple 的最新技術，將這些功能更進一步地發揮，協助自訂加密等重要安全工具的實施、強制執行與報表生成。

...透過 Jamf 強化。

雖然 MDM 為組織奠定了良好的基礎，但許多人想知道還能做些什麼來進一步增強安全態勢並強化員工隱私。這就是 Jamf 的用武之地。

眾所周知，當達到一定規模時，裝置管理會耗費大量團隊資源。更多的人意味著更多的硬體，而更多的硬體則意味著更多的 IT 成本負擔。

至少在像 Jamf 這樣的平台出現之前是如此。

藉由「藍圖」(Blueprints) 和「智慧群組」(Smart Groups) 等專利技術來協助分類公司裝置並自動執行管理功能，IT 團隊可以減少在管理細節上耗費的時間，將精力投入到其他日常 IT 任務中。智慧群組會密切監視裝置清單，隨著裝置狀態的改變，即時將裝置加入或移出預定義的群組。

macOS 上的現代化身份識別管理

現代化安全的核心是身份識別——為終端使用者提供安全且自訂的存取權限。傳統 IT 依賴本機目錄服務來作為員工資訊（如姓名和部門）的集中記錄。隨著安全與部署需求的演進，企業必須採用全新的身份與存取管理方法作為其企業策略的一環。透過完整的身份識別管理架構，企業可以統一裝置與應用程式的身份驗證機制，解鎖更多功能、提升效率，最終實現數位轉型。

建立在目錄服務資訊之上，雲端單一登入 (SSO) 確保終端使用者使用安全的憑證來存取公司資源。

Jamf 擴展了這些常見的身份 管理形式。

Jamf 透過無縫的認證工作流程，統一了所有公司應用程式與使用者 Mac 上的身份識別。終端使用者只需使用單一雲端身份，即可輕鬆快速地存取維持生產力所需的資源。

透過 Jamf，組織可以獲得：

- 簡化開箱即用的配置與身份驗證，全面支援遠端與辦公室 員工。
- 自動同步使用者身份與裝置 憑證。
- 讓 IT 在所有服務與裝置上具備全面的身份管理能力。
- 一個零信任網路存取 (ZTNA) 解決方案，用來取代傳統 VPN，並滿足現代混合型企業的需求。

針對 Mac 上的威脅進行回應與補救

Jamf 提供的儀表板能協助組織評估 Mac 裝置的狀態，並標記出需要注意的硬體。透過專利的「智慧群組」功能，IT 管理員可以鎖定需要更新或修補的裝置，以改善安全態勢。這一切都可以遠端完成並自動化，因此 IT 人員完全不需要親自接觸 裝置。

當 Jamf Protect 與 Jamf Pro 搭配使用時，威脅補救能更進一步。利用智慧群組技術，可以針對活動警報觸發所有的 MDM 與 Jamf 指令進行編排響應。這包括自動化網路隔離、阻斷不符合條件的存取、使用者通知，或是任何數量的其他目標補救方案。

超越裝置管理的安全性

閱讀我們關於企業 Apple 安全現狀的報告，該報告調查了 1,500 名 IT 與資訊安全專業人士。內容涵蓋目前的裝置使用情況與應對方法、裝置安全面臨的挑戰，以及端點 安全的未來狀態。

Jamf for Mac

現代化組織需要一種統一的方法，來進行大規模的 macOS 裝置管理與安全維護。Jamf for Mac 透過將 Apple 的內建保護功能與身份、特權管理、抽取式儲存控制以及威脅預防等進階功能整合，來實現此目標。這建立了一個分層且符合 Apple 標準的安全態勢，能即時保護裝置，且不會干擾使用者所預期的熟悉 macOS 體驗。

透過 Jamf for Mac，組織能更深入地了解裝置活動、加強與合規基準的一致性，並具備執行最小權限原則、控制抽取式媒體以及預防網路威脅的能力。這些功能有助於降低整個 Mac 裝置群的風險，同時維持使用者生產力並保留無縫的 Apple 體驗。

透過將管理、身份識別與端點安全整合在單一且專注於 Apple 的解決方案中，Jamf for Mac 讓組織能全面保護 macOS 裝置，並在 Mac 部署規模持續增長時仍能充滿信心地運作。

jamf

立即開始

或聯絡您偏好的經銷商，免費 試用 Jamf。

www.jamf.com/zh-tw/