jamf

Apple 端點遙測實務指南

所見即所得

可見性始於遙測

你是否曾走進一間完全漆黑的房間？沒有光線，就無法清楚辨識物體輪廓，例如牆面的邊界與家具的邊緣。端點安全，延伸至合規作業，情況與此十分類似。沒有遙測資料，就無法保護那些看不見的資產。

這聽起來或許顯而易見，但無法從受管 Apple 裝置機群取得即時的端點健康狀態資料，是現今組織面臨的重大挑戰之一。當然，IT 可以輕易得知已註冊的 macOS、iOS、iPadOS 裝置數量；資安團隊也可以產生報告，詳細說明六個月前遷移專案當中有多少裝置升級到 macOS 的最新主版本。

但您的 IT 與資安團隊，能否在此刻驗證 Mac 與行動裝置機群的整體合規狀態？**換句話說，團隊對於手上用來驗證以下項目的資料，有多大的信心：**

- 哪些處理程序正在執行？
- 系統完整性是否受到影響？
- 是誰執行這些變更？
- 各端點是否符合合規要求？

請留意識別與驗證兩個詞之間細微但重要的差異。因為兩者的差異，正好對應兩類裝置：已註冊裝置，僅在行動裝置管理（MDM）解決方案中留有紀錄，只會在排程回報時更新（識別）。以及合規端點：透過主動監控蒐集並分析豐富的遙測資料，提供端點健康狀態的即時洞察（驗證）。

前者仰賴最近一次的回報；視排程與資源不同，該資料可能已經過時，會為組織帶來未知風險。後者仰賴最新的健康狀態資料，即時驗證端點合規性，並向稽核人員提供帶有時間戳記的裝置合規證明。

對各種規模的組織來說，縮小「識別」與「驗證」之間落差的關鍵就是遙測。**在本指南中，我們除了闡述遙測在現代管理與資安策略當中的關鍵角色，也會涵蓋以下內容：**

- 遙測能做什麼與不能做什麼
- 遙測對於取得裝置機群洞察所扮演的角色
- 可見性如何：
  - 實現全面的 IT 營運
  - 達成預期的商業成果
  - 透過更高程度的協同創造價值
  - 強化組織安全狀況

為明確預期，雖然擁有專職資安營運中心、專業分析師團隊或是威脅情報背景確實有所幫助，但這些並非必要條件。真正必要的是理解遙測可提供哪些資訊，讓團隊依據即時、資料導向的決策建立主動式工作流程，而非仰賴建立在陳舊過時資訊之上的被動處理程序。

何謂遙測

探究遙測（telemetry）的詞源，可發現該詞是由兩個源自希臘文的字所構成的複合詞：tele 代表「遠端」，metron 代表「測量」。大致可翻譯為「遠端測量」。

放在端點安全的脈絡下，遙測指裝置回報自身健康狀態與活動的一連串測量資料：執行過哪些項目、發生哪些變更、由誰執行變更、發生時間，以及裝置連接的對象。

以 macOS 端點來說，遙測通常包含以下內容：

- **存取追蹤**會記錄登入者、登入時間與來源位置、所請求的資源，以及被授予或拒絕的權限，例如權限提升請求。
- **程序執行**會追蹤應用程式啟動、背景任務、相關子處理程序，以及其與核心及使用者空間的互動。
- **系統事件**會記錄組態偏移、更新成功與失敗、系統檔案修改，以及硬體或軟體狀態的變更。
- **網路活動**會擷取連線詳細資訊，例如加密強度、網路類型、IP 資訊、連接埠、通訊協定，以及傳輸資料的應用程式。
- **診斷記錄**會蒐集系統運作與效能資料，同時包含當機報告、程式碼狀態與記憶體傾印。

在檢視遙測資料時，人們常會將個別資料項目視為無足輕重而予以忽略。然而，就像單一拼圖碎片本身作用有限，唯有把所有碎片組合起來，才能看見完整全貌。將資料整合後，可為 IT 與資安團隊提供詳細分析，用以驗證該特定時間點的端點健康狀態。

團隊運用這些測量資料執行的作業，不論是威脅搜捕、修補程式管理或是驗證合規，都屬於獨立的後續步驟。

遙測「不能」做什麼

如同深度防禦策略中的多數資安控管，管理員必須認識資料缺口，才能透過多層防禦盡可能彌補缺口。同樣，若要有效運用遙測，對於其限制與優勢都應同等熟悉。

遙測並非：

- 監控使用者個人活動或瀏覽習慣。
- 用來取代執行管理任務或資安修復工作流程的工具。
- 在端點整個生命週期內提供全面的合規證明。

遙測資料只不過是記錄於日誌當中、針對單一裝置（或是整個裝置機群）所蒐集的資訊。若沒有後續處置，遙測本身幾乎沒有實用價值。 組織加以運用，遙測才能產生價值：首先檢視資料，或是將資料串流至安全資訊和事件管理（SIEM）解決方案進行分析，再將該脈絡資訊做為資料導向的決策，套用到管理、資安與合規工作流程。

這項區別相當重要。

只蒐集遙測資料，卻未套用到 MDM 與端點資安解決方案，就好比 Apple 用來打造每一台 MacBook 的鋁錠。鋁錠本身無法協助使用者完成工作相關任務。但 Apple 將鋁材運用在製造流程，就能生產出筆電，讓使用者得以履行職責或是從事創作。

在此比喻當中，遙測就是原材料（鋁）。組織唯有加以運用，才能以此建構自身的合規計畫；一切始於完整的可見性，以及彙整各筆獨立資料點後浮現的行為模式。

遙測如何運作：從查詢到洞察

現在我們已經解釋何謂遙測，接下來稍微轉換視角，說明存放於端點的遙測資料如何改變裝置與組織安全狀況的相關決策。

若要充分理解遙測的資料流向，我們需仔細檢視資料管線的四個階段：

1 蒐集

macOS 平台會產生一連串系統層級事件，即時捕捉裝置上發生的所有活動。這些健康狀態資料在核心層級與硬體感測器進行蒐集，記錄由 Apple 端點安全 API 所監控的效能指標。

2 彙整

原始資料蒐集完成後，下一步透過統一記錄系統（ULS）解析這些資訊。此階段會將擷取到的資料格式化，以符合各裝置的結構與儲存需求。

3 處理

資料完成記錄之後，macOS 原生工具（例如 XProtect 與 MRT）以及第三方資安代理程式，會即時接入日誌串流。它們會讀取並分析資料串流，將高價值事件優先交由最後階段處理。

4 報告

此階段，經過結構化與處理的豐富遙測資料，會透過第一方標準通訊協定進行傳輸，例如 Apple 用於檢視當機報告與使用行為分析的診斷伺服器，以及第三方資料分析工具。

當遙測資料完整流經資料管線後，IT 與資安團隊在評估端點健康狀態以找出潛在問題時，通常會檢視裝置日誌。由於單一裝置就會產生大量日誌，再乘以整個機群的裝置數量；因此強烈建議組織將源源不斷的資料串流匯入 SIEM 解決方案，依嚴重等級或是組織合規需求進行彙整。簡而言之，不需要人工翻閱數千筆紀錄大海撈針，由技術承接繁瑣的篩選作業，優先呈現最重要的事件供人員檢閱。

視組織規模與可用資源而定，此時跨功能團隊會依據遙測資料的詳細內容，處理被標記出來的問題。

舉例來說，擁有專職 IT 與資安團隊的組織，日益整合為同一個部門，運用各自的專業，針對缺少重大修補程式的端點強制執行合規原則。資安團隊確認該發現屬於真陽性，IT 團隊則確保這些不合規裝置在 MDM 當中完成對應分組。雙方協同作業即為轉折點：由端點資安解決方案執行自動修復，並透過蒐集更新後的遙測資料完成合規驗證。

補充說明：團隊要理解遙測如何帶來洞察，並不需要把底層流程牽涉的每一項通訊協定、資料類型或是 API 呼叫都牢記在心。重點是理解資料如何沿著管線傳遞，以及這些資料向 IT 與資安團隊透露的裝置即時狀態資訊，進而指出最符合合規要求的處理方向。

可見性：遙測帶來的成果

遙測與可見性有一項重要差異：遙測是輸入，可見性是輸出。這兩個術語因為概念相近經常被混用，但切勿混淆，兩者的差異值得明確區分。

分辨兩者差異的簡單方式：原因與結果。遙測會釐清問題的「原因」，例如裝置組態錯誤。可見性則會明確指出組態錯誤的具體內容，以及受影響的裝置，也就是所謂的「結果」。

從營運的角度來看，可見性代表團隊可以掌握裝置機群當下精確的實際狀況。同時也給出可執行的處理路徑，用以緩解浮現出來的各項問題。它可解答諸如以下的問題：

- 是否觀測到基準行為模式？
- 哪些裝置健康狀態良好？
- 哪些裝置存在風險？
- 是否存在正在發作的威脅？

遙測就是實現可見性的彙集資料。它由組織內所有受管端點所蒐集的資訊所構成，可即時提供裝置健康狀態的相關細節，例如：

- 遺失系統或安全修補程式
- 已安裝未經核准的應用程式
- 偏離基準的組態設定

遙測雖然能夠實現可見性，但這不會自動發生。組織可以持續監控端點，蒐集大量遙測資料，卻依然無法掌握裝置機群的健康與合規狀態。

遙測 = 輸入

可見性 = 輸出

為何蒐集了遙測資料，卻仍缺乏可見性？

遙測不等同於可見性。

唯有在資料經過檢視、賦予脈絡，並轉化為決策或行動之後，前者才能促成並供給後者。若未進行資料檢視與決策制定，遙測就如同一本從未翻閱的書籍，僅存放於儲存空間，內含豐富知識，卻無法為使用者帶來任何效益。

不要把可見性視為單純的開關，將其看作連續範圍會更貼切。範圍的一端代表具備可見性，另一端則代表毫無可見性。以此為前提，評估您的組織位於可見性範圍的哪個位置。

與此同時，我們來看一間企業分別處於可見性範圍兩個極端的狀況範例：

毫無可見性：某組織要求裝置必須註冊至 MDM，預設每 12 小時回報一次以更新裝置紀錄，此場景僅能提供有限的裝置健康資訊，不具備即時可見性。受限於回報延遲，所能取得的資料在最理想狀況下也至少已經過 12 小時。倘若裝置錯過排定的回報時段，就只能等到下一個排程週期才會重新蒐集，資訊也會變得更加陳舊。

行動裝置管理雖然功能眾多，但設計上並非用來取代端點安全解決方案。這也就代表，惡意軟體存在或可疑行為監控這類風險指標不會被蒐集。此外，隔離處置工作流程無法自動執行，會因為缺乏可見性而損及安全狀況。

具備可見性：某組織要求裝置必須註冊至 MDM，預設每 12 小時回報一次更新裝置紀錄，同時導入會主動監控端點的端點安全解決方案。兩者搭配運作，可完整掌握裝置健康狀態，擁有即時可見性。即便 MDM 存在排程回報延遲，主動監控機制下，資安代理程式會持續透過資料管線傳送遙測資料，從而即時取得機群內每一台裝置的精確端點健康狀態。

在 MDM 解決方案整合端點安全之後，風險行為、危險應用程式與程式碼會持續受到監控，一旦偵測到就自動進行阻擋。除此之外，也可以執行受入侵端點隔離、風險緩解這工作流程，同時為團隊提供最新的裝置健康資料，透過政策導向管理落實合規，或是使用攜帶時間戳記的證據向稽核人員證明合規狀態。

簡而言之，可見性就是把遙測真正化為資安優勢之後所得到的成果。重點不在於增聘人員或是採購更多工具，而是把 macOS、iOS/iPadOS 裝置本來就會產生的遙測資料轉化為洞察。以此作為可擴展決策與行動的基礎，信賴當下持續擴張之裝置機群的真實健康狀態，而不是推測的狀態，或是一兩天前上次檢查所留下的舊資訊。

偵測、調查與回應，皆由可見性提供動力。

可見性的價值，不只是為技術團隊帶來有關合規與安全狀況的洞察。其價值也體現在日常的 IT 與資安營運，具體如下：

偵測

IT 團隊依據最佳實務並配合組織需求制訂基準，藉此定義正常作業流程與效能水準。遙測，以及其所衍生的可見性，讓團隊掌握裝置健康狀態，例如組態是否符合基準，或是已經偏離基準。可見性也會凸顯異常行為，包含所有偏離基準的狀況。隨著裝置機群規模擴大，這一點尤其有用，可以提早發現異常。換句話說，即時可見性可以主動偵測潛在問題，從而避免問題潛伏，直到演變成安全事件才被察覺。

調查

可以說，這是可見性發揮最大作用的環節。一旦偵測到異常，資安團隊就會進入調查模式以驗證問題，接著回答一連串問題，例如：

- 發生了什麼事？
- 事件何時發生？
- 發生的原因為何？
- 影響層面有多廣？

坦白來說，如果沒有遙測資料，針對這些及其他關鍵問題的回覆只能仰賴猜測、推論以及使用者的口頭陳述。並非這些使用者敘述一定有誤，而是會加重技術團隊查證的負擔。但遙測就是證據，是還原事件時間軸、解釋實際經過的明確依據。

回應

最貼切描述可見性在此環節作用的一句話便是：「從理解落實為行動。」在問題完成偵測且資安團隊審閱證據之後，以遙測為驅動的事件回應工作流程，讓團隊取得執行任務所需的洞察，並且按照可重複的順序執行任務，在降低暴露風險的同時最大化修復成效：

- 隔離受入侵的端點，控制影響範圍。
- 依照嚴重等級與重要性對威脅排定優先順序。
- 緩解風險，根除殘存威脅。
- 修復端點，將狀態恢復至基準效能。

> > >

事件回應：缺乏可見性與具備可見性

本電子書前面章節已經對比過組織具備可見性與毫無可見性的兩種狀況。核心差異在於：前者會實際運用蒐集到的遙測資料；後者只蒐集資料卻不加運用，或是依賴陳舊資料。雖然本指南有多處範例說明這點，但在技術團隊承受壓力進行事件回應時，對比會最為鮮明。

下面呈現兩組團隊 A 與 B，處理同一事件的明顯差異：公司配發的裝置安裝了有漏洞的未經核准應用程式，進而引發勒索軟體攻擊。

團隊 A：缺乏可見性

- **僅能取得局部資訊：**可以看見已安裝的應用程式，但無法驗證漏洞風險等級。
- **只能等到症狀浮現才被動反應：**裝置一開始效能遲緩，後續發生資料無法存取。
- **資料來源無法驗證：**資訊來自受影響使用者的主觀陳述，無法查證。
- **解決問題需要額外投入作業：**缺乏可佐證的指標，需要更多除錯步驟才能修復根本原因。
- **無法隨裝置機群規模擴展：**裝置數量增長，工作量會指數級上升，風險因素與暴露時間窗也隨之擴大。

團隊 B：具備可見性

- **完整資料填補資訊缺口：**可以從內部視角看待同一事件，清楚呈現成因、發生順序與造成的影響。
- **從偵測一路到問題解決：**依據完整事件時間軸處理事件，而非仰賴猜測。
- **資訊即時、精確且經過驗證：**可向團隊與稽核人員證明端點的健康狀態。
- **在脈絡下審閱資料：**彙整取自核心與硬體感測器的各項指標，還原事件全貌。
- **擴增裝置數量，卻不增加工作負荷：**流程具備擴展性，進行調整時不會帶來額外的管理負擔。

聰明工作，而非埋頭苦幹

遙測是自動化的驅動因子。

當整合行動裝置管理、端點安全以及身分及存取管理時，以遙測為驅動的工作流程能夠透過多種創新方式強化裝置管理與資安策略，善用技術在多種場景下承擔繁瑣的作業，讓管理人員得以將專業能力專注於提供更佳的使用體驗，並讓營運作業更貼合商業目標。

舉例來說，政策導向自動化機制可由端點安全標記出有安全漏洞的應用程式，並透過 MDM 解決方案觸發修復作業。 這套簡易的工作流程可維持安全狀況並降低風險，不會打擾使用者、無需 IT 支援介入，也不會演變成安全事件。

現代企業已經見證，AI/ML 技術能夠成為各規模團隊的效能倍增工具。AI 驅動的程序能以極高速度在裝置機群中搜捕複雜威脅。它會關聯從各端點蒐集而來的遙測資料，即時進行分析，並與多個開源及封閉來源的威脅情報資料庫交叉比對，藉此偵測未知威脅並向團隊發出警示。透過可擴展的自動化選項，針對有需要的資安事件保留人為介入機制，就如同導入政策導向工作流程自行處理較輕微問題一樣，可以輕鬆納入工作流程當中。

藉由客製化解決方案以符合組織的獨特需求，資安事件可以憑藉更完備的資訊更快獲得解決，除了最大限度降低風險與手動作業負擔，也能最佳化作業效率並發揮最大成效。

脈絡下的遙測：合規、營運與組織價值

除了前面探討的威脅搜捕與事件回應效益之外，組織在思考遙測議題時，還有另外兩個層面同樣值得重視。

合規

醫療保健、金融與教育等產業，正面臨來自全球法規越來越嚴格的審查。聯邦與各地區的強制規範，要求組織必須證明資料受到妥善保護，且接觸資料的裝置組態皆符合合規要求。

有一點必須再次強調：合規主張必須經過驗證。多數稽核人員預設的核心觀念為：若無法驗證裝置處於合規狀態，即代表該裝置並未合規。道理就是如此簡單。

遙測就是實現驗證的關鍵要素。如同前文所述，遙測本身只不過是一組資料彙集。若未經過檢視、賦予脈絡、制訂決策或執行對應行動，就無法實現可見性。同理，倘若尚未建置適當的資安控管機制與政策，僅靠遙測並無法保證達成合規。

在導入脈絡資訊並建置控管機制之後，遙測便可做為驅動依據，於評估階段證明（或反證）各項機制是否正常運作。除正式稽核之外，遙測這類證據資料在其他合規事務中也相當重要，包含下一節將探討的營運層面以及網路安全保險。在此特定場景下，核保人員經常要求組織出示資安作業的執行證明，才會開啟或續保保單，或是受理組織提出的理賠申請。

營運

如同前面偵測、調查與回應的範例所示，同一批遙測資料也能為 IT 營運帶來效益。這除了協助 IT 與資安團隊執行職掌相關任務，也讓 IT 主管與高階管理者無需額外流程、追加作業或產製個別報告，就能即時掌握組織整體健康狀態與合規情形。

遙測具備多元用途，以即時遙測做為報表基礎時，可發揮雙重價值：一方面可供技術團隊做日常營運使用，另一方面也透過具可信度、有證據佐證的合規狀態與風險評估文件支援商業用例，以精確且最新的資料做為決策依據，協助推動未來業務成長相關討論。

簡單來說：遙測的核心價值不會隨團隊規模或組織架構而改變。不論是由單一 IT 經理審閱，或是由一組資安分析師團隊進行檢視，遙測所執行的工作都維持一致。它的應用層面應更為廣泛。遙測並非「只有資安團隊才會使用」的工具，它會依據使用者的提問面向發揮不同用途。

評估您的遙測與可見性態勢

從觀念層面理解遙測與可見性具備實用價值。而瞭解其如何協助組織掌握自身現況，則更具實用意義。組織可以先針對自身的遙測與可見性現況進行自我評估，無需採購新工具、接受專業訓練或是調整現有技術堆疊的組態。

請先回答以下問題：

1. 貴組織的端點紀錄資料是儲存於裝置本機，還是會串流傳送至中央位置（SIEM 解決方案）進行分析？
2. 團隊是否能夠確實掌握裝置機群內任一裝置的即時安全狀況？
3. 團隊是否能夠透過證據還原事件時間軸，還是只能單純仰賴受影響使用者對事件的描述？
4. 若稽核單位今日提出要求，貴組織是否可產出附有時間戳記的合規驗證資料？
5. 當偵測到合規違反狀況時，是否會自動修復，或是需要手動後續處理？

上述問題的答案，能夠充分反映組織的安全狀況；更重要的是，可以看出**團隊究竟是能夠主動降低風險，還是只能在事件發生後被動回應**。以下為幾項需要留意的常見缺口：

- 豐富的遙測資料儲存於端點，或是僅與既有技術堆疊部分共用，會產生團隊可能察覺不到的可見性缺口。
- 在跨平台環境中，轉發部分事件（Windows），卻將另一部分事件（Apple）予以隔離，仍然會讓組織暴露於風險之下。
- 蒐集遙測僅是解決方案的一部分，必須定期檢視並據以執行對應處置，才能發揮其真正價值。

相對地，成熟的資安技術堆疊具備以下共通特徵：

- 遙測持續流轉並內嵌於工作流程之中，而非等到有人記得才進行檢視。
- 所蒐集的資料會比對多種來源進行分析，完成資料關聯，並依據嚴重程度排定優先順序。採用手動分類，有可能會遺漏關鍵細節。
- 擁有完備合規計畫的團隊，並非規模最大或是預算最充足。而是會在進行決策與執行動作之前，善用所產生的遙測資料。
- 以既有資料為基礎建置可見性，幾乎永遠比導入未經整合的全新工具來得更為快速。

結論

必須再次強調：未經檢視的遙測，只不過是儲存於檔案當中的一堆資料。

這些源源不斷、附有時間戳記的事實紀錄，記載裝置的執行動作、組態狀態與漏洞等級；唯有組織運用這些資訊並依發現結果採取行動，避免小問題悄悄演變成代價高昂的違規事件，資料才會產生價值。

原始遙測資料可實現資料導向決策，依據即時健康狀態及時採取對應行動，這就是所謂的可見性。資料的精確度與即時性，會為後續作業帶來一層可信度保障，從資料管線一路傳遞至最終的決策者。

「受到管理」與「獲得資安防護」之間的缺口是可以彌補的。這不見得需要採購新裝置、團隊具備高深專業知識，或是大規模調整現有技術堆疊。機群內的裝置本來就設計會記錄自身的執行狀況，它們其實已經把所有發生的事都告訴您。

真正的問題在於，貴組織是否已經做好準備，接收這些資訊並據此採取行動。

準備好親身體驗了嗎？

立即體驗 Jamf