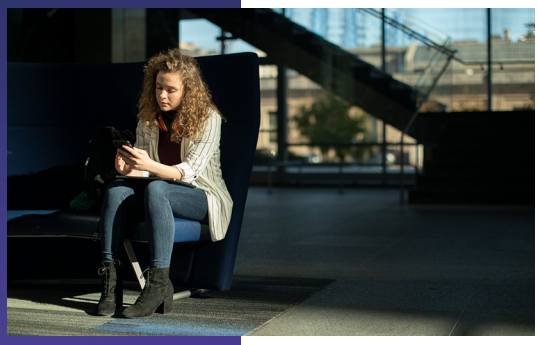
jamf

評估自家資安需求



評估自家資安需求，為何如此重要？

了解你服務的機構獨特的資安需求彷彿是一門藝術，體現了理論與實踐的結合。儘管概念上為相對立的兩個面，但是源頭的邏輯概念，其實是建立在運用風險評估、對端點設備的可見度與監控得來的關鍵弱點資料，以及認識監管要求的基礎之上。所有元素相結合，為機構開創達成與維持合規目標的輔助資安工具。

時時掌握機構的資安脈動可說是無比的重要。「請問貴公司維持成功的秘訣是什麼？」，如果你問任何一間公司這個問題，得到的回答不外乎是：「熟悉自身需求並確保執行相應措施。」，其中最大關鍵在於如何將風險降至最低，同時又能將推動業務的機會極大化。對那些沒有被經濟衰退淘汰、在不健康的大環境下仍設法維持營運，或已經營長達數十年的公司來說，更是成功印證了這個說法。

這份白皮書將探討：

- 如何借助遙測數據的力量，透視裝置狀態與整體資安態勢，以及認識我們所謂的「風險」
- 為什麼在資安防護作業中，不可不反覆與定期的評估風險
- 如何運用遙測數據，協助機構判定資安需求，抵禦當今與未來的資安威脅
- 為什麼將風險資料與端點防護平台相結合，有助於機構實現合規目標，也能確保維持強大的資安態勢

這套信念適用所有產業，就舉電影和音樂產業為例吧。娛樂產業已發展了數個世紀，它在不同程度上通過了時間的考驗，並按照目標受眾的需求，調整產品，與時俱進。

整個革新過程從未間斷。

網路安全的變換頻率也大致相同。各機構為了確保持續安全營運下去，則必須審視組織內部的需求，而非評估客戶端需求，再決定有哪些條件是必要的。風險評估作業一共涵蓋設備、軟體、基礎設施、資料、系統流程、政策等各項內容，把所有碎片組合在一起，便形成一間機構的「資安態勢」。

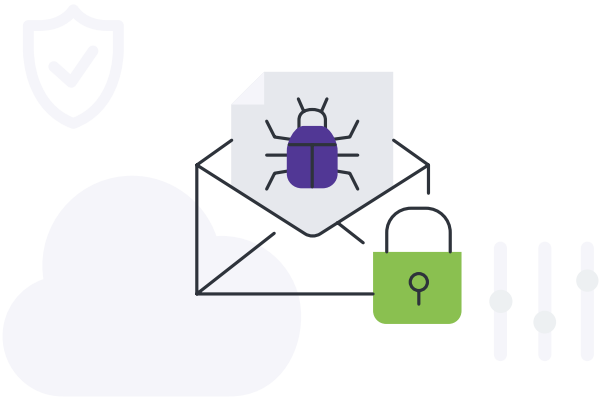
如果能掌握這些資訊，機構便可評估自家當前網路安全策略的風險和義務，視情況採取措施來糾正，減輕威脅並將風險最小化。

風險評估無法「一勞永逸」。每間機構都應參照最佳做法，定期進行風險評估，因為科技向來素有不斷變遷的特性，一切都瞬息萬變。就資安而言更是如此，因為本質上必然會出現錯誤問題需要修正，若沒有即時修正則可能會演變成漏洞，進而降低資安態勢，最終容易招致入侵事件。

這都還沒考量到那些積極測試網路防護底線的威脅人士，他們以找尋弱點跡象和可利用媒介為目的。

白話一點的說，「風險評估」應設為完整網路安全策略的一環，其中所獲得的評估數據不僅協助機構了解當前的安全狀態，還可確保機構擬定的深層防禦計畫，時時都握有下方列舉的關鍵資訊：

- App 與裝置生命週期各階段的資訊
- 採購、配置和部署安全性控制
- 符合監管目標並實施合規機制
- 識別既有與新型威脅，並按照嚴重程度分級
- 確保風險胃納和緩解策略維持一致
- 調整並實施事件應對流程
- 更新與制定威脅預防策略，如使用者教育訓練



風險評估

既然我們已經解說風險評估的重要性，實際又該如何擬定評估機制呢？有哪些東西實際上正面臨風險？雖然確切的細節可能因產業類別或公司而異，但重點在於了解：

- 威脅態勢
- 自家資安漏洞
- 遭受攻擊的可能性
- 若遭受攻擊，將面臨哪些影響
- 需花費多少時間才能從重大攻擊事件中恢復

> 「知己知彼，百戰不殆。」——**孫子**

讓我們來看看一些有關風險評估的提問。

我服務的機構，在哪個方面最容易受影響？

攻擊人士可透過多個管道，如硬體、軟體、系統介面、廠商與網路基礎設施間的互動，甚至是竊取具有權限的使用者身分，藉機嘗試入侵系統，即使只是一般業務流程與政策，也可能出現漏洞。

審視與分類這些項目，才能徹底了解自家基礎設施。以下為必須掌握的資訊：

- 哪些裝置正在存取你的網路
- 哪些使用者可以存取你的資料
- 了解自己是否有遵循資安防護的最佳做法 (如最小權限原則、高強度密碼政策等)
- 系統上的漏洞是否由你的廠商所造成
- 使用者是否訓練有素，並有能力辨別潛在威脅與維持良好的資安習慣

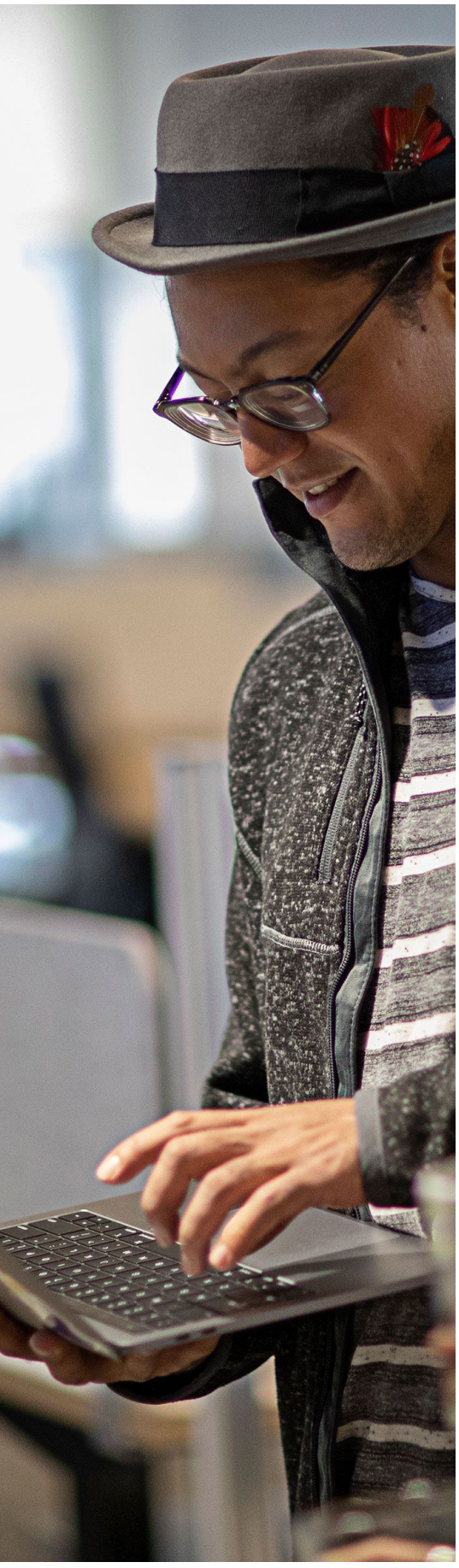
現在需要防範的威脅，有哪些？

風險評估的另一項好處，就是能夠認識資安的生態，了解哪些風險可能對你的系統造成影響。IT 與資安團隊可分析組織中最脆弱的部分、推斷攻擊發生的可能性以及對你的業務帶來的潛在影響。

示範案例

資安團隊可參考 MITRE ATT&CK 框架，了解惡意人士發動攻擊時可能採取的途徑或方法。面對未知型威脅，團隊則可考慮以威脅搜捕，並使用人工智慧 (AI) 和機器學習 (ML) 軟體來識別可疑或惡意行為。低於網路最低標準的異常行為，則可透過在背景運行 AI 與 ML 系統來偵測，它們能夠處理大量威脅情報、將類似模式的資料做匹配，因此這些工具可說是網路安全彈藥庫中的關鍵工具。再者，你也可以將軟體蒐集得來的數據與整個資安社群分享，進一步增加網路安全專業人員的知識量。

多多認識常見的威脅手法，將有助你評估防禦的先後順序，以及哪些位置最需要防護層。資安威脅的形式十分多樣，Verizon 發佈的《**2023 年資料洩露調查報告**》指出，攻擊人士最常見以竊取得來的憑證、釣魚連結和漏洞利用等方式滲透組織。資料洩露的起源一般來自外部，但也有相當程度的一部分 (高達 40%) 是源自合作廠商的系統。為防禦這些資安威脅，我們建議必須對現有的設定與政策進行詳細的分析，稍後我們會再進一步分享作法。



網路攻擊可能對機構造成哪些影響？

了解威脅事件發生的機率，才能進一步評估防禦策略的輕重緩急。資安威脅的影響還可能攸關財務，IBM 的《**資料洩露成本報告**》就指出，2022 年資料洩露的平均總成本為 435 萬美元；這些成本可以是時間，比如識別和遏制洩漏事件平均需花費 277 天。威脅事件還可能會損害你與客戶的關係、危及自家聲譽，或因為資料洩漏而必須調高價格，60% 受影響的組織 2022 年時就曾這麼做，這都還沒加上因為未遵循合規規定，而遭到監管單位懲處的費用。

下一步該怎麼做？

發生機率越高、影響範圍越廣大的資安攻擊，則重要性自然越高。影響範圍與發生機率兩大指標，有助於量化資安威脅的風險高低程度。對資安風險有完整的認識，才能排定優先事項並判定：

- 哪些系統最為關鍵，因而最迫切需要優先保護 (哪些系統對重大功能的影響最甚)
- 需要實施哪些管控措施，才能實現最佳防禦策略
- 哪些軟體或工具可以強化資安態勢
- 風險胃納 (即風險容忍度)

一旦從風險評估中獲得所需資訊，就是時候實施所學的知識了。下一節我們將介紹如何分析網路和設備遙測數據，以及你可以遵照哪些準則來制定或修訂資安策略。

資安可見度與監控作業

假設今天你已對風險做出分析，並將風險胃納調整至可接受的程度，你採取了必要的變更動作，並為降低風險而採買和配置所需的安全性控制。你的資安機制相當穩健，相關人員也參與了必要的教育訓練，知道如何識別、回報和應對當今的資安威脅。沒有半台裝置超出保護範圍，所有端點設備皆受到妥善保護，也都有符合合規目標。然後呢？

這是否代表 IT 與資安團隊已經完成任務，可以提前去放假？很抱歉，時候未到。

我再重申一次，日新月異是科技的本質，某些東西縱使現在是安全的，也不代表它永遠都會維持在安全狀態。若要確保設備、基礎設施和組織能遠離無所不在的資安威脅，關鍵就在於要對任何時間點的運行狀況都瞭若指掌。

> 「不知山林、險阻、沮澤之形者，不能行軍…。」
> **——孫子《孫子兵法》**

主動監控可給出大量有關設備維護和機構安全態勢的遙測數據，不僅如此，在談到合規性時，遙測數據是確保依照法規要求正確配置端點的關鍵資訊，它也可在任何指定時間，為端點設備的合規性提供佐證，如在取得安全支付與處理卡費的 **PCI-DSS 認證**時，這項關鍵功能可提供合規證明。

更重要的是，監控作業可獲得對設備的可見度，進而在 App 生命週期各階段和各裝置階層貫徹周到且全面的決定。監控作業的目的，在於為 IT 或資安團隊提供有關設備運行狀況、設備上運行的軟體，以及使用者採取的操作等最新資訊，它還能為管理者與管理階層提供細緻的遙測數據，反覆確保設備維持合規、使用者與資料維持安全，隨時根據情資以適時做出必要調整。

監控作業蒐集的是哪類型的資料？

在開始探討監控作業所蒐集的遙測數據類型前，先讓我們探討兩大監控法：

- **被動式監控：**在一段時間內，緩慢的蒐集裝置運行資料，以最大程度減少對使用者或受監控裝置性能等級的影響。資料擷取的次數本質上並不頻繁，這意味著需要較長的時間來蒐集數據，從而可能耽誤到完整裝置基準的建立。此外，每次擷取間隔可能數日，甚至是數個月，而任何延遲都可能直接影響數據的準確性與及時性。
- **主動式監控：**裝置運行資料經常在端點設備之間相互溝通。定時對端點進行輪詢 (polling)，再將數據傳輸至集中式資料庫，而這個動作一般都是即時進行。

儘管兩者捕獲的資料差異不大，但主要的區別在於：

- 擷取遙測數據的**方法**
- 建構基準描述檔所需的**時間**
- 資訊的**準確性**
- 以及遙測數據的**更新頻率**

雖然這兩種監控法各有優缺點，但是當今的威脅範圍仍舊廣大且瞬息萬變，除了主動式監控外，其它方法都無法成為蒐集最新設備運行資料，再將它轉為填補資安計畫斷層可用資料的有效手段。正如 SecurityWeek 在**《Active vs. Passive Monitoring: No longer an either-or proposition》(主動式與被動式監控, 並非一道是非題)一文中所述，「不夠了解，就不會知道該怎麼保護」**。

遙測數據的類型，以及這些資料就資安態勢而言，有什麼意義：

- **作業系統更新：**確定作業系統 (OS) 的更新版本，了解裝置是否支援最新功能，或是否足以抵禦已知威脅，可將漏洞的傷害降至最低。
- **App 修補等級：**與作業系統一樣，在修復 bug 和緩解可能帶來風險的漏洞時，你需要使用修補程式在處理階段保護 App 資料。
- **配置設定：**就資安態勢而言，強化裝置防護力相當的重要，你除了會希望確保正確配置最安全的機制，也致力最大程度減少錯誤配置的可能性，**因為 Verizon 發佈的《2023 年資料洩露調查報告》就指出，21% 的資料洩露事件與錯誤配置有關**。
- **網路活動：**裝置會與哪些 Web 內容交流？不受信任的連線是否受到保護？哪些通訊埠正在傳輸資料？這些問題的答案，以及有關網路利用率的其它重要問題，對判定裝置的安全狀況來說至關重要。
- **行為分析：**「使用者」是資安環境中最薄弱的環節，不是沒有原因的迴對使用者操作了解的深與淺，將決定社交工程攻擊是否會成功迴如果對使用者在裝置上的操作有更深的理解，管理者便可以更清楚了解使用者是怎麼引發這些風險，也更清楚未來該如何防範。
- **身分審核：**身分識別協定和密碼管理，是解鎖設備和機敏資料的鑰匙迴再怎麼強大的門鎖，或者再怎麼複雜的密碼，都無法讓我們得知使用者是否與他人共用憑證，或使用者的帳戶是否遭到入侵，這一點對遠距和混合辦公環境來說影響更是加倍，因為在這些環境中，高度仰賴晦政策械來確保遠端端點的安全性。
- **惡意程式碼：**惡意程式碼可以各種形式存在，它可能是偽裝成正當 App 的特洛伊木馬程式壞側載而來的 App，或讓你在未察覺的情況下，造訪已遭到入侵的網站，甚至可能是在後台安靜運行的威脅，無論哪一種，都可能危及合規性，尤其在行動裝置採用率攀升和攻擊趨勢不斷增長的情況下更是如此。
- **錯誤日誌：**裝置會記錄所有內容，因此管理者負責的裝置越多，就越難逐一解決每個問題，這會有利於威脅人士，並對管理者不利迴不過，並非一定得要如此迴如果裝置管理得當，並搭配安全資訊與事件管理 (SIEM) 平台，便能對龐大的遙測流壞錯誤日誌記錄和威脅偵測資料進行高效排序和整理。
- **系統流程：**端點安全管理人員必須知道設備上運行了哪些 App。若有人使用未經批准 (影子 IT) 或不被允許 (受限) 的工具，將直接影響設備的平均最低標準迴管理人員會在使用者違規時收到通知，而放任發生資料外洩 、**讓使用者隱私承擔更高風險，**可能就因此降低了安全門檻。
- **合規稽核：**對端點運行狀況的可見程度，與已知和未知的內容都息息相關；對高度監管的行業而言，組織若能了解自己處在合規旅程的哪個位置，便意味著在蒐集合規佐證資料的同時，已經非常清楚實現合規目標的必要條件。

遙測數據究竟能否為我們自動降低風險？

確實可以。事實上，以下幾項因素，會使得風險管理更加困難：

- 訂購大量裝置與不同的裝置類型
- 同時兼顧公發與個人 BYOD 裝置的安全性
- 在遠距與混合辦公模式下，為行動工作族群提供支援
- 對目標執行多管齊下，且融合了兩種或多種威脅類型的複雜攻擊
- 實施安全性設定以維持端點合規性

比起手動完成每個步驟，將蒐集、分析和整理遙測數據的作業自動化才是更受青睞的方法。考慮到需要梳理的龐大資料量、既使以最快速度完成每筆數據，依然需要花費可觀的時間，還有人類的休息時間和有限的產能等等。

電腦不會有上述任何一種限制。

運用系統自動化執行「繁複的工作」，可以為組織節省寶貴的時間和金錢，轉而可以把這些成本運用在如何更好的防範攻擊事件，而不是在事發後才爭先恐後的進行清理。

你可以透過主動式監控深化對自家資安需求的了解，而這也是資安計畫在風險評估之後的第二階段。持續監控設備，即時蒐集和交付遙測數據，以獲得最新的端點運行狀況資料，再將這些資料傳輸至端點防護平台進行分析和處理，藉此確定每個設備的堆棧組成方式。任何系統偵測到的缺陷部分，或回報的異常行為，可設定自動將通知發送給 IT 或資安團隊以決定後續步驟。你也可以設定在偵測到異常後，啟動自動化事件回應工作流程，例如自動從裝置上移除已知的可疑軟體，或將受勒索軟體感染的端點做隔離。

若將端點防護方案與其它工具加以整合，例如身分識別、行動裝置管理方案，則可創造更穩健與進階的工作流程，提供更強大的自動化能力，潛能無限。

合規性

本文中多次引用孫子的《孫子兵法》名言來為幾個核心的主題做總結，用意是希望在資安團隊評估風險與更清楚了解所服務機構的需求時，以清晰的概念幫助到他們，並彌合認知上的落差。建立「每個環節都相當重要」的觀念十分的重要，因為每個階段都環環相扣，任何一個步驟出差錯都可能引起連鎖效應。

只是了解特定時間內出了哪些資安問題，不代表你已真正了解自身資安需求。你還得知道解決問題所需要的工具、選擇對的策略來確保端點符合合規要求，不論你服務的機構是否屬於應受監管的行業。最終目標是確保符合法規要求，假使你的企業不屬於受監管行業，目標則是確保與機構策略維持一致，設立目標的用意，是希望藉由結構化框架來降低風險，維護使用者的隱私與安全，強化你的裝置與資安回應實力。

> 「最高兵法是不用打鬥便能制服敵人。」——**孫子**

在資安的場域裡，「敵人」即代表威脅人士，或可能給組織帶來風險的任何人事物。畢竟，風險就是一種可能演變為漏洞或更嚴重後果的負擔。然而，在了解自身資安需求時，若不去擔心網路層更直接和具體的狀態，反倒去擔心數不盡的敵人，只是白白浪費精力，你的注意力最好集中在風險本身，而不是它們起源的地方。這麼做反而可以讓管理者重拾專注力，思考如何以更好的方式維持合規性，並保護設備、使用者和資料免受當前、不斷升級或瞬息萬變的各式威脅影響。

哪些行業指導對識別和最小化風險有益？

在繼續討論下去前，先讓我們區分「建議指南」、「框架」和「基準」，三者的不同。「建議指南」在一定程度上，與「最佳作法」雷同，它比較像是行業慣例，而不是硬性規定，它的目的在於協助組織在普遍的能力範圍內，管理各類型的風險。

「框架」與目標將所有必要資訊、實踐方法、設定、控制內容、工作流程串連起來，以滿足甚至超越特定組織或合規目標的「最佳作法」有異曲同工之處。

「基準」雖然與前兩項類似，目的都在於達成與維持合規性，只不過切入的角度不同。「建議指南」專門提供「最佳作法」的點子，而「框架」則負責以結構化的方式組織「最佳作法」，讓實現最終特定目標的方法格式化，但「基準」的方式不太一樣。「基準」的角色有點像晴雨錶，機構可用它來衡量合規性或自訂目標是否達標。

再白話一點的說，「建議指南」扮演食材的角色。「框架」會透過組合食材，製作一道菜餚。「基準」則猶如美食評審，他們會根據食材和食譜來判定菜餚是否準備得當。最後，你就能好好的享用餐點。

既然已經了解了這些差異，現在讓我們繼續探討「框架」和「基準線」，因為我們的目標是了解自身的資安需求，並盡可能精準的找出解方。

資安計畫中常見的「框架」

NIST SP 800-53 (修訂第 5 版)：由美國國家標準暨技術研究院 (NIST) 發佈的《Security and Privacy Controls for Information Systems and Organizations》一文中，列出資訊系統和機構可用的標準目錄，以確保組織的營運與資產遠離各式威脅與風險。

NISTIR 8011 (Vol. 4)：《Automation Support for Security Control Assessments》側重在個別資安能力所及範圍的自動化安全控制評估，同時對軟體中網路端缺陷所造成的風險進行管理。

ISO/IEC 27001 國際標準規範：資訊安全管理系統 (ISMS) 是一套相當知名的框架，它定義了達成 ISMS 的要求，並提供如何建立、導入、維護和持續改進 ISMS 的指導。

Cyber Essentials 認證：一套由英國政府制定的框架，適用各規模的機構，為你提供抵禦一系列常見網路攻擊的指導。此認證設有多個等級制度，其中也包含可以判定合規性的技術實作驗證。

MITRE ATT&CK：匯集各種對敵方實際手法的觀察，並以此為基礎而建的策略知識庫。這套知識庫可套用在各產業、社群或端點防護方案，你可將它視為設計特定威脅模型或方法的基礎。

COBIT 2019 評估框架：由國際電腦稽核協會 (ISACA) 制定的一套資安風險量化標準，它可定義通用 IT 管理流程，並將流程與 IT 和業務目標串連，其中的評估元件可確保團隊高效達成目標，同時靈活的與其它框架 (如 ISO 27001、ITIL 和其它熱門的專案管理框架) 結合使用。

支付卡產業資料安全標準 (PCI-DSS)：在處理信用卡支付資料時，組織在技術與營運規範方面使用的資安標準，全球主要發卡機構皆有實施這項標準。

CMMC 2.0：根據多個 NIST 特別刊物發佈的安全要求，這個多階層模型可為機構提供與網路安全成熟度模型認證(CMMC) 級別相符的認證等級，以及其它跨網域的相關實踐法。

OWASP Risk Assessment：此 OWASP 框架，係由安全測試、風險評估和掃描工具組成，目標是消除因環境設定過程的相容性和複雜性問題而衍生的不確定性；無需任何額外的設定，便能以簡單的方法來「分析和審視程式碼的品質和漏洞」和「協助開發人員編寫和生成安全的程式」。

macOS 安全性合規專案：由 NIST、美國太空總署 (NASA)、美國國防資訊系統局 (DISA) 和洛斯阿拉莫斯國家實驗室 (LANL) 的聯邦營運資安工作人員所負責的開源聯合專案，旨在有計畫性的生成安全指南，其中提供像是可實現特定監管目標的配置設定。

網路安全世界中,「基準」所扮演的角色

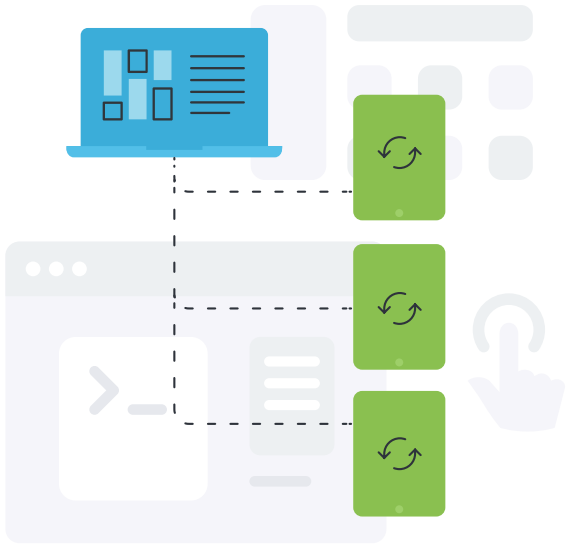
DISA STIG：STIG 係由美國國防部 (DoD) 管理的配置標準，內容涵蓋明確保護運算系統的要求，從邏輯設計、到硬體上運行的通訊協定，甚至是軟體，它的目標是「透過強化軟體與硬體、實際架構與邏輯架構的安全性，進而減少漏洞」。

FIPS 200：聯邦資訊處理標準 (FIPS) 也是由 NIST 專為美國而制定的框架，適用於美國政府和承包商使用的非軍事運算裝置和系統。雖然 FIPS 涵蓋了一系列的安全基準，但 FIPS 200 可確保聯邦機構或在代理聯邦機構取用數據時，能符合目標中每個類別的最低資安要求，根據風險等級斷定適當的資安級別，同時以 **CIA 資安鐵三角原則**按影響程度對安全目標進行分類。

NIST SP 800-39：在與全方位企業風險管理 (ERM) 方案整合時，這個涵蓋範圍廣泛的框架就顯得十分好用，文件中給出的具體細節，闡述了如何結合其它標準、準則與框架，持續評估、應對和監控風險。

網際網路安全中心 (CIS)：CIS Benchmarks 為超過 25 種產品系列，提供配置規範的建議。每個訂定的基準，都是全球網路安全專家協力取得共識的成果，提供全球政府與各行業可接受與採納的安全性配置指導，也可作為整合至端點防護方案的基礎。

CISA CPG：在與 CISA、NIST 和跨機構社群協調下發展而來的網路安全績效目標 (CPG)；它可作為關鍵基礎設施最低的通用一致要求，為中小型組織開闢網路安全之路，同時可作為衡量和提升網路安全成熟度的基準。



風險評估 + 持續監控 + 安全指導 = 成功掌管合規性

> 「知己知彼，百戰百勝。」——**孫子**

如果每塊拼圖都獨立的存在，能為組織提供的能力就十分有限，但如果將拼圖拼湊在一塊，不僅可以：

- 判定自己的責任範圍
- 了解終端設備的運行狀況
- 強化設定內容以充分降低攻擊範圍
- 實現合規目標

此外，還可透過建立最低標準來維持合規性，根據這些基準主動監控並重新評估細緻的遙測數據，完成持續改善設備資安態勢，以及整個基礎設施安全狀況的動作。

前面已經提過，這是一個不斷重複而非靜態的過程。一旦完成上述動作，這個討論可能只會繼續延續下去，並進入一個涵蓋所有階段的循環，從安全性控制、一般流程、工作流程、規範，到機構的每部裝置、每位使用者，甚至是每一筆資料的設定。

不論你服務機構的規模、或者是否屬於應受監管行業，你純粹希望確保網路安全策略與組織策略和行政管理內容維持一致 (如實施適當使用原則，或簡稱 AUP)，此時每個核心要素彷彿機械的齒輪一樣共同協作，幫助你更深入了解自身資安需求，以及填補落差所需要的資訊。

你心裡可能會想，「我是 Mac 的管理者，我知道我的機構面臨了哪些風險，也快被龐大的運行狀況資料給淹沒。」而此白皮書特別針對我們目前的所在階段，與需要達成的合規標準之間的落差多做說明。那麼下一步該怎麼做？如何往下一階段邁進？

探索 Jamf

Jamf 協助各機構順利管理並保護 Apple 裝置。

這段話不只是個口號，更代表了 Jamf 的使命，我們正是為此而生。Jamf 被奉為管理 Apple 工作裝置的圭臬，不是沒有原因的。Jamf 能夠獲得這般肯定，是因為我們一流的解決方案，已幫助無數機構成功管理和確保全球各行各業數百萬台裝置的安全。

我們的服務確保你在工作中可以充分發揮 Apple 產品的潛力。為你提供需要的工具，全方位管理你的 Apple 設備，同時識別、了解和滿足你的獨特需求和合規目標。想知道背後的運作原理嗎？

消除對端點驗證的疑慮。

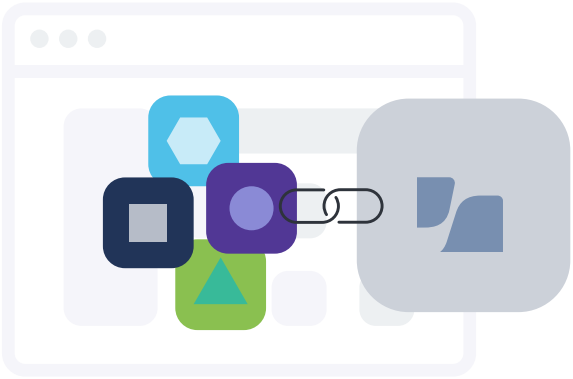
要深入了解自身資安需求，很大程度上必須非常清楚端點設備的狀態。如果沒有透過細緻的遙測數據驗證每台裝置的運行狀況，管理者便只能猜測，沒猜錯算運氣好，要是完全誤判，那麼就可能帶來無法設想的後果。

身為管理人員，**你不該只是「想知道」，而是「必須知道」設備運行的狀況**。在合規方面，你需要決定該實施法規要求，還是確保與機構政策維持一致即可，你還需要隨時驗證端點運行狀況，才能確保每一階段都符合機構的需求。

社交工程是攻擊人士經常利用風險漏洞而發起的主要攻擊手法。更具體一點來說，社交工程會利用已存在的風險，在遭到入侵的裝置連線到企業資源時，藉由竊取憑證或散播惡意程式碼的手段來引入破壞力更強的風險。

零信任網路存取 (ZTNA) 這樣的技術，會根據一系列的資安規範查驗設備運行狀況，確保符合最低安全性要求，才會授權存取請求，以此確保設備的安全。奉行「永不信任，一律驗證」的精神，ZTNA 解決方案 (如 **Jamf Connect**) 以身分和存取管理作為資安策略的基礎，並會驗證存取請求是否來自已註冊且受信任的設備。

端點防護解決方案 (如 **Jamf Protect**) 可為你的 macOS、iOS、iPadOS、Android 和 Windows 裝置強化防護層，確保裝置和使用它們來辦公的使用者可以遠離惡意軟體和威脅，對裝置端和網路端的威脅進行分析，實現更快的偵測與事件回應能力，以及**不會影響安全性、隱私或性能的高效自動化威脅緩解與修復作業**。



傳遞備受喜愛與信賴的體驗

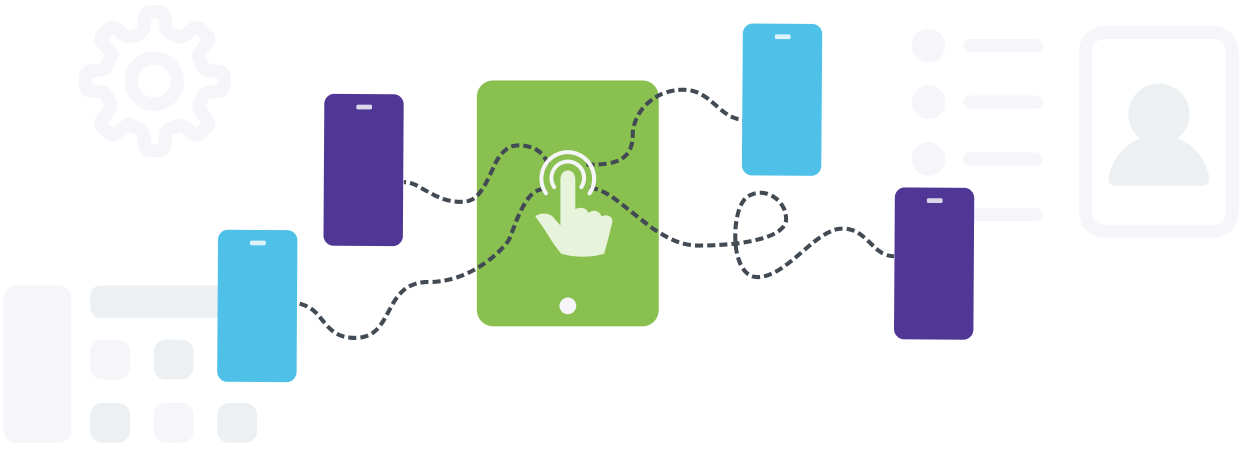
資安需求在開箱裝置前就已經存在了，等到第一次連線至企業資源時才去思考，早就為時已晚。請聽我們娓娓道來。

零接觸部署是指**在使用者首次啟用電腦時，設備就已經準備就緒**的工作流程，它可自動且安全的將「Apple 商務管理」或「Apple 校務管理」與 Jamf 密切整合。

Jamf Pro 確保不論是公發裝置，還是使用者自備裝置 (BYOD)，都能維持安全與保障隱私，它可支援多元的所有權模式，如個人 BYOD 裝置、使用者自助註冊裝置。一提到安全性，就不得不提我們**可當日支援所有 Apple 功能 (含安全性與隱私強化功能) 的 MDM 解決方案**，它可讓你支援和管理幫助使用者更聰明而不是更奮力工作的功能，在端點防護方面也不需要做出妥協。

App 管理是資安需求方面，十分關鍵的部分。可即時將更新版本部署至 App 與作業系統 (OS) 的能力，將左右資安計畫的成敗。畢竟在出現問題時，若是無法採取任何措施來補救問題，那麼試著了解自身資安需求又有什麼用呢？Jamf Pro 的另一大亮點是，**它可為 Mac 管理者以批量管理指令，縮短 App 生命週期管理的工作**，使裝置隨時與作業系統更新維持同步。別忘了也要更新 App。Jamf 的 **Self Service 自助服務區**以及強大的「App 安裝程式」確保使用者所需的 App 可輕鬆取得、始終受到管理、自動更新至最新版本，並維持在最安全的狀態。

簡化身分識別與存取配置流程是全方位、深層資安防禦策略的主幹。若實施「可信任的資源存取」，則可確保只有受信任的使用者，才能隨時隨地存取裝置與資源，尤其在管理行動辦公勞動族群的裝置時，至關重要。這為使用者提供了一個簡易在裝置上驗證身分的方法，從流暢的零接觸部署入職體驗、日常辦公，到存取企業資源，在在都奠定了使用者達成工作的基礎。ZTNA 與 **Jamf Connect** 的條件式存取兩者協作，證明了**高效、可靈活調適的安全機制並非可有可無**。



三個安全性要素，一個可靠的平台

> 「善戰者，立於不敗之地，
> 而不失敵之敗也。」——**孫子**

Trusted Access 是一個達成安全性的綜合方法，這個全方位的解決方案，可包辦各行各業組織與機構的管理與資安需求。

Trusted Access 的各個面向，舉凡**裝置管理**、**端點防護**以及**資安可見度與合規性**，對於達成深層資安防禦策略而言，缺一不可。此防禦策略可對裝置、使用者和資料，實施進階存取管控與安全配置設定，同時運用遙測數據來適應日新月異的資安態勢或裝置與組織的環境，不僅維持安全性與保障隱私，還能確保隨時合規。

隨時隨地，輕鬆的為你的 Apple 裝置確保靈活多元的使用與安全性。

歡迎聯絡我們，了解 Jamf 如何透過一流的解決方案，為你評估資安需求

立即開始

或聯絡你偏好的 Apple 經銷商，來試看看 Jamf 的服務

jamf

www.jamf.com/zh-tw/