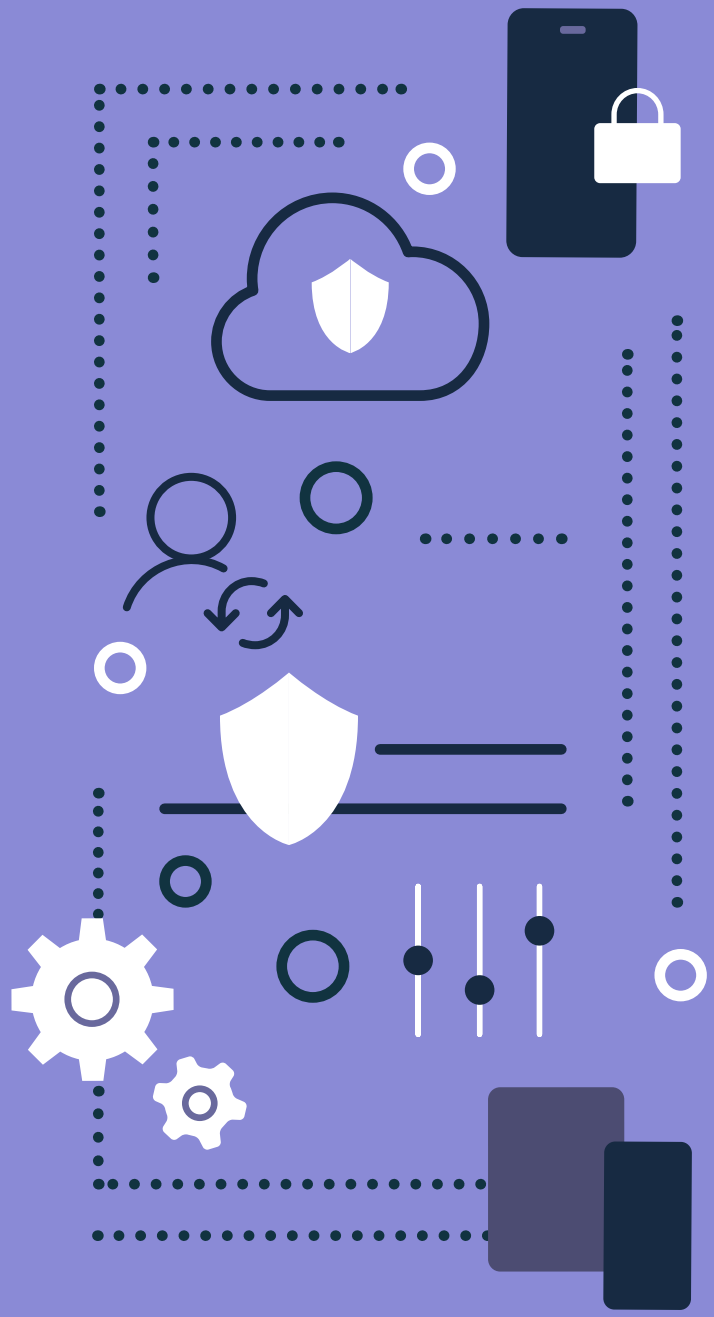


jamf

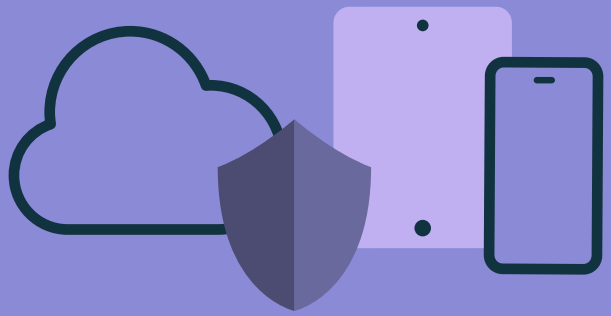
基礎指南

Mac 適用的防毒之道

隨著企業 APPLE 裝置數量日益成長，針對 MAC 的惡意軟體自然成了重要議題

總體來說，所有系統平台的偵測能力皆呈上升趨勢，在此背景下，Apple 的表現其實相對出類拔萃，至於偵測惡意軟體的能力，在對照其他更具針對性的惡意軟體類型後，反而算是處於停滯狀態。

採遠端與混合辦公模式的機構日益增加，技術的格局也因此產生了巨大轉變。惡意軟體開發者和攻擊者為因應這樣的轉變，也正著手變更攻擊的範圍和規模，來替他們的彈藥庫加強攻擊能力。攻擊者開始同時利用多種威脅類型來增加攻擊複雜性，而仰賴自動化技術的攻擊目標，則因為自動化而可讓使用者納入更多提升生產力的協作工具。



在這份指南中，我們將探討以下內容：

- 定義何謂 Mac 專門的防毒 (AV) 機制
- 說明惡意軟體對 Mac 使用者漸增的影響
- 說明了解這些趨勢對於保護個資的重要性
- 分享 Jamf 確保您的 Mac 設備受到保護的功能

MAC 專門的防毒軟體

防毒 (AV) 機制是多數公發裝置在資安方面的基本要求，而 Apple 的 macOS 已具備基本的 AV 機制，包括 XProtect、「門禁」與「惡意軟體移除工具」。但是，這些工具不時會進行更新，機構也無從得知這些工具採取的行動。必須要有更完善的防毒功能，機構才有辦法完整防止與隔絕專門針對 Mac 的惡意軟體，這樣的需求是 macOS 上以 Windows 系統為重心的解決方案所辦不到的，若等待惡意軟體、廣告軟體或其他垃圾軟體問題出現才正視問題，並非解決之道。

機構需要的 AV 機制應能有效識別並修復針對 Mac 的攻擊，而不是將寶貴的資源浪費在尋找 Mac 中針對 Windows 系統的威脅。況且，高效並且完善的 Mac AV 機制，不論是對安全性或裝置使用體驗來說都至關重要。

根據卡巴斯基實驗室的一份報告，隱私遭侵犯的例子如取得 GPS 座標、解密日誌紀錄，以及監控/錄下通話內容等，而這還只是眾多問題中的冰山一角。

瞬息萬變的威脅態勢

越來越多的網路釣魚活動會趁勢利用社會事件，尤其是當事件涉及供不應求或受全球貨品短缺影響時，來引起個人恐慌與擔憂，再偽裝支援團隊行使詐騙。

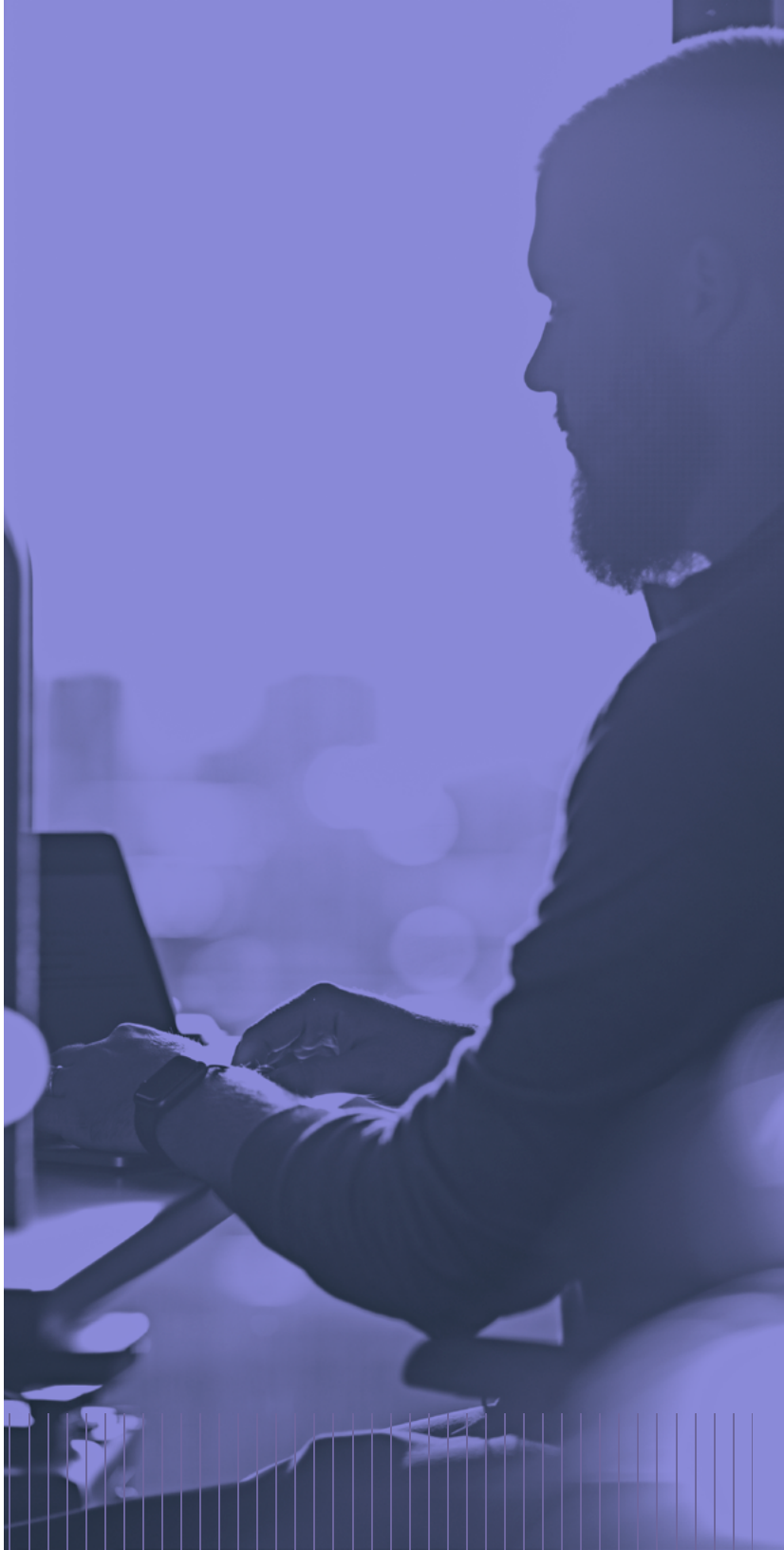
數位跟蹤

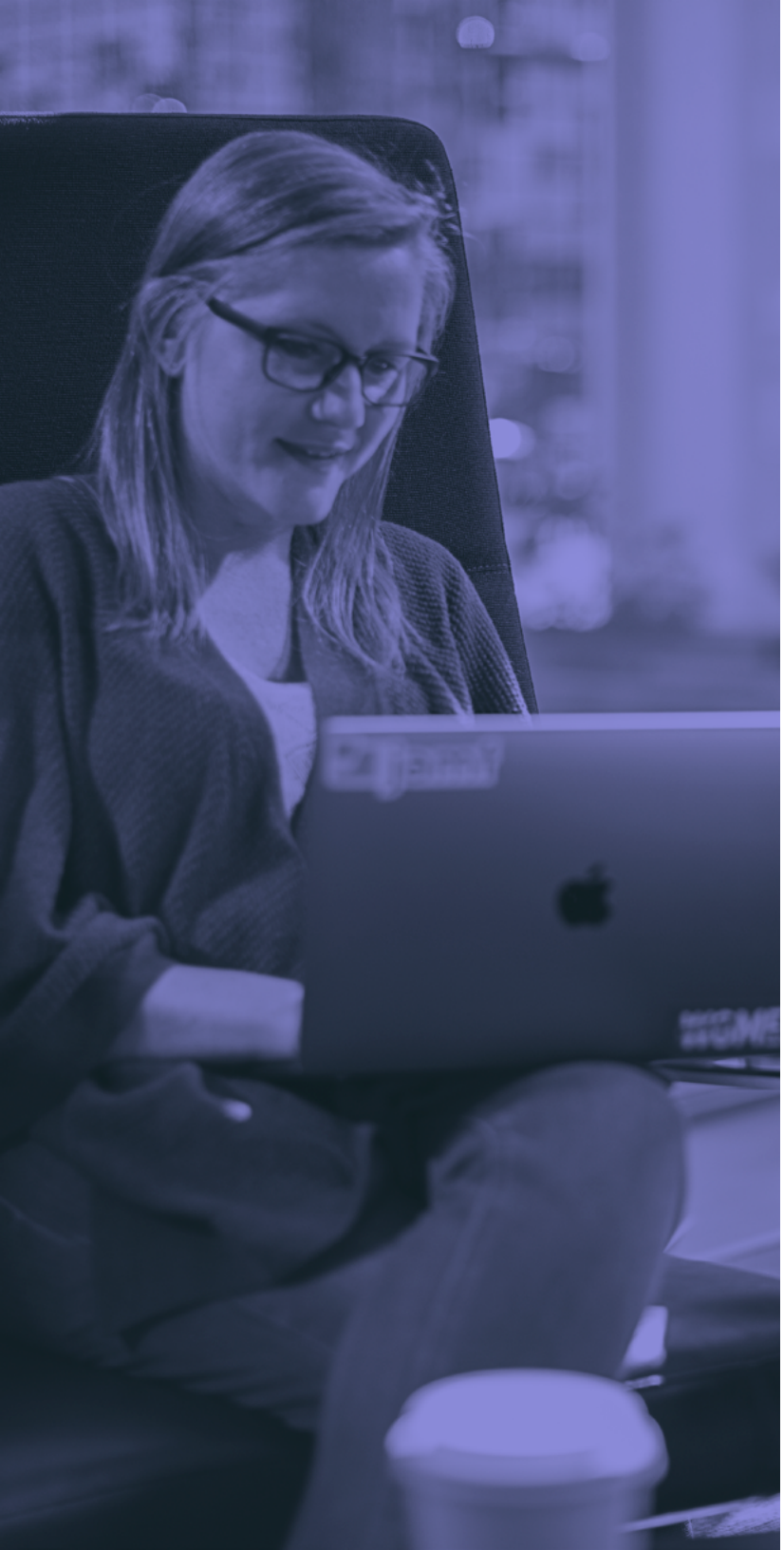
廣告軟體、間諜軟體及追蹤軟體都是用來竊取和洩露使用者個資的惡意軟體類型。追蹤軟體則是因利用各種個人識別資料 (PII) 而得到了「數位跟蹤」的稱號。

如同一場漫長的象棋賽局

我們希望正在閱讀此電子書的您可以明白，威脅抵禦通常是長期抗戰，這意味著攻擊活動可能持續直到攻擊者達成目的為止，他們會嘗試各種惡意軟體，並試圖找出任何弱點直到取得存取權才會罷休。拖延戰術讓他們有時間變更攻擊策略或改裝工具，並盡可能蒐集情報，最終便使得惡意軟體更深入潛藏在受影響的系統中。

這樣的策略通常是有週期性的，且每個層面環環相扣，單一個問題可能接連造成一連串的影響。





MAC 防毒軟體的當前狀態

惡意軟體數量一般呈上升趨勢，AV-Test.org 光在 2022 年便一共發現了 1,227,048,144 個惡意軟體，其中還包括可能有害的應用程式 (PUA)。那麼 Mac 使用者還有希望嗎？作業系統在分配後發現，所有惡意軟體中只有 220 個是針對 macOS！

會有如此龐大改變的原因包括：

- Apple 裝置數量在企業市場上持續增長
- 消費者透過員工自選裝置方案或選擇自備裝置時，選擇了 Apple 產品
- 全球逐漸邁向遠端和混合/在家辦公模式的轉變，深化了過去劃分辦公室和在家辦公的分界線

先別高興得太早

作為使用者，自然樂見數字下降，並認為這是值得歡慶的好消息，然而，從各個來源蒐集得來的遙測數據已顯示，在個人空間中使用的設備依然無法避免潛在有害程式 (PUP) 的影響，而且這些傷害經常是由廣告軟體帶頭造成。

從企業面來看，這樣的問題可能又是不同的討論，但對於使用 Mac 裝置的個人戶來說，PUP 和廣告軟體可被視為竊取使用者的 PII 的手段，甚至可能導致更嚴重的事情發生，當惡意廣告成功感染時，個資會被鎖定，又或者系統會自動下載聲稱要清理您 Mac 的不良 App。

惡意軟體五花八門

雖然距離上一個已知針對 Mac 的新型勒索軟體，早在好幾年前就被發現，直到 2020 年，才又有勒索軟體 EvilQuest 的出現 (又名 ThiefQuest)。這款惡意軟體具備勒索軟體的所有特徵，只不過它的要求付費加密警告只是掩護，它真正的詭計是持續且具針對性的盜取個人和企業資料。

像這樣的惡意軟體與普通軟體無異，日子一久也會變種，多了造成更多傷害的附加功能，逃避偵測的隱身能力也會強化，它甚至可以在感染設備後自我更新進化。看待 EvilQuest，就猶如觀賞一齣未完結的戲劇，隨著劇情在未來發展，值得我們持續關注。

即便是老狗，
也能學習新花招

目前被列為「惹人厭」的廣告軟體，同時也不斷在進化。有鑒於較新的 macOS 版本可以在允許啟用 App 之前就驗證 App 簽署，一些惡意軟體開發者甚至用盡手段跳出傳統思維，一切都是為了存取您系統上寶貴的資料，並從您瀏覽網頁上的廣告獲利。

這些攻擊類型，如複製 Safari App，再對其進行修改和安裝未經授權的擴充功能來追蹤使用者、使用描述檔 (與 IT 管理者用於管理設備設定的描述檔相同) 誘騙使用者在設備上安裝惡意軟體、有效地授予惡意人士執行更多攻擊所需的權限。

值得注意的是，雖然廣告軟體被認為危險性較小，但它是 macOS 中最常見的惡意軟體威脅，感染形態最為創新，加上遠端新增惡意軟體有效負載能力已經越來越普遍，結合這些因素，即使只是廣告軟體也會帶來龐大影響。

用更聰明的方法做事，而不是埋頭苦幹

不幸的是，沒有任何一種解決方案，可以解決眼下所有不斷升級的威脅，其中關鍵的一個要點就是，威脅不會每次都來自同一個地方。發動攻擊的人會改變策略，並針對效果最好的設備和服務來進行攻擊。因此，數據能斷言的只有這件事——攻擊者不會善罷甘休。

這對每個需以電腦維生和工作的人來說，代表著什麼？簡單來說，建立安全框架來防禦、轉移、預防或補救出現的任何威脅，勢在必行。保持警惕的態度也是資安防護重要的一環，您可訓練使用者辨別網路釣魚、不安裝未知軟體等常見的威脅類型來達成。

IT 與資安團隊還必須將警惕的做法納入其工作流程，才能由始至終確保強化和維護機構的安全態勢。善用偵測軟體，並根據已知特徵或啟發式方法來定位威脅，偵測軟體會執行行為分析，在未知威脅發生前便可以提早偵測來獲得威脅的詳情，如此才有辦法進一步找出威脅的位置及來源，還有抵禦威脅的方法。

迅速回應以及自動化的能力也是成功的必要關鍵，如此才可以快速回應偵測到的威脅，同時修復發現的任何問題。這兩種能力對於最大程度縮小攻擊層面、更聰明地有效管理風險來說必不可少，同時可為深層防禦策略多加一層保護。

畢竟當我們在使用 Mac 時，通常是為了完成某些任務——不太可能是用在啟動 App 前掃描數萬行 App 代碼來找出 App 的錯誤，對吧？而且正是在這些時刻，我們才會想起 Apple 優秀的使用者體驗，正是因為這些，Apple 裝置的使用者才有辦法創造出非凡的東西。那麼，資安軟體又何嘗不是這樣呢？

JAMF 整合功能與支援服務

Jamf Protect 透過 Mac 上的署名制偵測和行為分析，來防禦惡意軟體並修復惡意行為。由上而下的方式 (top-down approach) 來洞察裝置詳情，企業的 IT 和資安部門便可以從安全層了解影響設備性能的原因。此外，當與 Jamf Pro 結合使用，將可啟用集中式修補程式管理，解決任何可能出現的問題。最後，Jamf Connect 是完成這個完善資安方案的最後一哩路。Jamf Connect 的身分驗證與存取管理 (IAM) 解決方案採用雲端身分服務，來保護設備和資源存取。

善用 Apple 內建的資安工具並將這些力量發揮至極致，Jamf 提供的深層防禦策略將有效保護 Mac，並提供順暢的使用者體驗，同時維持提供設備的所有相關見解和分析。這樣的分層式策略使 IT 人員能夠在決定防禦位置、保護使用者個資時，做出最佳的決策。

Jamf 是管理企業 Apple 裝置的業界標準，我們的產品和解決方案可為您的機構與使用者制定最佳的安全策略。

我們稱這項服務為——Trusted Access。**深入了解這項服務。**

別只聽我們說

實際試試才知道

當您準備好要保護 Mac 設備，使其免受不斷升級的安全威脅所害、防禦已知惡意軟體，以及修復惡意攻擊時，歡迎您預約免費試用或者聯絡您偏好的經銷商。

立即預約免費試用

或在您想進一步強化安全性時，聯絡您偏好的 Apple 經銷商。

立即前往 jamf.com/zh-tw/，進一步了解 Jamf Protect 與 Mac 端點防護。