jamf

行動威脅防禦

入門

Apple 平台開箱即有的安全性，確實無人能及。然而，對有心人士來說，這個平台逐漸成為顯眼的攻擊目標，機構因此必須有能力應對並抵禦當今和未來的威脅。

常見的攻擊活動，如網路釣魚、惡意軟體和易受攻擊的 App 等，經常成了取得企業資源與敏感資料的不當管道：

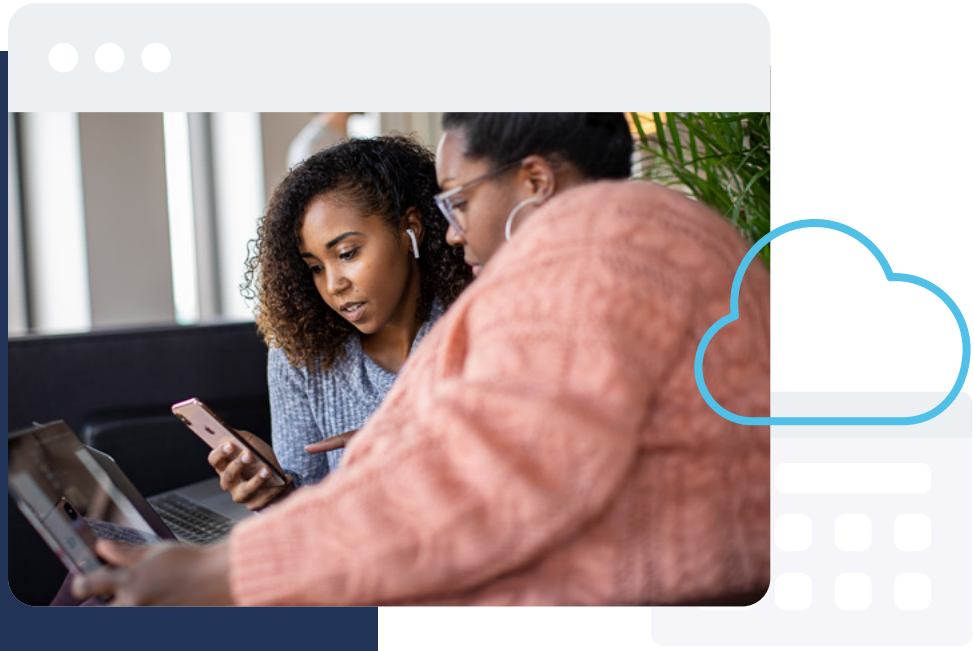
- 機密資料外流
- 取得存取企業服務的許可
- 蒐集使用者個資
- 攔截網路通訊

透過威脅偵測、零日網路釣魚與惡意軟體防禦機制，Jamf 可保護你的行動端點免遭入侵。由於針對行動裝置的攻擊事件頻頻增加，此議題儼然成為所有機構最關心的項目之一，尤其是那些採取遠端或混合辦公模式的組織。

在這份指南中，我們將探討以下內容：

1. 全方位威脅偵測和預防
2. 為各種使用案例提供強大的保護能力
3. 即時回報功能
4. 政策管控與條件式存取
5. 統一作業管理

APPLE 平台逐漸成為有心人士的眾矢之的...

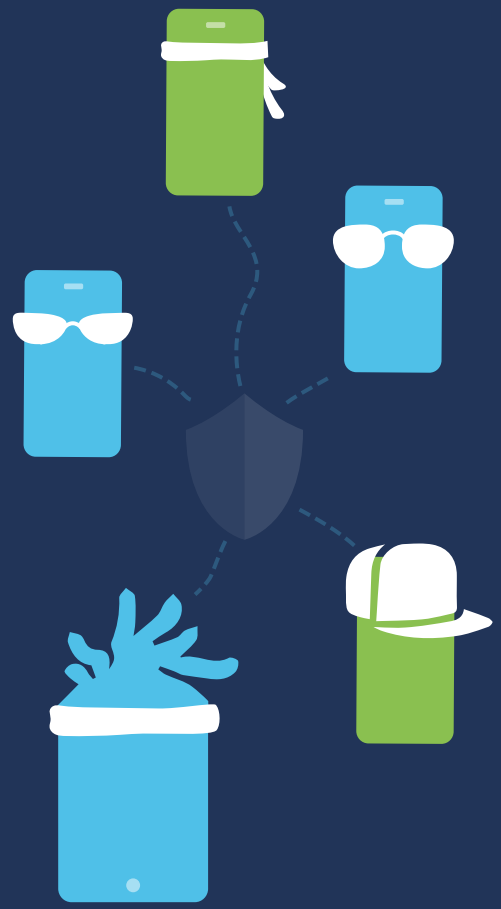


他們經常實行無差別攻擊

立即加入 **Jamf Protect**——一個專門設計的解決方案，它可保護行動裝置和使用者遠離惡意威脅，維持低負載並佔用較小的網路足跡，同時將對設備性能和使用者體驗的影響降至最低。

部署 macOS 裝置給使用者的機構需仰賴 Jamf Protect 提供端點防護機制，以保護其設備免受資安威脅、惡意軟體影響，並取得裝置健康度的深入分析。那麼如果是 iOS、iPadOS、Android 行動裝置呢？有哪個端點防護平台適合行動裝置，既能滿足手機和平板的獨特需求，又能與 **Jamf Pro** 深度整合？

“PROTECT YA NECK”



回歸正題，這邊下的標題來自樂團武當幫的創意歌詞，指的是保護敏感資料最重點的部分。就本指南而言，最重點的部分是指行動裝置，因為攻擊者經常會以行動裝置作為媒介來取得敏感資料。

根據 2021 年的雲端安全報告，**41% 機構**的遠距工作者設備上曾遇過惡意軟體攻擊，這不僅是一個驚人的數字，而且比起上一年更增長不少。**歡迎閱讀我們的《安全性 360：年度趨勢報告》，了解 2023 年的資安趨勢與風險。**

對那些不確定事件激增背後原因的人來說，答案既簡單又複雜。由於近年來逐漸轉向遠端或混合辦公模式，網路安全邊界受到侵蝕，當使用者不在辦公室工作時，更多時候會使用行動裝置來維持生產力。這是簡單的部分。複雜的部分是機構該如何藉由轉變其基礎架構以確保裝置與數據的安全。

為了最大程度降低所涉及的複雜性，Jamf 採取了雲端式做法，提供可靈活擴展的強大進階資安技術，包括即時監測、偵測及回報功能，使資安團隊能夠控管設備的運行狀況。

網路防護

在現代企業面臨的多種資安威脅中，網路釣魚只是其中一種，但仍可以說它是最為氾濫的類型，因為它針對的是安全鏈中最薄弱的環節——使用者。可悲的是，即便是立意良善和訓練有素的使用者，出錯的機率仍然過高，也就是說入侵他們裝置的成功率依舊偏高，攻擊人士當然也就持續在攻擊鏈中濫用這些弱點。

借助網路內防護，你便可以即時主動封鎖零時差攻擊，如釣魚網站。如此一來，設備就可以在執行攻擊之前免受這些活動的影響。藉由禁止在所有通訊管道存取這些惡意網域 (有線、Wi-Fi 或行動數據)，機構便可以確保使用者和端點設備的安全。

擴充能力

與其他資安解決方案相比，我們在建構階段便已考量到與供應商 API 框架的相容性，因此 Jamf Protect 可與更多他廠的統一端點管理 (UEM) 和安全資訊與事件管理 (SIEM) 平台高度整合。對資安團隊來說，這意味著他們可以充分利用既有的已投資項目，如管理安全性與裝置的設備、App、服務，真正發揮威脅分析、修復工作流程與自動化的功效。

一個很好的整合案例是利用 Jamf 風險 API 與 Jamf Protect 的功能來實現良好的溝通能力。有了這項整合功能，兩個系統間的數據將可即時共享，使你可以依據機構行動裝置的健康度來適度進行修復，並獲得可自訂的報表內容。

調適型存取

為抵禦無數毫無放緩跡象的網路攻擊，不讓它們影響行動裝置安全性，Jamf Protect 將全天候運行

與存取權有關的威脅如此有效的主因之一就是，假設今天裝置遭到入侵，使用者也無從辨別 (裝置看似可以正常運行)，則使用者仍然可以存取資源，這意味著裝置將照常處理請求並授予存取權，進而使資源遭駭。

藉由僅允許安全連線與受信任裝置存取企業資源，Jamf 不僅解決了上述的問題，同時還可提升你的資安態勢。你問我們如何辦到的？

透過持續監測遙測數據和收錄每台裝置特有的情境資料，找出是否存在異常

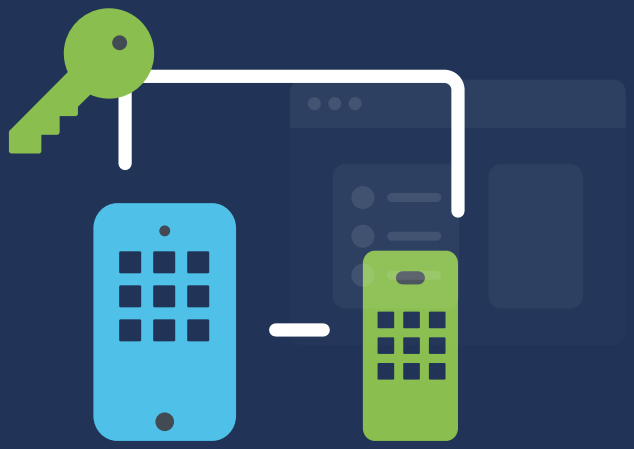
如果確定端點為高風險或已遭到入侵，Jamf Protect 將強制實施自訂政策來禁止資源的存取。

進階機器學習

在認識 Jamf 如何保護你的企業和行動裝置後，我們將帶你探討軟體組成的基礎，讓你更深入了解它確保設備免受威脅的做法。我們探討的並不是功能本身，而是為上述功能提供支援的一些內建核心防禦技術。

向你隆重介紹——MI:RIAM。它不是 Siri 替代品或武當幫的新成員，而是一個先進的情資引擎，可以最大範圍即時識別已知與零日威脅。
MI:RIAM 透過全球最大的威脅數據集，從 4.25 億個感應器蒐集資訊並收錄至演算法，使用先進的資料科學方法提供有關最新資安威脅與活躍攻擊手法的即時見解。

所有行動裝置皆適用



你的機構只有使用 iOS 和 iPadOS 裝置？那再好不過了。因為像 Jamf Protect 這類型的安全防護機制，是專為 Apple 手機、平板、使用者抵禦現有和新型威脅而生。

你的機構有使用他牌的行動裝置嗎？那也沒問題。Jamf 可確保 Android 和 Windows 作業系統的安全，並致力為所有類型的行動裝置提供強大的保護力。此外，Jamf 可支援不會影響安全性的多種所有權模式，例如企業所有裝置或自備裝置 (BYOD)。

身為使用者，你或許會好奇自己是否受到完善的保護。而身為資安團隊的一員，你則會希望了解你的使用者受哪一種方式保護。能讓惡意人士知道的越少，就越能更好地維護網路的安全性，確保資訊安全。還有幾種類型的資訊，你需要不惜一切代價來維護安全，以確保其完整性、確保資安團隊完全掌握公司端點設備的安全性狀態。

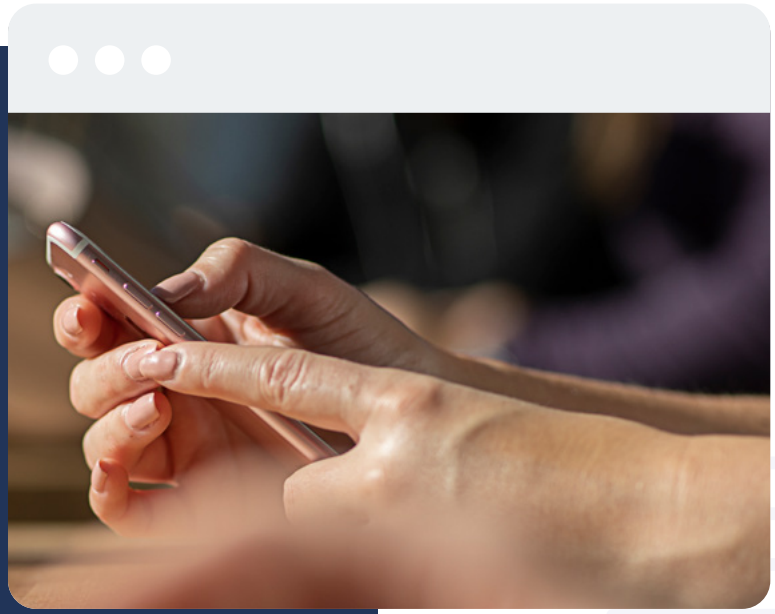
使用者隱私

個人識別資訊 (PII) 與個人健康資訊 (PHI) 是威脅者極力獲取的數據類型之一。這是一個惡性循環，攻擊者蒐集到的資料越多，所能採取的手法就越多樣，因此更讓他們有機可乘。

幸好我們可以透過 Jamf 將通訊往來加密、抵禦網路釣魚攻擊，藉此維護線上隱私。這套機制可應用於使用者個資保護，以及可能需要遵從法規的敏感資訊。 進階隱私功能和政策管控可防止不安全的使用者或裝備存取企業資源和資料。

即時見解

資安團隊可以透過內建提供的預設回報功能取得裝置健康度的詳細報告，或依據自家機構的特定需求，來調整和自訂需要的詳細資訊。自訂報表功能可在控制台上提供管理人員即時資訊，使 Jamf Pro 的能力躍升至下個境界，你也可以透過內建整合功能把資料傳輸至 SIEM 平台，將資料視覺化呈現在儀表板上、運用 API 與統一管理解決方案整合，比如透過 Jamf Pro 在軟體間傳輸資料，實現自動化裝置管理和自動偵測，並修復端點問題程序。



你可以為機構和使用者克服眾多難題，確保資料、設備和人員皆安全無虞。我們甚至沒有在此電子書中提及太多內容，所以我們建議你採取的下個動作就是：

免費動手實際操作看看，你也可以與偏好的經銷商合作，深入了解 Jamf 的功能。

預約試用

無論是哪一種方式，我們都歡迎你的加入。