



縱深防禦：

透過整合和分層解決方案彌補安全漏洞



網路安全並不「重要」。

保護企業的裝置、使用者、資料和資源免於不斷變化的威脅和攻擊，這是「必要」。

過去，資訊安全只不過是在每台電腦上安裝一個防毒解決方案，為少數不在辦公室工作的員工（如出差的銷售團隊）提供一個 VPN 用戶端。

但時代變了，我們處理網路安全的方式也隨之改變。

在本白皮書中，我們將介紹：

- 威脅情勢的演變
- 保護所有裝置類型和作業系統的重要性
- 安全的關鍵不僅是保護資源
- 實施縱深防禦策略的重要性
- 整合安全方法對企業的重要性



不斷變化的威脅情勢

這麼久以來，這個產業在行動科技已經有了長遠的進步，這對使用者和企業組織來說，都指向一個明確的方向——我們已經準備好改變工作的方式。演變並未就此止步。威脅行動者也改變了戰術，透過不斷演變的威脅和攻擊來適應變化。它們變得更加複雜——終端使用者越來越難發現這些威脅，專業資安人員也更難抵禦。

簡而言之：現在的威脅來自於各個層面。針對所有裝置類型和作業系統，還可透過任何網路連線部署。

會這麼會這樣呢？因為傳統的邊界保護「單一解決方案策略」在過去確實能有效保護資料和端點安全，但這個做法已經不足以應付現在的威脅。網路邊界因為以下因素而不再那麼有效：

- 轉向雲端服務和應用程式
- 過渡到遠端／混合工作環境
- 將個人持有的裝置用於工作上
- 使用不受信任的網路進行溝通
- 依賴共享工具進行協作

毫無疑問地，這些要點中的每一個都為使用者帶來了能夠隨時隨地、在任何裝置上、透過任何網路連接工作的可能性，無論實際地理位置、架構、軟體的偏好如何。但也同時增加了裝置的攻擊面，潛在漏洞利用的可能性也跟著提升。

以下是一些威脅情勢演變的不同方式，以應對行動科技和分散式勞動力的興起。

進階持續性威脅（APT）、融合威脅和攻擊複雜性增加

威脅情勢已經發生了變化。任何稱職的資安專業人士都知道這個說法是對的。但究竟是怎樣變化的，這就是本章節要探討的主軸。惡意程式碼就是惡意程式碼，無論它是偽裝成應用程式，還是透過被入侵的網站執行，其結果始終是一樣的——感染您的裝置，執行攻擊者要它執行的任務。



現在我們所看到的是，多年來所依賴的 1+1=2 公式已經改變了。攻擊變得越來越複雜，往往與其他威脅結合在一起，或透過其他手段進行部署，如入侵攻擊目標的可信合作夥伴，進而從後門存取攻擊目標的資源。其中一些複雜攻擊的例子可以追溯到 1 到 3 年前：

- 在這短短幾年內發生的兩起攻擊事件，影響了 **1 億** 多名客戶，洩漏了他們的個人識別資訊 (PII)。
- **2023 年**，供應鏈攻擊增加了兩倍，已知漏洞的下載次數達到 **21 億次**（即使當時已有修復版本）。
- 賭場和飯店在社交工程活動中遭遇勒索軟體攻擊，影響了營運、洩露了客戶資料並導致財務損失。
- 社群媒體平台的 API 遭到攻擊後，**540 萬** 使用者的資料曝光，另有 **4 億** 使用者的公開和私人資料在暗網上出售。
- 透過對個人所有的行動裝置進行未經授權的監控，高風險個人不斷成為國家使用 Pegasus 間諜軟體侵害隱私的目標。

融合威脅

融合威脅也被稱為網路 - 實體融合，其名稱源自於我們的數位世界和實體世界日益交織在一起。由於這兩個世界之間的界線越來越模糊，它們似乎越來越緊密地結合在一起，一個世界（網路）的影響也會對另一個世界（實體）產生非常確鑿的影響。除了對系統、流程和資源造成實體破壞外，網路威脅還擴大了攻擊範圍，加劇了連鎖反應，從而引發更大的影響：

- 實現持久化
- 特權提升
- 橫向移動
- 惡意軟體部署
- 資料外洩

我們在各行各業的公司中都能看到這種情況，對科技的依賴已成為業務連續性的關鍵，例如，遭受網路攻擊後，使用者便無法存取電子郵件，在恢復存取之前，業務幾乎就會停擺。這如果時間一拉長，對業務的影響可能會導致更嚴重的問題，如生產或收入損失，甚至迫使受影響的企業永久關閉。

2021 年，美國最大的成品油管路商（每天可輸送 300 萬桶燃料）在遭受勒索軟體攻擊後被迫關閉五天，就是這種情況。這對關鍵基礎設施的影響是什麼？最常聽到的就是向威脅行為者支付了 500 萬美元贖金，以重新獲得加密系統和資料的存取權。自從這次攻擊以來，這多年間發生了一些變化。其中之一就是司法部採取了更積極的方法，以摧毀勒索軟體攻擊背後的基礎設施和犯罪分子。然而，威脅行為者的策略也在不斷演變，因為「90% 以上的攻擊不再加密受害者的裝置，而是直接外洩資料並勒索所有人。」

社交工程

在現代威脅環境中，社交工程的威脅似乎是無窮無盡的。曾幾何時，人們唯一擔心的問題就是偶爾會有人試圖冒充公司員工，或者是一位慷慨卻又憂心忡忡的王子發來的電子郵件，他急需你的銀行帳戶資料，才能保住他的百萬家產。

哦，時代真的變了。

如今，社會工程幾乎成了一張分級流程圖，詳細列出了永無止境的攻擊類型，多到無法一一列舉。隨著每項新技術的發布，攻擊類型也會隨之增加。其實這些攻擊都是由網路釣魚延伸出來的變種，這點是無庸置疑的。

每一種新的迭代，如 QR code 網路釣魚，或是「quishing」這樣親切地稱呼，都會以多形態的方式出現在我們的資安詞彙中。社交工程學的演變有兩個層面：一個是表層，另一個是底層。前者很容易被發現。網路釣魚針對我們的當今工作方式進行了調整，排名前五的身份假冒威脅如下：

1. 電子郵件網路釣魚
2. 魚叉式網路釣魚
3. 捕鯨攻擊
4. 簡訊釣魚和語音釣魚
5. 社群網站釣魚

然而，後者本身並沒有一個巧妙的名稱。這使得這些新的威脅變得更加危險……並且難以被最終使用者、IT 和安全團隊發現。

Jamf Threat Labs 最近發現了這些篡改技術的兩個實例，它們的概念驗證（PoC）對當前和未來的行動安全造成了驚人的影響：

假飛行模式

一種利用漏洞後的持久化技術，可顯示功能正常的飛行模式。然而，深入觀察，您會發現在成功利用裝置後，威脅行為者編輯了系統文件，控制 UI 顯示飛行模式圖標，同時禁用除攻擊者應用程式之外的所有應用程式的網路存取。這樣，即使使用者認為自己已成功將裝置離線，[攻擊者也能保持對裝置的存取](#)（持久性）。

假鎖定模式

之前，我們提到過 Pegasus 間諜軟體，以及國家是如何利用漏洞追蹤高風險人員的。雖然我們在下一章節中將介紹國家資助的威脅，但減少攻擊面的一個重要工具是 Apple 的鎖定模式。

試想一下，如果您認為自己的行動裝置已被入侵，您應該就會啟用鎖定模式來保護自己，避免進一步暴露。卻發現[自己的裝置仍然很容易受到攻擊，因為威脅行為者已經精明地繞過了這項最後的保護措施](#)。

這些正是社會工程威脅的類型，它們欺騙使用者，讓他們相信自己是受到保護的，但事實上，他們卻被誤導，產生了安全感的假象，而威脅行為者卻能繼續存取和控制他們的行動裝置。

國家/有針對性的攻擊

在數位時代，無論是在公共場合、辦公室或在家中，人們都會對自己的一舉一動、一言一行、一則訊息回應產生偏執，因為科技已經滲透到我們生活的各個方面。

即使你像克里斯多福·沃肯（Christopher Walken）一樣選則不使用電腦或智慧型手機，您的隱私仍然有可能受到周圍使用行動裝置的人的影響。

國家資助的進階持續性威脅（APT）組織不僅對某些產業的企業構成威脅。在現代威脅情勢下，APT 的攻擊範圍已從關鍵基礎設施擴展到任何能促進國家利益的個人、組織和地區。

以下是一些國家級攻擊的資料點：

90% 的資安警報來自關鍵基礎設施以外的領域

全球最受攻擊的三大領域是：

教育 **16%**

政府 **12%**

智庫／非政府組織和資訊科技並列，各佔 **11%**

每 10 個組織中就有 9 個認為它們已成為與國家有關的威脅行為者的目標

每個事件給組織造成的損失平均為 **160 萬美元**

到目前為止，已經觀察到 **5 個 APT 將 AI 武器化**，以增強威脅能力

對任何威脅行為者而言，經濟利益當然是最重要的動機之一，但國家和國家附屬的威脅行為者的主要目標是竊取資料。這並不是說間諜活動和破壞網路系統與服務就變得不是那麼重要的目標了。在現代威脅形勢下，APT 越來越重視洩露敏感和機密數據，以此作為收集情報、進行其他惡意攻擊以及影響社會和政治活動的手段。

就後者而言，間諜活動，尤其是**用於監視高風險個人之行動惡意軟體的擴散**，與透過行動裝置中的無數感測器對使用者進行未經授權的監視而引發的隱私問題，已經合而為一。事情並沒有就此結束，國家還利用收集到的資料進一步鎖定受害者，如記者、政治家和高層——未經他們同意，也不知道他們的裝置已被入侵。由於具有類似隱形的功能，此類間諜軟體專為遠端部署、從受害者的行動裝置中提取各種資料類型而設計，通常是透過零點擊安裝和零時差漏洞來感染目標裝置。

通用方法並不適用於每個狀況

除了在第一章節中討論的網路威脅不斷演變的性質之外，這些要點中的每一個都有是推向我們走到今天這裡的原因之一。我們正在一個轉折點，在這個轉折點上，傳統的解決方案、程序和工作流程的目標是在保護：

- 公司擁有的桌上型電腦
- 運行一個受支援的作業系統

而該作業系統被 IT 部門限制為：

- 只能運行有限的軟體應用程式
- 無法執行任何與業務目標無關的任務
- 在公司網路安全邊界的相對安全範圍內運行
- 透過公司防火牆傳輸網路流量
- 使用反惡意軟體解決方案保護資料
- 透過 VPN 安全地進行遠端存取

為保護靜態端點安全而開發的傳統解決方案，已經不足確保電腦在當今威脅環境中的安全態勢，更不用說在現代企業，各種深具影響力的改變所塑造出的多變工作環境中了。

現代安全策略的優勢在於強大卻又有彈性。僅僅是採取禁止使用行動裝置、特定作業系統類型或個人裝置等的管理政策，並不能降低與這些硬體或軟體相關的風險。老實說，這樣的政策甚至無法阻止使用者試圖透過「受限端點」存取企業資源。他們將風險引入網路的可能性是真實存在的，更糟的是，管理員直到事件發生後才會意識到這一點。

那麼，最好的辦法是什麼呢？

IT 和資安團隊可以仰賴最佳的解決方案來管理端點及其安全性。管理和安全解決方案旨在原生支援各自的裝置類型和作業系統。這不僅確保了硬體和軟體最大的相容性，而且還為 IT 和資安團隊提供了所需的工具，以最佳方式管理和保護其基礎架構中的端點。

企業中的 macOS

考慮您的企業環境。在工作上，您應該大多是在管理 Windows 的裝置，但您對 macOS 電腦和筆記型電腦的看法如何？根據 [最近對中小型企业的一項調查](#)，「55% 的企業自己使用 Mac 裝置，或明確同意在公司內部使用 Mac 裝置」，無論行業如何。

在進一步討論之前，讓我們先來看看 [macOS 的市佔率](#)（截至 2024 年 2 月）：

全球：	美國：
15.46%	25.02%

僅在美國，macOS 就佔據了四分之一的市場份額，其中一半以上用於商業用途。因此，一個更好的問法可能是，當企業使用 macOS 端點時（而不是「如果」使用的話）如何確保它們的安全？因為無論您是否願意，您的終端使用者都可能或多或少使用 macOS 執行與工作相關的任務。無論是公司認可的企業配發裝置、員工自選方案的一環、BYOD/COPE 計劃，還是使用者使用的個人裝置（即使未經認可）。

Mac 的成長不僅正在加速，而且還會影響工作的應用，如果 IT 和資安團隊不使用專為 Mac 打造的原生管理和安全性工具來解決這一問題，那麼可能會對企業安全產生嚴重後果。

行動裝置：未檢查的風險

一般使用者通常只有一台電腦，但經常使用多種類型的行動裝置，如智慧型手機、平板電腦和智慧型手錶。事實上，根據 Statista 的一項調查，到 2023 年，[全球每位使用者平均使用的裝置數量](#)將增加至 3.6 台。

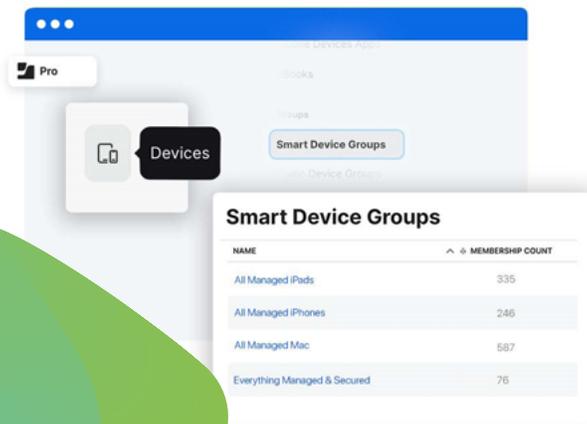
也就是說攻擊媒介多了四倍對於企業組織來說，保護桌面作業系統的裝置是「理所當然的」，但如果行動裝置在企業中不受檢查，它們很可能被允許連接到企業網絡，並在沒有保護措施的情況下存取業務資料和資源，成為員工工作流程的一部分。

行動威脅有哪些類型呢？

其實多數威脅都與桌上型電腦相同，只是沒有專門的端點安全軟體來提供對行動裝置檔案系統的可視性。

以下是常見類型的行動風險對企業的影響：

- **未經授權的存取：** 社交工程活動透過簡訊和社群媒體蒐集受害者的憑證，讓威脅行為者能夠存取企業服務。
- **引入惡意軟體：** 從不受支援的應用程式商店下載的應用程式（或側載的應用程式）在啟動時會執行惡意程式碼，從而影響業務和個人資料。
- **不合規：** 由於缺乏政策執行，當裝置不合規時，在受監管的產業中，企業可能要承擔責任與後果。
- **資料外洩：** 業務、個人和隱私資料被盜，使敏感和機密資訊直接落入威脅行為者手中。
- **橫向移動：** 網路攻擊利用外洩的憑證，將攻擊範圍擴展到整個基礎設施，從而擴大資料洩露的規模。
- **繞過保護機制：** 安全性和應用程式設定的錯誤配置導致攻擊面擴大，使威脅更容易在沒有緩解措施的情況下執行酬載。
- **特權提升：** 過時軟體中發現的漏洞可能會被利用，使威脅行為者有機會進入裝置，進而進到網路。



不僅僅是保護資源

在談到彌補安全漏洞時，資安專業人員會自然而然地思考降低風險的不同方法。完善修補程式管理流程，讓軟體和作業系統始終保持最新狀態，抵禦已知威脅，是常見的想法。另一種可能是跟上最近的人工智慧（AI）趨勢，將機器學習（ML）技術納入安全堆疊，以更快地回應事件，或透過自動化來簡化威脅搜尋。

雖然這些都是彌補安全漏洞的絕佳方法，但除了實施更新的控制措施以用更好的方式保護裝置、使用者和資料的安全性之外，還有其他一些因素。這些基本要素雖然不像技術或邏輯控制那樣「新奇有趣」，但卻能透過精簡、自動化和整合構成整體安全策略的程序、流程、工具和工作流程等，為企業帶來價值。此外，它還能將所有這些與負責確保裝置、使用者和資料合規並高效運作的 IT 及資安團隊匯聚在一起。

在本節中，我們將深入探討這些要素，並將其稱為「四個 C」，以強調這四個元素如何協作，在盡可能地提高效率的同時，也盡可能地減少對企業整體安全態勢的挑戰。

一致性（Consistency）

在企業安全方面，各企業應同等對待所有用於工作和連接業務資源的裝置類型，以及在這些裝置上運行的各種作業系統。畢竟，如果一家公司向員工發放 Windows 電腦，並部署端點安全控制以確保這些電腦的管理和安全，但卻不實施行動威脅防禦，以預防員工使用的未經許可的行動裝置中的業務數據，那麼這家公司就會面臨資料外洩的行動風險。

儘管在設計上是安全的，Apple 在安全性和隱私方面也十分著重，但威脅行為者還是有可能會像攻擊 Windows 或 Android 裝置一樣攻擊 Apple 裝置（macOS、iOS 和 iPadOS）。一致性的問題不在於把重點放在每個作業系統的不同之處，而是在於它們的相似之處。畢竟，桌上型電腦、筆記型電腦、平板電腦或智慧型手機儘管佔用空間不同，這些計算機工具在操作上的共同點比視覺上的差異來得多。

這就是一致性的關鍵所在：

對存取企業資源的所有端點

一視同仁，無論它們是什麼：

- 裝置類型
- 外形尺寸
- 操作系統
- 應用程式和服務

合規性 (Compliance)

合規的這個字定義是屈從於願望、要求、建議、制度或脅迫的行為或過程。

合規也可能還有其他不同的意義，這取決於您的企業所處的產業。對於受監管產業，有專門的法律來規定應該如何確保資料、程序和工作流程的安全，以防止受保護的資料外洩。而對於不受監管的行業，企業可能有自己的合規要求。這可能與內部業務政策一致，也有可能與他們希望業務營運能夠遵循的標準或框架相符。或者兩者兼而有之。

談到合規性，因為它與彌補安全漏洞有關，這代表著要解決兩個重要問題：

使用基線

第一點是基線更具體地說，創建基線是為了確立基礎設施正常運作時會是什麼樣子。基線的設計也為管理者提供了一個分界點，當端點偏離基線的可接受參數時，基線會發出警報，表示端點可能已不符合合規性要求。

向審計師提供證據

無論您的組織派遣內部審計師，還是接受獨立的第三方審計（作為監管義務的一環），總是需要某種形式的證據來證明合規性的維護。在證明端點合規性時，審計師的一般經驗法則適用於此：「如果沒有記錄，就表示沒有發生。」

管理基線和蒐集審計證據的關鍵在於遙測資料。它可為管理員提供端點的可視性，並可隨時參考，以深入了解用於存取、處理、儲存、修改、傳播或共享公司資料的裝置是否符合安全性計畫或監管制度的準則及要求。



合併 (Consolidation)

第三個「C」也是最容易被誤解的一個，因為它經常被誤認為是指整合解決方案。

「網絡安全不僅僅是 IT 部門的問題。」

— Stephane Nappo

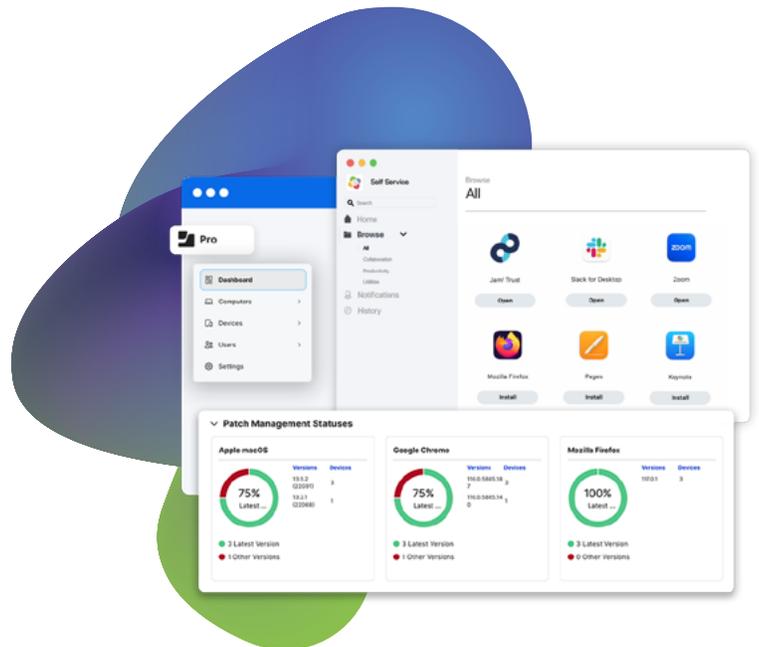
這裡所說的「合併」是指將 IT 和資安專業人員合併為一個有凝聚力的團隊。這會改變兩個團隊各自為政的運作方式。儘管這兩個部門都屬於資訊科技部門，但出於各種業務原因，企業通常會將這兩個部門的業務分開。

考慮到現代威脅情勢，這種運作方式的問題在於每個部門都要管理自己的軟體、供應商合作關係、程序、政策和工作流程。從理論上講，即使他們方法不同，但目的都是為了加強裝置和整個企業組織的安全態勢。但這樣的結構類型，在現實情況往往是達到相反的效果。

要有效的合併，就需要將網路安全架構和流程整合及現代化，以便：

- 集中最佳解決方案，原生管理支援的平台
- 減少供應商和合作夥伴的數量
- 打破各自為政的局面；加強資訊共享
- 建立知識管理實踐，消除把關現象
- 整合管理和安全方法
- 統一威脅防禦，加速事件回應
- 將保護拓展到整個基礎架構

轉向整合安全性+管理方法，企業管理員的任務是確保裝置和使用者在存取和處理敏感業務資料時，始終都能受到全方位的安全性防護，並全面擴展至整個公司資源。



節省成本 (Cost savings)

在合併 IT 和資安的同時，也應考慮投資回報 (ROI) 的重要性。投資回報率的一個特點是，當企業組織選擇「最適合」的解決方案來滿足其合規需求時，也就可以節省成本。這不僅需要了解相對於解決方案成本的價值，還需要平衡其他對投資回報率有直接 (和間接) 影響的因素，這些因素與您的深度防禦策略有關。

影響投資報酬率的直接和間接因素包括：

- 選擇既能原生支援企業裝置和作業系統，又能整合出整體解決方案的工具
- 將耗時的手動工作自動化，提高效率，同時也讓管理員專注於能帶來更多價值的計畫
- 簡化安全流程和工作流程，將其擴展到整個基礎架構並最佳化，以大規模地支援端點和應用程式
- 降低解決方案和事件回應之間的複雜性，盡可能地減少安全事件發現和修復所需的時間 = 減少停機時間，提高生產力
- 主動監控和報告豐富的遙測數據，讓管理員能夠即時掌握資訊，在合規性受到影響之前主動檢測／糾正風險向量。

將個人擁有的裝置用於工作上，也是與節約成本和現代威脅情勢有關的另一個考慮因素。許多企業組織都在進行 BYOD 計畫，尤其是在遠端／混合環境中，以便與團隊成員保持聯繫和協作。毫無疑問，BYOD 對僱主來說是有利的，這也是為什麼 [Zippia 最近報告指出](#)，美國近 70% 的 IT 決策者贊成 BYOD 計畫的原因。

96% 連接到企業網路的行動裝置為個人所有

80% 的高級企業領導者認為行動裝置是員工工作的必需品

使用穿戴式科技的員工將增加 30%

對於實施員工選擇計畫的企業來說，這也是一個福音，員工可以選擇他們認為最有生產力的硬體和軟體，而無需購買和維護數百、數千甚至數萬台行動裝置 (除電腦外) 的庫存所帶來的財務影響。這樣一來，既能帶來巨大的優勢，又能節省成本。



縱深防禦：有效的分層安全

美國國家標準與技術研究院（NIST）將縱深防禦（DiD）定義為「整合人員、技術和運營能力的資訊安全戰略，以在組織中橫跨多個層面和任務建立多重屏障。」

將其應用到網路安全計畫中，可以得到額外的保護，從而加強安全態勢。這種分層控制的方法可以為企業組織提供一個安全網。實施權宜之計，防止企業資源受到威脅。如果威脅繞過了一個層級的控制，在攻擊路徑上遇到的下一個層級，就會在風險演變成影響合規性的事件之前被攔截，並減輕風險。

我們在本節中回答的一些問題包括：

- 整合對企業網路安全計畫有何整體影響？
- 為了實現縱深防禦（DiD），您可以實施哪些類型的全方位安全控制？
- 啟用縱深防禦（DiD）網路安全計畫對滿足合規要求有什麼影響？

在下面的章節中，我們將深入探討一些技術，這些技術不僅可以透過整合實現，重點是它們可以如何大幅降低風險、防止惡意軟體，以及檢測和緩解高級威脅：

- 零接觸部署
- 威脅搜捕
- 零信任網路存取 (ZTNA)
- 進階威脅回應

管理+身份識別+資訊安全

您可能對管理、身分識別和資訊安全等裝置管理概念並不陌生。就其本身而言，每一個都是重要的基礎要素，提供與各自類別相關的一套特定技術和最佳實踐：

- **裝置管理**：電腦和行動裝置的管理，包括管理設定、部署安全性設定、安裝軟體和執行政策。
- **身份與存取**：一個政策和技術框架，確保已驗證的使用者和授權裝置能根據分配的權限存取受保護的資源。
- **端點防護**：基於軟體的技術，目的是盡可能地降低風險，保護裝置和使用者的安全，同時維護受保護的資源。

在設計豐富、深入的網路安全深度防禦計劃時，這三個基本要素的整合可作為基石，以確保企業資源免受未經授權的存取，盡可能地減少端點風險向量，並保證使用者的安全和生產效率。

零接觸部署：從最一開始就確保安全

資訊安全通常是一個被動的過程。「事件回應」這個名稱說明了等到發現威脅後才能處理的被動性質。就像因果關係一樣。

雖然管理員無法改變這種因果關係，但至少可以採取多種措施來減少攻擊面，從而盡可能地減少威脅對裝置的影響。

應該沒有比裝置首次開機更適合作為討論開頭的吧？這就是佈建和零接觸部署的神奇之處...在管理 Apple 裝置時，尤其容易利用零接觸部署的優勢。

這是因為在初始設定畫面期間，企業零接觸部署仰賴於自動傳送給裝置的管理、身分識別和存取工作流程。具體來說，在使用者使用企業憑證成功驗證身分，並完成裝置註冊和安裝管理描述檔後。MDM 會立即開始部署使用者工作所需的一切，並依照企業組織標準配置裝置。

在零接觸的佈建階段可以部署什麼呢？

- 強化裝置安全性
- 安裝受管理的應用程式
- 配置應用程式設定
- 分配使用者帳戶
- 策劃 Self Service 選項
- 更新系統修補程式
- 部署安全軟體
- 設定強制執行政策

您可能會想，這些功能對於公司自有裝置來說確實很有用，但是自攜裝置呢？

零接觸工作流程適用於任何所有權模式，包括個人擁有的裝置。針對這種情況，Apple 設計了「使用者註冊」，在不犧牲企業資安防護的前提下，也能維護使用者隱私。

當使用者主動將個人裝置註冊到企業 MDM，便可以有以下功能：

- 安全存取企業資源，如電子郵件、聯絡人、日曆、Wi-Fi 和加密網路連接
- 業務資料儲存在裝置上單獨的加密磁碟區中，個人資料不受影響
- 可使用兩個 Apple ID：一個個人 ID 用於個人資料和設定，另一個受管理的 ID 用於業務資料
- 管理員只能查看、存取和刪除自攜裝置上的業務資料；個人資料和隱私資料仍無法存取且不受影響
- 在整個企業內實現安全標準化，確保所有裝置無論其所有權為何，都能得到相同的保護



威脅搜尋：主動>被動

在管理團隊有權執行的專業的任務中，事件回應是其中之一。當端點安全軟體發出惡意行為或威脅已被標記的警報時，管理員就可以開始檢測和分類潛在問題。派遣事件回應小組來確認、控制並修復問題。

雖然處理已知問題對事件回應人員來說是家常便飯，但透過整合管理和安全解決方案來增強工作流程和程序，還可將被動的反應轉為主動的出擊。

建立安全基線

在網路安全領域中，基線就是指企業端點的正常運作。建立基準需要的不僅是測量效能，還包括安全配置、設定、端點安全軟體、應用程式和服務——簡而言之，就是使用者安全可靠地履行工作職能所必需的東西。這也代表著遵守合規要求以及與公司政策保持一致。

防止已知威脅

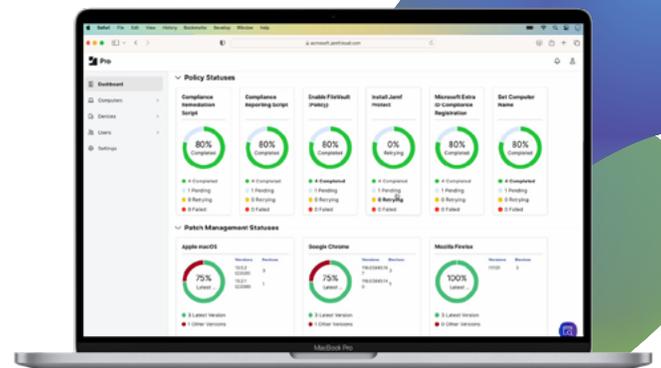
透過設定和以必要的參數作為基線，管理員更可以確認端點的運作狀況是否在可接受的範圍內。如果不在可接受範圍內，端點紀錄會提醒管理員注意任何差異，同時也提供手動緩解的機會。或者，在與管理解決方案進行配置整合的情況下，兩個解決方案之間共享的遙測資料將觸發自動工作流程，以修復事件。

檢測未知威脅

主動與被動是科技的核心主題，也是在威脅不斷整合與演變的情況下維持端點管理與安全的關鍵。其中一種積極主動的做法是威脅搜尋。

有效執行這項工作需要：

- 為您的環境提供極佳的資料搜集能力
- 強大的資料分析和模式識別 能力
- 對硬體和 軟體有深入的瞭解
- 強大的安全工具以及知道怎麼使用它們
- 調查未知問題的時間、耐心和努力



ZTNA：永不信任，始終驗證

隨著時代的進步，曾經被認為是最前沿的技術逐漸過時，然後被淘汰，最終完全停產，取而代之的是更快、更好、更強的技術。零信任是一種安全模型，它能以 VPN 等傳統技術根本無法比擬的方式去應對現代威脅環境的挑戰。

以下是將安全性、身分識別和管理融為一體的 ZTNA 建立網路安全新模式的幾種方式。

阻止網路威脅

身為科技人員，您肯定對防火牆不陌生。不管是它們的用途和作用。雖然防火牆是功能強大的工具，可提供邊界的安全防護，抵禦網路攻擊，但鑑於當今的工作團隊已轉為分散式勞動力，並依賴個人裝置來工作，因此保護區域網路邊界的防火牆對於保護遠距工作的員工，以及使用個人、未受管理的裝置工作的員工等，作用並不大。ZTNA 可在裝置上和網路內提供保護，抵禦威脅和攻擊。不僅如此，它還能在多個平台上提供保護，使運行 macOS、iOS、iPadOS、Windows 或 Android 作業系統的電腦和行動裝置的安全性標準化。

隔離和加密連接

ZTNA 也會加密任何網路連線上的通道，並以始終保持開啟狀態進一步確保其安全性，甚至在使用者或惡意軟體將其停用時又自動啟用。此外，ZTNA 還能透過與身分識別和存取管理的整合增加了另一層保護：每次與受保護資源連線時，ZTNA 都會為特定應用程式或服務產生自己專屬的微通道。這不僅能防止使用公共熱點時常見的中間人 (MitM) 攻擊，還能預防網路橫向移動，因為微通道是相互隔離的。最後，它強制執行最小權限原則，要求使用者進行身份驗證，允許他們存取分配給他們的資源，在其他情況下則預設為拒絕存取網路基礎設施中的其他部分（這與傳統 VPN 不同，VPN 一旦通過身份驗證就允許存取整個網路）。

驗證端點狀況和存取請求

零信任模式要求每次提出請求時都要驗證端點和憑證的狀況，而不是盲目地「信任」裝置。它會將端點當前的狀況與企業可接受的狀況進行比較。如果兩個檢查點都通過，則允許存取請求的資源。如果身份驗證或裝置狀況均未通過，則繼續拒絕存取（預設行為），並部署補救工作流程以糾正差異。修復完成後，再次執行檢查點。只有在裝置和憑證通過驗證後，ZTNA 才允許存取請求的資源。

無論行動裝置是：

- 公司發放的還是個人擁有的
- 連接到公司網路或公共熱點
- 通過裝置檢查點，但未通過憑證檢查點

也無論使用者帳戶是：

- 屬於特定的工作職位，例如高層人員或是行政人員
- 一小時前還是五分鐘前認證成功
- 通過憑據檢查點，但未通過裝置檢查點

「從不信任 - 始終驗證」代表著在預設情況下都拒絕存取。裝置和憑證必須通過驗證：每次發出請求時都需要。

進階威脅回應：一級的保護

進階持續性威脅（APT）激增，其目標是全球所有產業的企業組織。

在本章節中，我們將討論管理員在整合安全性和管理解決方案時可以採取的防禦措施。憑藉在兩個工具之間蒐集和共享的威脅情報資料，更全面的解決方案可針對以關鍵員工／職位為目標的網路攻擊（如執行長和其他高風險個人）提供強大的威脅回應和修復。

整合安全性和管理功能，以降低高階威脅風險的主要優勢包括：

為行動裝置攻擊提供完善的可視性

行動裝置威脅呈上升趨勢現代威脅環境不斷演變，威脅直指行動裝置，越來越針對行動裝置使用者。

但是，不要只聽信我們的一面之詞，以下是一些重要的調查結果，讓數字來說話：

- 在所有被入侵的裝置中，**43%**的裝置已被完全入侵（未越獄或 root），較去年同期成長**187%**
- **80%**的釣魚網站專門針對行動裝置，或被設計為同時能在桌上型電腦和行動裝置上運行。
- 2022年發現的 Android 系統關鍵漏洞增加了**138%**，而蘋果 iOS 系統的零時差漏洞則佔了**80%**。

- 行動應用程式中不當的雲端儲存配置是主要的攻擊面。所有 iOS 和所有 Android 行動應用程式中，分別有 **±2%** 和 **±10%** 存取了不安全的雲端實例。
- 行動惡意軟體樣本總數增加了 **51%**，檢測到超過 **920,000** 個樣本

主動監控和可視性是深入了解行動裝置攻擊的關鍵。不僅要能夠識別它們，還要了解存取企業資源的端點狀況，並在被威脅者利用之前將風險因素降至最低。

完成任務後，端點防護解決方案會重新掃描裝置，以確認威脅緩解情況。如果成功的話，則允許存取公司資源；如果不成功，則繼續拒絕請求，並可能需要採取其他補救措施。

消除進階、持續性威脅

「一盎司的預防勝過一磅的治療。」

— Benjamin Franklin

了解威脅狀況代表著要認識到，雖然預防威脅遠大於應對威脅，但如果我們未能指出有時威脅會影響裝置並對網路造成影響，那就太失職了。說到 APT 背後的複雜程度，更多的是端點「何時」會受影響，而非「是否」會受到影響。能否迅速反應的關鍵在於團隊的準備程度。為此，他們應對 APT 的準備程度無疑會受到他們所使用的工具以及他們用來修復進階威脅的資料品質的影響。

這就是安全與管理的交叉點，以創建進階的程序和工作流程，從而：

- 檢測可疑行為
- 向管理員發出事件警報
- 評估威脅的入侵指標 (IoC) 或攻擊指標 (IoA)
- 分析來自多個威脅情報來源的調查結果
- 確認威脅是否為貨真價值的威脅
- 部署緩解策略
- 必要時執行補救任務
- 掃描裝置以驗證合規性

根據威脅的嚴重程度，安全性與管理之間的整合可以增強人工事件回應的流程，也可以由整合解決方案供應商自動執行。

將調查時間從幾週縮短到幾分鐘

並非所有威脅都是一樣的，最近的一些威脅和概念驗證 (PoC) 攻擊所顯示的複雜程度越來越高，這就要求事故回應團隊和威脅獵手進行更深入、更徹底的調查，以發現未知威脅的所有影響。以往，調查可能需要數週才能完成，這取決於威脅的嚴重性和複雜性。

進階的威脅需要進階的工具，以高效的方法偵測和應對行動裝置上的事件和攻擊。鑑於這些端點的「移動」的特性，事件回應必須能夠遠端執行，不僅要能發現行動裝置攻擊，還要能對行動裝置攻擊做出回應：

- 進行深入分析，識別入侵指標 (IoC)
- 建構可疑事件的時間線，顯示裝置被入侵的時間和方式
- 提出簡單明了的事件摘要，讓原先可能未被察覺的複雜型零日攻擊浮出檯面
- 利用內建工具消除 APT，同時持續監控確保威脅被摧毀

總結

彌補安全漏洞需要新一代的網路安全方法。分層全方位保護，將安全性和隱私全面擴展到基礎設施的所有裝置、使用者和資料。集管理、身分識別和安全性於一體的強大的縱深防禦解決方案



[開始使用 Jamf >](#)
或聯繫您偏好的 Jamf 經銷商