jamf

安全性 360:
年度趨勢報告

介紹

去年，我們探討了遠端辦公模式對全球企業資安態勢可能帶來的影響，許多機構在當時仍處於轉型階段，而今年的重點，則將側重在資安環境自轉型以來的變化，以及這些轉變趨勢如何以不同的手法——既有或新型威脅，攻擊您的機構。

Jamf Threat Labs 每一年都會分析影響現代辦公環境中裝置的資安威脅。在隨處辦公的浪潮不減反增的情況下，我們對現代威脅環境的認知也跟著強化，與端點合規要求趨於吻合，藉此確保資料安全，並在風險不斷升級的場域中，仍堅守使用者的隱私。

今年的報告探討了影響機構的五大安全趨勢，並以下述為前提：使用者仰賴跨平台的行動裝置，遠端存取大量託管於私人與公用資料中心的 App 與服務。

2023 年的趨勢如下：

1. **社交工程**
2. **使用者隱私**
3. **新型威脅**
4. **合規性**
5. **勞動人口分佈**

趨勢一: 社交工程仍是眾多威脅中的頭號要犯

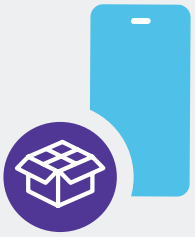
社交工程——尤其是網路釣魚攻擊，為重大資安威脅中最為迫在眉睫的類型。變動的勞動力分佈結構使得特定人口容易成為釣魚攻擊的目標對象，並藉此騙取使用者的憑證，這類攻擊又稱為「通往王國的鑰匙」，它們會給予未授權使用者存取本機上資料的權限。更糟糕的是，這類攻擊可能因此使其他系統也連帶受牽連，而這都是策劃好的一連串攻擊計畫。

社交工程最諷刺的地方在於，即使已採取符合各行業最佳做法的強大安全配置，無論再多的解決方案也難預防使用者被誘騙。若他們將自己的憑證交給攻擊者，便是任由自己的身分被他人胡亂假冒。沒有條理的內部流程更可能加劇原本的問題，許多使用者在收到看似需要緊急回覆的可疑電子郵件或簡訊時，時常無法立即取得資安人員的協助。

這些訊息通常會要求使用者採取立即回應，蓄意使他們因恐慌而點按連結以竊取其身分驗證的代號、執行專門利用設備上漏洞的惡意程式，或者拐騙他們造訪乍看合法的造假網站來騙取使用者的身分憑證——最不幸的是，當資安人員能提供協助時，通常早就為時已晚。舉例來說，**IBM 的報告就提到**，資料外洩最常見的起因為憑證遭竊或遭盜用，而且被認為需要花費最久的時間來識破，平均長達 327 天。

網路釣魚攻擊與其他類型的攻擊有很大的不同，他們不像騙取您帳號和密碼的匿名攻擊者。而詐騙可以透過不同形式來產生相同的結果，就拿人稱「邪惡雙胞胎」的攻擊類型舉例來說，這是一種經常在公共熱點 (如「免費 Wi-Fi」) 可用的地方發生的攻擊。邪惡雙胞胎會偽裝成合法的無線網路，使攻擊者在受害者不知情的情況下，有效竊取受害者傳輸的任何相關資料，若今天採用 **VPN 或零信任網路存取 (ZTNA) 解決方案**進行加密，則可以避免這種情況。

2022 年，共 31% 的機構有至少一名釣魚攻擊受害者



2022 年，有 16% 的使用者因連線到**不安全的熱點**，使得企業機密資料外洩

這兩項數據已顯示：

1. 比起以往，使用者擅自改造裝置的情況已經少了許多，而且...
2. 對企業設備的攻擊已順勢跟著強化

來源：Jamf Threat Labs

Statistica 估計，**全球目前有 4.325 億個的可用公共 Wi-Fi 熱點。**2022 年，有 16% 的使用者因連線到不安全的熱點，致使敏感資料外洩。現在假設每個不安全的熱點都只有一人使用，即便如此，加總起來也意味著一共有 4.325 億名使用者正透過不安全的網路連線來傳輸資料。

這個得出的數字，不考量任何可以專門預防使用者存取惡意釣魚連結與網域的內容過濾服務，也沒有刻意區分連線的對象是企業或個人使用者。

根據 EC-Council 的說法，他們思考的不是**如何以最完善的方式保護員工，**這類概念的措施包含像是對抗社交工程威脅、防止來自任何溝通管道的釣魚攻擊；其實最好的防禦措施之一不在於安全層面，而是人員管理層面——**提供強化資安意識的培訓。**規劃可用於入職和後續定期複習的資安培訓，讓使用者更有信心識別資安威脅和評估各種釣魚手法所涉及的風險與所需知識，並根據全球機構的資安態勢，定期更新培訓內容。

為公司相關人員提供資安培訓，是企業資安策略中不可或缺的環節，不應被忽視。這意味著導入更多不同內容的培訓，讓使用者學習資安防護的最佳作法，並介紹最有可能影響他們的新型威脅，幫助他們識別日新月異的攻擊類型，採取積極措施改善他們在生活上或辦公時，對於資安可能抱有的錯誤認知

網路釣魚攻擊十大類型：

1. **電子郵件：**
   收到聲稱來自信譽良好、值得信賴的機構的電子郵件。

2. **語音釣魚：**
   語音網路釣魚攻擊以電話作為犯罪媒介(TOAD)，通常會透過篡改電號碼來行騙，並假冒成可信的單位，比如聲稱自己來自聯邦調查局。

3. **簡訊釣魚：**
   與語音釣魚類似，只是威脅惡意人士改以簡訊的連結或附件來竊取使用者的資料。

4. **社群媒體/Angler 套件：**
   新技術催生了新的攻擊媒介，各社群平台的使用者因此成了目標對象。Angler 網路釣魚，是社群媒體攻擊類別較新的變異體，攻擊者會冒充客服人員，並使用假冒的個人帳戶來拐騙需要協助服務的客戶。

5. **魚叉式網路釣魚：**
   電子郵件網路釣魚的一種變體，採用較具針對性的做法，來攻擊機構內特定的族群，例如人資部門的員工。

6. **網路捕鯨：**
   與魚叉式網路釣魚類似，此類型的攻擊專門針對 C 字輩與管理階層。

7. **HTTP/S：**
   網站型資安攻擊，此類型攻擊的 URL 網址會透過細微拼寫錯誤來行騙，例如將 jamf.com 拼為 iamf.com。此外，申請過 SSL 的網域也在劫難逃，因為這類攻擊可以躲避現代瀏覽器中的安全檢查功能。

8. **偽造網站：**
   此類攻擊通常會與 HTTP/S 一起出現，以拼寫錯誤的 URL 冒充合法的網站，搭配上與正版網站高度相似的文本、logo、配色、功能，讓網站的外觀和觀感乍看之下與正版網站極為類似。

9. **水坑攻擊：**
   既帶有策略性，又具備魚叉式網路釣魚的特性，水坑攻擊的對象通常是特定的族群和這個族群經常造訪的網站。攻擊者會利用惡意軟體感染這些網站，等到目標對象造訪時，便會跟著連帶被感染。

10. **彈出式視窗：**
    與昔日的彈出式廣告一樣，這類型的網路釣魚變體會在惡意人士以惡意軟體感染網站後，接著若使用者誤觸嵌入式廣告或較新的通知提示時，他們就會在承載資料傳輸後被感染。

趨勢二: 使用者隱私在資安討論中, 佔有一席之地

而像 Apple 和 Jamf 這樣的廠商和開發商，早在很久前就開始極力宣傳隱私權的重要性。一般來說，他牌廠商重視隱私保護的程度，通常比不上對自家硬體和軟體的其他資安功能那般重視。

就像個資和企業資料外洩的後果一樣，使用者隱私若遭到侵犯，可能會有許多不堪設想的後果。未經授權便蒐集使用者的個資，帶來的傷害極為深遠，在其他方面也將有相應的代價：

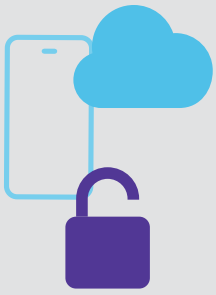
- 國家可能會透過惡意程式碼監視使用者的一舉一動，如攝影機的麥克風或受害者設備上的鍵盤側錄器
- 惡意人士將有機可乘，利用這些資料謀取個人或經濟利益，擴大社交工程活動和敲詐受害者
- 企業在未經使用者同意的情況下，向廣告商和/或第三方合作夥伴出售使用者個資來中飽私囊

還有其他案例是機構雖可合法蒐集使用者個資，但卻因為沒有足夠完善的保護措施，而受外部攻擊、機構內部促成的威脅或監管督察影響，使自己陷入危機。還有一些情形，是**機構絲毫未察覺自己正面臨資安威脅**，光是「 2022 年共有 5% 機構的裝置上裝有垃圾 App」這項數據就足以證明這一點。

5% 看似傷害不大，但在評估風險時，可不能只看數字。還必須考慮以下幾點：

- 找出攻擊者目標的資產
- 任何出現過的攻擊手法
- 可能的攻擊類型
- 發生攻擊的可能性
- 如果成功入侵資料或使資料外流，可能帶來的影響

從本質上來看，機構需綜觀這些項目，才有能力正確評估風險以及了解資安問題對長久營運可能帶來的影響。那麼，這套公式也可以套用在個資保護嗎？



「2022 年，有 0.4% 的 Android 裝置上被發現裝有 PUA，而 iOS 裝置的這一比例僅 0.1%。」

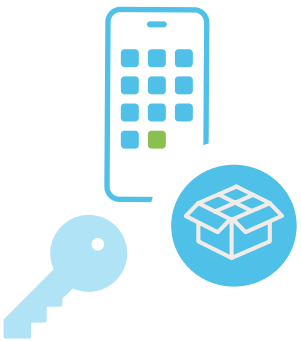
Android 是一個開放的生態系統，會產生風險更高的 App。Apple 則建立了一個精心打造的 App 生態系統，更嚴謹的使用者隱私保護能力，使得這些不安全的 App 可以進一步被限制。

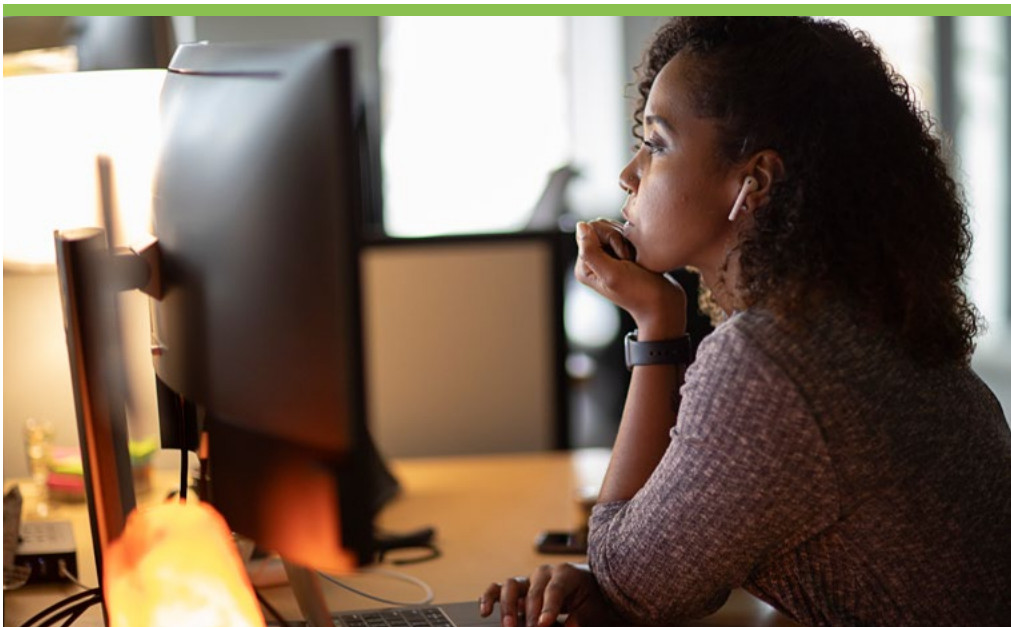
我們不容低估最後一點，因為評估事發後的影響與合規監管、降低風險的運作、預防違反資料外洩的監管法規，都有直接的關聯 (本報告稍後將詳細解說合規遵循性)。

有效的隱私管控逐漸也與安全性管控同等重要——除了在需要時實施合規標準，也需要在資安策略中納入限制揭露個資的方法。這些概念必須傳達至機構上上下下的解決方案、程序、相關人士、工作流程，並建構一套資料防護機制，在企業內部建立或導入所有所需元素，而不是事發後才開始找解決方法。

裝置管理解決方案能幫助機構將內部策略與法規要求維持一致，藉由派發 App 的功能，IT 人員的管理負擔也能進一步減輕，確保無論設備類型或位置何在，任何類型的資料都能在整個基礎架構中受到保護。

我們的裝置管理方案可支援各種所有權模式，讓企業在確保 App 與資料安全、套用安全配置以確保安全存取內部資源之間，取得了平衡，最終可讓使用者自行管控私有 App 與裝置用量上的相關個資。公司內部的專有數據通常敏感且高機密，在需要對使用者個資保持「不干涉」的原則之下，**我們讓使用者自行決定個資開放的程度，以此強化整體隱私保護力**，且不論使用者的設備為自備裝置 (BYOD) 或自選裝置 (CYOD)/公司配發 (COPE) 方案或者混合上述模式。





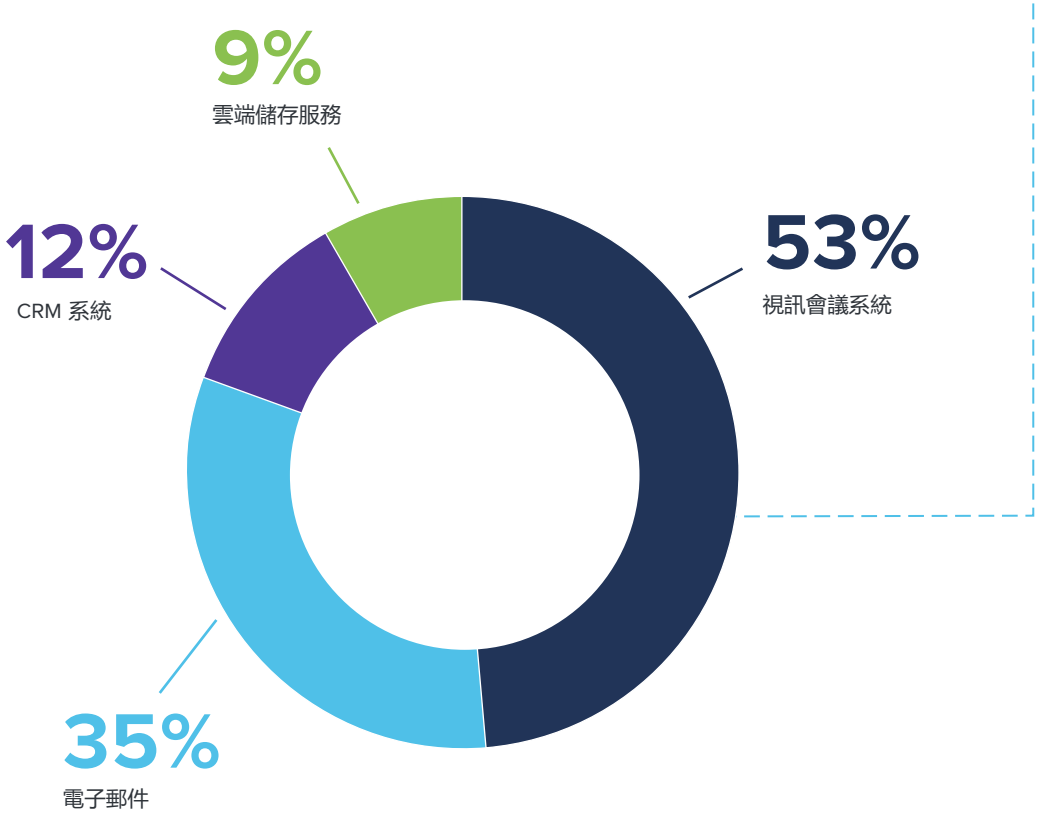
趨勢三: 惡意人士綜合各式攻擊所設計的新型威脅

有關 macOS 惡意軟體方面的一些好消息，惡意軟體感染總數與前一年相比沒有增長的跡象。更棒的是，2022 年根據 AV-Atlas 對惡意程式和可能有害應用程式 (PUA) 的統計數量來看，**新型惡意軟體**的數量從 1.5 億多，下降到約 1 億次。

惡意的網路流量，如網路型入侵指標 (IoC) 日漸普遍，可在設備和網路伺服器之間的規律溝通中發現，且通常只能在生產環境中找到，無法透過簡單評估靜態程式碼來識別。這也就凸顯了主動監控端點健康度，在評估綜合風險因素時的重要性。

混搭各式攻擊並不新奇，不過在現代威脅態勢下，眼見越來越多惡意人士利用組合型威脅，以新的方式瞄準特定類型的員工，未經授權就取得機構服務和資源。2022 年的某個月內，就有 53% 的設備駭入機構的會議系統、35% 駭入信箱、12% 駭入客戶管理系統 (CRM)、9% 駭入雲端儲存服務。

2022 年的某個月內，就有 **53% 的設備駭入機構的會議系統、35% 駭入信箱、12% 駭入客戶管理系統 (CRM)、9% 駭入雲端儲存服務**



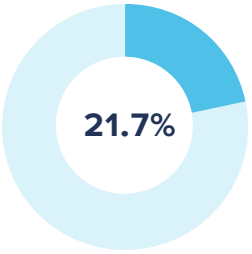
複雜型攻擊示例

一名員工收到看似來自同事的魚叉式網路釣魚信件。信內含有一個宣稱是「工作文件」的連結，點按後會在使用者裝置上安裝惡意程式碼，來蒐集使用者的憑證、傳輸勒索軟體承載資料。在贖回敏感資料時，攻擊者透過憑證便能擴大對企業基礎結構的存取範圍。最後，惡意程式碼的另外兩個功能：它會感染端點設備，使裝置成為殭屍網路的一員後用於攻擊其他機構，同時尋找其他可以感染的設備，殭屍網路隨後就開始不斷擴大。

重點在於，攻擊採取的可能不只一種形式，發生的時間不定，並且經常在未被偵測到的情況下發生。有些攻擊鏈會在入侵後立即發生，如勒索軟體，而其他類型像是透過分散式阻斷服務 (DDoS) 攻擊來建構殭屍網路，則更具策略性，因此花費的時間較長。

這樣的組合型攻擊很難預防，因為受害者不到下一波攻擊開始前，通常都渾然不知攻擊的程度與範圍。儘管如此，還是有些方法可以降低風險，並嚴格限制或減緩對受害者的影響。主動監測端點設備並蒐集有關裝置運行狀況的遙測數據，對管理人員來說至關重要，因為這些資料可提供深入的見解以及各方面 (如修補程式等級) 表現的分析，特別是當可疑行為已明顯指出設備正遭受威脅，但終端使用者卻毫無察覺時。

當我們提到修補程式管理，App 生命週期管理在降低系統漏洞風險，同時又要確保採用最安全的資安機制防範已知威脅時，只是最低要求。我們注意到，第三方 App 商店經常提供正當 App 但更新版本卻含有惡意程式碼，藉此感染使用者的設備，在這種情況下，達成最低要求就更顯得格外重要。其中一個例子就是原為付費的 App，出現了免費版本來誘騙受害者。



21.7% 的 Android 裝置造訪了第三方 App 商店，而 iOS 裝置的這一比例僅 **0.002%**

本該用來保護裝置和使用者的 App 審核流程，經常因採用第三方 App 商店，而遭到破壞

2022 年，**0.02%** 的 Android 裝置遭破解 Root 權限，但是僅 **0.001%** 成功**越獄 iOS 裝置**

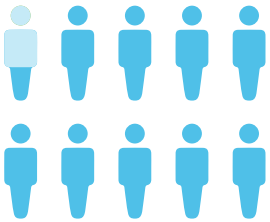
儘管兩個比例皆非常微小，但值得注意的是，受影響的 Android 裝置數量是 Apple 裝置的兩倍。如果想一想世界上 Android 和 Apple 裝置的抽象數量，那麼其實際規模不難想像。

有些作業系統可允許側載 App，但像是 iOS 這類的作業系統，須先經過越獄才能破壞保護 iOS 裝置、抵禦未簽署程式碼的保護層。鎖定設備只是其中一種措施，實際上更需要有即時識別越獄設備的能力，才能有效修復威脅事件。

針對供應鏈的攻擊

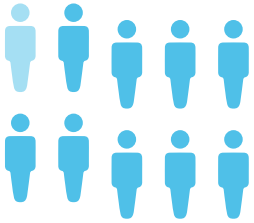
從過去的紀錄來看，**供應鏈或第三方廠商**遇上的攻擊在尚未達成**真正的目標**前，便已深入影響機構的許多層面，後續的影響更是深遠，儘管資安防護力有強有弱，影響範圍依然可擴及全球企業。

要預防這些攻擊並非容易事，主要是因為機構本身也缺乏有效要求供應鏈上每個廠商 (或其承包商) 降低風險的方法。不幸的是，若想保護自家機構遠離資安威脅，也差不多會遇到同樣的問題。但正如美國網路安全暨基礎設施安全局 (CISA) 和美國國家標準與技術研究院 (NIST) 在**《Defending Against Software Supply Chain Attacks》**中所述的一樣，「強化並緩解機構預防與回應此類攻擊的能力」的一個關鍵要素，便是遵循產業的最佳做法，將它納入機構的資安策略，其中還須透過獨立的第三方稽核廠商來驗證您的合作夥伴 (隨後合作夥伴的廠商也接續被規範)，確保在攻擊發生之前，已採取適當的緩解措施。



2022 年，有 **0.004%** 的使用者和 **0.3%** 的機構所使用的裝置遭到**越獄**或破解其 **Root 權限**

去年的統計數據：



2021 年，**只有不到 1%** 的機構使用的裝置遭到**越獄**或破解其 **Root 權限**

趨勢四: 安全技術堆棧應確保遵循法規

增長趨勢與機構內部的資料安全，構成了使用者隱私的重要性。此現象在合規方面最為普遍，尤其是州、聯邦和地區性的法規。不妨想想《一般資料保護規則》(GDPR) 和《加州消費者隱私保護法》(CCPA) 如何從國家與州的層面上，在使用者隱私保護方面取得更大進展，或是全球監管最嚴謹的行業之一——金融科技，如何各個方面都受到規範。

下列幾個例子，演示了各個監管法如何在各行業達成合規，不論是作為獨立法條或是與其他法條合併作用：

2002 年的《沙賓法案》(SOX)：規範了會計業務的具體條款

《金融服務業現代化法》(GLB)：解決了維護資訊安全所需的最低網路安全保護標準

金融業監管局 (FINRA)：明確列出證券業中公平和誠實的營運，確保投資者受到保障

由於法規影響的是特定產業的公司及其在全球的影響力，這使得受影響的機構可能需遵守超出其能力範圍的法規，進而使機構發現自己需要對工作流程掌握更大的控制權，以維持隱私保護能力和管理受保護的資料類型——如個人識別資訊 (PII) 、受保護的健康資訊 (PHI) 和商業情報資訊 (BII)——確保這些資料確實有按照使用者的意願和/或法規進行蒐集、處理、儲存、修改、共用、銷毀。

合規遵循是一項艱鉅的任務，需要好好斟酌、管理和提供支援，即便您的裝置和資料是交由機構來管理。但是，針對人員四散在各處辦公，需要能夠隨時、隨地、隨裝置來存取內部資源的模式，又該如何確保遵循合規規範呢？地端部署加上遠端/混合辦公的勞動力，這樣分外複雜的模式，可能是有合規要求並正在應對現代威脅環境的機構的一大痛點。

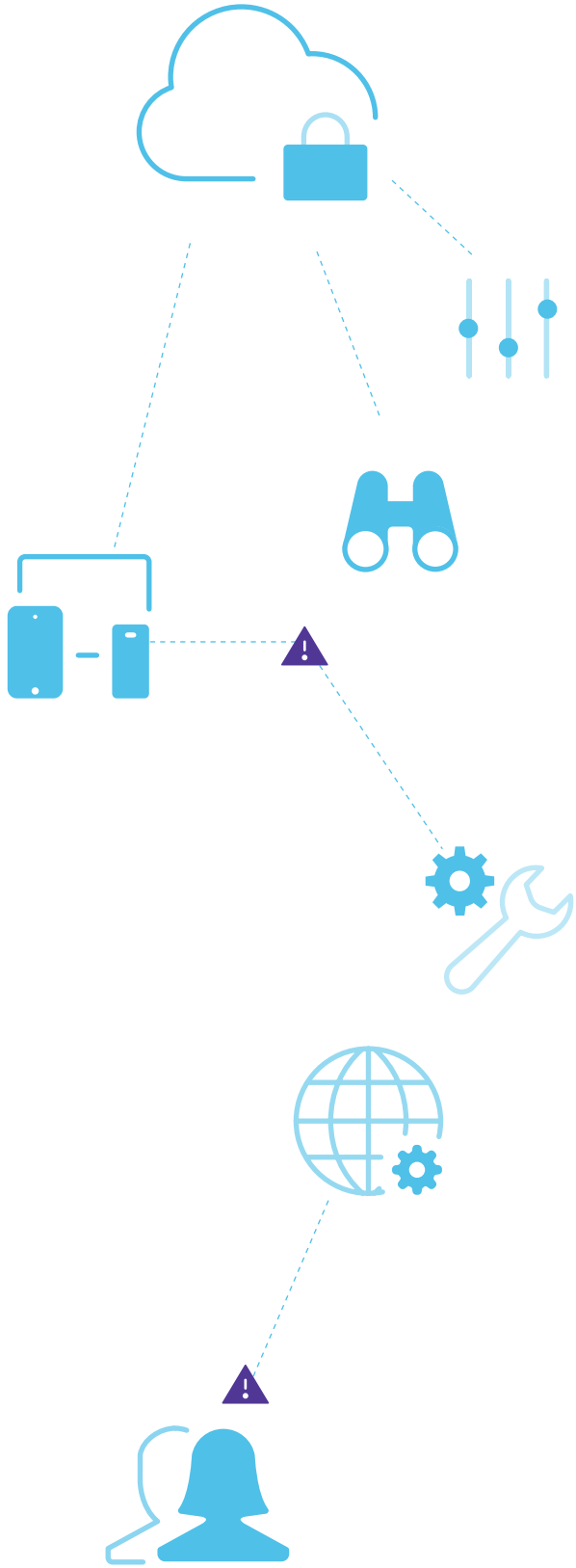
2022 年，有 21% 的員工因為使用**配置錯誤**的設備，而遭逢**資安風險**

不幸的是，若將自備裝置模式添加到組合中，合規這淌水只會變得更加渾雜。2022 年時，就有 21% 的員工因為使用配置錯誤的設備，而遭逢資安風險，講直白一些，還可能使敏感、機密、關鍵型，甚至是受監管的資料面臨流出的風險，若因此發生了違規的問題，則可能致使機構，乃至於使用者需承擔民事和/或刑事責任。

雖然許多機構已實施了某種形式的 BYOD 或員工自選裝置方案，讓終端使用者選擇他們認為最高效和最舒適的裝置類型和作業系統，但有效的合規管理解決方案不能只有鎖定所有設備 (受監管裝置除外)。**我們發現有 8% 的使用者和 21% 的機構因配置的安全漏洞而受到影響**，這意味著即使裝置為企業所有或受監管，仍會受到影響。因此，機構所選用的解決方案，必須要能夠兼具管理與資安雙重能力。

事實上，任何端點設備隨時都有可能遺漏修補程式，或因為各式漏洞而導致資料外流、丟失或被盜。不論是哪種情況，都需要採取不同的措施來降低風險。有些情況可以透過自動回應和修復工作流程來處理，但是不管怎麼樣都還是會有需要手動修復的地方。

與大多數的資安討論相同，沒有任何解決方案可以一體適用，也沒有萬靈丹可以讓所有基礎設施永保合規。我們建議實施深度資安防禦策略，提供多種綜合型解決方案，滿足您各式的合規要求。



趨勢五: 保護遠端/混合辦公環境中的資料仍具備一定的挑戰性

遠距勞動力的趨勢也同時引進保護使用者、資料和設備方式的轉變。由於網路安全邊界被成功攻破，地端解決方案改以雲端服務取而代之，確保提供使用者不限地點，也不限裝置的安全性服務。最終的結論便落在一個功能性更強、更完整的端點防護解決方案，同時還具備更高的靈活度與提供更強大的 App 安全。

然而，儘管有了上述的優勢，許多機構在遷移後的幾年，仍面臨遠端與混合辦公環境中資料安全的難題。可惜的是，事發肇因並非因單一個問題所引起，而是眾多的問題導致資料保護的能力不足。其中，有些問題緣於缺乏：

- 即時透視端點的運行狀況
- 兼具管理與資安能力的工具
- 自動化步驟與工作流程
- 分散式日誌紀錄與威脅情報
- 實施政策與合規要求
- 使用者資安教育訓練
- 一流的解決方案
- 對資產與威脅風險的評估

舉例來說，我們發現 **64% 的安全性薄弱裝置存取了協作工具，存取企業郵箱的則佔了 34%。**這代表雖然風險與入侵指標偏向主觀，對各家企業有所差異，但也不是所有的裝置都會執行修補程式管理這類的常規任務，這使得裝置本身與機構內部資源處於風險之中，影像層面甚至遠超過 App 和配置設定。Jamf Threat Labs 發現，**每五台裝置中就有一台未升級至最新作業系統。**為確保使用者與機構皆安全無虞，深層的資安防護策略應從作業系統層面做起，且必須遍及所有層面。

這進一步促進現實世界中透視設備資安可見度的需求，以及這些資料如何與機構的基礎設施相互溝通，若您的行業屬於受監管的類別時，這些功能又顯得尤其重要。考慮到多數的監管單位會要求機構透過定期稽核來證明其合規性，監管單位便希望能驗證受保護的資料和與之溝通的端點設備是否符合監管標準，因此，有了這項功能，將可滿足合規的需求。

但是，評估設備資產、機構所面臨的資安威脅、用來識別受影響端點設備的遙測數據，這些都只是解決方案的一部分而已。若要降低風險並給予即時的存取權限，我們需要現代化的解決方案。用於保護遠端連線的傳統 VPN 技術，當然不比旨在應對隨處辦公和現代威脅環境挑戰的新型技術。 零信任網路存取 (ZTNA) 要求設備與使用者皆須經過驗證，並符合最低的健康度要求後，才可連線至所請求存取的 App 和服務。

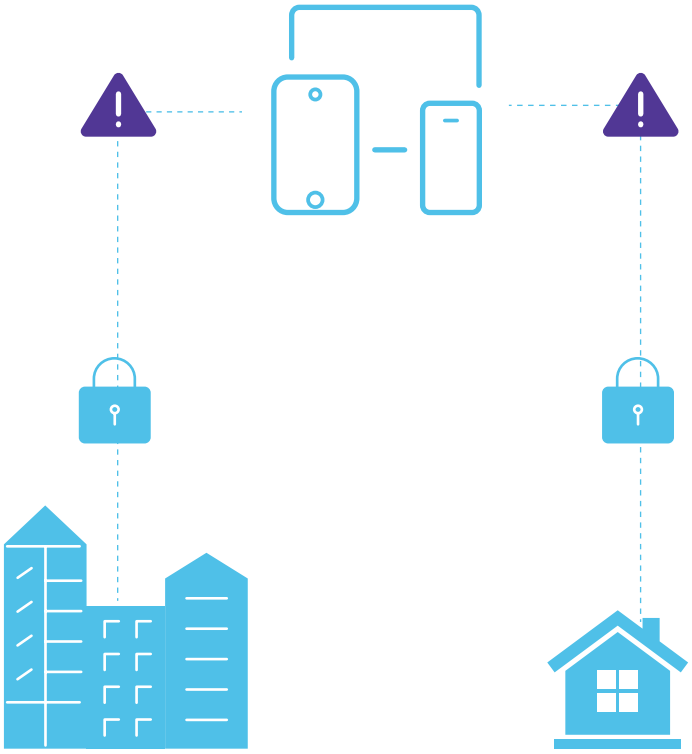
ZTNA 解決方案在設計時已考量到現代網路與工作流程，可降低風險並維護資料安全，同時又具備足夠的靈活性，可確保個人資料和 App 的隱私性。此外，授權的使用者會按照最小許可權原則，連線至他們被授權存取的 App，再將所有企業流量導至微型通道，當單個使用者的身分遭駭時，攻擊者也無法存取所有該使用者有權存取的 App。透過內建的分流技術，可防止攻擊者在整個網路上執行橫向移動，藉此有效限制威脅。

另一個亮點是運用 API 將遙測與裝置健康度等數據分享至解決方案，使該方案能保護設備、使用者、敏感資料，阻擋威脅不讓惡意人士得逞。這與附加型或無整合能力的解決方案形成鮮明對比，後者為可獨立運作的現成資安系統，但缺乏驅動深層完善防護的整合能力。

隨著惡意人士使用的工具不斷推陳出新，機構也必須利用其解決方案來防止已知攻擊，並降低新型攻擊的風險。威脅搜捕能力為因應新型威脅，在機構內持續成長與改良，使資安團隊在未知和新穎的威脅造成資料外流前便能夠早早識別、緩解並修復它們。人工智慧 (AI) 與機器學習 (ML) 技術早在數個產業中顯現成效，網路安全就是其中之一，因為越來越多的解決方案會運用擴大的處理能力和行為分析功能來學習、有效預測、應對威脅人士及其發動的攻擊，而這樣的速度是人類管理人員完全無法比擬的。

依據行動裝置管理 (MDM) 平台來制定策略，便可確保使用者的自備裝置與公司所有的裝置皆安全無虞，並使修補程式維持在最新版本。部署端點防護機制來防止惡意軟體，同時透過主動監測端點設備來蒐集豐富的遙測數據。API 則是這兩個解決方案之間，安全分享威脅情報資料的好方法，它還能使機構透過政策實施，來維持合規要求。身分驗證與存取解決方案可讓您集中管理憑證、機構內部資源的存取權限佈建，同時還多了多重要素驗證 (MFA) 功能來確保存取的安全。

這些若與現代化的資安解決方案 (如 ZTNA) 加以整合，便能保護任何網路上的連線、結合 ML 來搜捕新型威脅、在攻擊發生之前便加以阻止，並將傳統型 VPN 替換為現代化的解決方案，將存取請求分流以緩解網路型威脅。最後，即時蒐集所有有關威脅和設備健康度的運行資料，全面自動化裝置生命週期管理。



建議事項

隨著我們邁入全球疫情促使工作環境發生巨大轉變的第三年以來，許多人關注的項目早已從**「該如何確保業務正常運行？」**到**「我們如何持續確保遠距人員和內部資源維持安全？」**

Splunk 的**《The State of Security 2023》(2023 年的資安現狀)**報告指出，這樣思維上轉變的關鍵原因之一，就是儘管遠距辦公早已實行多年，但現今 (46%) 資安團隊需支援的使用者數量竟是疫情前的兩倍多 (21%)。Splunk 的全球研究報告更指出「攻擊數量不僅日漸增加，實際導致資料外流的事件也跟著增加。」

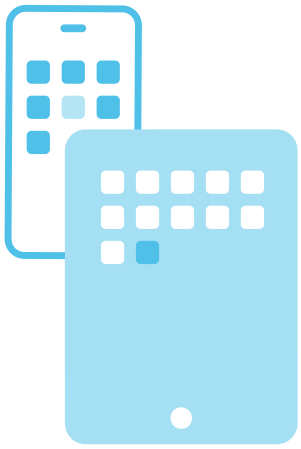
日益增加的攻擊數量與日新月異的威脅環境，還有確保遠距人員安全存取資源的需求不斷增長，這些都在在凸顯我們在去年的安全性 360 報告中提及的要點：

安全的遠端存取方案需足夠靈活與高效，才能確保實現、不阻礙或妨礙使用者的生產力

今年，我們想強調的重點為：

端點防護機制需匯集多種資安方案，透過 ML 這樣先進的技術，建置強大的基礎、取得資安高可見度，來發展自動化的安全工作流程，確保符合機構規範與產業法規

我們的結論是，機構應制定現代化的雲端型深層資安防禦策略，才能確保滿足自家的特殊需求並為明日的需求未雨綢繆，提供可擴充性。



關於本研究

我們的目標旨在識別混合辦公模式中可能出現的最大資安趨勢。本研究中所採用的資料和統計數據，是我們在 12 個月內對受 Jamf 保護的 50 萬台樣本的資安趨勢所進行分析的結果，包含了橫跨 90 個國家/地區的 iOS、macOS、iPadOS、Android 和 Windows 裝置。此分析於 2022 年的第四季度期間執行。本研究中採用的詮釋資料來自大量匯集而成的日誌，不含任何個人或機構辨別的資訊。我們進行此分析的目的並非引起恐慌，而是希望能向您和您的使用者傳達可用的選項，以及保護設備、使用者和機構內部資料等各個資安方面的最佳做法。