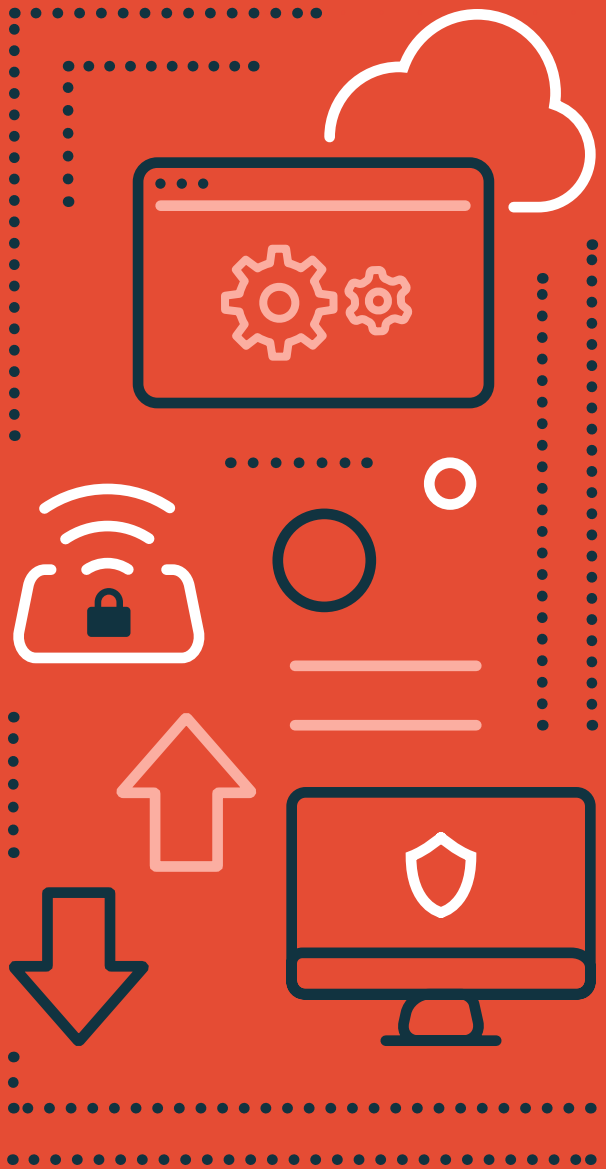


零信任網路存取

入門

jamf

第一次聽說零信任網路存取嗎？別擔心

根據 **Gartner 研究機構**，零信任網路存取 (ZTNA) **這項產品或服務可圍繞一個或一組 App 來建立身分與情境型且符合邏輯的存取邊界**。

白話一點的說，ZTNA 可說是新一代的虛擬私人網路 (VPN) 技術。有別於可追溯至 1996 年，依據點對點隧道協議 (PPTP) 所建立的 VPN，**Jamf Connect 的 ZTNA 解決方案在設計時便已考量到現代運算，結合了身分型資安模型、風險感知政策管理與 App 型微型通道三大功能**。這意味著此技術將進一步限制使用者有權存取的資源，將這些限制與雲端型基礎架構結合，如此一來不只可以簡化管理流程，而且在需要擴展時只需點按兩下，全程無需維護任何硬體設備。

繼續閱讀以獲得相關基礎知識：

- Jamf 的 ZTNA 是如何運作的
- 有哪些內建的安全性功能
- 為什麼你可能會需要驗證網路身分與維護安全性的新方法

而你，又該如何踏出第一步呢？

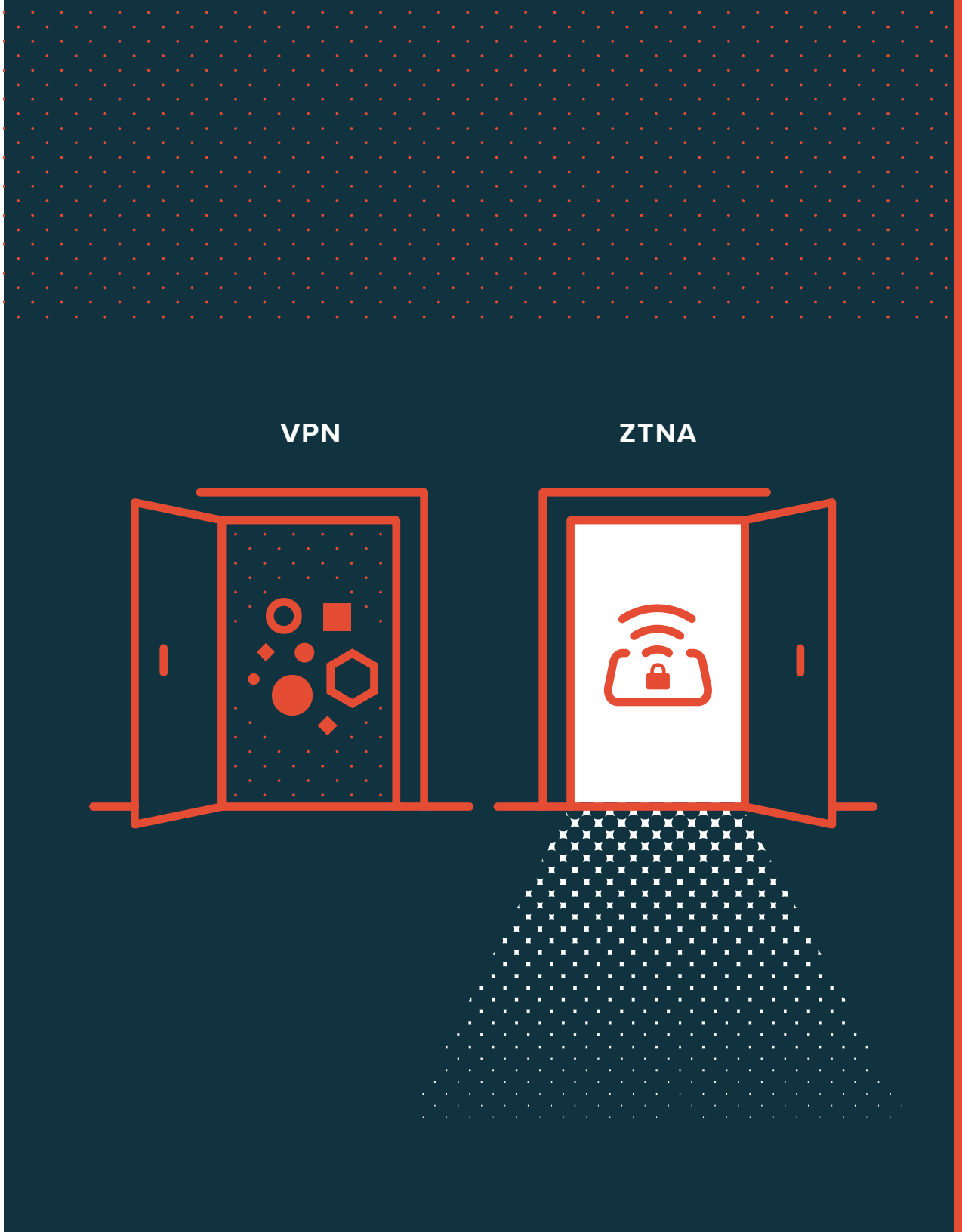
「這個世代，誰都不能信。」

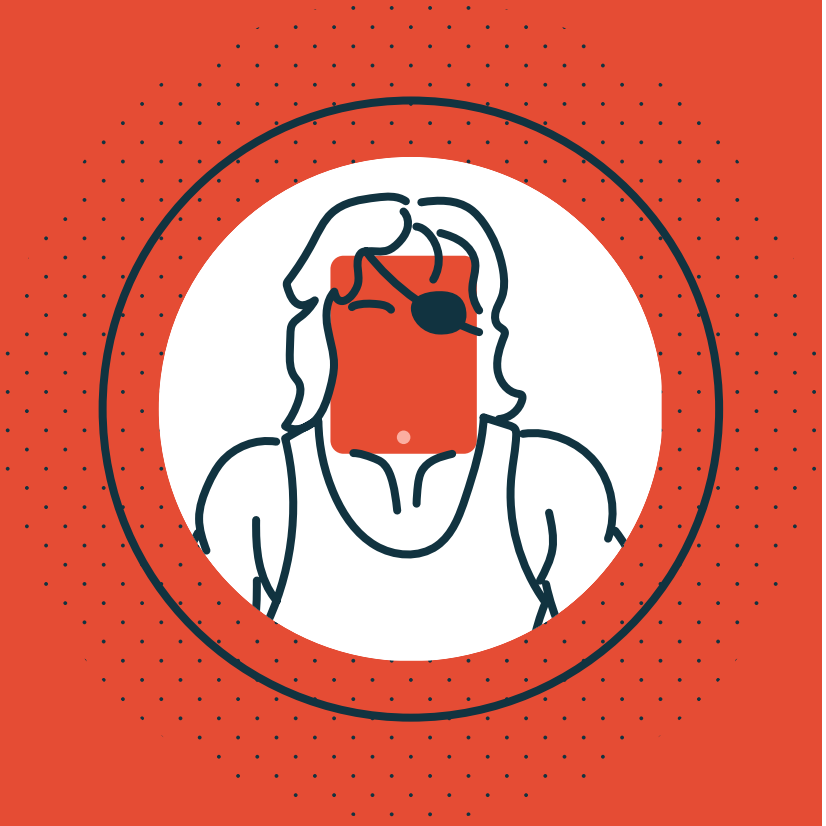
Kurt Russell 飾演的 R.J. MacReady 在電影《突變第三型》中，隨著劇情的發展和問題不斷堆積下而變得越來越不信任他的夥伴。從精神層面來看，MacReady 的想法與 ZTNA 共通，因為這個技術採取了最小權限原則的安全性配置，並圍繞「永不信任，一律驗證」這個概念。

透過實施最小權限原則與即時檢視裝置狀態，**這個技術只會將雲端存取權依 App 給予使用獨特憑證的已授權特定使用者**。

也就是說，使用者在裝置上驗證自己的雲端身分憑證後，企業連線便可獲得保障，其餘非企業用的 App 則將透過分流技術直接路由至網際網路，進而達成保護終端使用者隱私並最佳化網路基礎架構的目標。此外，這個做法還能改善底層網路，提升建立連線或微型通道的效率。運用微型通道技術，已批准的使用者身分、裝置、App 便可獲得端到端的保護。只要有任何一項存取條件未妥當配置 (如個人設備)，那麼無論是否輸入正確的憑證，都將無法存取企業資源。

有別於整體授予存取許可權的舊式 VPN 技術，ZTNA 不會給予整個資源網路的存取許可，因此這樣更為細緻的方法只會在使用者有需要時批准他們存取所需的內容，以此強化安全性。以專屬政策強化機構的資安防護力不僅可以達成合規要求，更可以更完善的方法保護終端使用者、公司設備與資料。





「你的規則開始有點煩人了。」

如同《紐約大逃亡》裡演出的對立局面一樣，惡名昭彰的 Snake Plissken 在法律限制 (為了維持和平與秩序而制定) 與被賦予自由的公民之間陷入困境時說出的對白，如今的 IT 團隊似乎也面臨類似的困境：

在提供使用者必要資源與資料存取權的同時，機構如何也確保兼顧資安防護？

這正是 Jamf 所提供的服務。

Jamf 採用了依據 App 與身分為中心的政策，既能提高工作效率，又能消除使用者原本可大量但不應存取的 App 與資料，確保導入統一的存取政策，並在資料中心、多個雲端基礎架構、SaaS App 以及所有現代作業系統 (OS) 和管理範例中都能維持持一致。

套用各種可強化機構安全性的風險感知存取政策極其重要，而達成這項目標的方法是透過：

- 避免不必要的資源存取
- 對設備執行定期檢查以評估運行狀況
- 主動識別可能遭到入侵，或對安全存取資源構成高風險的設備

「大家別緊張，我在這呢。」

以穩固的雲端基礎架構作為開始，使用 Jamf 技術完全無需管理硬體、無需維護支援合同，也不需安裝和/或配置複雜的軟體。

我們也別忘了，雲端的集中式、高度可擴展和即時啟動的特性意味著，在你的設備註冊至服務的那一刻起，資料就會受到保護——無論你有多少台設備，也不管它們實際上位於地球的哪一個角落，所有這些只需要連上網路就能達成。

就像《妖魔大鬧唐人街》中惹人喜愛但又有些冷漠的 Jack Burton 一樣，支援 Jamf 技術的雲端與擴展整合功能日以繼夜繁忙地運作，並透過以下方式保護端點設備：

- 加密連線
- 監測裝置運行狀況
- 部署自動化工作流程以修復偵測到的問題
- 強化裝置性能
- 確保資料與終端使用者的安全

JAMF 的運作原理

直白的說：Jamf 沒有更勤奮，只是改以更聰明的方式運作。

一個對 ZTNA 架構至關重要的整合功能，是能夠透過你偏好的**雲端身分廠商 (IdP) 以單一登入 (SSO) 啟用使用者身分驗證** 。
藉此不僅能消除管理使用者和/或裝置憑證的麻煩，也不再需要維護自己的專用憑證頒發機構 (CA)，更不需要在遠距或混合辦公環境中設置原先這類資安機制所需要的網路邊界。

這也使得管理人員可有效利用每部裝置的網路連線、與雲端的連線能力，來「更聰明而不是更勤奮地工作」。畢竟，開銷減少便意味著效率提升，而這從來都不是一件壞事。提到開銷減少，Jamf Private Connect 代理程式不僅為你的裝置、使用者和資料提供了最高級別的保護能力，而且還確保在此過程中盡可能運用最少的資源。

Jamf 可原生支援 Okta 與 Azure，但也可透過 Azure 同盟處理程序支援其他 IdP 大廠，如 Google、Ping 等

安全性功能：

身分型資安模型

只允予授權使用者連線至企業 App，並確保資料中心、雲端與 Saas App 所實施的政策是一致的。

App 式微型隧道

僅允許將使用者連線至他們有權存取的 App。微型通道採最小權限存取原則，並可防止橫向網路移動 (資安漏洞的常見類型)。

現代雲端基礎架構

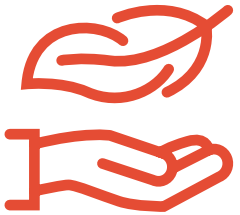
無需管理任何硬體、續訂支援合約或配置複雜的軟體，甚至無需對設備進行管理控制即可實現安全存取。

可與身分服務整合

透過 SSO 啟用使用者身分驗證並省去管理憑證的需求。

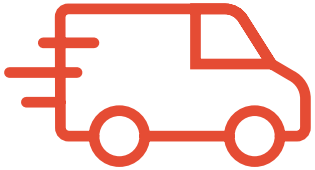
風險感知存取政策

透過防止可能造成入侵的使用者與裝置，來強化安全性。



輕量級 App

在 App 需要連線時自動建立通道，並在發生中斷時即刻重新連線。



快速高效的連線能力

以可避免被入侵的方式存取企業 App，並且不影響電池續航力，只會在後台安靜執行，不會干擾使用者體驗。

智慧分流技術

確保企業連線的安全，非企業類 App 則能夠直接路由至網際網路，進而保障終端使用者的隱私並優化網路基礎架構。

統一存取政策

橫跨所有託管位置 (地端、私有雲、公共雲及軟體 App) 以及所有現代作業系統與管理架構。

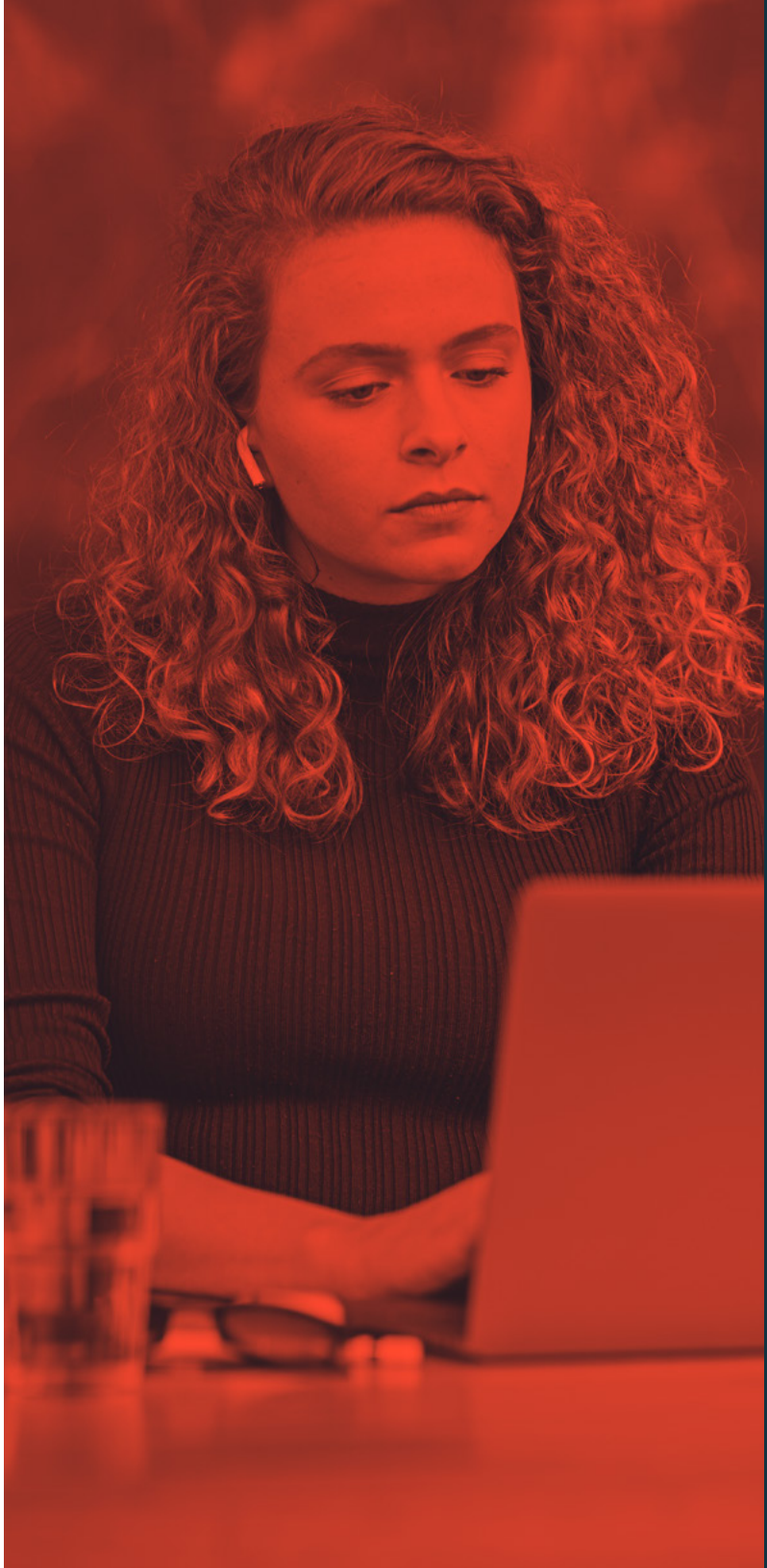
為什麼你該捨棄 VPN 並迎接 ZTNA

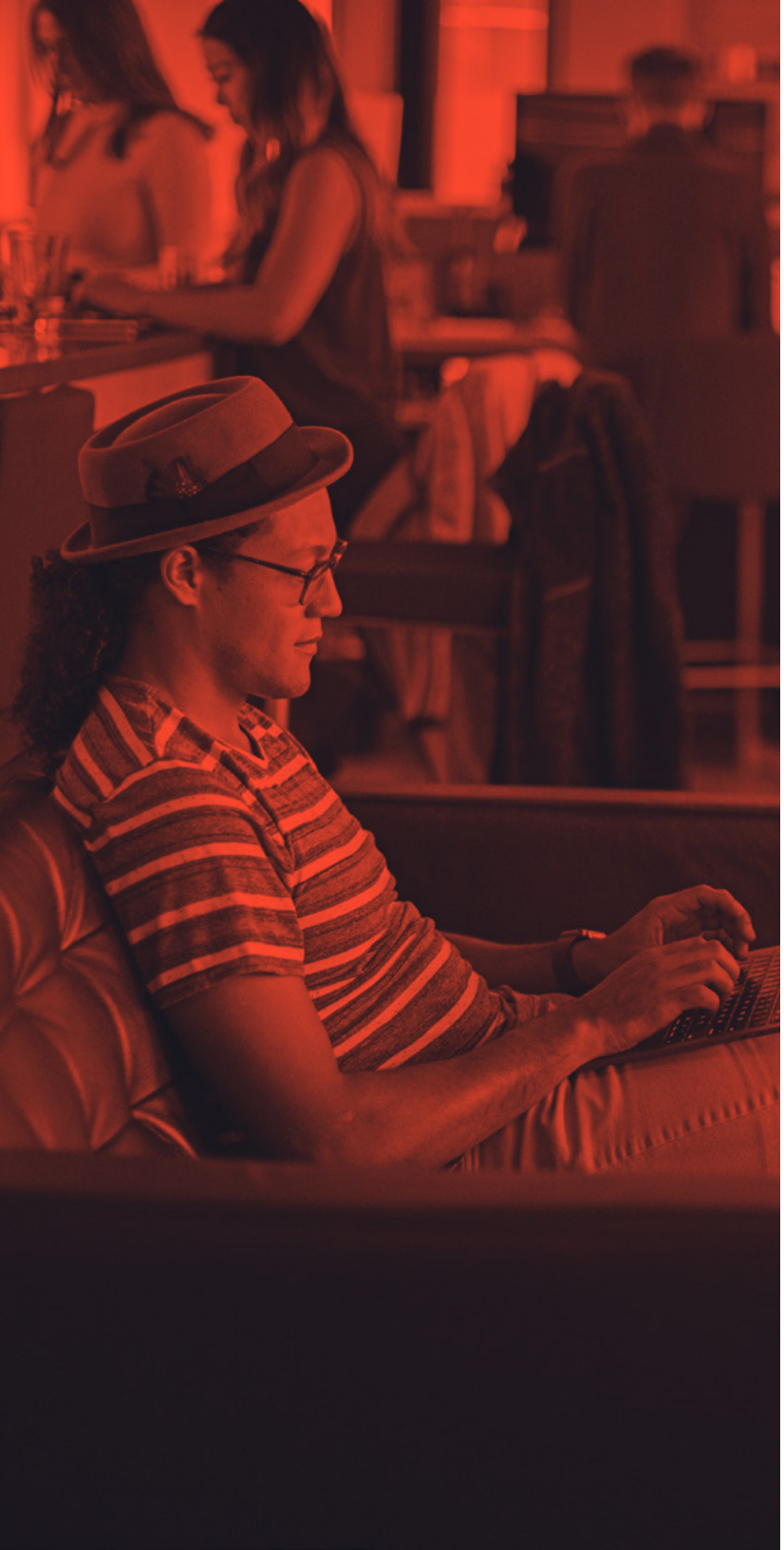
即使 VPN 可以解決你所有的安全性風險，仍會存在一個風險：使用者必須實際連接到 VPN。很多時候不情願，或者只是單純缺乏如何連接到 VPN 的知識，可能就會使機構資料面臨風險，因為這時還尚未進入網路安全邊界。

若使用 ZTNA，使用者便完全不需擔心何時或是如何才能存取安全的網站，他們只需登入設備，馬上就可以存取受保護的資料。在後台，ZTNA 確保使用者已經過身分驗證及授權，而且只要是受信任的設備就可以直接存取資料。ZTNA 可有效推動機構以正確方法保護自家資料，同時確保使用者仍可以輕鬆存取這些資源。

因為使用者忘記如何啟用 VPN，迫使資料面臨潛在風險的日子已成過去式。

無論使用者正在使用哪種裝置或作業系統，當 App 需要連線與重新連線時，ZTNA 都會自動建立微型通道，就像在會話結束或服務中斷時一樣容易。Jamf 不會佔用寶貴的硬體資源，也不會在不使用時耗用電池電量。





我們會像哨兵一樣隨時就緒，等待請求存取受保護資料的 App、使用者或服務才會採取行動。在保護資源之餘，也能確保維持順暢的使用者體驗，又能消除使用者原本可大量但不應存取的 App 與資料，提供雲端型的軟體定義邊界 (SDP)，以保護資料在各個 App 獨立連線上傳輸中的安全。

當 Jamf Connect 與 Apple 的「私密轉送」(iCloud 的訂閱服務，可透過隱藏個人 IP 位址和位置來保護個人隱私) 一起使用時，便可以安全存取企業 App，而不會面臨傳統企業 VPN 連線的性能、隱私和安全性挑戰。

這樣的組合可確保使用者無論是進行私人或工作上的瀏覽，都能受到保護。個人裝置也可以透過 Jamf 來部署、保護和管理工作時需要的企業流量；私人的瀏覽內容則會透過 iCloud 的「私密轉送」服務進行路由來維持隱私。Jamf Connect 與 iCloud+ 的「私密轉送」並用，是保護隱私和確保安全性的最佳作法，而且不會因此影響性能或使用者體驗。

下一步該怎麼做？

首先，改以現代化的資安辦法來保護你的遠距或混合辦公環境中的裝置、使用者與資料：Jamf 的身分型資安模型會執行最小權限原則，而你也可以：

- 執行設備運行狀況檢查
- 根據風險感知政策自動執行修復工作流程，以提升網路設備的資安防護力
- 可透過一站式的控制台完成所有操作，而不會影響直覺好操作的使用者體驗

不妨免費試用來探索這套機制的可能性，或者你也可以聯繫你偏好的經銷商來開始。

預約試用