

最佳做法：

ZTNA

零信任網路存取



下列 ZTNA 的最佳做法原則
應當每次都為諸事中的首要任務：

- 給予存取權時，應秉持最小權限原則
- 使用多重要素驗證 (MFA) 和雲端身分供應商 (IdP) 來驗證身分
- 設立合規要求以管理和保護使用者、設備及其他
- 永不信任，一律驗證，即使在初始造訪之後也應該持續驗證

如果您剛開始使用新型身分驗證與存取，請繼續閱讀來了解如何為此方法決定策略走向。

假設您現在要去銀行提款。您可透過身分證和銀行帳號驗證為本人，接著若您的大名顯示在某個帳戶上，則有權查看該帳戶。現在想像一下：您交出身分證後，出納員便直接帶您到金庫，任您索取裡面的內容物。聽起來很瘋狂嗎？同理，網路連線是否也不該任由他人隨意查看？

無論使用者是否需要所有資源，VPN (虛擬專用網路) 會讓使用者存取整個網路，進而可能危及您的資料。**ZTNA 技術僅給予員工所需資源的權限，同時嚴格驗證每個 App 的使用者和設備身分，限縮存取企業資料的權限**，這個做法還能減少網路的頻寬需求，並藉由智慧分流技術保護使用者的隱私。換句話說，VPN 早已不堪用。

那麼 ZTNA 是如何運作的呢？ ZTNA 基本須要取得三項資訊：

1

身分：您的身分是否屬實，以及此身分是否已經過授權？

2

安全：您的設備安全嗎？

3

內容：您有無請求其他不需要的資源？



若要成功運用 ZTNA 技術，則需要找出這些問題的答案。ZTNA 會要求驗證使用者本身和使用者裝置的身分，且這部裝置必須是已知並經過授權的設備。若要授權裝置，只需透過管理解決方案，將特定使用者所屬的裝置進行註冊，而使用者只需提供正確的憑證，再回應雲端身分供應商提出的 MFA 即可驗證身分。

不過儘管已經進行了身分驗證，還是請務必確保設備是處在安全的狀態，才能夠在存取公司資源時降低風險。若要確保裝置維持安全，則裝置應符合您所設立的資安政策、使用最新作業系統，且漏洞已修補完畢。

在驗證完身分和安全性後，使用者便可以順利存取所需的 App。ZTNA 資安框架只會允許使用者看到他們有權存取的內容，若要實現這個任務，則得事前將已核准的 App 佈建給每位使用者。如此一來，當使用者嘗試存取這些 App 時，他們便已具備權限。

Jamf 可為您完成這些任務：裝置管理、佈建 App、與多家雲身分供應商整合、軟體更新、端點防護等。歡迎閱讀我們的《零信任網路存取入門》電子書，進一步了解我們如何順利實現 ZTNA。

想透過 ZTNA 限制企業資料的存取權？來看看如何透過 **Jamf** 的 **Trusted Access** 實現此目標還有更多功能。

