

確保遠距員工安全的 8 個關鍵



只要可以上網並完成工作的人，都能以任何方式組成現代遠距團隊。這表示，許多不同類型的使用者以相同的工具共同合作 — 全職員工、約聘人員、自由工作者、廠商和合作夥伴。您如何保護於各處代管的資料，同時不會減緩速度？以下是 8 個最佳做法，以確保現代遠距團隊的安全，而不會減緩速度。



1. 保護內部管理應用程式的存取權限

您可能正在使用傳統 VPN 來保護公司的內部應用程式 — 但該模型可能逐漸不管用，因為員工會大規模遠端連線。更糟的是，VPN 過度寬鬆，信任任何讓其通過前門的事物。

現代解決方案依賴零信任模型：數位質詢每個資料封包，且不會出現阻礙或降低 VPN 效能。



2. 保護您的團隊免受網際網路的威脅

若您運用任何 SaaS 應用程式組合，則您的團隊可能會暴露於網際網路的猛烈風險中。過去，公司會將傳出的網際網路請求路由傳送回總部進行威脅掃描 — 但在大規模進行的情況下，這會減緩速度並且難以維持。

您需要一種可以識別並停止最新威脅、同時不會讓團隊停擺的方式。



3. 隨時隨地保護公司資料

您公司最有價值的資料可能橫跨 SaaS 廠商、內部應用程式、公用雲端等。確保此資料只會在受保護的地方流動，這類保護的設計應可支援內部部署和雲端式服務的任何組合。

確保遠距員工安全的 8 個關鍵



4. 利用簡單好上手的工具

如果您的安全性狀態讓團隊感到頭痛，您的 IT 職員會覺得負擔很重。員工可能會完全放棄使用內部工具（或者出現更糟的情況：嘗試尋找變通辦法）。

何不使用他們已熟悉的系統——亦即利用他們慣用的相同 Google 或 Okta 登入方式的系統？



5. 快速追蹤約聘人員

現代員工的流動性很高。當約聘人員和其他外部合作夥伴與您的團隊合作時，重要的是確保他們在第一天就擁有所需的一切——但以此為限。工作完成後，您需要確認撤銷他們的權限。

現代驗證解決方案將能透過各種身分識別工具順利運作，包括可用性廣泛且約聘人員可能已經在使用的免費服務。



6. 讓工具更容易被找到

高效能的遠距團隊可讓員工在需要時輕鬆找到合適的工具。應用程式啟動控制板的設計，就像工具海中的救生筏，將使用者可以存取的每個應用程式帶進一個簡單的圖形儀表板。

有些啟動控制板優於其他：確認您的啟動控制板支援精細許可 (granular permissions)，以確保員工只能看見他們可以存取的工具。



7. 考慮以新的解決方案處理舊有問題

若您已經受到舊版應用程式的束縛，可能是時候考慮眾多成熟的 SaaS 解決方案之一。若您有合適的工具來保護，則 SaaS 應用程式可提供高度功能性、持續更新和訂閱模型，這對於許多要處理延長期間的公司而言都更為簡單，而非面臨一大筆預付款項。



8. 在出現問題時獲得預先提醒

辦公室的儀表板可能已經變暗，但不代表您的見解也需如此。確保您使用支援廣泛記錄和稽核每個要求的解決方案——並且具有匯出至安全性資訊與事件管理 (SIEM) 平台的彈性。

解鎖更安全且更快速的遠距工作，以利您的團隊。立即在 teams.cloudflare.com 進行