Microsoft Entra 私人存取

探索全新的集中式身分識別零信任網路存取 (ZTNA) 解決方案。

保護所有私人應用程式的存取權

Microsoft Entra 私人存取建置在零信任原則的基礎之上，可協助免除風險並提升使用者生產力。 無論在內部部署或任何雲端中，都能安全快速地讓使用者透過任何裝置和網路連線到私人應用程式。

閱讀資料工作表 >　　取得資訊圖表 >

以 ZTNA 取代舊版 VPN

針對從任何位置、任何裝置、任何網路連線的使用者，升級至 ZTNA，以快速啟用所有舊版、自訂和新式私人應用程式的零信任存取權。

在所有私人資源強制執行調整條件式存取

在所有私人應用程式和資源上強制執行條件式存取控制，包括多重要素驗證 (MFA)、位置型安全性、進位分割，以及調整最小許可權存取原則，而不需要對您的應用程式或資源進行任何變更。

在全域提供快速且簡單的存取

透過基於 Microsoft 全域私人網路建構的龐大全域邊緣網路提供快速、簡單的存取，提高使用者工作效率。在所有私人應用程式和資源 (無論是內部部署或任何雲端) 上啟用單一登入。

輕鬆找出傳統 VPN 的替代方案

設定廣泛的私人 IP 範圍和完整網域名稱 (FQDN)，藉此快速啟用所有私人資源的集中式身分識別零信任型存取。

強制對舊版通訊協定使用多重要素驗證

在傳統通訊協定之前設置新式驗證，像是 Kerberos 和 NT LAN Manager (NTLM)。

啟用調適型個別應用程式存取

為所有私人應用程式設定精細的個別應用程式存取控制。

透過 Microsoft Entra ID 進行管理和保護安全

透過雲端身分識別和存取權管理解決方案，將員工、客戶和合作夥伴與其應用程式、裝置及資料連結起來，藉此保護貴組織的安全。

安全自適性存取

透過增強式驗證和風險式自適性存取原則，在不影響使用者體驗的情況下保護資源和資料存取權。

順暢的使用者體驗

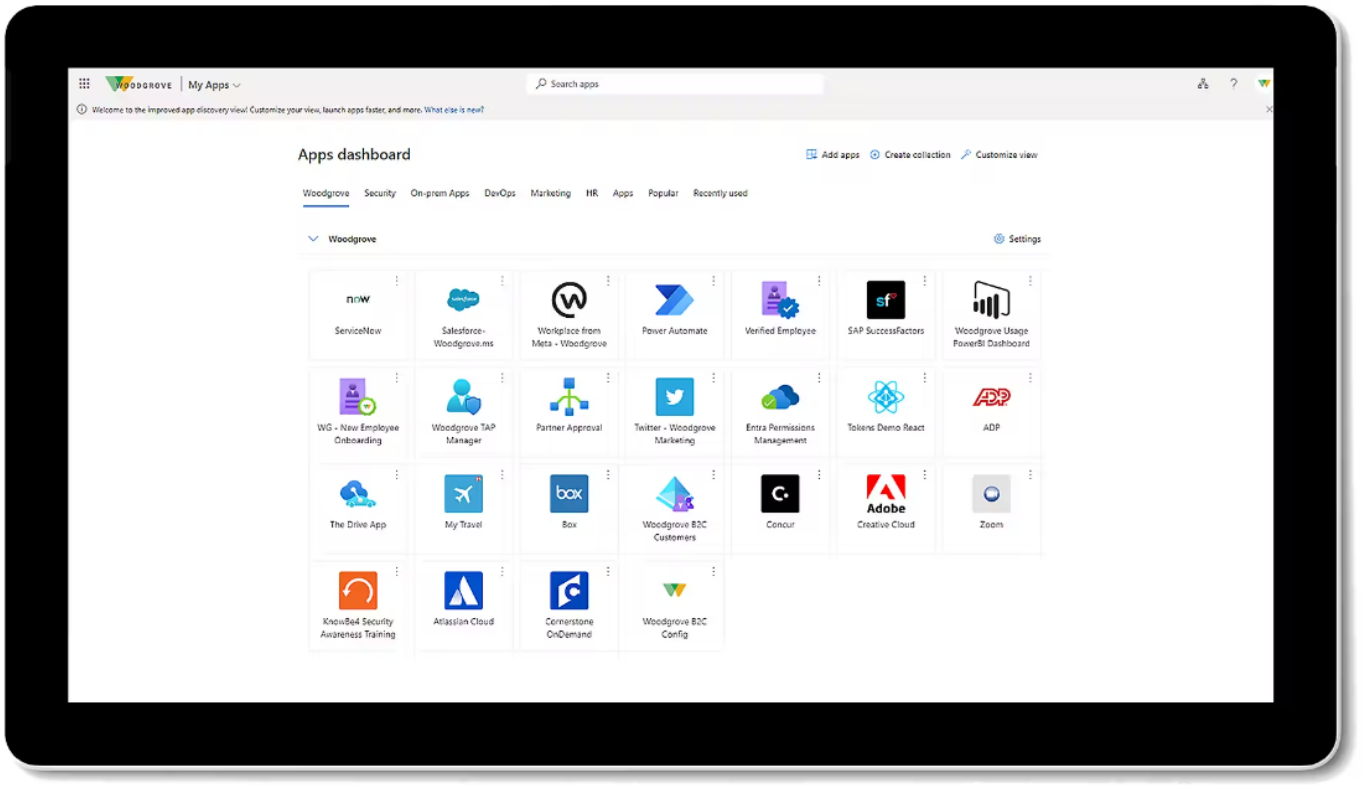
為您所有的多雲端環境提供快速方便的登入體驗，藉此維持使用者的工作效率、減少管理密碼花費的時間，並提高生產力。

整合式身分識別管理

在一個中央位置管理您的所有身分識別和所有應用程式的存取權 (無論是在雲端中還是在內部部署)，以提高可見性和控管能力。

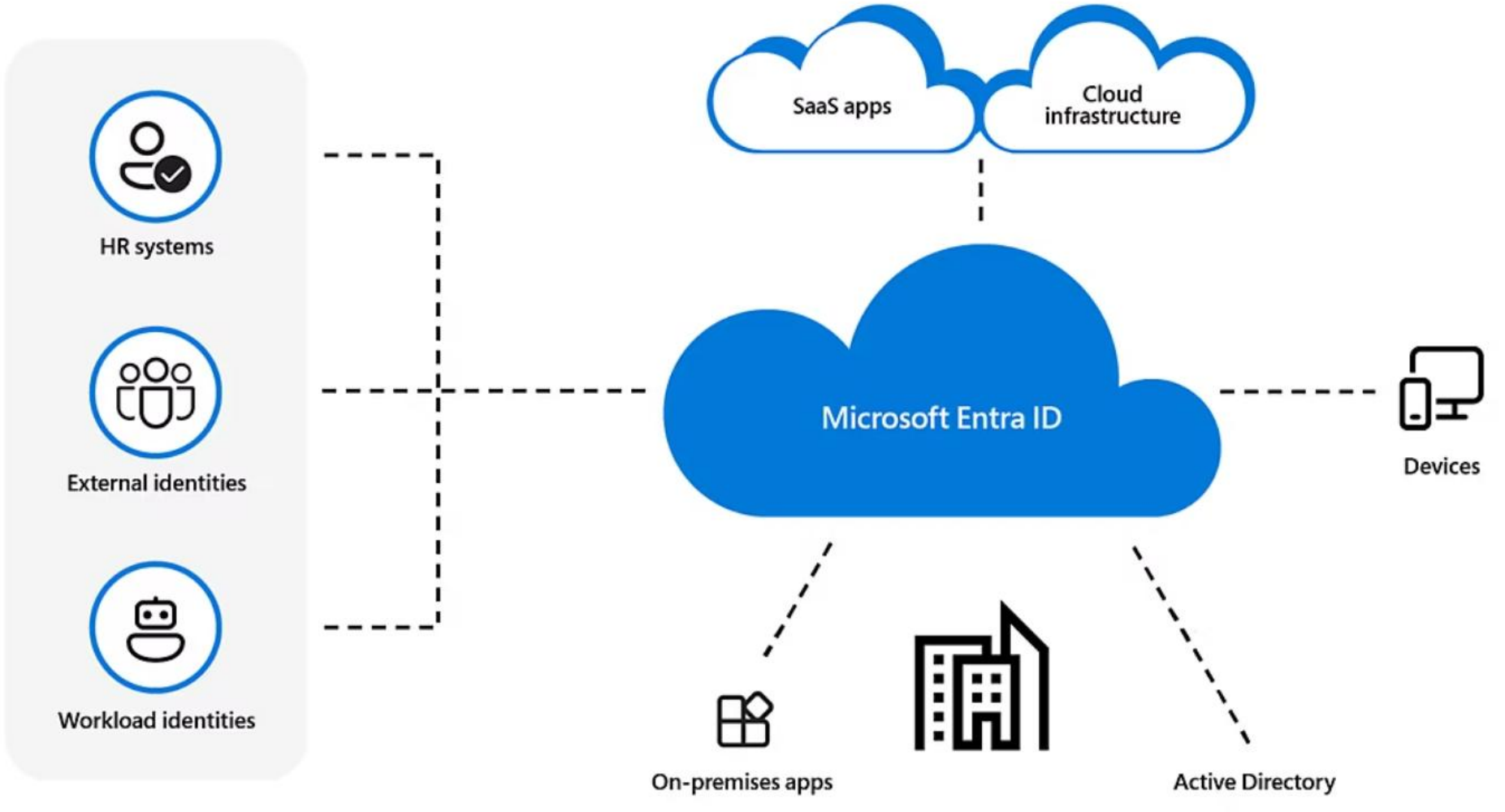
全方位功能

- 應用程式整合和單一登入 (SSO)
- 無密碼和多重要素驗證 (MFA)
- 條件式存取
- 身分識別保護
- Privileged Identity Management
- 終端使用者自助服務
- 整合式系統管理中心



多雲端身分識別和存取權管理

Microsoft Entra ID 是一種整合式雲端身分識別和存取權解決方案，也是管理目錄、授與應用程式存取權和身分識別保護的市場領導者。



Microsoft Intune

您的端點管理命令中心。

在同一個地方保護和管理端點

以較低的擁有權總成本更輕鬆地管理端點，並享受強大的資料與裝置保護措施。

簡化端點管理

將端點管理解決方案和工作流程整合在同一個地方，減少 IT 和安全性作業的複雜性。

強化安全性

透過使用 Microsoft 安全性訊號和進階端點管理功能來確保裝置健康情況和合規性，以緩解網路威脅並保護公司資料。

降低整體成本

透過整合供應商提高效率，以及具成本效益的授權來節省更多成本。跨裝置提升終端使用者的生產力和效能。

探索 Microsoft Intune 產品和功能

最大化生產力並簡化管理，且無須犧牲端點管理和安全性。

Microsoft Intune 核心功能

跨 Windows、Android、MacOS、iOS 和 Linux 作業系統管理和保護雲端連線的端點。

深入了解 >

Microsoft Configuration Manager

管理 Windows 電腦和伺服器等內部部署端點。

深入了解 >

Microsoft Intune 遠端說明

啟用安全的雲端式使用者連線服務台。

深入了解 >

Microsoft Intune 端點權限管理

可讓標準使用者執行通常專為系統管理員保留的 IT 核准工作。

深入了解 >

Microsoft Intune 企業應用程式管理

主動、簡單、安全地部署和管理應用程式。

深入了解 >

Microsoft Intune 進階分析

利用 AI、分析和可付諸行動的見解提升終端使用者體驗。

深入了解 >

Microsoft 雲端 PKI

簡化和自動化雲端憑證管理。

深入了解 >

透過 Intune Suite 整合任務關鍵性進階端點管理和安全性解決方案

- **簡化端點管理**。將端點管理解決方案和工作流程整合為單一環境，降低 IT 和安全性作業的複雜性。
- **加強安全性態勢**。透過使用 Microsoft 安全性訊號和進階端點管理功能來緩解網路威脅並保護公司資料，確保裝置健康情況和合規性。
- **降低總體成本**。透過整合供應商提高效率，以及具成本效益的授權來節省更多成本。跨裝置提高終端使用者的生產力和績效。

Microsoft Intune Suite 所有產品都可以與 Microsoft 365 和 Microsoft 安全性順暢地共同作業。Microsoft Intune Suite 包括 Microsoft Intune 遠端說明、Microsoft Intune 端點權限管理、Microsoft Intune 進階分析，Microsoft Intune 企業應用程式管理，Microsoft 雲端 PKI 和 Microsoft Intune 方案 2 中的進階功能。

需要 Microsoft Intune 方案 1 訂閱。

為什麼 DLP 很重要？

DLP 解決方案是您降低風險策略中的必要項目，對於保護在行動裝置、桌上型電腦及伺服器等端點而言更是如此。

資訊安全 (資安) 指的是避免敏感性資訊遭錯誤使用、未授權存取、干擾或破壞的安全性程序，包括實體和數位層面的安全性。下列是資安的關鍵元素：

基礎結構和雲端安全性。硬體和軟體系統專屬的安全措施，有助於防止未經授權的存取權和資料從公用雲端、私人雲端、混合雲端及多雲端環境中外洩。

加密。以演算法為基礎的溝通安全措施，可確保僅有訊息的預期收件者能夠進行解密和檢視。

事件回應。組織回應、補救和順利撐過網路攻擊、資料外洩或其他中斷事件所導致的後果的方式。

災害復原。發生自然災害、網路攻擊或其他中斷事件後重建技術系統的計劃。

DLP 解決方案的優點

DLP 的第一項優勢是可以對資料進行分類和監控，同時提升整體的可見度和控制能力。

分類和監控敏感性資料

了解自身持有哪些資料以及這些資料在數位資產中的使用方式，可讓組織更輕鬆地識別未經授權存取資料的行為，並避免資料遭人不當使用。分類是指套用規則來識別敏感性資料和保持符合規範的資料安全性策略。

偵測和封鎖可疑活動

自訂 DLP 解決方案，以便掃描所有經過您網路的資料，並阻止資料透過電子郵件、複製到 USB 隨身碟或其他方式離開網路。

自動化資料分類

自動化分類會收集相關資訊 (例如文件建立的時間、儲存的位置以及共用的方式) 來提升組織資料分類的品質。DLP 解決方案會運用這類資訊來強制執行 DLP 原則，而這有助於防止與未經授權的使用者分享敏感性資料。

維持法規合規性

各組織皆必須遵守資料保護標準、相關法律及規定，例如健康保險流通與責任法案 (HIPAA)、沙賓 (SOX) 法案以及聯邦資訊安全管理法案 (FISMA)。DLP 解決方案會提供完成合規性稽核所需的報告功能，其中還可能包含為員工制定資料保留計劃和訓練計畫。

監控資料存取和使用情況

為了防患未然，您需要監控誰能存取什麼內容，以及他們會利用這項存取權做什麼。在所有網路、應用程式和裝置上管理員工、廠商、承包商和合作夥伴的數位身分識別，藉此防範內部漏洞和詐騙。 角色型存取控制是其中一種方式，僅會將存取權提供給需要權限完成工作的人員。

提升可見度和控管力

DLP 解決方案能為您提供組織內敏感性資料的可見度，並協助您探查有可能將敏感性資料傳送給未授權使用者的人員。決定實際和潛在問題的範圍後，您可以進一步自訂設定以分析資料和內容，藉此強化網路安全性措施和 DLP 投入量。

DLP 最佳做法

按照這些最佳做法來協助確保成功地實施資料外洩防護：

- **識別並分類您的敏感性資料**。若要保護資料，您需要了解您擁有哪些資料。運用 DLP 原則識別敏感性資料，並據此加上標籤。
- **使用資料加密**。將待用與傳輸中的資料進行加密，未授權使用者將無法檢視檔案內容 (即使對方可存取檔案的位置)。
- **保護您的系統**。網路的安全性與其最脆弱的進入點相差無幾。請針對需透過網路來完成工作的員工限制存取權。
- **分階段實作 DLP**。了解企業優先事項，並建立試驗測試。允許組織發展該解決方案，以及解決方案所提供的所有內容。
- **實作修補管理策略**。為基礎結構測試所有修補檔，以確保組織內部不存在漏洞。
- **配置角色**。建立角色和職責以釐清需對資料安全負責的人員。
- **自動化**。手動 DLP 程序在範圍方面會受到限制，且無法經由擴大範圍來滿足組織日後的需求。
- **運用異常偵測**。機器學習和行為分析可用來識別可能會導致資料外洩情況的異常行為。
- **給予利害關係人相關指導**。DLP 原則不足以預防蓄意或意外事件出現；利害關係人和使用者必須了解自身在保護組織資料安全方面所扮演的角色。
- **建立指標**。追蹤指標 (例如事件次數和回應時間) 有助於決定 DLP 策略的成效。