Microsoft

使用 Azure Active Directory
管理並安全存取您的應用程式

第 1 節

什麼是身分識別與存取權管理？

什麼是身分識別與存取權管理？

數位轉型

雲端運算和行動裝置已轉換現代化工作場所。日益增加的全球工作力擁有靈活性，可以使用免費且低成本的軟體即服務 (SaaS) 應用程式隨時隨地工作，以解決生產力和共同作業的挑戰。大型企業正在將應用程式和運算移轉到雲端以現代化其架構，而企業營運正在利用新的雲端服務來建置滿足其特定需求的自訂應用程式。企業從激增的新技術中獲益而提升了生產力，但數位轉型也帶來了三個新挑戰。

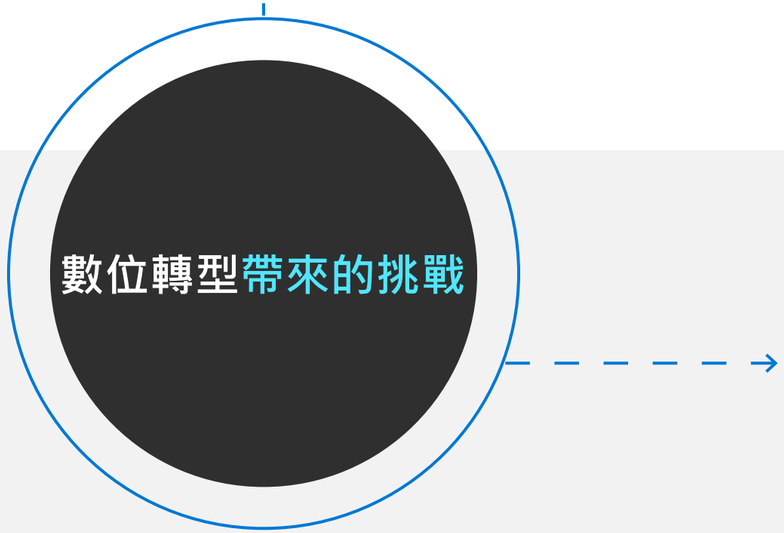
什麼是身分識別與存取權管理？

新挑戰

安全性風險：在雲端革命之前，IT 擔任技術守門員。您管理和保護的應用程式和平台都包含在網路界限內，而且登入到公司資源的每個人都會先由防火牆進行驗證。那些日子已經過去了。您的工作力更能掌控他們使用的技術，而這些大部分是透過網際網路進行存取。網路攻擊者已經學會利用這些漏洞。即使使用者知道帳戶的正確密碼，您也無法永遠保證他們的真實身分。

系統管理負擔：端點的爆炸成長為使用者提供了更多的連結方式，但這也造成了系統管理上的惡夢。許多企業並不了解員工使用的所有工具，即使企業擁有不錯的庫存，但絕對的雲端應用程式數量代表您需要管理多個身分識別系統，進而增加了成本並加重現有的安全風險。

不佳的使用者體驗：使用者也會感到痛苦。他們喜愛靈活性，但又對需要記住的大量認證感到挫折。



安全性風險

系統管理負擔

不佳的使用者體驗

作為中央控制平面的身分識別與存取權管理

這些痛點的共同點是驗證身分識別的系統效率低下。身分識別已取代網路界限作為新的控制平面。您需要能夠在整個企業中連結不同工具、架構、裝置和服務的解決方案，以更妥善地保護組織並管理員工和外部合作夥伴的身分識別與存取權管理 (IAM) 系統，將存取權集中在一個系統，讓您更能掌控。它們提供了跨組織界限的無縫共同作業，同時提高公司資源的安全性。優良的 IAM 解決方案可讓您透過一組認證，將使用者連結到其所有工作應用程式 (無論是在雲端中還是在內部部署)。IAM 解決方案的設計旨在讓使用者僅能存取所需資源，並封鎖未經授權的使用者存取不應存取的資料。您可以從集中式入口網站管理使用者存取權和權限，減少佈建和取消佈建使用者帳戶時涉及的許多手動程序。IAM 解決方案還提供工具來管理身分識別和應用程式中的安全性原則。最佳的 IAM 解決方案可以更妥善地保護身分識別、改善使用者體驗並提高系統管理效率。

IAM 解決方案
解決這些挑戰

更妥善地保護身分識別

改善使用者體驗

提高系統管理效率

第 2 節

Azure AD 概觀

全方位解決方案

Microsoft Azure Active Directory (Azure AD) 是雲端中的全方位 IAM 解決方案，也是管理目錄、應用程式存取和進階身分識別保護的市場領導者。Azure AD 讓組織能夠管理並保護員工、合作夥伴和客戶的身分識別，以便存取所需的應用程式與服務。Azure AD 協助數百萬組織管理和保護超過十億個身分識別。

現代化存取權

在內部部署和雲端中管理並安全存取貴組織的資料和資源。將所有使用者、應用程式和裝置連結到雲端，以實現無縫、安全存取，以及更佳的可見度和控管能力。自動化工作流程和啟用自助服務選項，協助降低成本並為您的使用者提升生產力。

保護與控管

每天都有大量的使用者認證受到攻擊，因此，避免遭入侵的方法是在可能的最廣泛的訊號範圍內連續追蹤正常和異常行為，套用人工智慧並自動化回應。透過及時存取合適的資源和定期存取檢閱與原則強制，來平衡生產力和安全性。

連結和共同作業

使用可靠的雲端服務來擴展商務，該服務可透過領先業界的安全性和靈活性擴展到數百萬個使用者。與您的外部使用者聯繫，並透過方便使用的自助服務體驗和內建的安全性控制措施，來提升他們的生產力。

開發與整合

建置讓使用者以輕鬆的方式使用其 Microsoft 個人、公司或學校帳戶或是社交帳戶登入的應用程式。開始連結到 Microsoft Graph (Microsoft 365 中存取資料和情報的閘道)，並建置功能豐富的應用程式。啟用單一登入與自動化使用者佈建，並與全球最大的組織聯繫。

第 3 節

適用於您應用程式的 Azure AD

適用於您應用程式的 Azure AD

通用平台

Azure AD 讓您可以為混合式基礎結構中的每個使用者管理通用身分識別，以存取他們所需的所有應用程式，包括雲端和內部部署企業營運應用程式。從通用平台管理所有身分識別，進而提高系統管理效率，讓您更能掌控。將精細的安全性原則套用到組織中使用的每個應用程式。

適用於您應用程式的 Azure AD

節省時間與費用

Azure AD 已預先整合了數千種應用程式，包括 Workday、ServiceNow、SuccessFactors、Adobe 和 Concur 等熱門選項，讓您能更簡單地將這些應用程式提供給使用者。透過單一主控台，部署一致的原則和監控存取權。您可以為使用者佈建和生命週期管理自動化工作流程，並透過自助式帳戶管理節省時間和資源。您也可以將來自人力資源工具的輸入使用者資訊作為真實來源，不需要自訂指令碼或手動程序就能管理使用者屬性。

透過 Azure AD 設定的應用程式啟用單一登入 (SSO) 以實現無縫存取，這代表使用者不必記住每個應用程式帳戶的認證，也不需要重複使用弱式密碼並避免資料外洩的風險。已設定進行自動佈建的帳戶，可讓使用者盡快存取新資源。針對輸入佈建的 Azure AD，確保新員工在第一天就可以存取其所有相關資源。

節省時間與費用

內建 SaaS 整合

單一登入

新使用者存取

適用於您應用程式的 Azure AD

為所有應用程式提供更安全的存取權

Azure AD 提供您所有應用程式 (包括 SaaS 應用程式和內部部署企業營運應用程式) 全方位的身分識別保護。無論使用者是否正在要求存取 Microsoft Word 或 Box，Azure AD 都會在授與存取權之前確保其身分識別已經過確認。您也可以制定存取控管原則，以確保使用者僅在需要時才能存取他們所需的內容。您可以要求使用者要求存取權，還可以設定使用者存取應用程式的時間限制，並針對存取權進行定期合規性檢閱。

Azure AD 也利用 Microsoft Intelligent Security Graph 和機器學習，來分析我們所有產品和服務中的數兆個訊號，以發現非典型行為並為每個工作階段指派相關風險。Azure AD 會查看裝置、位置和其他內容資訊，以評估登入風險。您可以建立自動套用安全性措施的 Azure AD 條件式存取原則，例如在認為登入存在風險或符合特定原則條件時，封鎖存取要求或要求重設密碼等措施。

應用程式安全性措施

身分識別保護

存取權控管

條件式存取原則

第 4 節

如何透過 Azure AD 管理並保護應用程式

Azure AD 使用自動化功能、自助服務和原則強制，讓隨時掌控變得簡單，並降低成本。

如何透過 Azure AD 管理並保護應用程式

Azure AD 應用程式整合

Azure AD 應用程式庫可讓您輕鬆設定數千個預先整合的應用程式，並將其連結到您的租用戶。這些應用程式都支援 SSO 體驗，並且可根據每個應用程式或整個企業原則，簡單設定應用程式以進行 Azure AD 條件式存取。新增應用程式並針對您的需求進行設定後，具有授權存取的使用者可以在 Azure AD 我的應用程式入口網站中輕鬆找到它，該入口網站是用於使用者應用程式探索和啟動的集中式入口網站。

如果您已經為組織建置應用程式或需要整合一個應用程式，您也可以要求將其列在 Azure AD 應用程式庫中。

探索數千種預先整合的應用程式 >

保護混合式存取

使用 Azure AD 應用程式 Proxy 來提供宣告式內部部署 Web 應用程式安全地遠端存取權，無需使用 VPN。應用程式 Proxy 需要安裝輕型連結器，並授與與透過 Azure AD 應用程式庫連結之 SaaS 應用程式相同的 IT 和使用者體驗。

或者，如果您想利用現有的基礎結構投資 (例如與 F5 ZScaler、SAP、Oracle 或 Ping Identity 等合作夥伴合作)，來連結其他類型的應用程式 (例如使用標題型或 Kerberos 驗證通訊協定的應用程式)，您也可以這樣做，而且仍然可以獲得 Azure AD 的集中式和安全性優勢。

閱讀如何透過應用程式 Proxy 新增內部部署應用程式 >

連結其他合作夥伴應用程式網路與雲端 >

如何透過 Azure AD 管理並保護應用程式

自動佈建

Azure AD 讓您能夠在熱門的 SaaS 應用程式中自動建立、維護和移除使用者身分識別。當新人員加入您的小組或組織時，您可以在正確的系統中自動為他們建立新帳戶。當人員離開小組或組織時，您可以設定原則，自動從正確的系統中停用其帳戶。透過自動執行這些工作，您可以確保應用程式和系統中的身分識別，會根據目錄或人力資源系統中的變更保持在最新狀態，進而減少錯誤並節省時間。

深入了解如何對 SaaS 應用程式設定自動提供和取消佈建 >

群組管理

Azure AD 透過為單一使用者或整個 Azure AD 群組提供存取權，協助您授與組織資源的存取權。使用群組可讓資源擁有者為群組的所有成員設定存取權，而不必一一提供權限。這是一種更安全的方法，因為您不太可能意外地授與個人不適當的存取權，而且可以節省您的時間。您也可以透過身分識別屬性為基礎的原則讓註冊自動化，以便動態擴展您的群組管理。

了解如何在 Azure 入口網站建立群組 >

如何透過 Azure AD 管理並保護應用程式

使用者自助服務

某些工作不需要 IT 專業人員即可完成，而 Azure AD 可讓您將這些工作委派給組織中的其他人。您可以提升使用者的工作效率，以在 Azure AD 中建立和管理自己的安全性群組。群組擁有者可以核准或拒絕成員資格要求，也可以委派群組成員資格控制。

設定自我管理群組 >

自助服務也可以擴展到使用者。如果使用者擁有已驗證的電子郵件，則可以透過自助服務入口網站註冊帳戶，並且可以使用入口網站重設密碼。這樣可以為您的技術服務人員節省大量時間和金錢。

設定自助服務密碼重設 >

現代化驗證

如果您目前使用的是內部部署驗證 (例如 Active Directory 同盟服務 (AD FS))，則可以考慮將應用程式移轉到 Azure AD。您仍擁有與 SSO 相同的使用者優勢，但是可從雲端中獲得擴展性和安全性優勢，例如使用 Azure AD 條件式存取套用每個應用程式的精細存取控制，或透過 Azure AD B2B 共同作業向合作夥伴授與資源存取權。可以移轉使用 SAML 2.0、WS-Federation、OAuth 或 OpenID 連線標準進行聯合登入的應用程式。

建置 Azure AD 條件式存取原則以安全存取您的應用程式 >

使用 Azure AD B2B 來與您的外部合作夥伴進行無縫共同作業 >

安全地在任何雲端或伺服器，將任何
應用程式連結到 Azure AD。

已連結 100 萬個獨特的作用中應用程式。

Microsoft

立即開始使用。

開始免費試用一個月的 Azure AD，了解管理使用者存取所有應用程式和保護貴企業有多麼簡單。