CYBERARK®
The Identity Security Company

解決方案簡介

CyberArk 身分安全平台

透過智能的特權控制保護所有身分

隨著三種條件在數量和速度上的增長，使安全團隊面臨極度嚴苛的考驗：

- 您的企業是推動雲端和數位計劃發展的先鋒。
- 您使用者的身分和電腦驅動計劃發展。
- 現今的攻擊者會利用創新技術濫用您的身分。

遭利用的身分無論是否具有特權，都是現今複雜攻擊者為取得敏感資源的針對目標。使安全挑戰更加複雜：內部使用者和第三方供應商可能濫用或誤用授予權限 (往往遠超出實際需要範圍)。

企業正在深入探究問題，以應對同時發生的數項轉變：

- **身分數量爆炸：**我們生活在沒有邊線的數位世界中。根據 CyberArk 研究，每個自然人平均有 45 種機器身分，[1]而身分數量每年以 3 倍的速度增加[2]。不再有需要保護的邊界；身分是新的邊界。
- **所有身分均可成為特權：**「特權使用者」不再只是 IT 管理員。52% 的員工身分可以存取敏感系統和資料，進而讓攻擊者可以輕鬆利用入侵。[3] 在這樣的環境下，所有存取點的身分都成為組織最有價值資源的閘道。現在特權隨處可見，因此相關風險也隨之而來。
- **網路攻擊者不斷創新技術：**攻擊者使用更複雜的技術冒充使用者，進而發動目標性網路釣魚並竊取身分。有 63% 的組織因身分安全問題遭到網路安全攻擊得逞。[4]
- **IT 環境複雜度：**推動數位轉型的組織因利用混合式和多雲端環境，使得其所有基礎設施中端點 (包含受管理和不受管理的) 更加擴散。如此的複雜性使安全團隊對於可見度、控管身分的難度都大幅提升。2023 年有 80% 的企業預計與 3 家或多家公用雲端供應商合作，有 57% 的企業有專屬團隊，負責防護內部部署和公共雲端的身分。[5]
- **降低風險的複雜性：**資安高階主管意識到達到與維持控制各個身分是阻止大多數現代攻擊的關鍵要素。然而他們在實施安全第一方法時卻遇到困難。每個新的數位計劃發展皆會帶來身分相關的新挑戰和要求。為確保營運順利，企業通常會採用新的安全工具。

[1,3] CyberArk《2022 身分安全威脅態勢報告》(2022)
[2,4,5] Enterprise Strategy Group《整體身分安全成熟度模型》，2023 年 2 月

- **營運效率低落：**功能重疊的工具數量增加反而使得安全團隊作業更加沒效率。團隊因為太多解決方案疲於奔命，從身分和存取管理 (IAM)、身分治理和管理 (IGA) 到特權存取管理 (PAM)，這些解決方案不見能相互整合。這不但限制了資安團隊對整個企業內身分的可見度和控制，並使內部資源更加緊縮。
- **資安供應商暴增：**對於平均使用 75 家資安廠商的企業而言，[6] 現今封閉式安全解決方案的成本和複雜性是首要考量。這些工具處理安全問題的方式可能各有不同，因此安全團隊很難發揮每個獨立解決方案的價值。因此 CyberArk 的研究中顯示，54% 的組織偏好使用少數廠商提供的整合平台。[7] 跨身分安全工具的廠商整合具備安全優勢、營運效率和更好的投資報酬率。

解決方案

身分安全是使用零信任並強制執行最小特權的策略方法。這套策略方法需要完整的核心技術、人員與程序，確保企業在任何環境或裝置中，都能防護人類和機器身分對於最重要資產和資料的存取權。

身分安全控制具有動態和自適性的本質，目的是確保依據風險程度提供正確的存取層級。特權控制 (例如工作階段隔離、監控、提升權限以及端點特權管理和委任管理) 是身分安全與存取的關鍵核心，尤其當具有特權存取的定義已不同往常。在現今環境中，幾乎所有身分皆可能具有高價值或高級別的特權存取權 (視其執行的活動而定)。

因此，特權控制和程序逐漸與更多的 IAM 功能整合，如生命週期和權利管理、安全單一登入、驗證、密碼管理和自動化協調。透過統一身分安全方法，特權控制適用於：

- 各式身分 (從員工到供應商、DevOps 團隊到其使用的自動化工具)。
- 所有 IAM 控制 (例如存取審查、認證和生命週期管理工作流程)。

身分安全解決方案有助於持續監控所有環境中的身分存取，以便根據即時風險分析，採用適當的身分安全控制和回應 (例如存取連線凍結和逐步驗證)。

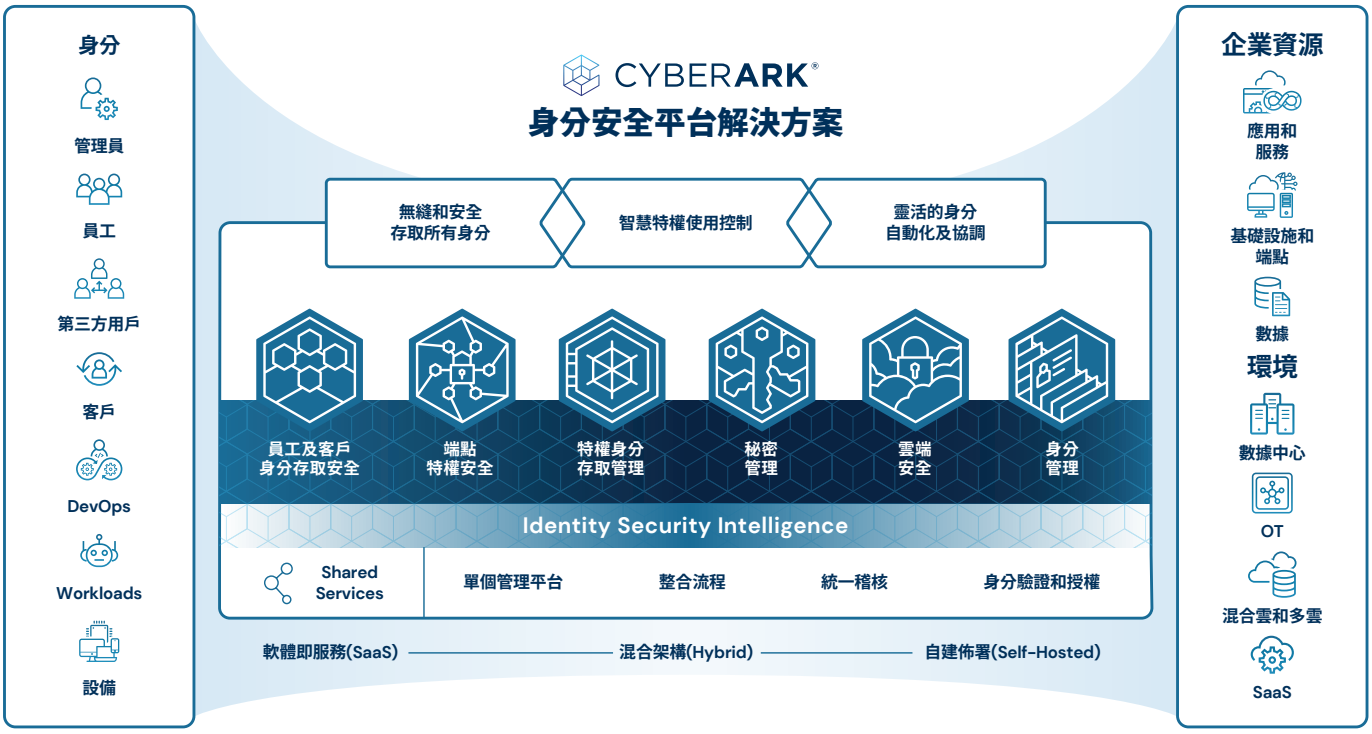
CyberArk 身分安全平台

CyberArk 身分安全平台以智慧特權控制為中心，採用統一方法無縫防護人類和機器身分自混合到多雲端存取的應用服務，並靈活自動化身分生命週期。CyberArk 提供最完整、可擴充的身分安全平台，包括跨員工和客戶存取、端點特權安全、特權存取管理、存取鑰匙管理、雲端特權安全和身分管理，以啟用「零信任」並執行最小權限。

CyberArk 身分安全平台包含一系列基礎共用服務 (包括 AI 驅動的身分安全情報)，可透過單一管理入口網站提供整合式使用者體驗，並透過強大的自動化和分析提升價值。透過我們龐大的合作夥伴網路和 300 多個現成整合，CyberArk 讓企業在身分安全旅途中的每一步都提供充分支援，同時幫助企業將現有的資安投資利益最大化。

[6] Panaseer《2022 年資安領導者同儕報告》(2022)

[7] Enterprise Strategy Group《整體身分安全成熟度模型》2023 年 2 月



主要功能: CYBERARK 身分安全平台

- **統一身分安全平台:** 使用提供多種功能的整合式平台，以便在自基礎設施中存取資源的週期過程中，透過實施特權控制確保所有個別身分 (人類或非人類) 的安全。
- **智慧型特權控制** 從端點到雲端，針對身分、基礎結構和應用程式實施最小特權安全控制。獲取情報以偵測異常行為 (單獨或結合特權存取的濫用)，這些皆可能是潛在威脅。
- **強化驗證:** 針對員工、合作夥伴、廠商和客戶，根據情境和風險和自適性進行存取管理。強大的無密碼驗證因素，包括生物識別、QR 代碼、行動裝置推播和 USB 權杖(Token)。
- **內容授權:** 防護人類使用者及機器身分的特權存取，例如應用程式。在全平台、端點和應用程式實施最小特權和即時存取原則。
- **無阻礙存取:** 利用專為管理、佈建、啟用存取及保護所有身分及資源類型而設計的單一窗格，透過自動化工作流程提供自助式服務使用者配置、帳戶及密碼重設、應用程式存取等。與數千種 SaaS、行動和自訂應用程式進行無縫整合。
- **稽核和權責:** 透過防護代理工作階段取得可見度和控制，確保權責劃分、監控和識別危險行為以及提供防篡改稽核軌跡。使用風險分析監控存取活動並即時對可疑行為採取行動。
- **無縫整合:** 體驗與現有技術工具 (包括第三方威脅情報和 DevOps 工具) 的無縫整合。

結論

採用身分安全的企業可以透過將供應商整合到統一平台，實現發揮重要的安全利益和營運效率。不過，由於 CyberArk 身分安全平台採用模組化，因此企業可以從我們其中幾個頂級功能起步或是使用整個平台。無論採用何種方法，最重要是讓組織具備強大的身分安全計劃，進而降低可衡量的網路風險。

透過 CyberArk，企業只需單一身分安全平台即可在完全可見度下使用零信任並強制執行最小特權，確保每個身分可以隨時安全存取任何位置的資源。

力悅資訊
cyberview.cloud

【臺灣區代理商】
公司：力悅資訊股份有限公司
電話：02-25429758
信箱：sales@cyberview.com.tw
地址：台北市中山區松江路54號4F-4

關於 CyberArk

CyberArk 是身分安全的全球領導者。CyberArk 以Privileged Access Management 為中心，為跨商業應用程式、分散式員工、混合式雲端工作量，以及整個開發維運 (DevOps) 生命週期中的任何身分 (不論人類或機器) 提供最全面的安全服務。全球領先的組織信任 CyberArk 可以協助保護他們最關鍵的資產。

CYBERARK®
The Identity Security Company