特權帳號安全解決方案

從最佳實務的規定來看，特權帳號應與組織的核心資安政策相互結合。特權帳號本身就是資安問題，需要採取單獨控管的方式來防護、監控、偵測及回應所有特權帳號活動。

特權帳號代表著組織現今所面臨的最大資安漏洞。幾乎所有外界攻擊都會利用這些高權限的帳號，而取得這些帳號的任何人都能夠控制組織的資源、停用保全系統，以及存取大量敏感資料。

為了防護這些特權帳號以及能夠存取的關鍵資源，組織需要備妥全方位的控管方式來防護、監控、偵測及回應所有特權帳號活動。

CyberArk 正是值得信賴的特權帳號安全防護專家。專為安全防護全新設計的 CyberArk 特權帳號安全解決方案，為內部部署、雲端及 ICS 環境提供了最全面的解決方案。這套完整的特權帳號安全解決方案立即可供企業使用，能抗竄改、彈性調整，並且特別針對複雜的分散式環境所打造，提供了阻擋進階外部和內部威脅的終極防護措施。

CyberArk 共享技術平台

CyberArk 共享技術平台

數位金庫 (Digital Vault™)。獲獎肯定的專利數位金庫 (Digital Vault) 是一部如堡壘般堅固的隔離伺服器，採用 FIPS 140-2 加密機制，只會回應金庫通訊協定，藉此提供無與倫比的安全性。

主要政策 (Master Policy™)。主要政策 (Master Policy) 是一款創新的原則引擎，能讓客戶透過單一、簡易、自然的語言介面設定、管理及監控特權帳號的安全政策。

帳號探索引擎。專為持續檢索 IT 環境變化所設計，帳號探索引擎能夠實現持續不斷的最新防護，確保所有特權帳號活動皆受到控管且安全無虞。

可彈性調整、靈活、影響極低的架構。CyberArk 特權帳號安全解決方案的架構方式僅會產生最低的影響，並且能防護您目前 IT 環境中現有的投資。

企業級整合。CyberArk 特權帳號安全解決方案讓組織得以搭配對眾多作業系統、網路裝置及應用程式 (包括 Web 應用程式在內) 的現成支援，充分運用現有的投資。

特權帳號安全產品

CyberArk 特權帳號安全解決方案中的每一項產品都可各自獨立，並且可單獨管理，同時仍分享共同基礎架構中的資源和資料。這些產品共同提供了一套完整、安全的解決方案。

企業密碼金庫 (Enterprise Password Vault™)

防護、管理和稽核特權憑證

企業密碼金庫會依據特權帳號安全原則，集中保護和控管對特權密碼的存取權。自動化的密碼輪替機制能減少耗時且容易出錯的人為工作，像是追蹤和更新特權密碼，讓企業能夠輕鬆遵循稽核與合規標準。

SSH 金鑰管理員 (SSH Key Manager™)

管理、輪替和防護特權 SSH 金鑰

SSH 金鑰管理員經過專門設計，能夠防止未經授權存取受 SSH 金鑰保護的特權帳號的行為。SSH 金鑰管理員可安全地保管及控管對私密 SSH 金鑰的存取權，自動輪替 SSH 金鑰配對，並且讓組織能夠回報使用金鑰的人員、種類及時間。

特權連線管理員 (Privileged Session Manager™)

監控、控管和隔離特權連線

特權連線管理員就像一部安全的跳板機，可保護特權使用者連線、防護端點上的目標系統不受惡意軟體威脅，並且能讓特權帳號進行存取而不會洩露敏感的憑證。監控和記錄功能可讓資安團隊即時檢視特權連線、從遠端終止可疑的連線，並且維護完整且可搜尋的特權使用者活動稽核追蹤記錄。

特權帳號威脅分析 (Privileged Threat Analytics™)

分析和警示惡意特權帳號活動

CyberArk 特權帳號威脅分析是業界唯一的目標式特權帳號威脅分析解決方案，能夠識別以往無法偵測出的惡意特權使用者活動。這款解決方案藉由在一組豐富的特權帳號行為資料當中採用專利的演算法，產生出精確、可付諸行動的情報，讓事件回應者能夠阻斷並直接回應攻擊。

應用程式身分管理器 (Application Identity Manager™)

防護、管理和稽核嵌入式應用程式憑證

應用程式身分管理器會消除應用程式和指令碼中的硬式編碼密碼和 SSH 金鑰，將它們取代成安全的動態憑證。本產品的設計在於因應企業對於可用性和企業永續性的高階需求，甚至在複雜的分散式網路環境中也能實現。本產品取代了靜態的嵌入式應用程式帳號憑證，不會要求變更程式碼，而且不會對應用程式效能造成任何影響。

隨選特權管理器 (On-Demand Privileges Manager™)

對 Unix 和 Linux 的最小特權存取控管

隨選特權管理器可讓特權使用者從自己的原生 Unix 或 Linux 連線執行經授權的管理命令，同時撤銷不必要的根特權。這款安全且立即可供企業使用、類似 sudo 的解決方案，為所有進階使用者活動提供了整合一致且相互關聯的記錄，並且與個人使用者名稱連結，同時提供執行職務所需的自由度。

CyberArk 終端特權管理器 (CyberArk Endpoint Privilege Manager)

保障端點上的特權安全性

CyberArk 終端特權管理器可保護端點上的特權，並且在攻擊週期中及早遏制其發展。在撤銷本機系統管理員權限的同時，仍可藉由順利提升經授權應用程式或工作的特權，將使用者工作效率受到的影響降至最低。透過自動建立原則控管應用程式，組織就有能力防止惡意應用程式執行，並且在受限模式下執行不明應用程式。與憑證竊取防護措施相互結合之下，還能有效防止惡意軟體趁機入侵，並遏制端點上的攻擊。

利用 CyberArk DNA™ 立即開始評估您的特權帳號風險

CyberArk DNA™ (檢索與稽核，Discovery and Audit) 是一項免費的評估工具，可幫助組織瞭解特權帳號安全風險的範圍。DNA 會檢索整個企業內特權帳號、SSH 金鑰、服務帳號、裝置及應用程式的位置和狀態。此工具可幫助組織排出專案的優先順序，建立企業案例，並規劃特權帳號安全專案。

規格

加密演算法：

- AES-256、RSA-2048
- HSM 整合
- FIPS 140-2 驗證加密

高可用性：

- 叢集支援
- 多處災難復原站台
- 與企業備份系統整合

存取權和工作流程管理：

- LDAP 目錄
- 身份識別和存取權管理
- 票證和工作流程系統

多語入口網站：

- 英文、法文、德文、西班牙文、俄文、日文、中文 (簡體和正體)、巴西葡萄牙文、韓文

驗證方法：

- 使用者名稱和密碼、LDAP、Windows 驗證、RSA SecurID、Web SSO、RADIUS、PKI、SAML、智慧卡

監控：

- SIEM 整合、SNMP 設陷、電子郵件通知

支援的受管理裝置範例：

- 作業系統：Windows、、*NIX、IBM iSeries、Z/OS、OVMS、ESX/ESXi、XenServers、HP Tandem*、MAC OSX*
- Windows 應用程式：服務帳號包括：叢集中的 SQL 伺服器服務帳號、排程工作、IIS 應用程式集區、COM+、IIS 匿名存取、叢集服務
- 資料庫：Oracle、MSSQL、DB2、Informix、Sybase、MySQL 和任何 ODBC 相容資料庫
- 安全設備：CheckPoint、Cisco、IBM、RSA Authentication Manager、Juniper、Blue Coat*、TippingPoint*、SourceFire*、Fortinet*、WatchGuard*、Industrial Defender*、Acme Packet*、Critical Path*、Symantec*、Palo Alto*
- 網路裝置：Cisco、Juniper*、Nortel*、HP*、3com*、F5*、Nokia*、Alcatel*、Quintum*、Brocade*、Voltaire*、RuggedCom*、Avaya*、BlueCoat*、Radware*、Yamaha*、McAfee NSM*
- 應用程式：CyberArk、SAP、WebSphere、WebLogic、JBOSS、Tomcat、Cisco、Oracle ERP*、Peoplesoft*、TIBCO*
- 目錄：Microsoft、Oracle Sun、Novell、UNIX 供應商、CA
- 遠端控制和監控：IBM、HP iLO、Sun、Dell DRAC、Digi*、Cyclades*、Fijitsu* 和 ESX
- 組態檔 (一般、INI、XML)

* 此外掛程式可能需要進行自訂或現場接受度測試。如需詳細資訊，請洽詢 CyberArk 銷售工程部。