



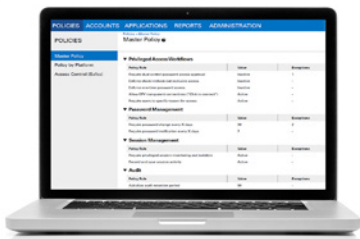
企業密碼金庫 (Enterprise Password Vault®)

對整個企業 IT 環境內所使用的特權帳號密碼進行主動式防護、輪換和存取管控。

挑戰

特權帳號存在於網路內的每一件硬體和軟體，只要掌握特權密碼就能全權存取和掌控機密資訊、商務應用程式 and 關鍵的 IT 基礎結構。若能適當使用，這些帳號可用來維護系統、輔助自動化流程、保護機密資訊和確保業務不間斷，但若是落入有心人士手中，這些帳號就可能被用來竊取機密資料和對業務造成不可回復的損害。然而，有些企業因為在清查和管理特權帳號及其憑證上意識到操作上的困難，而疏於解決此類風險。

若要降低對未經授權存取特權帳號的相關風險，又不加重 IT 人員的負擔，企業應採用可對特權帳號憑證（可比喻為是 IT 王國的鑰匙）的存取進行主動式防護、輪換和管控的工具。若無此類防護措施，企業將會面臨多項挑戰，包括：



從單一位置集中管理特權帳號身分識別和政策。

- **增加成功攻擊的風險。** 特權帳號是每個攻擊生命週期中至為關鍵的一步。當門戶洞開時，攻擊者就能輕易地非法存取這些高權限帳號，並且利用這些帳號進行具破壞力、產生重大損失的攻擊。
- **稽核失敗和罰鍰。** 企業必須對通常為公用的特權帳號存取進行控管和稽核才能符合規範。若沒有建立防護機制在各個層面上針對此類存取進行控管和稽核，企業可能面臨稽核不良和懲罰性罰鍰。
- **高營運成本。** 為了符合法規，部分 IT 團隊被派以人工方式輪換和更新特權帳號憑證的工作。這種程序相當耗時並且容易出現人為錯誤。沒有可以跨系統自動化和同步密碼變換的恰當工具，企業可能面臨高營運成本以及因帳號意外鎖定所造成的工作效率損失。
- **清查特權帳號。** CyberArk 企業密碼金庫會自動檢索和清查整個 IT 環境內的帳號。管理員可選擇應該加以保護的帳號或帳號群組，並自動將其佈建至數位金庫。
- **保護特權帳號密碼。** 一經佈建，特權密碼就會在 CyberArk 數位金庫 (CyberArk Digital Vault) 內集中獲得防護。CyberArk 數位金庫包括多重內建安全層，可為特權帳號資訊提供最嚴密的防護。
- **強制嚴格存取控管和作業流程。** CyberArk 企業密碼金庫依照組織政策強制嚴格存取控管和作業流程。本解決方案不但可讓已授權的使用者存取日常例行工作所需的特權帳號，並且支援自動化作業流程，讓使用者能夠視需要根據正當的業務理由，要求存取更高特權的帳號。

為何選擇 CyberArk？

CyberArk 是值得信賴的專家，能夠協助企業防堵最緊要的網路攻擊，使營運不致受到影響。

解決方案

CyberArk 企業密碼金庫 (CyberArk Enterprise Password Vault) 是根據組織政策來防護、輪換和控管對特權帳號密碼的存取所設計。本解決方案已經過實證可在最大型、最複雜的企業 IT 環境下擴充，並且可以保護用於存取絕大多數系統的特權帳號密碼。擁有 CyberArk 企業密碼金庫，企業就可以：

- **自動輪換密碼。** 本解決方案可依照既定政策，自動輪換和同步特權帳號密碼。密碼可以在每次使用後、定期或依照需要自動輪換。
- **稽核特權帳號的使用。** CyberArk 企業密碼金庫規定使用者必須先「簽出」密碼後才能存取特權或共用帳號，並且可以要求使用者在要求存取更高特權的帳號時提供具體的正當理由。如此可以建立詳細的稽核記錄，並讓安全和稽核單位輕鬆地報告何人在何時因何種原因存取了什麼。

- **自動使可能受入侵的憑證失效。**本解決方案能夠接收由 CyberArk 特權帳號威脅分析 (CyberArk Privileged Threat Analytics) 所發出有關有可能受入侵之特權帳號的警訊。收到警訊時，本解決方案會立即輪換受影響的密碼以使該憑證失效。

優勢

CyberArk 企業密碼金庫主動防護 IT 王國的鑰匙，協助企業保護機密系統資料免於外部攻擊者和惡意的內部人員的侵害。本解決方案讓企業：

- **了解特權帳號的範圍。**掌握有哪些特權帳號以及誰能夠存取這些帳號，以根據企業的風險承受能力建構有效的特權帳號安全性政策。
- **降低對未授權的特權帳號存取的風險。**集中防護特權密碼以預防特權憑證遺失、遭竊或遭到不法共用，並且緩和未授權存取特權帳號的風險。
- **緩和內部攻擊的風險。**主動防範內部未經授權的人員存取特權帳號憑證，並且分層分級追蹤所有特權帳號的存取狀況，以防止經授權的內部人員濫用特權造成損害。
- **限縮攻擊者得逞的機會。**將密碼的使用週期降至最低，以大幅地限縮攻擊者利用竊取的憑證存取特權帳號的空窗期。
- **自動抑制特權帳號的威脅。**透過立即使可能受入侵的特權帳號失效，以加速事件反應以及自動化威脅封鎖。

- **稽核人員一目了然。**讓稽核人員清楚看到設有哪些特權帳號政策和流程，並且輕鬆報告哪個個別使用者在何時因何種原因存取了什麼。
- **為已授權的特權使用者簡化使用者體驗。**讓使用者無須人工管理多組憑證，而改採用單一登入整個企業內的特權帳號。
- **減少 IT 人員的作業負擔。**免除手動輪換密碼這類耗時又繁複的工作，讓 IT 人員專注在更具策略性的專案上。
- **充分發揮 IT 投資的價值。**利用創新的整合方式，徹底發揮互補性的投資，例如健全的驗證、票證核發、身分識別存取和管理，以及 SIEM 解決方案。

全方位的解決方案

CyberArk 企業密碼金庫是 CyberArk 特權帳號安全解決方案 (CyberArk Privileged Account Security Solution) 的一個元件，這是一套完整的解決方案，可主動防護、隔離、控管和持續監控虛擬和實體伺服器、資料庫、網路裝置、hypervisor、安全裝置、SaaS 和商務應用程式等上面的特權帳號。本解決方案包含 CyberArk SSH 金鑰管理器 (CyberArk SSH Key Manager)，這是用於防護和管理另一種強大特權憑證的 SSH 金鑰的解決方案。CyberArk 特權帳號安全解決方案的所有原件皆共用單一共有的基礎結構，讓客戶可以擴展解決方案，以滿足業務需求的變化。本解決方案內的產品可單獨進行管理，或是結合成一套整合性和全面性的特權帳號安全解決方案。

規格

- 加密演算法：
- AES-256 - RSA-2048
 - 硬體安全模組 (HSM) 整合
 - 通過 FIPS 140-2 驗證的加密編譯

存取和作業流程管理：

- LDAP 目錄
- 身分和存取管理
- 票證核發和作業流程系統

多語言入口網站：

- 英文、法文、德文、西班牙文、俄文、日文、中文

驗證方法：

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

監控：

- SIEM 整合、SNMP 陷阱、電子郵件通知

支援的管理裝置 (列舉部分)：

- 作業系統：Windows、*NIX、IBM iSeries、Z/OS、OVMS、HP Tandem、MAC OSX*、ESX/ESXi、XenServers
- Windows 應用程式：服務帳號包括 SQL 伺服器叢集服務帳號、排定的工作、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 相容的資料庫
- 安全裝置：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 合作廠商、CA
- 遠端控制監控：IBM、HP iLO、Sun、Dell DRAC、Digi*、Cyclades*、Fijitsu*
- 虛擬環境：VMware vCenter 和 ESX
- 儲存裝置：IBM、HP iLO、Sun、Dell DRAC、Digi*、Cyclades*、Fijitsu*
- 雲端應用程式：Facebook、Microsoft Azure Management、Amazon Web Services、Twitter*、SalesForce*、LinkedIn*、Microsoft 365*
- OT/SCADA：GE*、Industrial Defender*、RuggedCom*
- 通用介面：所有 SSH/Telnet 裝置、Windows 登錄檔、所有 Web 應用程式，例如：Facebook、WMI 遠端命令執行、資料庫資料表內儲存的密碼、設定檔 (一般、INI、XML)

* 此外掛程式可能需要進行客製化或是現場驗收測試。請諮詢 CyberArk 銷售技術單位取得詳細資訊。