CYBERARK

產品簡介

核心特權存取安全

高效率保護、監控及控制本地、雲端及混合基礎架構中的特權存取

規範

加密演算法：

- AES-256，RSA-2048
- HSM 整合
- 符合 FIPS 140-2 驗證的加密技術

高可用性：

- 支援叢集
- 多個災難恢復網站
- 整合企業備份系統

存取及工作流程管理：

- LDAP 目錄整合
- 身份識別及存取管理整合
- 簽核系統整合及工作流程系統

多語言入口網站：

- 英語、法語、德語、西班牙語、俄語、日語、中文（簡體及繁體）巴西葡萄牙語、韓語

身份驗證方法：

- 使用者名稱及密碼、LDAP、Windows 身份驗證、RSA SecurID、Web SSO、RADIUS、PKI、SAML、智慧卡

監控：

- SIEM 整合、SNMP Trap、電子郵件通知

下頁待續 ...

挑戰

在所有網路硬體及軟體中，特權帳號及特權帳戶存取是目前企業面臨的最大資安隱患。這種權限強大的特權帳號都隨處可見。如果使用得當，特權帳號可用於維護系統、協助實現自動化流程、保護敏感資訊並確保業務連續性。但如果不加以妥善管理，這些特權帳號可用於竊取敏感性資料，造成企業無法挽回的損失。

幾乎所有網路攻擊都利用特權帳號。心懷惡意的攻擊者會利用特權帳號來繞過資安系統、控制關鍵 IT 基礎架構並獲得機密業務資料及個人資訊的存取權。

在保護、控制及監控特權存取方面，企業面臨多方面挑戰，包括：

- 管理帳戶憑證。許多 IT 部門依賴容易出錯的手動的密集型管理流程來更替及更新特權憑證——這種方法效率低、風險大而且成本高。
- 追蹤特權活動。許多企業不能集中監控特權連線，因此面臨重大資安威脅，而且可能無法達到合規性要求。
- 監控及分析威脅。許多企業缺乏全方位威脅分析工具，不能預先識別可疑活動並採取措施來預防資安事件。
- 控制特權使用者存取。企業通常耗時耗力來有效控制特權使用者對雲端平台（IaaS 及 PaaS）、SaaS 應用程式及社交媒體等的存取；導致合規性風險及運營複雜性不斷增加。
- 保護 Windows 網域控制站。攻擊者可以利用 Kerberos 身份驗證協定中的弱點，冒充授權使用者並存取關鍵 IT 資源及保密資料。

解決方案

CyberArk 核心特權存取安全解決方案是業界最全方位解決方案，可有效保護、控制及監控本地、雲端及混合基礎架構中的特權存取。專為保護資安而精心開發的 CyberArk 解決方案可幫助企業高效率管理特權帳號憑證及存取權限、積極主動地監控特權帳號活動、智慧地識別可疑活動並快速應對資安威脅。

- 根據管理者定義的安全性原則來集中保護及控制對特權憑證的存取。自動特權帳號憑證（密碼及 SSH 金鑰）的更替可取代耗時而且容易出錯的手動密集型管理工作，有效保護本地、混合及雲端環境中使用的各種憑證。
- 隔離並保護特權使用者連線。監控及記錄功能使安全團隊可即時查看特權連線，自動暫停並從遠端終止可疑連線，保存全面可搜尋的特權使用者活動稽核記錄。對多種雲端平台及 Web 應用程式的原生支援提供統一的安全連線方法，可有助於提高運營效率。

規範

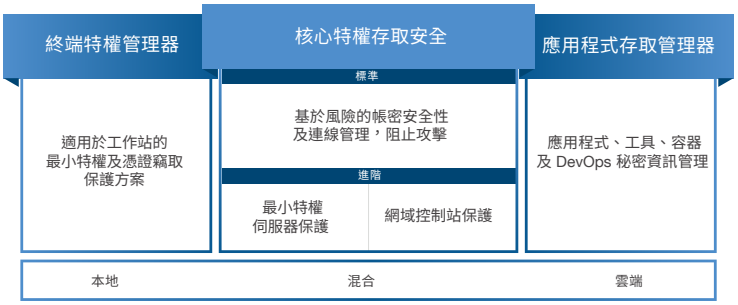
支援的可納管設備範例：

- 作業系統、虛擬化及容器：Windows、*NIX、IBM iSeries、Z/OS、OVMS、ESX/ ESXi、XenServers、HP Tandem*、MAC OSX*、Docker
- Windows 應用程式：服務帳戶，包括叢集中的 SQL 伺服器服務帳戶、Scheduled Tasks、IIS 應用程式集區（Application Pool）、COM+、IIS 匿名存取（Anonymous Access）、叢集服務
- 資料庫：Oracle、MSSQL、DB2、Informix、Sybase、MySQL 及任何符合 ODBC 要求的資料庫
- 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*
- 網路設備：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 廠商、CA
- 遠端控制及監控：IBM、HP iLO、Sun、Dell DRAC、Digi*、Cyclades*、Fijitsu* 及 ESX
- 設定檔（Flat、INI、XML）
- 公有雲端環境：Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）

* 外掛程式可能需要客制或實機測試。歡迎諮詢 CyberArk 銷售工程團隊，獲取更多資訊。

- **偵測、警示並回應異常特權活動**。該解決方案可收集多種來源的資料，並結合利用多種統計及確定性演算法來識別惡意特權帳號活動。
- **落實 *NIX 及 Windows 的最小特權存取**。該解決方案允許特權使用者從原生 Unix 或 Linux 連線中執行已授權的管理命令，同時避免不必要的 root 特權。該解決方案亦可以阻止及遏制對 Windows 伺服器的攻擊，以降低資訊被盜或被加密勒索的風險。
- **保護 Windows 網域控制站**。該解決方案在網域控制站上實施最小特權及應用程式控制，而且可以偵測正在進行的攻擊。該解決方案可防止假冒及非法存取，幫助偵測各種常用的 Kerberos 攻擊手段，包括萬用票證（Golden Ticket）、超雜湊傳遞（Overpass-the-Hash）及特權屬性憑證（Privilege Attribute Certificate，PAC）操作。

CYBERARK 特權存取安全解決方案



優勢

- **降低資安風險**。增強特權存取安全，保護對特權帳號密碼及 SSH 金鑰的存取，保護系統，免受惡意軟體及攻擊威脅；高效率偵測並應對可疑活動及惡意行為，防止非法特權帳號存取、假冒、欺詐及竊取。
- **降低營運支出及複雜性**。取代耗時且容易出錯的手動密集型管理流程。簡化操作，提高 IT 資安團隊的工作效率，使寶貴的 IT 人員可集中精力於策略性任務以支援核心業務活動。
- **改進監管合規性**。制定基於原則的特權存取控制措施，確保遵守政府及業界法規，向稽核機構輕鬆展示資安原則及流程，同時可產生詳盡的稽核記錄及存取歷史記錄以確保合規性。
- **縮短呈現價值的時間**。保護並繼續利用原有投資，利用可立即整合多種 IT 操作及資安系統的優勢，包括身份驗證系統、簽核流程解決方案、身份識別存取以及管理平台及 SIEM 解決方案。
- **增強可視性**。瞭解特權帳號的位置以及有權存取它們的使用者，並制定合理有效的特權帳號安全性原則，同時監控即時及過去的特權帳號活動。