核心特權存取安全性
(CORE PRIVILEGED ACCESS SECURITY)

有效保護、監控及控制跨內部部署、雲端及混合基礎架構的特權存取權限

規格

加密演算法：

- AES-256、RSA-2048
- 硬體加密器(HSM)整合
- FIPS 140-2 驗證加密

高可用性：

- 叢集支援
- 多個災難恢復站點
- 與企業備份系統整合

存取及工作流程管理：

- 輕型目錄存取協定(LDAP)目錄
- 身份及存取管理
- 工單及工作流程系統

多語系入口網站：

- 英文、法文、德文、西班牙文、俄文、日文、中文(簡體及繁體)、巴西葡萄牙文、韓文

驗證方式：

- 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 陷阱、電子郵件通知

接續下頁...

客戶的問題點

特權帳戶及其存取是組織目前所面臨的最大安全漏洞。這些權限強大的帳戶存在於網路上的每個硬體及軟體之中。如果運用得宜，特權帳戶會用於維護系統、促進自動化流程、保護敏感資訊，並確保業務連續性。但使用不當的話，這些帳戶可能用於竊取敏感資料，並對業務造成無法彌補的損害。

幾乎每個網路攻擊都會利用特權帳戶。不良行為者可利用特權帳戶停用安全系統、控制重要的 IT 基礎架構，並存取機密業務資料及個人資訊。

組織在保護、控制及監控特權存取上，面臨許多挑戰，包括：

- 管理帳戶憑證。許多 IT 組織依賴經常手動、容易出錯的管理流程來輪換及更新特權憑證——一種低效率、高風險且高成本的方法。
- 追蹤特權活動。許多企業無法集中監控及控制特權工作階段，使其業務曝露於安全威脅及合規性違規之下。
- 監控及分析威脅。許多組織缺乏全面的威脅分析工具，無法主動辨識可疑活動，並修復安全事件。
- 控制特權使用者存取。組織通常很難有效地控制特權使用者對雲端平台(IaaS 及 PaaS)、SaaS 應用程式、社群媒體等等的存取權限；造成合規風險及營運的複雜度。
- 保護 Windows 網域控制器。攻擊者可利用 Kerberos 身份驗證協議中的漏洞假冒授權使用者，並獲取對重要 IT 資源及機密資料的存取權限。

解決方案

CyberArk 核心特權存取安全性解決方案(Core Privileged Access Security Solution)是業界最完整的解決方案，可保護、控制及監控跨內部部署、雲端及混合基礎架構的特權存取權限。CyberArk 解決方案專為安全進行全新設計，可幫助組織有效管理特權帳戶憑證及存取權限、主動監控及控制特權帳戶活動、智慧識別可疑活動，並快速回應威脅。

- 根據以管理為基礎的安全策略，集中保護及控制對特權憑證的存取權限。自動特權帳戶憑證(密碼及 SSH 金鑰)的輪換省卻經常手動、耗時且容易出錯的管理工作、保護用於內部部署、混合基礎架構及雲端環境的憑證。

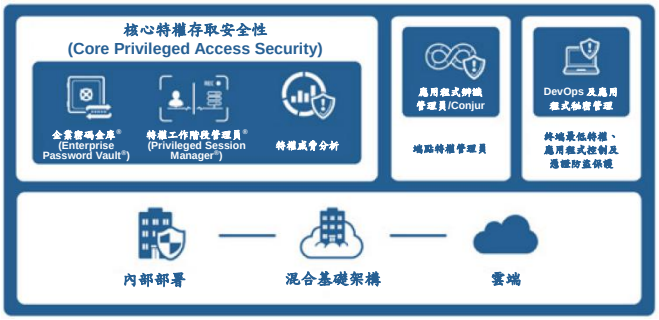
規格

支援的管理裝置模型：

- 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 Server 服務帳戶、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 及任何相容於 ODBC 的資料庫
- 安全設備：CheckPoint、Cisco、IBM、RSA 認證管理員、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 vendors、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)
- 公共雲端環境：Amazon 雲端運算服務(AWS)、Microsoft Azure、Google 雲端平台(GCP)

*此外掛程式需自訂或進行現場驗收測試。欲知更多資訊，請諮詢 CyberArk 業務工程人員。

- 隔離並保護特權使用者的工作階段。監控及記錄功能讓安全團隊能即時檢視特權工作階段、自動暫停及遠端終止可疑工作階段，並維護完整且可搜尋的特權使用者活動的稽核紀錄。對多個雲端平台及網頁應用程式的本地及透明存取，提供一項一致的安全措施，同時提高營運效率。
- 偵測、警示及回應異常的特權活動。此解決方案由多個來源收集資料，並應用統計及確定性演算法的複雜組合來辨識惡意的特權帳戶活動。
- 控制*NIX 及 Windows 的最低權限存取。此解決方案允許特權使用者從其本機的 Unix 或 Linux 工作階段中，執行經授權的管理命令，同時清除不需要的 root 權限。它也使組織能阻止及控制對 Windows 伺服器的攻擊，降低資訊遭竊，或被加密並勒索贖金的風險。
- 保護 Windows 網域控制器。此解決方案對網域控制器執行最低的特權及應用程式控制，並提供進行中攻擊偵測。它可防禦冒名頂替及未經授權的存取，並有助於防止各種常見的 Kerberos 攻擊技術，包括 Golden Ticket、Overpass-the-Hash 及特權屬性憑證(PAC)操控。



優點

- 降低安全風險。強化特權存取的安全性。保護特權帳戶密碼及 SSH 金鑰的存取。防護系統免於惡意軟體及遭受攻擊。有效偵測及回應可疑活動及惡意行為。防止未經授權的特權帳戶存取、冒名頂替、詐欺及盜竊。
- 降低營運費用及複雜度。減少經常手動、耗時且容易出錯的管理流程。簡化營運並提升 IT 安全團隊的效率。讓有價值的 IT 員工有時間專注於策略工作，以支持核心業務活動。
- 提升法規合規性。實施政策式的特權存取控制權，確保符合政府及產業法規。輕鬆向稽核人員展示政策及流程。產生詳細的稽核紀錄及存取歷史紀錄，以展現合規性。
- 加速獲利。保護並擴展先前的投資。利用與各種 IT 營運及安全系統的開箱即用整合，包括身份驗證系統、工單解決方案、身份存取與管理平台，以及安全性資訊及事件管理(SIEM)解決方案。
- 改善可視性。了解有哪些特權帳戶及擁有存取權限者。制定完整的特權帳戶安全性政策。監控即時及歷史的特權帳戶活動。