CYBERARK

DATA SHEET

特權帳號安全解決方案

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 設限、電子郵件通知

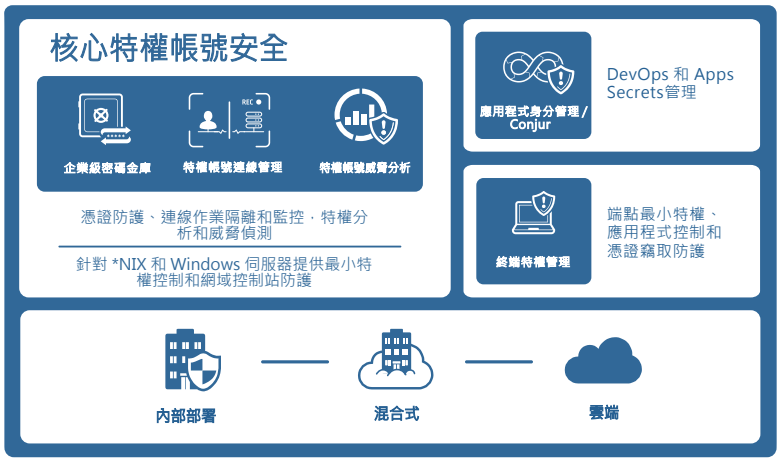
支援的受管理裝置範例：

- 作業系統、虛擬與容器：Windows、*NIX、IBM iSeries、Z/OS、OVMS、ESX/ESXi、XenServers、HP Tandem*、MACOSX*、Docker

下一頁接續...

特權帳號為「通往 IT 王國的重要鑰匙」，此類型帳號可以在整個企業、雲端和 DevOps 管道中完全控制資料、基礎架構和資產。

在特權帳號安全防護領域中，CyberArk 擁有廣泛的市場佔有率，是值得信賴的專家。專為安全防護全新設計的 CyberArk 特權帳號安全解決方案，透過 DevOps 管道，從每個端點為內部部署和雲端的所有系統提供全方位的解決方案。這套完整的特權帳號安全解決方案可立即供企業使用，具有防竄改性及可擴充性，適用於複雜的分散式環境，為進階的外部和內部威脅提供終極防護措施。



核心特權帳號安全性 (PAS)

憑證防護和管理

CyberArk 解決方案依據特權帳號安全原則，集中保護和控管對特權憑證的存取權。自動化的密碼和 SSH 金鑰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。

隔離、控制、監控和記錄特權連線

CyberArk 解決方案可隔離並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。該解決方案支持廣泛的連接方法，可為雲端系統管理員和特權業務使用者、Windows 用戶端 (例如 RDP、SSMS 等) 和原生指令列 SSH 裝置連接提供原生存取。監控和記錄功能使安全防護小組能夠即時查看特權連線、自動暫停並遠端終止可疑連線，並維持特權使用者活動全方位、可搜尋的稽核軌跡。

規格

- 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、BlueCoat*、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*、McAfeeNSM*
- 應用程式：CyberArk、SAP、WebSphere、 WebLogic、JBOSS、Tomcat、Cisco、OracleERP*、Peoplesoft*、TIBCO*
- 目錄：Microsoft、Oracle Sun、Novell、UNIX 供應商、CA
- 遠端控制和監控：IBM、HPiLO、Sun、Dell DRAC、Digi*、Cyclades*、Fijitsu* 和 ESX
- 組態檔 (一般、INI、XML)
- 公有雲環境：Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)

*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。

對惡意特權存取活動進行分析和警示

威脅偵測和分析使組織能夠偵測、警示與回應正在進行攻擊的異常特權活動。該解決方案從數個資料源收集目標數據，並執行複雜的統計及演算法。這讓組織能識別惡意特權存取活動，在攻擊生命週期中及早偵測到危害的跡象。

該解決方案使用機器學習演算法來檢查各個特權使用者、特權帳戶和系統活動的一般模式，以確定「正常行為」的基準。它將即時活動與基準進行比較，以識別異常的使用者行為和疑似攻擊的系統活動，其中包括可疑的憑證竊取、水平擴散和權限提升。

*NIX 和 Windows 的最小特權帳號控制

CyberArk 解決方案可讓特權使用者從自己原生的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，同時提供執行職務時所需的自由度。

此外，組織還能夠阻止和遏制對 Windows 伺服器的攻擊，以降低資訊遭到竊取或加密挾持以勒索贖金的風險。該解決方案透過連鎖特權管理、應用程式控制和目標憑證竊取防護來防止利用特權憑證的進階威脅，以阻止並遏制對關鍵伺服器的破壞性攻擊。

網域控制站防護

攻擊者可以利用 Kerberos 身份驗證協議中的漏洞來模擬特權使用者，取得對機密資料和關鍵 IT 資源的存取權限。CyberArk 提供輕量級 Windows 代理程式，可執行網路行為分析以偵測進行中的 Kerberos 攻擊。該解決方案提供全面的網域控制器防護，防止冒充和未經授權的存取。它在網域控制器上強制執行最小特權和應用程式控制，並有助於防止各種常見的 Kerberos 攻擊技術，包括 Golden Ticket、Overpass-the-Hash 和 Privilege Attribute Certificate (PAC) 操作。

DevOps 和 Apps Secrets 管理

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 (Application Identity Manager™) 會從應用程式和指令碼中刪除硬式編碼密碼和 SSH 金鑰，並使用安全的動態憑證加以取代，而對應用程式性能沒有任何影響。該產品旨在滿足高端企業對可用性和業務連續性的要求，即使在複雜的分散式網路環境中也沒問題。

保護整個 DevOps 管道中電腦和使用者所用之機密安全

CyberArk Conjur 是專為滿足原生雲端和 DevOps 環境之獨特基礎架構要求，而量身訂做的機密管理解決方案。該解決方案可幫助 IT 和資訊安全組織防護和管理整個 DevOps 管道中由電腦身分識別 (應用程式、微服務、CI / CD工具、API 等) 以及使用者所用的機密。

端點最小特權、應用程式控制和憑證竊取防護

在端點上強制執行特權安全防護

終端特權管理器 (Endpoint Privilege Manager) 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。應用程式控制與憑證竊取防護措施相互結合之下，能有效防止惡意軟體趁機入侵端點。