

竊取最高權限帳號 — 特權帳號安全

建立特權帳號安全存取與符規、適法性 | CyberArk PAS

企業密碼金庫 (EPV)

對特權帳號的保護、管理和稽核，自動化符合金檢內外稽核、ISO法規，並進行密碼自動變更。

特權連線管理器 (PSM)

對特權帳號的保護、管理和稽核，自動化符合金檢內外稽核、ISO法規，並進行密碼自動變更。

特權帳號威脅分析(PTA)

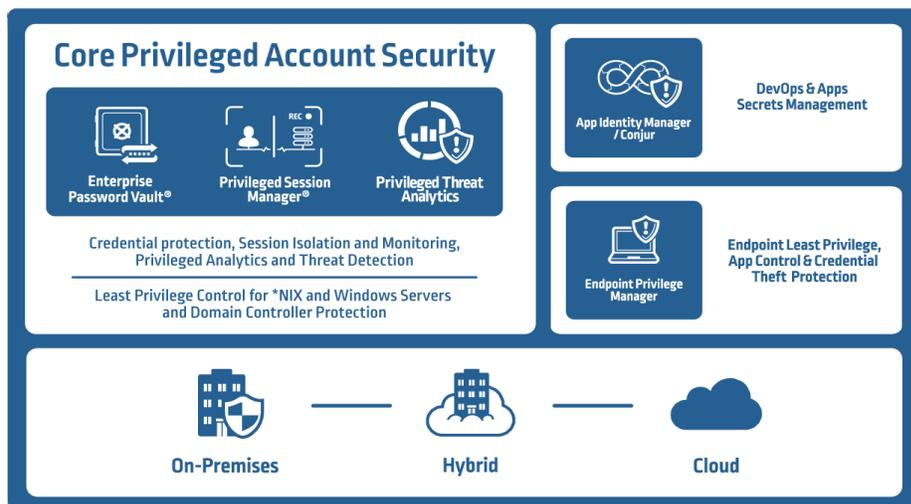
惡意特權帳號活動的分析與警示，可防範PTH攻擊、AD防護、DC控制存取控管。

應用程式身分管理器 (AAM)

保護、管理和審核嵌入式應用程序憑證。

本機帳號權限與應用程式控管 (EPM)

實現本機帳號「權限最小化」管理機制，避免來自於內、外部攻擊者植入不權軟體。防範ATP攻擊(進階持續性滲透攻擊)、零時差攻擊、加密勒索軟體/綁架CryptoLocker病毒。避免安裝違法軟體(如：綠色軟體、免安裝檔..等等)。



CyberArk Gartner 魔術象限領導者 —

CyberArk 實現特權帳號安全存取完整方案

特權帳號安全存取核心方案：

提供系統管理者安全連線與隔離機制，並保留完整操作軌跡以符合安控、稽核規範要求，一旦發現異常或不當操作，即時發送事件告警並阻止危害，保護所有系統之特權帳號與密碼不遭竊取。

應用程式內嵌密碼管控：

將原本寫死在程式碼或設定檔之「萬年不變的密碼」，安全存放在高度安全與強化之密碼金庫內，避免因AP密碼遭竊，取得資料庫登入權限，竊取機敏資料，造成無法復原之重大危害。

本機帳號權限最小化：

為避免來自內、外部攻擊者不當安裝軟體造成對內網各種危害，需建立本機帳號權限最小化與應用程式控制(應用程式白名單)；並保留臨時提權之彈性管理機制。

為何選擇CYBERARK?

CyberArk 是特權存取資安領域的全球領導者——特權存取安全是保護整個企業、雲端及 DevOps Pipeline 內資料、基礎架構及資產的 IT 安全性的關鍵層。

CyberArk 提供業界最方位解決方案，可降低特權憑證及安全憑證引起的資安風險。

公司深得全世界領先企業的信賴，包括 50% 以上的財經 500 大公司。這些公司利用 CyberArk 產品來防止外部攻擊者及內部惡意使用者所發起的攻擊。