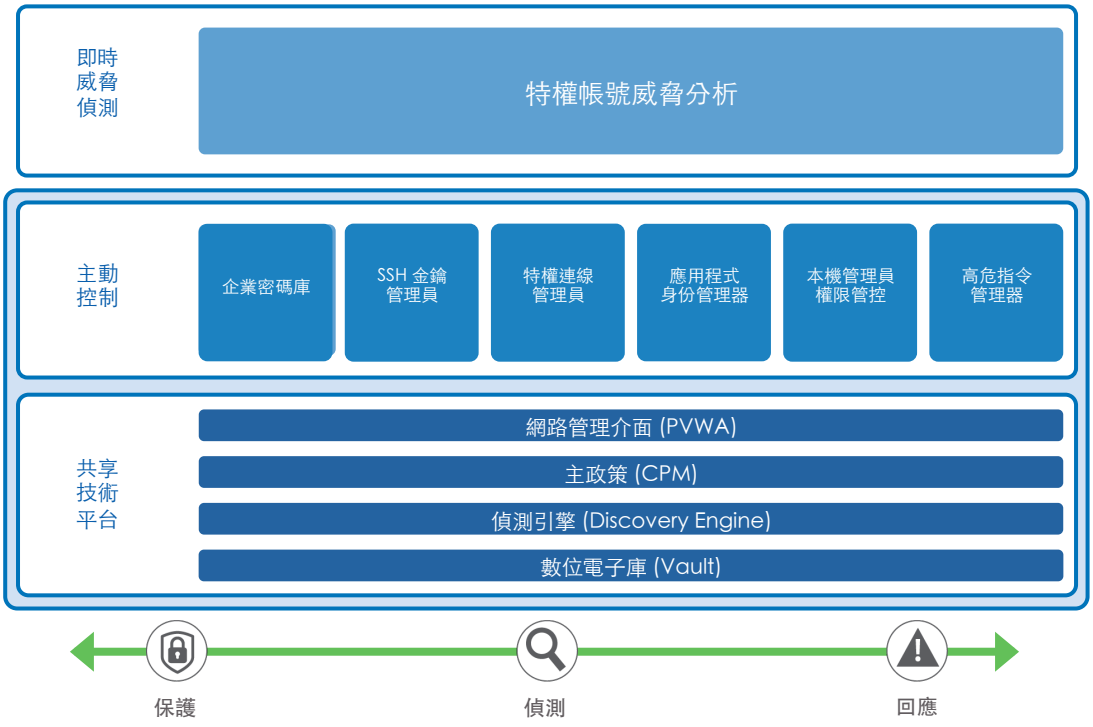
CyberArk 產品介紹
特權帳號安全解決方案

保護、監控、偵測、警告與回應特權帳號的完整解決方案

特權帳號是組織目前面臨的最大安全弱點。 一旦落入外來攻擊者或有惡意的局內人手中，特權帳號能讓攻擊者完全掌控組織的IT基礎設施，造成防護控制失效，竊取機密資訊，進行金融詐騙，並且擾亂運作。 幾乎所有攻擊事件都是透過竊取、濫用或盜用特權帳號憑證。 這種威脅日益嚴重，組織必須進行控制，主動保護，偵測和回應進行中的網路攻擊，以免重要系統遭受攻擊，被取得敏感資料。

CyberArk是值得信賴的特權帳號防護專家。 CyberArk專注於全面性資安防護的嶄新設計，發展出一個強大的模組技術平台，提供業界『唯一』最全面性的特權帳號安全解決方案。 每個產品都能分開或一起管理，因為這種連貫完整的解決方案，才能確保重要核心營運系統、資料庫、應用程式、虛擬機器管理員、網路裝置、資安設備…等等，不致遭受內外部的惡意攻擊行為而影響關鍵的營運與營收。 這種解決方案是專為自有系統、混合雲端和OT/SCADA環境設計。



為何需要CyberArk?
只有CyberArk能全面防禦進階攻擊及內部威脅，幫助客戶將風險減至最低，同時又能達成高標準的符規要求。

CyberArk在大規模分散及虛擬環境有更多的佈建案例，相較其他廠商，我們更有能力解決特權帳號所面臨的安全挑戰。

企業密碼庫® (Enterprise Password Vault®)
對特權密碼的保護、管理和審計

企業密碼庫可以防止惡意使用特權帳戶密碼，並針對易受攻擊的帳號帶來秩序和保護。企業密碼庫依據特權帳戶安全政策，確保特權密碼的安全，並控制哪些人可在何時使用哪些密碼。此自動化程序降低了費時且易產生錯誤的人工特權密碼追蹤和更新作業，使其得以很容易符合審計與合規性標準。

- 找出特權帳號和相關服務，並將這些帳號提供給數據庫(Digital Vault)作管理
- 依據政策，控制對特權帳號密碼的存取
- 針對密碼申請提供可客製化的作業流程，包括服務台開單系統的雙重控管與整合
- 具備點擊連結的能力，以防止終端使用者對密碼的暴露
- 依據需求執行自動密碼變更排程
- 提供一次性密碼的控制
- 與服務台和工單系統整合
- 以持續性基礎檢驗憑證，並於不一致性發生時自動回復並重設密碼
- 接收來自特權威脅分析(Privileged Threat Analytics)有關特權帳號可能遭受攻擊的警示，並自動輪轉受影響的密碼

關於力悅資訊

力悅資訊為企業資訊系統的專業代理商，提供資訊安全領域相關之解決方案，成立迄今已成功引進多種 IT 產品，並為大中華市場中不同規模的客群，提供專業分析、顧問與系統建置。秉持著「運用資訊技術幫助企業獲利」的信念，力悅資訊不斷引進全球最新的產品與觀點，導入 CyberArk 等管理系統，深入了解企業需求，藉此提供量身訂做的 IT 服務。

力悅資訊股份有限公司
聯絡電話：02-25071601
sales@cyberview.com.tw

特權連線管理員® (Privileged Session Manager®)

隔離、控管，以及即時的對話監控與記錄

特權期間管理員針對關鍵的Unix、Linux、和視窗系統的資料庫、虛擬主機、網路裝置、主機系統、網站、Saas和其他設施，監控特權使用者的存取和活動，以確保安全。它提供單一存取控制點，防止惡意軟體跑到目標系統，並記錄每一個鍵盤輸入和滑鼠點擊，以執行持續性的監控。
數位影像錄影提供特權期間完整的影像，對敏感事件具備搜尋、定位和警示的功能，而無需循序檢視所有的日誌。即時監控確保對特權存取的持續性保護，以及在發現可疑活動時即時介入並終止特權期間。特權期間管理員亦提供與第三方SIEM解決方案的完全整合，能夠針對不尋常的活動提出警示。

- 針對特權期間，建立單一控制點
- 保護特權密碼和SSH金鑰，使其不受高級的駭客攻擊，如：按鍵側錄和傳遞雜湊攻擊
- 控管特權期間，確保安全，防止惡意軟體或零時差攻擊繞過控管作業
- 將特權期間的監控擴展到具自定義連結點的應用程序客戶端、網路應用程序、或網站
- 建立具索引的、防竄改的特權期間記錄
- 提供命令行控制和本地SSH存取，同時仍以密碼或SSH金鑰提供對特權使用者的安全存取
- 將數據輸出到SIEM產品，用於對特權期間的鑑識分析
- 提供活動目錄橋接站台(AD Bridge)的功能，讓組織能夠集中式管理經由CyberArk平台與AD連結的Unix使用者和帳號

特權帳號威脅分析™ (Privileged Threat Analytics™)

惡意特權帳號活動的分析與警示

CyberArk的特權威脅分析是智慧型的安全解決方案，讓組織能夠偵測、警示、和回應異常的特權活動，表示正在進行的攻擊。此解決方案從不同來源收集特定目標的數據集，這些資料來源包括CyberArk數據庫(Digital Vault)、SIEM、和網路分接點/交換器。然後，此解決方案再使用複雜的統計和確定性演算法的組合，讓組織能夠辨識出惡意的特權帳號活動，得以在攻擊生命週期的初期就偵測到安全威脅跡象。

- 即時偵測並警示
- 能夠自動回應偵測到的事件
- 建立典型的特權用戶行為檔案
- 辨識出異常狀況，包括惡意特權帳戶活動和可疑的Kerberos通訊流量，顯示出進行中的攻擊
- 以自我學習的演算法，讓威脅偵測去適應不斷變化的風險環境
- 將事件之間予以關連，並指定威脅等級
- 開箱即用的整合能力，強化現行SIEM解決方案的價值
- 以用戶模式和活動為基準的資訊數據，改進審查作業

本機管理員權限管控 (Viewfinity)

最小權限執行，對於重要主機和使用者電腦的應用軟體控制，建立自動化學習白名單機制

Viewfinity讓組織能夠針對業務用戶和IT管理者實施最少特權政策，同時在需要執行獲授權的應用程式或指令時，可無縫地提升特權。這可幫助組織縮小被攻擊面，並將端點和伺服器有意或無意的損害降至最低，且可在視窗伺服器上區隔管理責任。互補應用控制可防止惡意應用程式滲透到環境中，且可允許未知的應用程式在安全且受限模式下執行。

- 讓組織可從日常業務用戶中移除管理者權限，而不會造成生產停頓
- 針對作業環境中超過90%的應用程式，自動建立特權提升和應用控制政策
- 以使用者角色來控制管理員特權的方式，在視窗伺服器上區隔責任
- 當需要執行獲授權的應用程式或指令時，依據政策無縫提升特權
- 防止惡意應用程式進入作業環境中並擴散
- 讓使用者可在“受限模式”下執行未知的應用程式，使其保持生產力
- 與Check Point、FireEye和Palo Alto Networks的威脅偵測解決方案整合，可對未知應用程式執行自動分析
- 辨識出作業環境中惡意應用程式的原始來源和所有的位置，以加速補救措施
- 支援三種佈署方式，包括伺服器、SaaS和微軟的GPO

應用程式身份管理器™ (Application Identity Manager™)

刪除嵌入應用程式憑證，改善安全與服規

應用程式身份管理員從應用程式和腳本語言中移除了硬編密碼和本機儲存的SSH金鑰。CyberArk的應用程式身份管理員確保實現你對可用性和業務延續性的高端企業需求，即使是在複雜的分散式網路環境中，也會符合這些需求。這產品移除了內嵌式的應用憑證，且通常不需要更改程式碼，對應用程式的效能也不會有任何影響。

- 用腳本語言更換硬編密碼和本地儲存的SSH金鑰，這腳本語言可讓應用程式隨時依據要求，從數據庫中擷取這些憑證
- 在伺服器上提供本地安全的快取暫存區，以獲致高可用性並維持高效能
- 提供執行中應用憑證的更換，且不會增加延遲效應。
- 依據實體特性，例如路徑或應用簽章，驗證要求憑證的應用程式
- 針對生產系統提供高可用性和高可靠度
- 針對應用伺服器上數據來源憑證的管理，提供獨特專利的解決方案

高危指令管理器™ (On-Demand Privileges Manager™)

Unix和Linux最小特權和應用控制

請求式特權管理器讓特權用戶可在其本機的Unix/Linux作業期間使用管理性指令，同時移除不需要的根目錄存取或管理員權限。這個安全和為企業準備的類似虛擬碼的解決方案提供所有超級用戶活動記錄的整合和相互關連，並與個人的用戶名連結，提供執行作業功能所需的自由度。執行細粒度存取控制，並持續性監控超級用戶依其角色和任務所下達的管理性指令。

- 以集中式的選項更換通用的虛擬解決方案，該選項提供細粒度特權控制和審計日誌的安全儲存
- 對審計人員提供安全的、受管理的、和受控制的超級用戶特權證明
- 提供詳細的審計蹤跡，顯示哪些個別特權提升到根部，是在何時，且理由為何
- 超級用戶特權的限制僅限於降低曝露於濫用或錯誤風險所需的管制
- 授權對最高權限根部的存取，讓使用者可依據工作流程直覺性地作業
- 把一個根帳戶和活動鏈接到個人的用戶名
- 以每一使用者和/或每一系統為基準，讓指令可列示於白名單/黑名單

SSH金鑰管理員™ (SSH Key Manager™)

安全捍衛,輪換和保護SSH金鑰

SSH金鑰管理員幫助組織防止對SSH金鑰未獲授權的存取，而這些金鑰常被Unix/Linux特權用戶和應用程式用來驗證特權帳號。SSH金鑰管理員依據特權帳戶安全政策，輪轉特權SSH金鑰，確保其安全，並管制及監控對受保護的SSH金鑰的存取。此解決方案讓組織能夠獲得對SSH金鑰的控制，而這些金鑰提供了對特權帳號的存取，但卻經常疏於管理。

- 將SSH私鑰安全儲存於數據庫(Digital Vault)並控管對這些金鑰的存取
- 依據組織政策，自動輪轉SSH公私金鑰組
- 支援並實施強大的存取控管，以驗證和管理提升特權的請求
- 針對SSH金鑰的進出，堅持預設的政策
- 讓管理者能夠依據使用者和應用程式，追蹤SSH金鑰的使用，並提出報告

關於 CyberArk

CyberArk 是唯一一間高度專注於去除針對性威脅的網路安全公司，這類網路威脅意圖在於打通直達企業核心的途徑。

CyberArk 致力於在這些攻擊使企業停擺之前阻止它們，並受到世界領導企業的委託 – 包含 Fortune(財富)雜誌100強企業中的40家企業 – 保護其最有價值的資訊資產、基礎設施和應用程式。

想知道更多的資訊，請參考

http://www.cyberview.com.tw/
02-2507-1601
sales@cyberview.com.tw