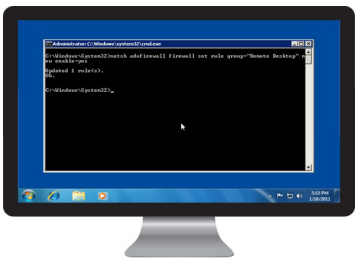
特權連線管理員 (Privileged Session Manager)

隔離、監控和管制特權帳號連線以縮減威脅的範圍，快速偵測和回應可疑的活動，並且確認合規性。



CyberArk 特權連線管理員可直接將使用者連接到目標系統，在不將特權憑證暴露給使用者或其端點下，監控和記錄連線。

挑戰

特權帳號可存取關鍵系統和機密商業資訊，如果遭到濫用，特權帳號也可能造成有毀滅性之虞的損害。若要保護企業的核心，企業應對特權帳號的活動採用「零信任」(Zero Trust) 機制。

這種機制包括主動監控和記錄特權連線，以協助防範居心不良的內部人員、第三方使用者或外部攻擊者破壞系統，或未經授權而存取機密資料。企業也應該隔離特權連線，以確保惡意軟體無法從使用者端點擴散至關鍵的系統。若沒有主動管理特權連線，企業將面臨多種風險，包括：

- 對關鍵系統造成有意或無意的破壞。使用者更容易在僥倖的心態下濫用自己的特權。此類濫用，不論是惡意、不小心或是單純為了方便，都會對企業造成巨大的損害。
- 增加受到高階威脅的機會。當使用者直接連線至遠端系統上的特權帳號時，特權憑證就暴露在使用者所在的端點，而可能在該處被駭或被重複利用以獲得未經授權的特權存取機密系統。
- 高管理成本及增加資料洩漏的風險。若無法輕鬆搜尋、找出和審查可疑活動，取證分析可能非常困難且耗時。人工流程既緩慢且管理成本高，使事件應變人員難以迅速在損害擴大前阻擋攻擊者。
- 法規稽核失敗和高額的罰鍰。數項法規規定企業必須追蹤和監控所有包含機密和受監管資料的系統的存取。無法監控此類存取可能導致稽核不合格、處罰和高額罰鍰。

解決方案

CyberArk 特權連線管理員 (CyberArk Privileged Session Manager) 是關鍵系統的中央存取控管點，可以讓企業隔離、監控和控管所有特權連線活動。以安全為重建置而成的 CyberArk 特權連線管理員已獲 Common Criteria 和 UC APL 認證。本解決方案可擴充以滿足大型企業的需求，同時又能便利使用者。

CyberArk 特權連線管理員可以讓企業：

- 隔離關鍵系統。充當安全代理伺服器，本解決方案可以將端點從目標系統分隔，並且隔離特權使用者的連線。如此有助於限制攻擊者在網路內橫向移動的能力，並且可以防止惡意軟體從終端使用者裝置擴散至目標系統。
- 監控和記錄特權連線。本解決方案能夠讓企業即時地監控特權連線活動，讓安全人員可以偵測特權帳號的濫用；也可以記錄特權使用者的活動，並且產生詳細的稽核記錄檔和視訊錄影。在與 CyberArk 特權帳號威脅分析 (CyberArk Privileged Threat Analytics) 整合時，可針對已記錄的連線指派風險值評分，協助安全和稽核人員決定該對哪些連線優先審查。
- 迅速對威脅作出反應。稽核記錄檔和記錄會安全地儲存在抗竄改的數位金庫中，以防範惡意軟體使用者修改自己的活動蹤跡。記錄檔資料可以即時傳送至 CyberArk 特權帳號威脅分析，讓安全人員能夠自動偵測高風險的活動，並且快速地對可能的事件作出反應。必要時，安全人員更可以從遠端終止可疑的連線以阻斷潛在的攻擊。
- 控管第三方對特權帳號的使用。第三方使用者，例如合作廠商或顧問，通常與企業間並沒有直接建立的信賴關係，並且一般是從未受管理的端點存取關鍵系統，而造成更高的安全風險。為了減緩此類風險，CyberArk 特權連線管理員讓企業隔離並監控第三方連線的活動，以迅速識別未經核准而可能造成損害的活動。

- 防止對關鍵系統的直接存取。本解決方案可以設定成關鍵系統的唯一存取點，規定使用者必須先通過 CyberArk 解決方案的驗證後，才能存取目標系統。由於監控是在代理伺服器上進行，而非透過目標系統上的代理程式，因此有經驗的使用者也無法停用控管機制。並且，若與 CyberArk 企業密碼金庫 (Enterprise Password Vault) 整合，企業就可在不將目標系統的憑證暴露給使用者或其裝置下，提供特權存取。
- 在不影響使用者體驗下提供安全的特權存取。一旦通過 CyberArk 解決方案的驗證，使用者只要按一下滑鼠就可以直接存取目標系統。CyberArk 解決方案讓使用者從自己的原生環境存取目標系統，藉此保有使用者體驗。
- 符合法規規範。CyberArk 特權連線管理員協助企業達到法規強制主動監控和記錄特權連線的規定。為確認符合相關法規，可授權稽核人員存取唯讀連線的稽核記錄檔和視訊記錄。

全方位的特權帳號安全性解決方案

透過隔離、監控和控管特權活動，企業可以縮減攻擊面、偵測高風險的特權使用者活動並作出反應，以及確實遵守業界法規。CyberArk 特權連線管理員可與

CyberArk 特權帳號安全解決方案 (CyberArk Privileged Account Security Solution) 完美整合，讓企業能夠從單一共同的基礎結構保護特權帳號憑證、控管和監控使用者活動，以及快速偵測潛在的威脅並作出反應。

規格

可連線至：

Unix、Linux 和 Network 裝置：

- SSH
- Telnet

Windows：

- Windows RDP
- Windows Remotely Anywhere
- Windows RAdmin 工作階段

IBM：

- OS/390 (Z/OS)
- AS400 (iSeries)

網站和應用程式：

- 網站架構應用程式 *
- SAP*

資料庫：

- Oracle
- Microsoft SQL Server

虛擬環境：

- vSphere / vCenter / ESX hosts
- HyperV 主控台

雲端、SaaS 和社群媒體：

- Amazon (AWS)
- Azure
- Office365*
- Salesforce*
- Facebook*
- Twitter*
- 和其他等等 ...

遠端存取：

- Citrix*
- VNC

儲存裝置：

- NetApp*

通用連接器：

- 所有其他平台監控功能皆可透過通用連接器輕易加入 *

* 此外掛程式可能需要進行客製化或是現場驗收測試