CYBERARK 特權帳號安全解決方案第 10 版快速參考指南

CYBERARK 特權帳號安全解決方案第 10 版簡介

CyberArk 特權帳號安全解決方案第 10 版是徹底突破舊規的創新解決方案，採用自動化與「API 優先」(API first) 方法，可簡化我們解決方案的導入與部署，並且將「模擬攻擊者思維」理念直接納入到產品設計中。

CyberArk PAS v10 提升使用者體驗，採用更佳的的使用者介面，簡化功能單元來提供現代化的使用者體驗。我們正協助客戶實現特權帳號管理任務的自動化與簡化，並透過 REST API 實現與現有資安、維運及 DevOps 工具的無縫整合。在雲端方面，我們進一步增強對 3 大主要雲端平台的支援，包括 AWS、Azure 與 Google Cloud Platform。

我們還增加與 AWS CloudWatch 的整合，使資安團隊可以運用自動啟動功能 (Automatic on boarding) 來節省時間並降低不受管理的 SSH 金鑰所引發的風險。

此外，我們還大幅增強終端特權管理器，包括提供一種新的應用程式風險分析服務來協助偵測惡意應用程式。我們最先進的應用程式控制功能現在可以將我們的終端保護解決方案應用到 Mac 平台上。最後，我們還將來自 CyberArk 研究實驗室團隊的一些憑證或帳密竊取攻擊向量研究成果直接納入到產品設計中。

市場觀察

特權無處不在：從存取公司內與託管在雲端中應用程式的 IT 管理者、終端使用者與機器身份到目前很多以 DevOps 驅動的企業中所採用的自動化解決方案。保護特權是資安團隊需要解決的優先問題，因為攻擊者在時間與資源方面有著明顯的優勢。80% 的安全性漏洞涉及特權憑證或帳密。[1]

在雲端中使用相同的憑證或帳密來存取多種運算、儲存與應用程式執行個體，被認為是最大的公有雲安全性漏洞。[2] 特權的盜竊與濫用導致的資安事件已經造成企業無可挽回的嚴重業務損失。為了降低風險，企業必須「模擬攻擊者思維」，消除所有特權攻擊可能性。目前只有 25% 的企業為 DevOps 制定並實施特權帳號策略；而對於雲端，這一比例只有 50%。[3]

[1] The Forrester Wave™：特權身份管理，2016 年第 3 季度，Andras Cser，2016 年 7 月 8 日

[2,3] 2018 年 CyberArk 全球進階威脅趨勢調查

本版本包含什麼新功能？

- 適合終端使用者與稽核人員的全新使用者介面
- 「API 優先」策略
- 雲端：支援 Google Cloud Platform 與 AWS CloudWatch
- 終端特權管理器：應用程式風險分析服務、Mac 桌面應用程式控制、伺服器原則範本、獨立運作的代理程式 (loosely connected agent)、防止憑證或帳密竊取的改進
- 特權連線管理器：外部連線記錄儲存 (確保 GDPR 合規性)、HTML5 支援、特權任務自動化與管理支援
- 下一代的集中原則管理器 (Centralized Policy Manager

詳細資訊

適合終端使用者與稽核人員的全新使用者介面

我們改進 PVWA 使用者介面 (UI)，可以為終端使用者與稽核人員提供更好的使用者體驗。此全新的 UI 包括現代化圖形與功能單元，可以提高我們解決方案的簡便易用性。這些提升可以簡化日常管理任務，協助將管理者的工作效率提高最多 10 倍，同時將 IT 稽核團隊的特權連線審核效率提高 5 倍。

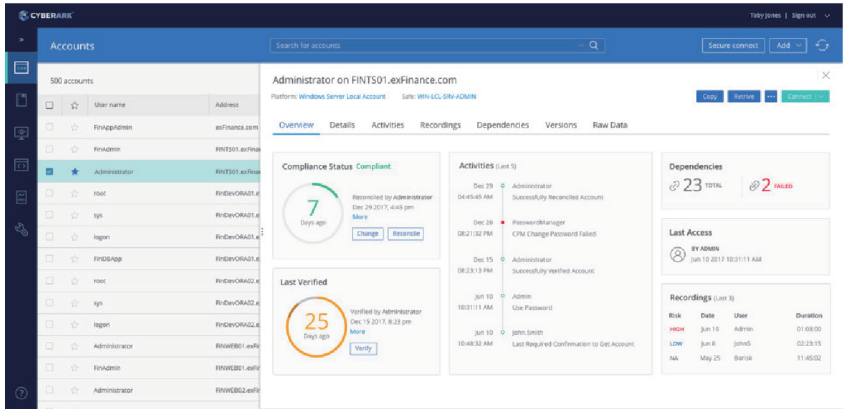

圖 1: CyberArk 的全新使用者介面可協助更輕鬆地瀏覽工作流程、直觀地顯示風險、監控特權活動並遵守稽核與原則要求。

「API 優先」策略

本版本運用 REST API 提供全面的自動化功能。我們全新的「API 優先」策略使客戶可以自動完成常見的特權帳號管理任務並輕鬆整合現有的資安、維運與 DevOps 工具。對 REST API 的支援可協助自動完成帳號工作流程、權限分配及許多其它 PAS 管理任務。這種增強功能可以根據原則實現自動帳號啟用，將管理者的工作負擔減輕 90%。此外，我們對 REST API 的支援讓客戶可以透過整合多種 ISV 解決方案來整合複雜的生態系統。

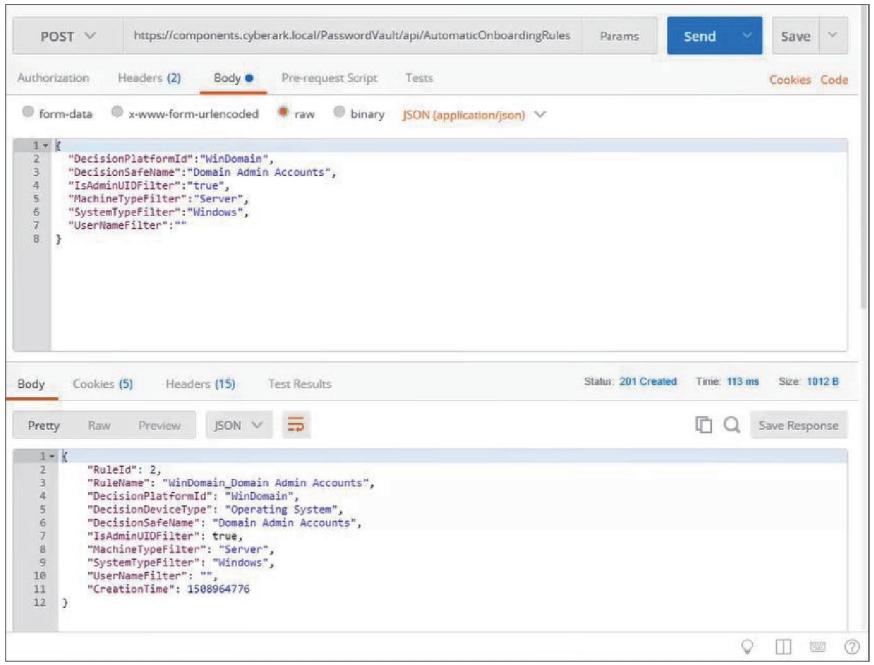

圖 2：CyberArk 的 REST API 可協助 IT 運營團隊縮短完成許多不同特權管理任務的時間。

雲端

本版本可透過支援廣泛的雲端平台選擇來簡化客戶的雲端之旅，包括：Amazon Web Services (AWS)、Microsoft Azure 與 Google Cloud Platform (GCP)。CyberArk 支援所有主要的雲端平台並繼續加強對這些雲端平台的支援。

在 Amazon 中，CyberArk 現在可以自動啟用新建立實例的 SSH 憑證或帳密。此種靈活的架構利用 AWS CloudWatch 來自動完成啟用操作，不論建立實例的方式，從主控台或腳本、DevOps 工具或 AWS Auto Scaling。整合 AWS 使資安團隊可以透過自動啟用功能來節省時間並且降低不受管理的 SSH 金鑰所引發的風險。

圖 3：整合 CyberArk 與 AWS CloudWatch 可以自動完成啟動工作，在雲端中降低不受管理的 SSH 金鑰引發的風險。

終端特權管理器

終端特權管理器包含全新的威脅偵測功能，在主控台上提供新的風險視窗 (framelet)，顯示憑證或帳密可能被盜的用戶帳號的數量。我們還對 Windows 及瀏覽器所儲存的帳密之竊取防護中增加兩項新實驗性威脅偵測原則 (beta rule)：

- 防護對 Windows 帳密管理器中的帳密竊取
- 防護對 Microsoft Internet Explorer 與 Edge 帳密竊取

而用於伺服器的立即可用的原則範本則新增可以在不同類型的伺服器中簡化原則的建立與部署。這是一種獨特的特權管理方法，可以協助企業在特定伺服器上更好地管理 IT 管理者職責的區分，且不需用任何特權帳號就可以賦予更大權限給特定伺服器管理應用程式。

本版本新增 Mac OS 平台的應用程式控制功能。藉由可以控制 Mac 平台上執行的應用程式，IT 與資安團隊將能夠更加有信心完成整個企業部署工作。

終端特權管理器現在可以提供獨立運作的代理程式，該代理程式在安裝與啟動時知道需要套用哪些原則而不需要與伺服器進行通信。如此可以更好地支援氣隙 (airgap) 網路與核電及工業控制環境 (這種環境中不可能建立對外連線)。此外，CyberArk 現在還在非持久性 VDI 設備中提供支援。這種改進主要體現在性能與授權方面，推薦用於不斷建立與拆除終端設備的客戶。

最後，CyberArk 現在可以為終端特權管理器伺服器提供一種風險分析服務，協助伺服器版與 SaaS 版客戶可支援內網與外網終端設備的應用程式風險分析服務。透過在雲端中利用基於檔案的機器學習，該服務可以在內外網完成惡意軟體偵測與威脅風險評分。此外，該服務可以增強並實現及時、正確的特權與應用程式控制原則決策。

特權連線管理器

本版本中的特權連線管理器新增多種新的增強功能。特權連線管理器現在可以將記錄的連線與文字檔案保存在外部，而不是將檔案保存在 CyberArk 數位金庫 (CyberArk Digital Vault) 中。這與歐盟 GDPR (文件 44-47) 中有關檔案儲存與地區間傳輸相關的具體要求一致。

特權連線管理器現在可以支援 HTML5，實現更簡單的通信來提高安全性，簡化工作流程並提供更加直觀的體驗；終端使用者可以直接選擇連線帳號 (而非下載 RDP 檔)，然後瀏覽器開啟新的索引標籤 (tab)，就可以建立連線。

最後，我們現在還可以透過 Universal Connector 來實現對多種特權任務的自動化與管理。如此可以降低有意或無意地破壞關鍵系統的風險，協助運營團隊提高工作流程效率與工作效率，例如：開始與終止服務、管理資料庫物件、維護與佈建任務等。

下一代集中原則管理器 (CENTRALIZED POLICY MANAGER)

下一代集中原則管理器大幅度增強性能與延展性，可以將集中原則管理器查詢金庫的次數減少 95%，將查詢金庫所需的時間縮短 85%。此新版本實現最佳集中原則管理器運作效能，可以安排任務優先順序分配、更快回應的平台組態設定、更有效的交易處理與搜尋，而且需要的重啟次數更少。利用這些增強功能大幅度減輕金庫負載，可以達到更高的延展性。