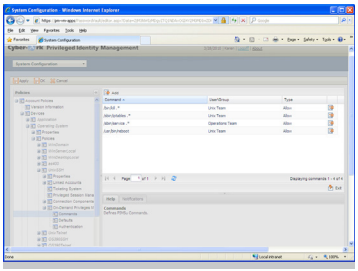
隨選特權管理器 ™ (On-Demand Privileges Manager™)

隨選特權管理器 (On-Demand Privileges Manager) 是針對 Unix / Linux 設計，以嚴密控管和監控超級使用者的統合式存取控制解決方案。



超級使用者和其他類型特權帳號的單一存取點，提供容易使用的網頁介面，管理和定義全企業的所有特權帳號政策。

挑戰

無論是故意或是意外，當企業最關鍵的系統和資料遭到濫用時，不僅會對營運、業務持續性和財務造成重大的衝擊，也會嚴重損害企業的商譽。

掌控即便最高權限的使用者

在許多企業中，IT 管理員、應用程式開發人員、資料庫管理員和其他人都具有永久、持續且匿名的超級使用者特權。對業務關鍵系統和資料具備某種層級的特權存取雖然是必要的，但是許多使用者擁有的特權都遠超過日常職務所需。

在 Unix 和 Linux 環境下，企業經常為了能有效控管和稽核超級使用者對儲存機密資料和業務關鍵應用程式的系統存取而大費周章。企業因而面臨下列風險：

- 無法遵守法規規範。諸如 PCI DSS、Sarbanes-Oxley 和許多其他法規標準都要求對超級使用者進行更嚴密的控管和追蹤。
- 營運複雜性。有多個不具備命令控制特權的超級使用者可能會導致更多人為錯誤，而降低任務關鍵系統的可靠性、可用性或效能。

安全、業務和營運需要之間的取捨

雖然很多企業使用 sudo 控制 Unix/Linux 系統上的特權，但這個工具會造成營運上的重大挑戰，特別是大型環境下。此外，sudo 缺乏管理者和稽核人員需要的報表機制，而且因為系統的稽核記錄檔是儲存在每台機器的本機內，這些記錄檔很容易遭到具有根權限之使用者的人為竄改。

解決方案和關鍵優勢

CyberArk 隨選特權管理器 (CyberArk On-Demand Privileges Manager) 是專為企業集中提供在 Unix/Linux 環境下統合管理和控制超級使用者特權所設計。

降低內部威脅：嚴格存取控管

控制 Unix/Linux 超級使用者可以使用的命令，以降低內部濫用或出錯的風險。

符合規範、萬無一失：客製化稽核和記錄

將根帳號活動與個人使用者名稱鏈結，以稽核根特權的個別使用狀況，並且確保使用者對自己的活動負責。報告哪個超級使用者存取過哪些系統，記錄更高權限的超級使用者連線期間的活動，並且將此稽核歷史記錄儲存在抗竄改的 CyberArk 數位金庫 (CyberArk Digital Vault) 內。

執行業務更順暢：特權帳號和使用者管理一站到位

CyberArk 的整合式解決方案透過集中化超級使用者憑證和特權的管理，以及集中且可靠地報告超級使用者活動，協助企業提升效率。

CyberArk 隨選特權管理器在於協助企業：

- 將不受控存取根帳號相關的資料洩漏和中斷降至最低。
- 透過可靠地稽核超級使用者的存取、特權和活動達到法規規範。
- 以集中化的解決方案取代孤立的 sudo 工具，以控制和稽核超級使用者對 Unix/Linux 系統的存取。

特點

透過網頁架構的入口網站提供 IT 管理員和稽核人員專用的單一存取點，使用者可以管理和定義共用帳號的政策以及搜尋已記錄的連線。

- 使用超級使用者帳號時的嚴格存取控管包括授予根權限和其他超級使用者執行特定命令的權限。
- 與 CyberArk 特權帳號安全解決方案 (CyberArk Privileged Account Security Solution) 的立即整合提供了一套可防護、控制和持續監控特權帳號的全方位解決方案。

- 容易使用的網頁介面可讓您輕鬆地瀏覽和搜尋所有特權帳號網域，還有直覺化的逐步引導式作業流程定義畫面。
- 按鍵和命令輸出記錄 提供稽核和報告。
- 營運和稽核報告的中央報告引擎提供所有超級使用者活動之統合且互相關聯的稽核記錄檔，並與其他特權帳號管理活動整合。
- 與 SIEM 產品完美整合透過深入掌握特權帳號活動 ·而充實全面性的系統稽核和事件管理。
- 企業就緒而能與企業現有的基礎結構輕鬆整合，並且可隨著企業的成長擴充規模。
- 安全的抗竄改金庫是專為保護特權帳號資訊而設計，包括政策、憑證、稽核記錄檔和連線記錄。

CyberArk 終端特權管理器 (CyberArk Endpoint Privilege Manager)

Windows 桌面和伺服器的管理員特權散佈整個企業。但是，標準使用者並不需要時時使用管理員特權來進行日常工作。CyberArk 終端特權管理器可控管端點上的特權並且在攻擊初期加以遏止。

使用 CyberArk 終端特權管理器，企業就可以在 Windows 環境下實施「最小權限」政策，讓使用者以標準使用者模式工作，並且以受控制和預先定義的方式提升個別應用程式的權限。企業因而能夠在享有成本效益和保持使用者的生產力的同時提升安全性。

規格

加密演算法：

- AES-256、RSA-2048
- 硬體安全模組 (HSM) 整合
- 通過 FIPS 140-2 驗證的加密編譯

存取和作業流程管理：

- LDAP 目錄
- 身分和存取管理

作業系統驗證 (SSO)：

- LDAP/AD

監控：

- 硬體安全模組 (SIEM) 整合
- SNMP 陷阱
- 電子郵件通知

保留所有權利。未經 CyberArk Software 事前書面同意，本文件之任一部分皆不可以任何形式或方式重製。CyberArk®、CyberArk 標誌和其他上列之貿易或服務名稱皆屬 CyberArk Software 在美國和其他司法管轄區的註冊商標（或商標）。其他貿易和服務名稱之所有權屬於各自所有權人。U.S., 12.16 Doc。150

CyberArk 確認本文件內之資訊於出版日期之時正確無誤。

所提供之資訊不提供任何明示、法定或是默示之保證，如有變更，恕不另行通知。

©CyberArk Software Ltd. | cyberark.com