

Privileged Account Manager

有了 Privileged Account Manager，貴組織就可以控制和監控資料庫、應用程式和雲端之間的授權使用者存取。

產品綜覽

據專家估計，約半數的資安侵害事件出自於組織內部。當員工擁有過多存取權限，超出其實際所需，內部威脅就會變得特別嚴重。無論權限濫用事件是員工所為，還是網路犯罪利用內部人員存取身分證明來存取公司的 IT 網路，管理這種風險的最佳方式仍然是密切控管和監控高權限使用者的存取行為，例如超級使用者和資料庫管理員等等。

有了 NetIQ Privileged Account Manager，不再需要將帳戶身分證明交給整個管理團隊的所有人員。該系統會使用集中化規則來委派管理存取權限。您可以設定讓這些規則依照全方位的「人、事、地、時」條件檢查使用者名稱、輸入的指令、主機名稱和時間，判斷要允許或拒絕該項使用者活動。透過這種方式管理權限，即可控制使用者有權執行的指令，以及執行的時間與位置。

Privileged Account Manager 內建企業身分證明保管庫，或稱為加密密碼「保管庫」，能夠安全儲存所有系統、應用程式和資料庫密碼。企業身分證明保管庫能協助您集中管理公司的高權限帳戶，並提供直觀的介面讓高權限使用者借出與交還密碼。同時，它也能為應用程式（如 SAP 系統）、資料庫（如 Oracle DBMS）以及雲端服務（如 Salesforce.com）支援更多樣化的高權限帳戶。

Privileged Account Manager 具有業界僅有的圖形化拖放式介面，可簡化規則建立程序，幾乎能完全免除複雜的手動撰寫程序檔作業。整合式測試套件工具則可讓您先行制訂並測試新的規則組合，再將組合套用於線上用途。

Privileged Account Manager 採用獨特的風險分析引擎，在輸入每個指令時就會進行分析，並根據所要執行的指令、執行該指令的使用者以及位置，為其指定 0 至 9 的風險等級。高風險指令以紅色標示；低風險指令以綠色標示。介於兩者之間的風險則以不同色調標示，方便管理員立即辨識出可能造成安全風險的事件。此外，您也可以透過搭載播放功能的直覺式介面，檢視任何記錄的按鍵動作活動。如果某個事件需要進一步分析，工作流程程序會將該事件呈報給可立即採取行動的適當管理員。

Privileged Account Manager 可延伸這項風險式活動管控功能，在授權使用者工作階段期間提供自動化的規則強制執行功能。若使用者執行存取機密資料或中斷服務等高風險活動，則管理員可設定 Privileged Account Manager 自動中斷工作階段，或撤銷使用者存取任何高權限帳戶的能力。

系統要求

如需 Privileged Account Manager 支援平台的詳細清單及安裝需求，請參閱[此處](#)的安裝指南。

與我們聯絡：

www.microfocus.com

喜歡本文內容嗎？歡迎分享。



主要優點

在您的整個異質環境中，控制並監控未獲授權且未受監控的授權使用者存取。

- 由單點集中管理安全規則。
- 持續協助遵循內部規則與外部法規。
- 幾乎不需要複雜的手動程序檔。
- 透過集中管理，在整個環境中強制執行一致的規則。
- 落實、分析與報告存取作業，以符合隱私權法律和法規。

主要功能

從單一位置設計、設定、測試並部署整個環境的一套高權限帳戶管理解決方案。

- 使用企業身分證明保管庫安全保管密碼
- 適用於使用者、工具和應用程式的資料庫授權帳戶監控功能
- 風險式工作階段控制，能夠自動終止工作階段或撤銷存取
- 作業系統的遠端工作階段建立與控制
- 可快速辨識高風險使用者的風險設定
- 以潛在威脅分析為基礎的智慧風險評等



圖 1. 指令控制主控台可讓管理員保護和控制使用者指令。

主要獨特優勢

建立目前最全面的稽核追蹤。透過 Privileged Account Manager，您可以藉由完整按鍵動作登入與影片擷取功能稽核，針對所有身分證明式環境來稽核所有使用者活動，其中包括應用程式（如 SAP 系統）、資料庫（如 Oracle DBMS）以及雲端服務（如 Salesforce.com）。

針對特定存取事件，稽核員可播放整起事件的每個按鍵動作，檢視分色標記的各行細節，並對每項事件套用「已授權」或「未授權」狀態。

欲進一步瞭解 Privileged Account Manager 或試用，請造訪此處。



網址：<https://www.microfocus.com/zh-tw>

電話：+886-2-5592-4949

電子信箱：taiwan.sales@microfocus.com