MAVIS

PNTL

混合多雲特權管理平台

挑戰

資產管理

企業在提供內部和外部網路服務的過程中，不可避免地需要建立相應的伺服器來滿足服務需求。根據公司的政策選擇，可能會使用虛擬機器的雲端服務，也可能建立本地資料中心，甚至可能會採用混合多雲的方式。這些方法中的任何一種都需要 IT 人員來維護額外的記錄並管理使用者權限。這不僅增加了工作量，而且由於跨平台、跨機器操作以及需要第三方工具而增加了出錯的可能性。此外，如果這些記錄未加密，則會增加公司面臨漏洞的風險。由於缺乏身分控製或資料洩露，這可能會給公司帶來重大損失。

身分權限

身分和權限管理為公司使用的資訊系統帶來重大安全風險。實現綜合管理通常需要大量的人力和周詳的規劃，以滿足公司的要求和適合營運商的營運環境。如果沒有公司或管理員的定期維護，系統身分或權限很容易超出業務流程的要求。在這種情況下，如果這些帳戶被盜或洩露，就可能被用來竊取機密信息，給公司造成不可挽回的損失。成功的駭客攻擊通常涉及濫用或破壞特權帳戶，這凸顯了保護身分和特權的重要性，這是公司需要關注的關鍵方面。

操作日誌

目前無論是本地資料中心或雲端服務的操作都受到工具限制，難以有效記錄操作日誌和使用操作的過程。因此，需要更多的工具來輔助記錄或捕捉，這可能會導致某些文件的遺漏和無效的管理。這包括需要額外的儲存空間來進行文件儲存管理，以及需要較長的保留期才能正確利用記錄文件，從而在發生危機時實現追溯和搜尋功能。除了保存日誌或操作記錄外，審計或管理還受到時間或操作管理問題的阻礙，導致人員難以有效地查看過去記錄的操作日誌。在這種情況下，通常需要大量時間來尋找需要審查的實際文件或記錄。

功能說明

- 合規性和安全標準
  - 符合 ISO 27001 國際認證要求，包括 A.9 控制和 A.12 記錄。
  - 參考 NIST CSF 標準，特別是 PROTECT (PR.AC) 和資料保護 (PR.DS)。
  - 符合 PCI DSS 標準，涵蓋三大領域的第 2、7、8、10 條。
  - 遵循 IEC 62443 國際標準，包括 IEC 62443-2-1 和 IEC 62443-3-3。
- 身份驗證和安全機制
  - 雙重認證 (TOTP RFC 6238)：透過要求基於時間的一次性密碼 (TOTP) 來增強系統登入安全性。
  - 憑證管理：管理和更新平台憑證，以實現安全、加密的資料傳輸。
  - 加密保護：使用 AES-CBC 128 位元加密並支援 HTTPS/TLS，確保靜態和傳輸中敏感資料的保護。
- 使用者和角色管理
  - 基於角色的存取控制（RBAC）：精確控制使用者對資產和服務的訪問，確保只有授權人員才能存取特定資源。
  - 使用者管理：即時監控和管理使用者帳戶狀態，允許立即設定或停用帳戶。
  - 群組管理：透過管理使用者群組並與 LDAP 系統同步來簡化權限分配。
- 即時存取
  - 優化審批流程：加快請求處理速度並提高準確性。
  - 靈活的申請管理：支援提前提交和修改請求。
  - 透明的歷史記錄：輕鬆查看並匯出歷史運行資料。
  - 快速重新申請功能：透過重複使用先前的資料來加快新申請的速度，從而節省時間。
  - 可自訂的通知：透過自訂的通知條件增強安全性，特別是對於重複的申請。
- 資源、資產和連結管理
  - 無代理雲端整合：透過消除對代理軟體的需求來降低網路安全風險，從而最大限度地降低維護成本。
  - 雲端憑證管理：快速匯入和管理 AWS, GCP, Azure 和 VMware 等私有雲平台的雲端憑證。
  - 專案管理：透過一體化框架有效管理多個資產，輕鬆編輯和刪除，同時維護完整記錄。
  - 存取服務管理：安全管理設備連線訊息，防止使用者直接存取敏感憑證。
  - 設備管理：透過手動和批次匯入選項簡化伺服器管理，透過網頁應用程式介面實現快速、直接連線。
  - 網頁應用程式管理：透過自動登入功能和網域白名單集中控制 AWS, GCP, Azure 主控台和 GitHub。
  - 資料庫管理：管理和監控常見的資料庫（例如 PostgreSQL）以確保資料安全性和完整性。
- 即時監控和記錄
  - 即時監控：監控即時會話活動和指令使用情況，以便立即終止有風險的連線。
  - 日誌管理：全面記錄使用者操作，包括存取日誌、保留原則和特權操作。支援 Syslog 格式並與 SIEM 系統無縫整合。為使用者會話提供視訊記錄，確保完整的活動追蹤。
- 系統管理與備份
  - 系統管理：授權、管理、檢視系統版本資訊。備份機制可確保系統故障或資料遺失時的復原能力。高可用性 (HA) 設計可透過提供冗餘和自動故障轉移功能來最大限度地減少停機時間，從而增強系統可靠性。
  - 連線設定：確保系統連線穩定安全，可調整區域設定以滿足跨國企業的需求。
  - SIEM 整合：增強系統安全監控與回應能力。

MAVIS
混合多雲特權管理平台

解決方案

核心價值

MAVIS 混合多雲特權管理平台 — 結合四大核心功能，有效提升企業安全水平，協助管理人員，減輕管理負擔。

身分訪問監控管理

MAVIS 採用零信任架構進行即時存取管理，確保特權存取的安全性和合規性。透過整合即時存取功能，進一步提高了資產管理效率和保護。

混合多雲資源整合

MAVIS 跨雲端集中整合納管企業所有 IT 資產。

全面記錄追根朔源

MAVIS 能完整錄影記錄所有連線操作，並能輕鬆查找內容。

網頁應用程式整合納管

單一介面收納納常用的應用程式，以解決帳號共用權責劃分問題。

模組

雲憑證管理

- MAVIS 提供多雲整合功能，包括三大公有雲的管理：AWS, Azure, GCP 和私有雲 VMWare。透過匯入雲憑證或透過 API 的方式，實現公司資產的快速管理。
- 除了管理雲憑證外，人員還可以使用 MAVIS 的管理流程來選擇和管理必要的伺服器，避免包含過多和未使用的機器信息，從而導致管理麻煩。
- 當使用者選擇匯入和管理的機器時，MAVIS 自動化流程會將 MAVIS 管理的機器狀態與雲端同步，使人員能夠透過單一平台實現多雲管理。

資產存取管理

- MAVIS 允許連接到允許 SSH 連接的設備，例如網路管理設備和 Linux，以及 Windows 伺服器等 RDP 設備。
- 除了透過雲端憑證管理匯入伺服器外，還可以由使用者手動新增伺服器，只需要 IP 位址和相關設定即可在平台內統一管理。
- 匯入或手動新增雲端機器後，需要新增連線設定才能存取服務管理。這些設定包括連接裝置的帳戶密碼或金鑰。配置完成後，連接設備可以選擇直接連接到目標電腦。透過安全保險庫機制，資產連結敏感資訊受到保護。
- MAVIS 透過代理伺服器連接到目標機器，除了啟用 SSH 或 RDP 連線之外，還透過 SFTP 提供直接檔案上傳或下載。這減少了對第三方工具的熟悉程度要求和工具之間的差異。
- 此外，使用者可以管理系統內的網頁應用程式。除了帳號和密碼管理外，使用者還可以透過系統登錄，無需記錄相關網頁的存取資訊。連接由 MAVIS 記錄。
- 透過 MAVIS 連接後，所有操作記錄都完整記錄，操作輕鬆可追溯。用戶可以透過視訊回放回放該連接的操作，或查看日誌中的命令詳細信息，達到快速回溯和搜尋的目的。
- MAVIS 管理的所有設備無需安裝額外的代理軟體，確保企業最安全的管理，無需在重要資產上安裝任何陌生的軟體。
- 除了操作日誌記錄外，MAVIS 還完整記錄了系統中的所有人員操作，並根據項目或系統權限進行分類，方便檢索。

身分和權限管理

- MAVIS 實現即時帳戶控制，管理人員可即時建立和配置帳戶，方便有效率登入和操作。多重認證機制為帳戶安全提供多重保護，有效保障企業資產及存取權限。
- MAVIS 還提供特定的權限控制，允許為每個帳戶或身分指派不同的資產權限。這種基於責任的方法可確保對身分和資產權限進行細緻的控制，同時降低與配置錯誤相關的風險。
- 基於專案的資產管理功能根據專案結構組織資產，輕鬆分類和標記，從而簡化大量設備的管理。管理人員可以有效率地監控目前登入帳戶；如果發起任何有害活動，他們可以透過系統介面迅速解決這些問題，以防止持續的危險操作。
- 最後，即時存取整合功能可讓使用者提前提交連線請求並根據需要進行修改，從而增強了連線管理。這確保了透明的審批流程並有助於快速重新提交，從而簡化了整體存取管理。