MAVIS

PNTL

混合多雲特權管理工具

挑戰

資產管理

企業提供內、外部網路服務的過程中，勢必需建立對應的伺服器以達到服務要求，在企業方針的選擇下會使用雲服務的虛擬機或是建置本地地端機房甚至是混合多雲的方式。上述的任一方式，都會導致IT人員需要額外的紀錄並管理人員的使用權限，除造成工作附載增加外，也容易因為跨平台、跨機器、需使用第三方工具導致人員出錯率大幅提升；除此之外，若該記錄檔案在未加密的情況下，更容易讓公司暴露在高風險中，甚至因為沒有身份控管或外洩導致公司需承擔非常大的損失。

身份權限

身份權限控管是企業所使用的資訊系統時常面臨較大的安全風險。若企業想要有完善的管理，通常需花費大量的人力與完整規劃，才能達到既符合企業要求也可以有適於操作人員的使用設定。若企業或管理員在未定期維護下，很容易會導致系統的身份帳號或權限高於企業流程要求；在這前提下，此帳號被盜用或外洩，將可能會被用來竊取機密敏感的資料，並對企業造成無法彌補的損害。成功的駭客攻擊中，通常都是利用特權帳戶來進行竊取或破壞，因此身份權限尤其是特權帳戶的保護，都會是企業需要重視的一部分。

操作記錄

以現行不論是對地端機房的操作或是雲服務的使用，都會因為工具的限制，無法有效的紀錄操作的日誌與使用操作的過程，從而需使用更多的工具協助進行記錄或錄製，除容易造成遺漏外，更容易導致部分的檔案無法有效地被管理。其中包含檔案儲存時需要有額外的儲存空間做管理，同時也需要有相當年限的保護，才能夠將紀錄檔案做妥善的運用，達到危機發生時，有回朔與查找的可能。除了日誌或操作的紀錄保管外，在稽查或管理時，更容易會因為時間或操作管理上的問題，導致人員無法更有效的查看以往所紀錄的操作日誌，在這樣的前提下，通常都需要花上大量的時間，才有辦法找到實際需要查看的檔案或紀錄。

功能說明

加密保護方式
- AES-CBC 128-bit

雙因子驗證方式
- TOTP RFC 6238

符合 ISO 27001 國際認證要求

Agentless 雲地整合
- 降低資安風險、減少人員維護成本

專案管理
- 透過專案架構的方式管理資產與對應的存取角色權限

儀表板
- 專案、資產資訊與使用者紀錄透過分析圖表的方式一覽無遺

裝置管理
- 提供手動添加或是匯入的方式統一納管伺服器
- 透過網頁介面即可直接連線目標機器

網頁應用程式管理
- 針對 AWS console, GCP console, AZure console 以及 Github 做納管
- 透過自動化登入的方式，讓人員不必紀錄存取資訊，即可進行連線並被紀錄

雲憑證管理
- 快速匯入三大公有雲 AWS, GCP, Azure 及私有雲 VMWare 做管理

專案
- 管理專案的角色存取與成員組成，加強權限管理與資產的維護

存取服務管理
- 添加裝置連線的資訊，透過權限設定避免專案成員直接取得連線資訊
- 提供 Linux OS, Windows OS 及檔案上傳與下載機制

日誌
- 記錄使用者於系統中的任何操作
- 紀錄使用者連線裝置的操作日誌

使用者管理
- 透過使用者的帳號狀態管理，即時設定開放、關閉使用者登入存取

專案管理
- 可針對現有專案進行編輯、刪除，並保留完整記錄

系統資訊
- 可進行授權的管理與查看系統版本資訊

系統日誌
- 紀錄較高權限的操作，如專案或使用者設定等

MAVIS
混合多雲特權管理工具

解決方案

核心價值

Mavis - 您的 IT 團隊行車記錄器，集結三項核心功能，協助管理人員，減輕管理負擔

身份訪問監控管理

基於零信任架構與 PAM 實現安全完整的 IT 維運與管理

地雲資源集中整合

Mavis 跨雲集中整合納管企業所有 IT 資產

全面紀錄追根溯源

Mavis 完整錄影紀錄所有連線操作並能輕鬆查找內容

模組說明

雲憑證管理

■ Mavis　提供多雲整合的功能，其中包含管理三大公有雲：AWS, Azure, GCP 以及私有雲：VMWare，透過匯入雲憑證或是 API 的方式，快速的將公司資產做管理

■ 人員除了納管雲憑證外，也可透過 Mavis 提供的管理流程，將必要所需的伺服器選擇並納管，避免造成人員有過多無用捨棄的機器資訊被做加入，導致管理上的麻煩

■ 當人員選擇機器做匯入納管後，透過 Mavis 的自動化流程，即可同步被 Mavis 納管的機器與雲端狀態一致，讓人員透過一個平台即可達到多雲的管理

資產存取管理

■ Mavis　提供多雲整合的功能，其中包含管理三大公有雲：AWS, Azure, GCP 以及私有雲：VMWare，透過匯入雲憑證或是 API 的方式，快速的將公司資產做管理

■ 除透過雲憑證管理匯入的伺服器外，也可透過使用者手動加入的方式，只需提供連線機器的 IP 及相關設定即可統一至平台中管理

■ 將雲端機器匯入或手動加入伺服器後，則需至存取服務管理中添加連線設定，該設定包含連線裝置的帳號密碼或金鑰，設定後，連線裝置則可選擇設定直接連線至目標機器，並透過安全庫機制，保護資產連線機敏資訊

■ Mavis　透過代理伺服器的方式連線至目標機器中，除上述所提的 SSH enabled或 RDP 外，亦可選擇 SFTP 的方式直接對目標機器進行檔案上傳或下載，降低人員對於第三方工具使用上的熟悉度要求與工具差異性

■ 另外人員也可以將網頁應用程式納管至系統中，連同帳號、密碼的部分也可透過系統代為登入，讓一般操作人員不用在紀錄相關網頁的存取資訊，透過 Mavis 即可進行連線並被紀錄。

■ 透過 Mavis 進行連線後，該次連線的任何操作紀錄皆會被完整的紀錄並錄製該次操作，人員除了可以透過影片播放的方式回放該次連線的操作外，也可同步於該次日誌中查看連線過程中於哪一個時間點下過什麼指令，以達到快速溯源、查找的目的

■ Mavis　所納管的所有裝置，皆不需要安裝額外的代理軟體至目標中，協助企業以最安全的方式進行管理，不必安裝任何不明來源的軟體於重要資產中

■ 除操作的記錄日誌外，Mavis　也會完整記錄任何人員於系統中的所有操作，並依據是專案下的操作亦或是系統權限下的操作進行分類，以便於查找

身份與權限管理

■ 管理人員可透過帳號的建立與設定帳號狀態的方式，對於人員登入系統的管理進行即時的管控，與此同時人員才可登入 Mavis 並針對管理員設定的可使用功能進行權限上的操作

■ 多因子驗證機制，多重保護企業資產與存取權限的帳號安全

■ Mavis　提供以專案的架構進行資產的管理，除協助人員透過專案的方式將資產做有效的分類，也可以透過標籤的方式，快速的於專案下再將資產進行細分，即便需要納管的裝置數量較多時，仍可有相當程度的分類，降低管理過程中的複雜操作

■ 資產透過專案的控管下，也可個別的指定個別帳號、身份於每個專案被賦予不同的權限，Mavis 提供角色權限存取控制的方式，以達到分權分責分專案的處理，將身份與資產的權限做到最細部的控制，避免管理員控制設定的錯誤導致資產的風險值提高

■ Mavis　另外可針對當前登入的帳號進行管理，如因當前登入中的帳號進行任何操作以達到危害程度，可透過管理介面的操作，快速中斷該帳號於系統的使用，防止危險操作持續造成企業災害