ANCHOR

智弘軟體

Global Wisdom Software

特權帳號管理與稽核平台

Ark of Network, Cyber Hamper for Operations Reliability

www.globalwisdom.com.tw

ANCHOR 模組功能列表

模組別 / 功能別	全功能(AIO)	帳號管理(AM)	連線側錄(SR)
平台存取			
跨瀏覽器存取	V	V	V
支援多外部認證	V	V	V
支援OTP	V	V	V
單一簽入			
帳密集ㄧ管理	V	V	
代登入或不代登入	V	V	
不代登入	V		V
工作流程			
支援臨時帳號申請	V	V	V
支援密碼申請	V	V	
支援緊急申請流程	V	V	V
支援群組式授權	V	V	V
操作軌跡			
紀錄與調閱操作軌跡	V		V
即時稽核能力	V		V
工作報告			
線ㄧ填寫工作報告	V	V	V
日誌集中			
可支援SIEM的CEF格式	V	V	V
可支援外送Syslog	V	V	V
稽核作業			
支援即時/事後稽核能力	V		V
自動化產出稽核報表	V	V	V
報表訂閱機制	V	V	V
持續營運			
支援帳號救援功能*	V	V	
支援HA/DR架構**	V	V	V

*需加購帳號救援模組

**需加購升級套件(Upgrade Kit)

ANCHOR 智弘軟體科技 為帳號的管理與稽核要求建立新標竿

導入ANCHOR能迅速消弭資安風險

透過ANCHOR系統有助於IT部門進行帳號管理時消弭下列可能風險：

■ 帳密被盜取:
透過ANCHOR系統管控這些高度敏感的特權帳號，可以避免特權帳號因為帳密被取得而遭受利用，造成入侵事件。

■ 使用者蛙跳行為(Leapfrog):
使用者藉三登入某台主機的機會，可以開啟 Telnet、SSH 或 RDP 遠端桌面連線到其他原本其無法連到的主機而帶來風險。

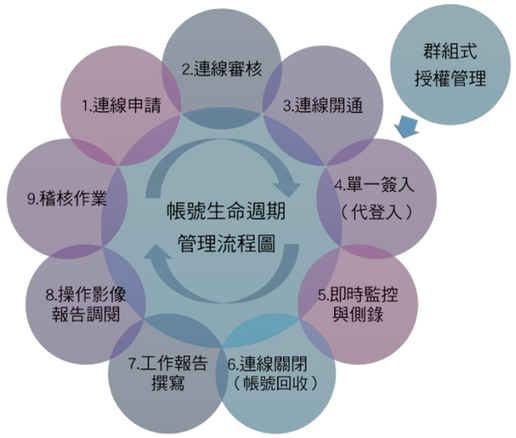
■ 多重系統權限:
組織中人員因為職務輪調、職務代理人的需求，往往會獲得多個系統的特殊權限，雖然這些人員的職務調動了，不過權限常常忘了被回收，就有可能帶來風險。

■ 共享帳密:
諸如Administrator 帳號、Linux 的 root 帳號，或 SQL 的 SA 帳號等，以往為了業務、唯運需求，經常多人持有，這些帳號的登入也很難歸責到哪個人員所登入。

以最佳實務理念出發 化繁為簡

ANCHOR以符合ISO精神與最佳實務經驗的新思維出發，從帳號生命週期中的每個管理環節(申請、審核、啟用、通知、認證、監控、停用)對應出符合管理流程與稽核要求等各項功能，作成一集中化的管理平台，省卻了傳統上所需要的高額建置費用與系統整合成本，將管理工作化繁為簡，一條鞭的方式讓IT人員不僅能提升工作效率，系統仍保有必要的稽核記錄，以符合資安內控與法規查核所需。

ANCHOR 帳號生命週期管理流程圖



ANCHOR 模組架構圖

ANCHOR提供各種角色定義之使用者，提供整合式入口網站方便針對受管理設備/服務等進行帳號集中控管、單一簽入及操作稽核等管理作業

ANCHOR 產品特色

隨時隨地進行存取與管控

ANCHOR系統僅需透過WEB UI就可以讓使用者與管理者進行連線存取與管理，並支援透過手機、平板等手持式裝置登入平台進行申請與審核，以增加使用者的實務方便性。

內建帳號/密碼申請及簽核流程

ANCHOR系統內建臨時帳號/密碼申請功能，簽核通過後，利用簡訊EMAIL等方式通知申請者一次性密碼，以應付需緊急連線或代理工作時的需要。除了可以避免假冒身分的惡意連線以外，也可以符合資安政策的需求。

無須安裝代理程式便可以進行管理

ANCHOR系統無須透過安裝代理程式(Agent-less)便可以進行帳號集中管理與密碼調和作業。可配合帳號生命週期管理定期進行帳號盤點，針對異常新增或修改之帳號資料進行告警或處理，以保障系統安全性與一致性。

支援管控之平台及連線方式：

- OS-Windows/Unix/Linux/BSD
- DB-MSSQL/Oracle/MySQL/Sybase/Infomix
- 網路與資安設備-Cisco/Juniper/F5/Websense/ Imperva/SourceFire/Fortinet/ALU/Extreme等
- 中、大型主機-IBM AS/400, z/OS
- 虛擬化平台-VMWare
- 連線方式-Telnet/SSH/HTTP/HTTPS/RDP/RFB(VNC)

必要之稽核記錄與連線側錄

「凡走過必留下痕跡」，ANCHOR系統採動態式錄影，可留存使用者存取過程中必要之連線記錄與操作歷程。管理者可以設定過濾條件(如指令關鍵字)調閱連線記錄與側錄檔，操作歷程可以全程回播，也可匯出記錄檔及擷取操作畫面，以滿足稽核查閱之需要。ANCHOR系統亦提供管理者同步監看使用者連線畫面，除了線上服務支援以外，當使用者違反存取政策時，可以訊息通知修正或立即中斷其連線，以維護系統安全。

指令過濾與蛙跳(Leapfrog)防止

ANCHOR系統可針對可執行指令設定黑名單進行過濾，對未授權之指令操作能加以阻斷，並寫入違規操作記錄中，提供事後調閱。另帳號/密碼已納入ANCHOR系統進行控管，可防止使用者以蛙跳(Leapfrog)方式連線至非取得授權之被管理主機。

高可用性與災難備援機制

針對企業等級產品之用戶，ANCHOR系統亦提供了高可用性(High-Availability，HA)及災難備援之系統功能架構，當主要系統/主要機房異常時，可以切換至備援機房之ANCHOR系統，以保有服務不中斷之IT等級水準。

不同加密金鑰，保障資料庫安全

各設備帳號密碼以AES256加密方式並採不同加密金鑰，可整合硬體式PKI或TPM模組，加強資料庫安全。

為需求應運而生的新一代ANCHOR-ANCHOR Plus

ANCHOR為了更貼近使用者應用需求，新一代ANCHOR系統-ANCHOR Plus，特針對系統架構進行調整，除了新增並強化全功能版本(AIO，All-in-one)以外，並將帳號管理(AM, Account Management)及連線側錄(SR, Session Recording)兩大功能系統採模組化設計，可方便企業依需求彈性採購所需模組，必要時仍可透過升級套件(Upgrade Kit)進行系統架構強化。

ANCHOR 版本	FDT 基礎版	STD 標準版	ETP 企業版	ETP+ 企業進階版
受管理端支援: 作業系統(Unix,Linux,Windows) 檔案存取(FTP,SFTP,SCP)	•	•	•	•
受管理端支援: 資料庫(Oracle,SQL Server,MySQL) 網路設備/資安設備(SSH)		•	•	•
支援高可用性架構(HA);受管理端: 中、大型主機(IBM AS/400,z/OS) 網路設備/資安設備(Web)、VMWare			•	•
支援異地備援架構(DR) 帳號救援系統(破窗)				•