ANCHOR

智弘軟體科技

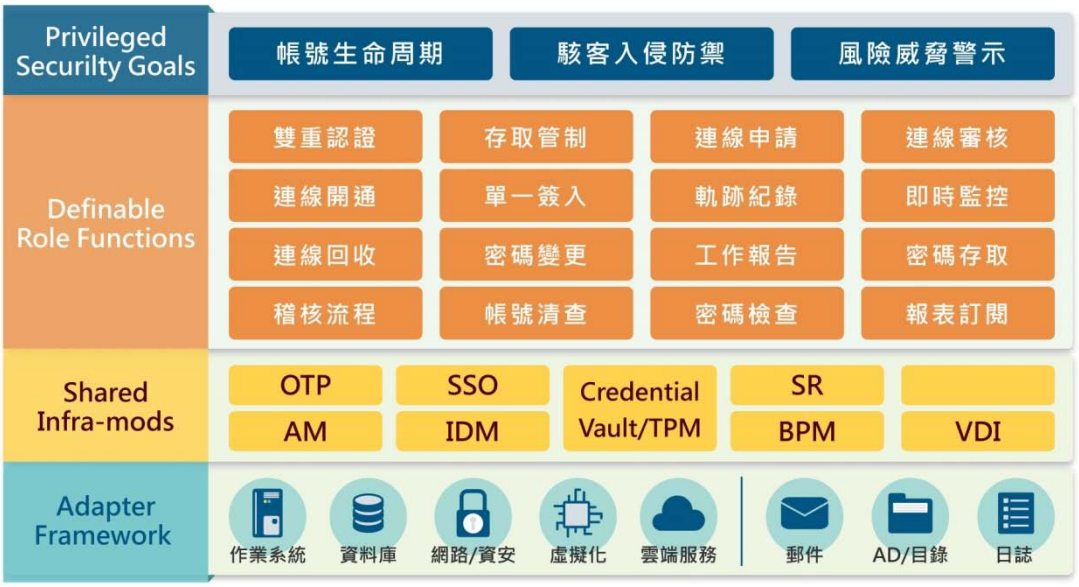
產品白皮書

智弘軟體科技股份有限公司

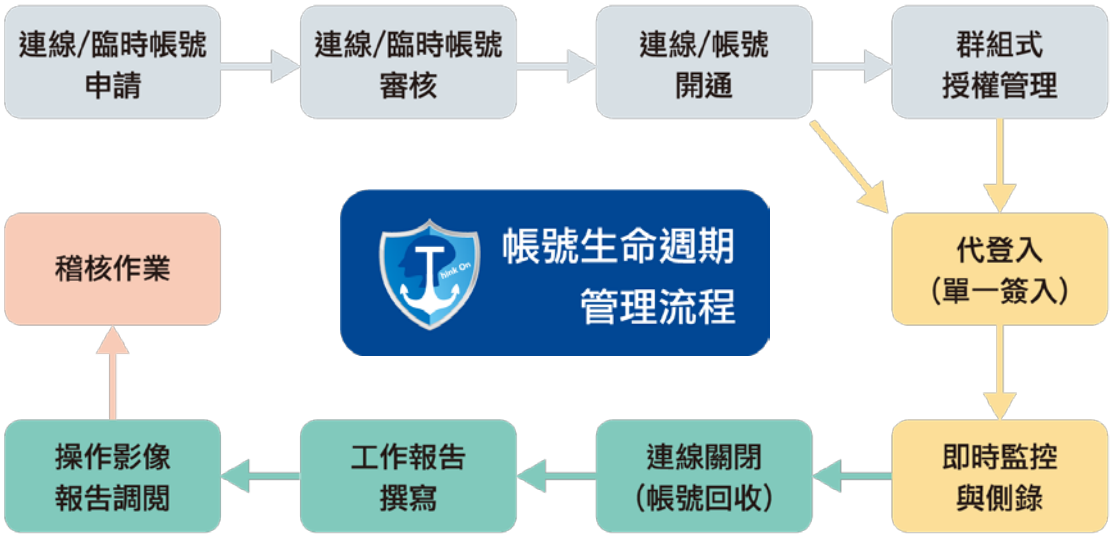
ANCHOR 特權帳號與稽核管理平台：

智弘軟體科技所開發之特權帳號與稽核管理平台 ANCHOR，以符合 ISO 精神與最佳實務經驗的新思維出發，從帳號生命周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，而簡化的管理方式不僅能提升 IT 人員工作效率，且系統可自動產生並保存必要的稽核記錄，以符合資安內控與法規查核所需。

ANCHOR 特權帳號與稽核管理平台之解決方案：



帳號生命周期管理



針對特權帳號使用者的身分與其存取行為，進行身分識別、權限授權及行為監控，嚴格控制對於敏感資料之存取，並且滿足稽核與法規遵循的需求；整體包含帳號線上連線申請/密碼申請/臨時 ID 申請、審核作業、開通管制、密碼管制(取出及歸還密碼)/單一簽入(代登入)、即時監控與側錄、連線關閉(帳號回收)、工作報告撰寫、操作影像與報告調閱，及設定式稽核作業流程等。同時為免除不必要風險及避免後續維護爭議，受控端設備均以無需裝設任何軟體或開立目錄為原則(Agent-less)，並支援個人化多國語系(如：繁、簡、英、日等)，為一同時兼具安全性與方便性之整體解決方案

駭客入侵防禦

同時藉由代登入機制免除傳遞與輸入帳號的非必要風險；並且於每次連線結束後「自動」變更密碼；內建雙因素認證；具備與 AD、LDAP 等標準方式與外部認證機制整合能力；並可「自動」進行帳號清查(最短半小時一次)，且於每次登入使用後可立即進行密碼變更，達到密碼

不落地之機制，避免密碼遭側錄竊取之虞，因此透過本平台的導入，可以有效降低整體駭客入侵之風險。ANCHOR 平台可針對可執行指令設定黑名單進行過濾，對於未授之指令操作加以阻斷，並立即發出警訊通知審核者即時介入處置，同時寫入違規操作記錄中，提供事後調閱稽核所需，為本專案之最佳解決方案

風險威脅警示

後門或幽靈帳號為機敏資料外泄的重要隱患，也是 APT 攻擊用於遙控與傳輸資料的媒介，ANCHOR 特權帳號與稽核管理平台可密集進行帳號盤點，並於發現有後門/幽靈帳號時，可立即通知相關人員進行處置。另外針對使用者透過特權帳號執行所定義之違規指令時，ANCHOR 除可即時阻絕指令外，同時可將該行為立即通知相關人員，即時進行「過程稽核」，相關人員可以進行該操作過程的「即時監看」，如有爭議可以「遠端進行斷線」，避免問題或傷害的持續擴大，對特權帳號的使用達到預防重於治療的效果。

產品特色

靈活的管理與稽核流程

ANCHOR 平台採單一整合性入口網架構，以單一管理網站，即可線上完成帳號生命週期管理流程中各項工作，以達最佳使用方便性，同時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。

完整的高可用性架構

針對企業用戶，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/主要機房發生異常時，可以切換至備用系統/備援機房之 ANCHOR 系統，以確保服務不中斷之服務品質。

操作介面簡單易懂

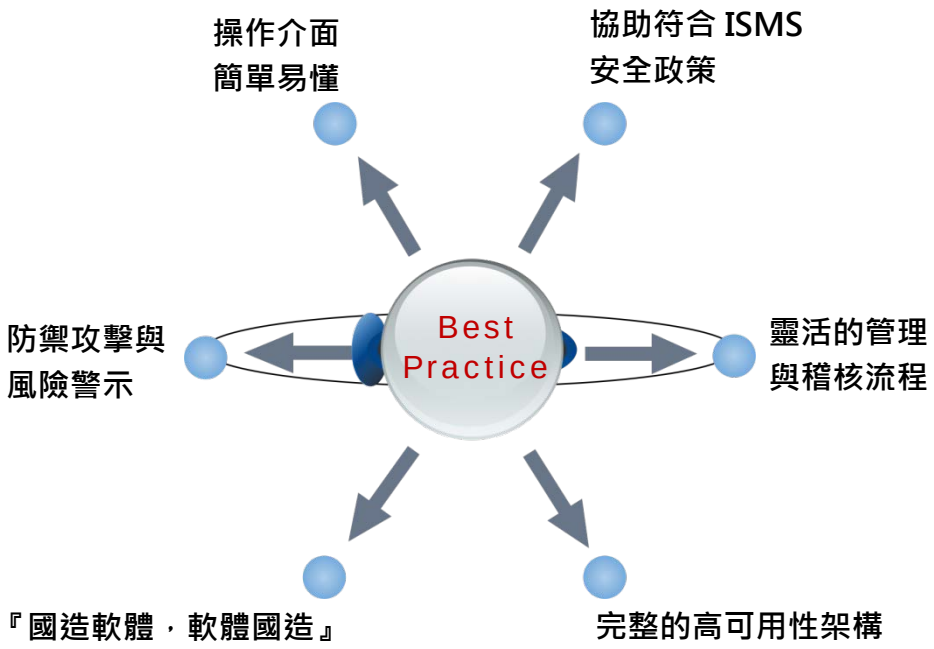
ANCHOR 系統透過 Web UI 即可簡單進行管理，依據國人使用上的習慣進行頁面編排設計，並支援中文操作介面，且可透過手機、平板等手持式裝置登入平台進行申請與審核等流程，以增加使用者的實務方便性。

防禦攻擊與風險警示

ANCHOR 平台可定期自動進行帳號盤點，在發現異常時發送通知予相關人員，避免遭有心人士偷建及偷刪帳號，同時於使用者連線作業結束後可立即變更連線帳號之密碼，降低密碼遭竊取之風險。ANCHOR 平台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。

『國造軟體，軟體國造』

ANCHOR 特權帳號與稽核管理平台，為第一套由國人自行研發的產品，依照國內使用者習慣進行設計調整，同時深耕在地服務並即時回應客戶需求，為一最適合國情及國內使用者操作習性之產品，且目前已有超過 30 家國內客戶選用，是在佈署資訊安全管理中最重要也是最後一道防線。



管理操作便利性優勢

個人帳號集中維護

減少個別維護主機的人工成本

跨瀏覽器

Chrome, FireFox, IE 或 Edge 等

連線工具功能保留

如右鍵、Copy/Paste 或功能鍵

批次指令

多部同類型設備，可執行一系列相同指令

資料備份及移轉

多組備份/移轉可依週期自動執行

緊急申請流程

審核人員不需開機亦可完成授權

可定義式稽核作業流程

可線上填寫內容、附件、通知、退回及結案

連線工作報告

可線上填寫，節省調閱時間

報表訂閱

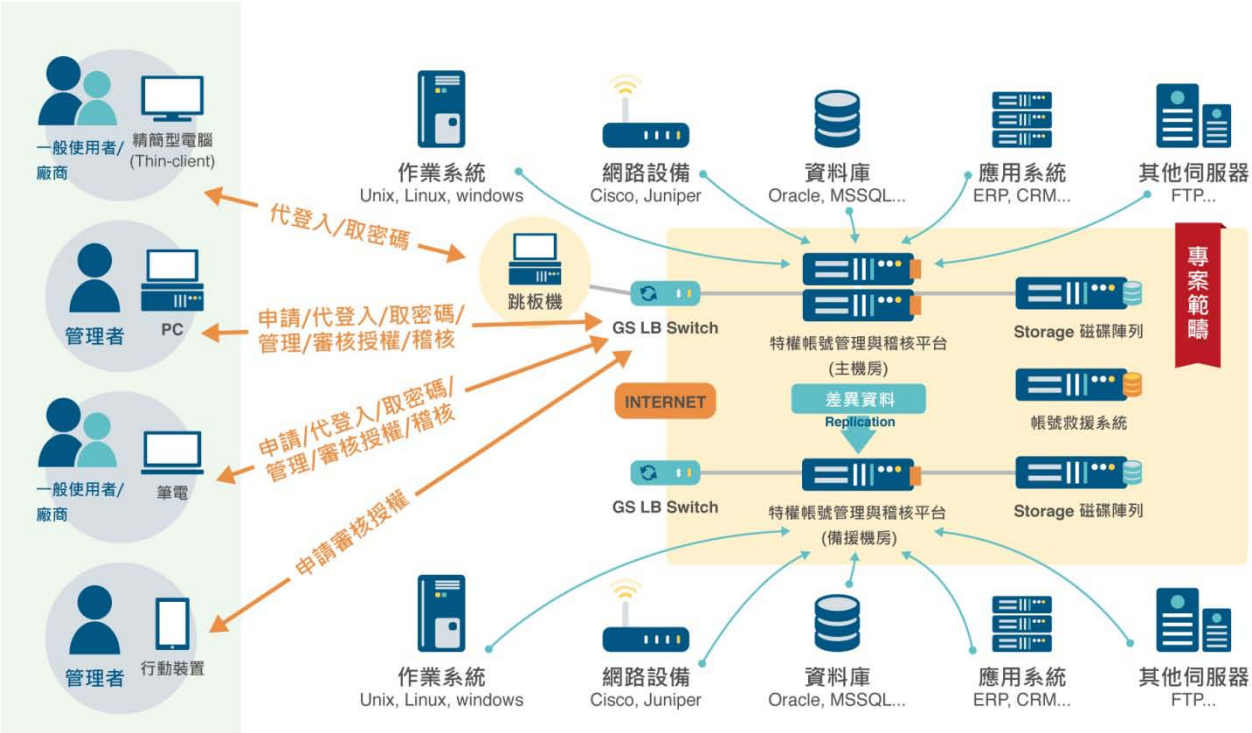
可訂閱日、週、月等周期性報表，自動寄送

多國語系支援

支援個人化多國語系(繁中、簡中、英文及日文等)

高可用性建議架構說明：

為提供本案所需高可用性架構，ANCHOR 平台可建置為(High-Avilability,HA)架構，在主要系統發生異常時，可切換至備援系統使用，提供服務不中斷之運作能力。同時亦可依需求於異地機房建置異地備援系統，在主要機房發生災變時可立即切換至異地機房使用，以確保整體服務可正常運作。為提供更加完整之高可用性服務，ANCHOR 平台亦可搭配帳號救援系統進行配置，提供所有平台均無法使用之情境下，可直接將所有帳號取出進行緊急維運所使用。



效益說明：

藉由導入 ANCHOR 特權帳號與稽核管理平台，建置具備記錄特權管理者之相關使用資訊，並提供使用者登入使用設備或系統時，需進行作業申請之流程機制，同時可留存及匯出相關記錄資訊，以供資安監控有效掌握資通訊系統遭受破壞、不當使用等資通安全事件時，能迅速通報及緊急應變處置，以確保資通訊系統之正常運作。另外針對特權帳號進行完整帳號生命週期的流程控管，不但具備可歸責性之稽核功能，同時提供操作行為側錄證據之不可否認性，對於本案建置在資料中心之關鍵設備或系統可統一納管相關特權帳號，以符合「政府機關（構）資通安全責任等級分級作業規定」使用者之識別與鑑別之要求，並協助本案符合行政院國家資通安全會報相關作業規範相關要求。

ANCHOR 特權帳號與稽核管理平台另具備下列效益：

- 協助符合法規遵循要求(如 ISO 27001、行政院資通安全法、F-ISAC 等法規要求)
- 集中控管特權帳號之存取與使用行為，提高整體資安防護等級
- 自定義式的稽核流程，靈活支援單位稽核流程的變化
- 針對偷建/偷刪帳號排程清查，並可立即通知以利單位立即採取行動，預防資料外洩
- 完整的特權帳號生命週期管理流程，藉由申請→審核→開通→代登→操作(可即時監控及側錄)→連線關閉(帳號收回) →稽核，達到特權帳號的完善管理
- 內建雙因素認證機制，不需搭配其他解決方案或額外購置
- 側錄影像採用動態錄影並進行加密儲存，提供側錄影像之證據不可互認性