ANCHOR 2.0 產品特色

(一) 平台存取	(八) 永續服務
1.透過WEB UI 讓使用者與管理者進行連線存取與管理。	1.支援高可用性HA(High Availability)架構，運作異常時自動進行偵測與切換。
2.單一平台滿足帳號生命週期管理需求。	2.支援異地備援DR(Disaster recovery)架構，資料可自動進行同步。
3.支援IE、Chrome、Firefox及Edge等。	
4.支援以AD、LDAP及平台帳號進行登入。	3.支援帳號救援系統(破窗)，即便主機房與異地備援機房同時損毀，仍可取出被管理設備之密碼。
5.內建OTP(One Time Password)，支援APP、E-mail及簡訊進行產製/派送。	
6.提供「儀表版」，顯示平台綜合資訊。	4.另設計將密碼設分A-B Part方式，以 E-mail分寄給二位保管者，以供救援所需。
(二) 單一簽入	**(九) 平台安全**
1.使用者藉由登入本平台，即可代登入至被管理端設備，以減少記憶帳號密碼與逐一登入的人力。	1. ANCHOR套用微軟最嚴格之Security Baselines策略，最小化系統本身運作權限。
2.支援代登入與不代登入(帳號密碼採人工管理)。	2. ANCHOR針對儲存之密碼均使用2道以上(AES-256)進行加密，以避免密碼遭破解之疑慮。
(三) 工作流程	
1.結合臨時ID、連線申請及密碼申請、簽核通過自動授權連線。	3. ANCHOR支援微軟BitLocker功能，提供系統達到FIPS標準之加密需求。
2.支援夜間/緊急申請流程。	4.ANCHOR可支援使用TPM及HSM等硬體安全模組，以提高平台整體安全性。
3.支援設備群組式授權，提高使用意願、降低導入阻力。	
(四) 操作軌跡與安全管控	**(十) Agentless**
1.連線後進行操作軌跡紀錄，可使用關鍵字(含SSH、Telet指令)搜尋並調閱錄影檔，滿足稽核查閱之需要。	1.ANCHOR無須安裝代理程式便可進行帳號集中管理與密碼調和作業。
2.可即時監看操作畫面，當使用者違反存取政策，可以訊息通知或立即中斷連線，以維護系統安全。	**(十一)帳號盤點**
3.操作軌跡採動態錄影並加密儲存。	提供定期進行帳號盤點機制，針對異動之帳號資料進行告警或處理，以保障系統安全性與一致性。
4.管理者可以設定過濾條件(如指令關鍵字及KeyLog)調閱連線記錄與側錄錄影檔。	**(十二)指令過濾**
(五) 工作報告	可在ANCHOR系統上設定指令黑名單，對未授權的指令操作進行阻斷，並寫入違規操作記錄，提供事後調閱。
1.線上填寫電子化工作報告，以節約紙張使用並提供線上快速調閱。	
2.工作報告支援版本控制。	
(六) 日誌集中	**支援被管理端設備:**
1.支援以CEF(Commo Evet Format)格式將平台日誌整合至SIEM日誌事件管理系統。	☑主機作業系統- Windows, Unix, Linux, BSD ☑資料庫-MSSQL, Oracle, MySQL, Sybase, Informix ☑網路設備/資安設備-Cisco, Juniper, F5, Websense, Imperva, SourceFire, Fortinet, ALU, Extreme ☑中型與大型主機- IBM AS/400, z/OS ☑虛擬化平台 - VMWare ☑Connected Mode –Telnet, SSH, HTTP, HTTPS, RDP, RFB (VNC)
2.支援TCP及UDP協定派送。	
(七) 稽核作業	
1.支援即時稽核與事後稽核。	
2.支援帳號生命週期管理稽核。	
3.支援稽核報表轉出PDF及Excel等格式。	
4.支援稽核報表訂閱。	