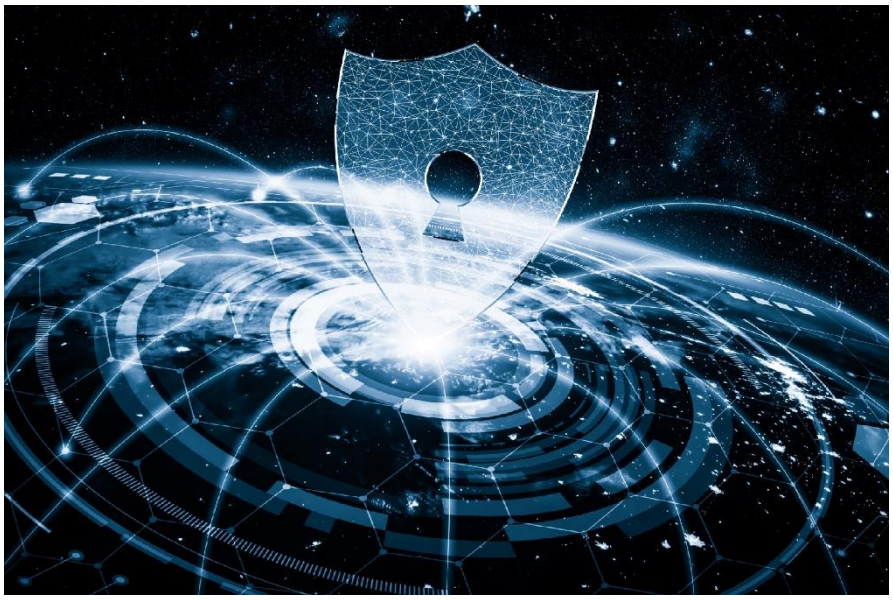
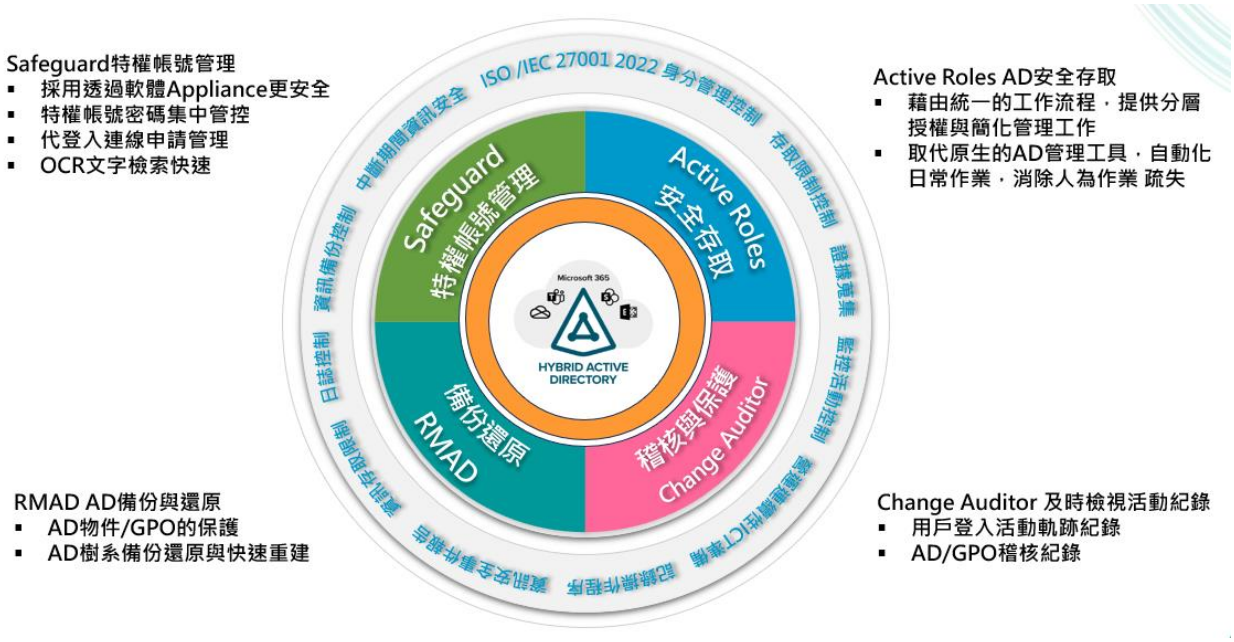
全方位 AD 存取安全與防護



近期國內外資安事件頻傳，其中包括美國的 AT&T、日本的 NTT West 以及臺灣某電子公司。AT&T 爆出 7300 萬使用者個資外洩事件，涉及敏感資訊如姓名、出生日期、社會安全號碼等，造成資安風暴和服務中斷。NTT West 則因涉及 928 萬客戶資料洩露事件，導致總裁辭職，公司被指未能適當監管和管理客戶資料。這些事件顯示了 AD 特權帳戶攻擊的嚴重性，企業應該加強對特權帳戶的管控和監視，以防止內部人員的不當行為，我們應該規劃一個全方位 AD 的存取安全與防護及零信任，以強化資安韌性邁向企業永續經營。

以下依企業重要性及完整性提供建議：



1. 特權帳號管理

One Identity Safeguard 提供密碼管理 (Safeguard for Privileged Passwords)，透過軟體 Appliance 將特權帳號密碼集中管控並提供申請管理流程、代登入連線申請管理 (Safeguard for Privileged Sessions)，可以實現密碼不落地目的，無論是 Windows RDP 或是其他主機 ssh 連線均可提供申請管控並進行操作即時側錄，可供清晰影像重播與 OCR 影像文字操作的指令關鍵字查找、以及具備威脅偵測與分析能力的監控方案 (Safeguard for Privileged Analytics) 。它能夠安全地儲存、管理、記錄和分析特權存取，減輕您保護特權帳號的壓力，同時滿足您管理面和稽核面的需求。

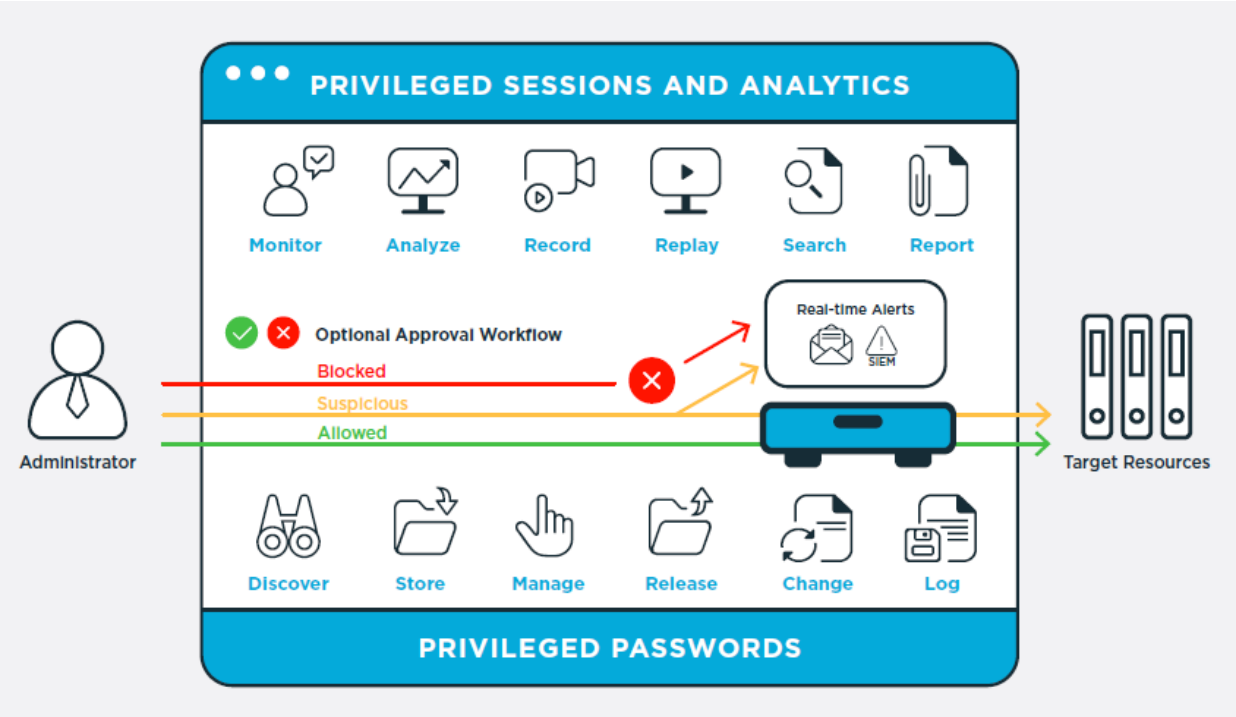


圖 1-One Identity Safeguard 產品功能架構

2. AD 即時稽核與防護

Quest Change Auditor for AD 是一款可提供 AD 和 Entra ID 的異動稽核和報告功能，包括對群組原則物件 (GPO)、網域名稱系統 (DNS)、伺服器組態、巢狀群組等其他項目的變更，即時對事件內容進行人、事、時、地、物及操作來源 IP 等資料正規化，且不使用原生稽核方式來收集事件資訊，以降低對伺服器效能的影響，並省下儲存資源。另一項特點是即時警示及預防擅自變更行為，並限制授權使用者的控制能力，利用此保護機制強化內部控制符合相關國際法規 (GDPR、SOX、HIPAA、PCI DSS、FISMA 及 SAS 70)。

圖 2-Quest Change Auditor 產品功能架構

3. AD 備份與還原

大部份的企業針對 AD 備份大多採用是 DC 全機 OS volume 備份方式 (含 VM 快照)，但這種備份方式其實存在許多問題，包括無法還原整個 AD 網域和樹系、以手動還原 AD/DC 費時費力，且 Offline 方式進行會影響企業運作及傳統備份不提供"精細"還原，也無法得知哪些物件或屬性已被更改或刪除等，Quest Recovery Manager for AD 即是有別於傳統方式進行備份與還原，僅針對相關 AD Database、 log files、SYSVOL 及 Registry 進行備份，不受主機作業系統遭受勒索軟體等惡意軟體影響，可以透過乾淨同版本 OS 進行 AD/DC 線上不停機直接還原，或是針對 GPO 物件誤刪還原都可以，還原時間依 AD 檔案大小而定，從幾分鐘到數

小時就可完全還原，相當安全及快速，且平時也可以在網路隔離環境進行災難還原演練，驗證備份檔的有效性，提供災難還原計劃和工作流程，以符合合規性要求，強化企業資安韌性。

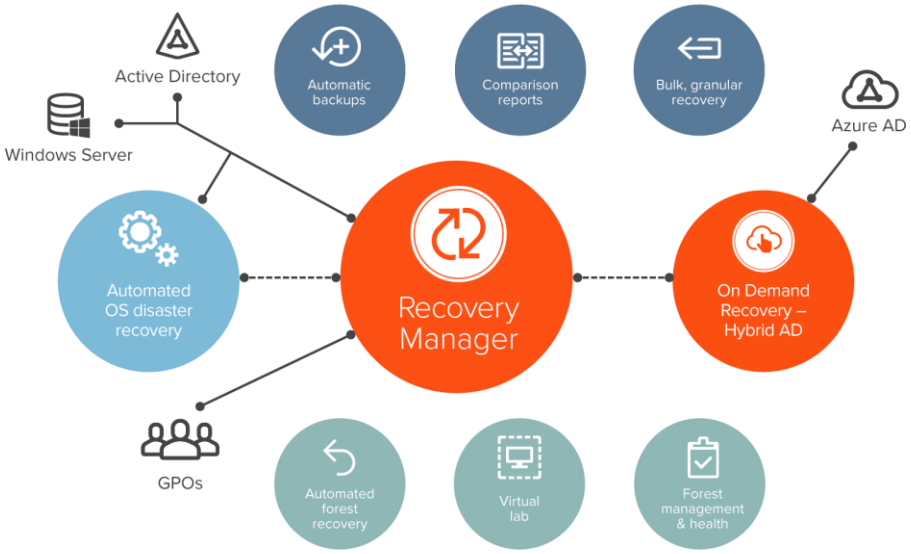
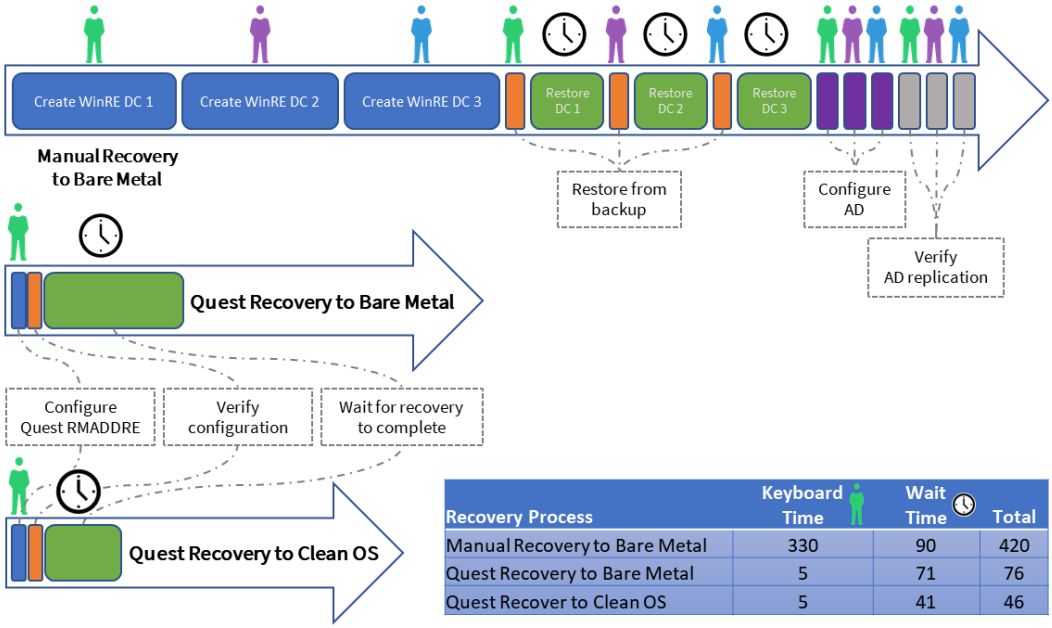


圖 3-Quest Recovery Manager for AD 產品功能架構



Recovery Process	Keyboard Time	Wait Time	Total
Manual Recovery to Bare Metal	330	90	420
Quest Recovery to Bare Metal	5	71	76
Quest Recover to Clean OS	5	41	46

圖 4-Quest Recovery Manager for AD 與傳統備份還原時間比較

4. AD 管理優化

One Identity Active Roles 提供 AD 及 Entra ID 雲地混合環境單一界面來進行帳戶管理及報告，透過自動化和自助服務來簡化和加速帳號管理流程，提升安全性和合規性，減少人為錯誤和管理成本，以下是幾點 AD 管理工具的效益：

- 分權管理：在組織中不同區域單位，可分層授權交由 OU 管理人員自行管理及 reset 個人密碼功能。
- 簡化 AD 管理：面對帳號變動頻繁或複雜環境下，透過管理工具執行等同在 AD 上執行多個複雜動作，可排定工作流程自動化執行，降低人為疏忽風險。
- 異動紀錄：擁有物件 audit trail 稽核軌跡及相關報表，可細到單一屬性或群組成員新增異動。

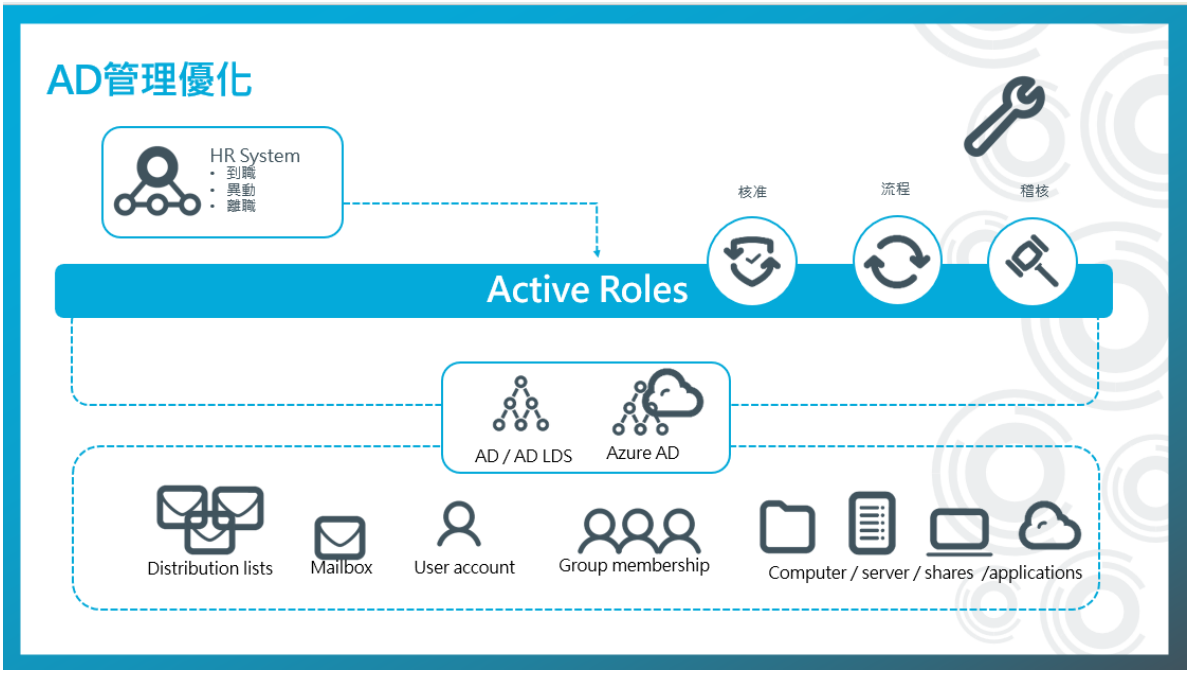


圖 5-One Identity Active Roles 產品功能架構

通過實施全面的 AD 存取安全與防護解決方案，企業可以有效地預防、檢測和應對各類潛在的威脅，保障企業內部系統和資料的安全性，具體措施包括強化身份驗證、嚴格的權限管理、及時的安全更新版本，以及持續的監控和風險評估。

AD 的安全防護不僅是技術問題，更是企業整體資安策略的重要組成部分。若想了解更多強韌企業資安的相關信息，誠摯邀請您一同參加於 6/20 台北茹曦酒店舉辦的【強韌資安 邁向永續】交流會活動，確保資訊系統和資料機密性、完整性及可用性，企業方能在追求永續發展中獲得信任與支持，實現永續經營目標。

**附上產品與 ISO/IEC 27001:2022 對應表

控制名稱	RMAD	CA	ARS	SG
5.16 身分管理控制			√	√
5.17 身分驗證資訊控制				√
5.18 存取權限控制			√	√
5.19 供應商關係資訊安全				√
5.28 證據的收集		√		√
5.29 中斷期間的資訊安全	√			
5.30 營運連續性資訊通訊技術準備	√			
5.37 記錄操作程序		√		√
6.7 遠端連線工作控制				√
6.8 資訊安全事件報告		√		
8.2 特權存取權限控制				√
8.3 資訊存取限制控制			√	√
8.5 安全認證的控制				
8.13 資訊備份的控制	√			
8.15 日誌的控制		√		
8.16 監控活動的控制		√		
8.18 使用特權工具程式的控制				√
8.24 使用加密的控制				√

以下資安事件網路資料，不代表倍力立場，僅供參考：

1. AT&T 個資外洩事件 https://www.bnext.com.tw/article/78718/at&t-cyberattac-telecommunications-industry
2. NTT West 客戶資料洩露事件 https://www.theregister.com/2024/03/01/ntt_boss_resigns_dataleak/