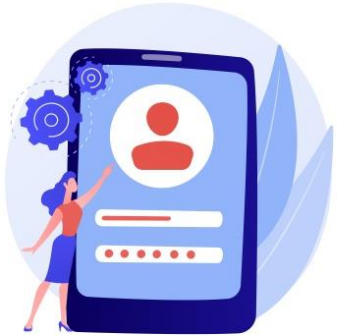
重塑零信任 防禦新戰略

ASUS OmniStor 企業儲存雲

企業網路環境的改變，帶來零信任架構需求

2020/8 頒布 SP 800-207 標準



BYOD 與雲端服務興起

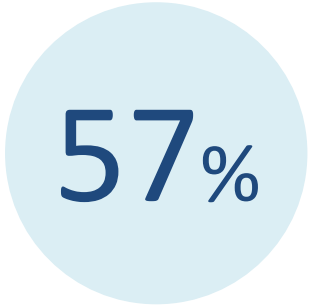
WFH 驅動數位轉型

asusCLOUD

企業須重新思考如何做到更嚴謹的資料存取控制

企業大量使用雲端服務
帶來的新風險

企業認為在家工作期間
難以控管員工檔案使用行為



企業開放 BYOD
和透過家用網路連線的風險

Source : Palo Alto Networks《2021台灣資安現況報告》

asusCLOUD

突破思維，打造企業零信任資安架構

Source : Stealth Labs《How Businesses Can Implement “Zero Trust Security”？》、NIST《Zero Trust Architecture》

企業面對行動及遠距辦公趨勢下的隱憂

企業 BYOD 如何確保
裝置登入安全？

強制綁定，保障員工裝置
的應用安全性

如何避免裝置遭竊或遠距辦公
導致的惡意登入？

身分登入控制與裝置管理
阻斷威脅

如何舉證員工符合
最小權限存取的管理機制？

完整報表及盤查
隨時稽核，確保企業內存取授權

ASUS OmniStor

最適合中大型企業的 雲端儲存與分享平台

以 SaaS 商模提供原生於雲、安全且支援多雲應用的資料保護服務，讓企業在面對混合型態的數位辦公，兼顧資料安全治理與高效協作，透過應用及服務虛擬化、雲端化逐步實現新一代資料治理，強化企業數位韌性

OmniStor Platform 核心儲存平台

提供企業使用者針對一般、機密與外部檔案進行儲存、分享、編輯等檔案協作應用

OmniStor Manager (OSM) 管理平台

提供企業 IT 管理者帳戶存取、群組授權、檔案日誌及資源監控等應用，可設置多位管理者

OmniStor Apps 使用者存取應用程式

提供使用者透過電腦、行動裝置、網頁瀏覽器、檔案串流 (Remote Drive) 及郵件傳輸 (Outlook Add-in) 等多元應用程式同步、存取與分享檔案

OmniStor Add-ons 加值應用服務

OmniStor Office 文件共同編輯 (加購)

提供企業於安全的內網環境下進行常見文書個人及共同編輯，支援行動平台響應式操作

OmniStor Protect 個資及敏感資料偵測 (加購)

提供企業針對個資及敏感資料設定風險審核原則與盤點機制，建立風險檔案安全性政策

OmniStor 零信任四大戰略為企業打造堅實防護力

行動可用

控管及保護員工裝置
保障行動應用安全性

存取可控

從網域、身分到檔案
實施最小權限控管

風險可治

假設可能風險行為
建立零信任防護機制

軌跡可視

完整掌握使用者
到管理者的操作行為

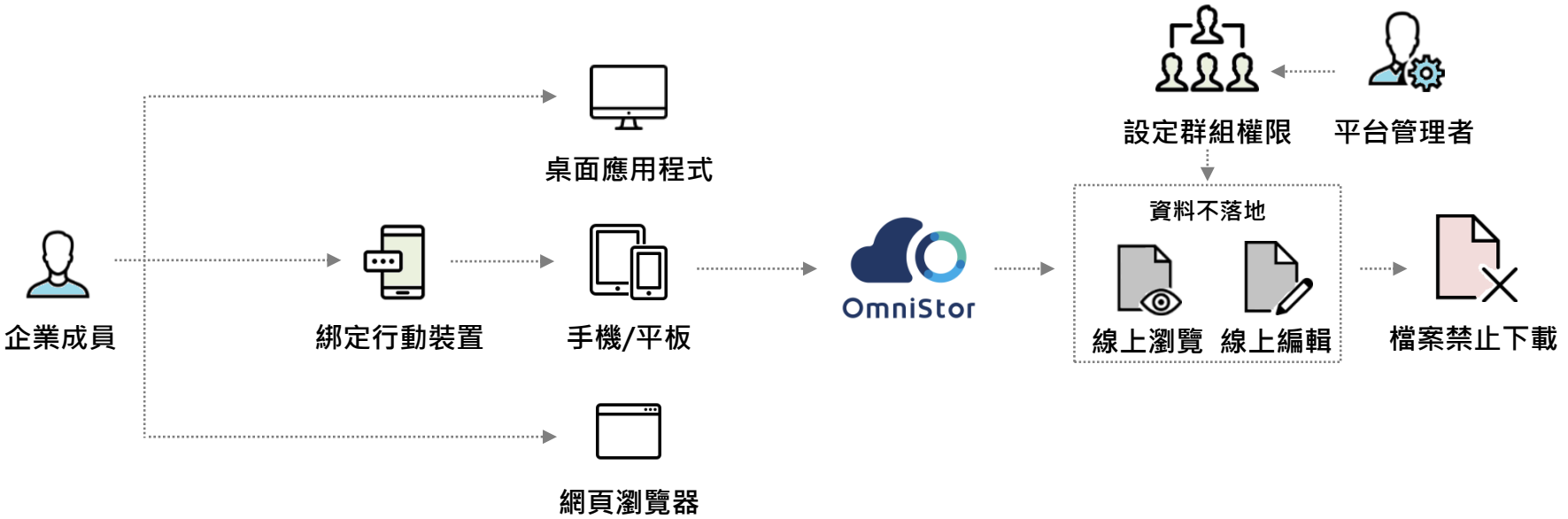
asusCLOUD

零信任4大防禦戰略

打造遠距及 BYOD 全方位檔案安全架構

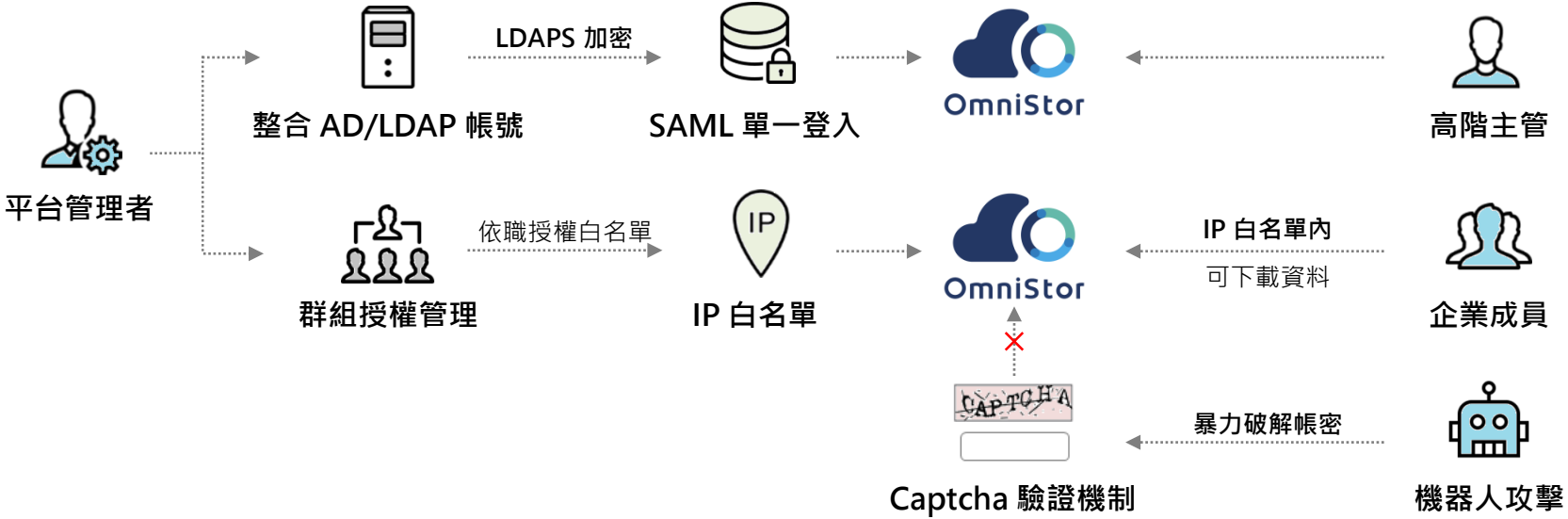
行動可用：多元存取，員工 BYOD 行動裝置綁定管理

「員工使用自己的手機或平板，企業如何保障使用的安全？」



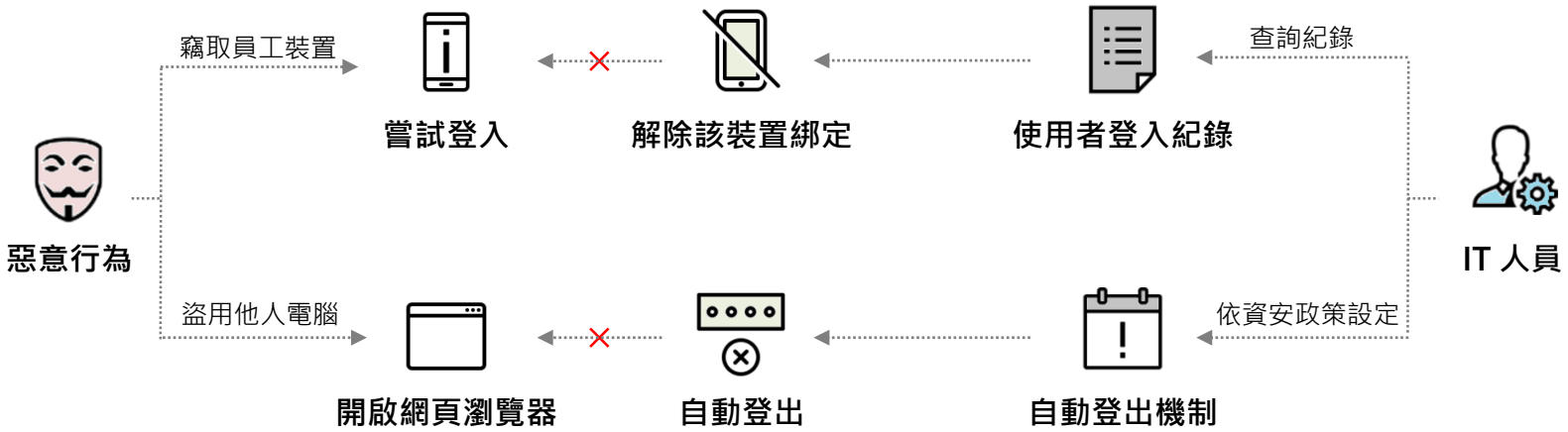
存取可控：遠距辦公登入驗證，強化第一道資安防線

「遠距辦公時，企業如何確保員工登入存取的安全性？」



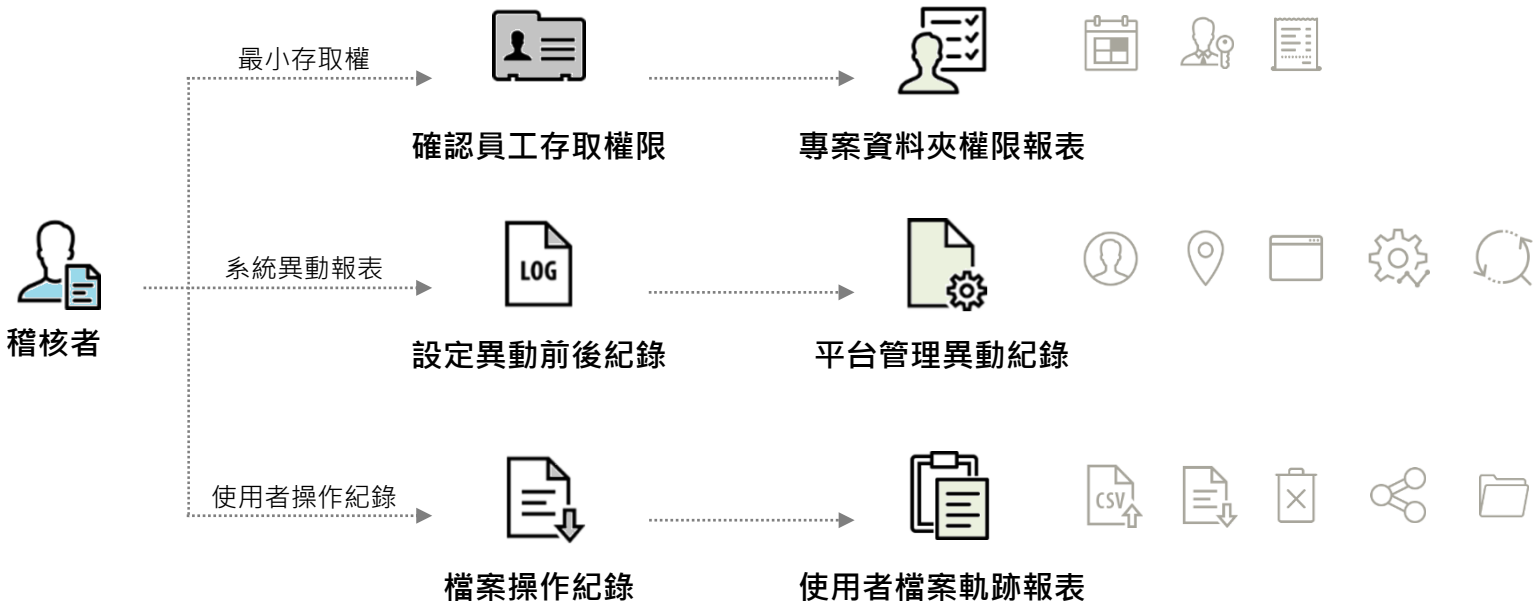
風險可治：防範惡意行為，強化內外部威脅防護政策

「資安攻擊事件不斷，企業如何防範有心人士的惡意行為？」



軌跡可視：完善使用與管理軌跡紀錄，滿足稽核需求

「企業例行性內外部稽核，如何舉證企業檔案行為符合資安原則？」



滿足行動化商務需求，兼顧企業資安控管機制

行動可用

隨時隨地存取

強化行動裝置管理

存取可控

登入限制

確保身份驗證安全性

風險可治

強化防護機制

預防可能的惡意行為

軌跡可視

完整行為紀錄

確保最小存取權限

asusCLOUD

ASUS OmniStor

想了解更多產品資訊，請與我們聯繫： info@asuscloud.com

asusCLOUD

THANK YOU