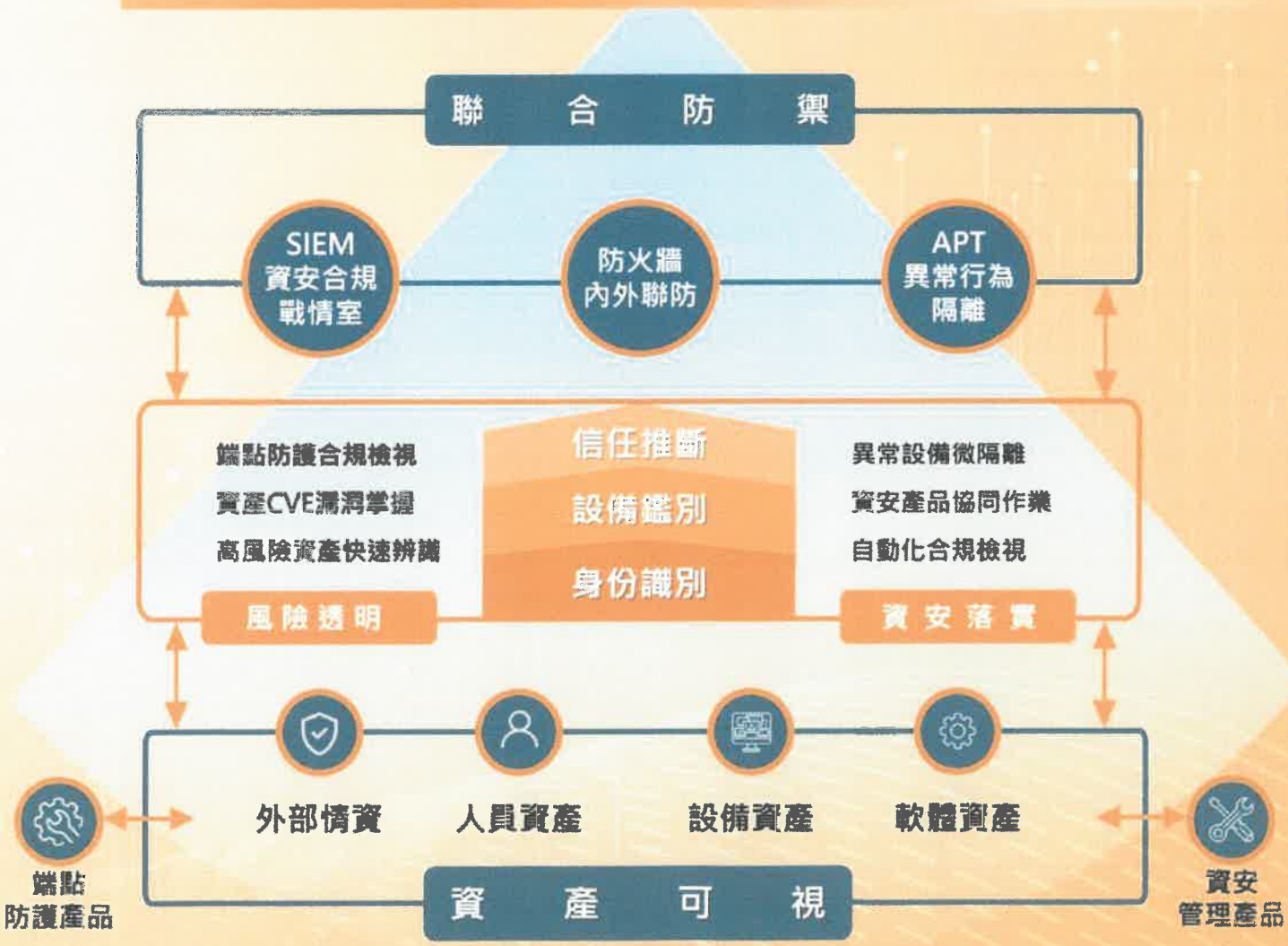
e-SOFT
曜祥網技

零信任解決方案

全方位資安智慧平台
Security Intelligence Portal (SIP)

精準落實 資安治理



ZTA零信任資安框架 全面落實零信任防禦

全方位資安智慧平台
Security Intelligence Portal (SIP)

全方位資安智慧平台(Security Intelligence Portal, SIP)，提供企業全面性的自動化合規檢查及矯正機制，透過整合企業既有資安管理系統，有效的提供企業環境資訊資產的風險可視性及透明度，結合企業落實資安管理政策，強化資安基礎建設防禦力，提高資安治理成熟度。

全面落實零信任框架

- 支援各種網路架構部署，無需改變企業現有環境。
- Agentless 資料搜集技術，真正將設備全面納管。
- 完整的端點設備資安合規檢查，提早找出風險設備。
- 內建80種以上國際資安查核ISO27001:2002 (ISMS)、供應鏈資安合規報表。

Pre-Check、Re-Check 自動矯正

- 發現不符規設備立即告警並阻斷網路。
- Pre-check：針對新接入設備自動檢查相關資安管理agent 落實安裝。
- Re-check ：於設備日常運作過程，持續檢測資安防護措施正常運行，提早發現漏洞。

集團企業，集中控管

三層式架構整合，集團總部可透過單一介面管理及掌握全球各區的資安管理政策完整性及有效性，如防毒部署率、Hotfix派送率等，統一管理、即時掌握各區設備健康狀態。

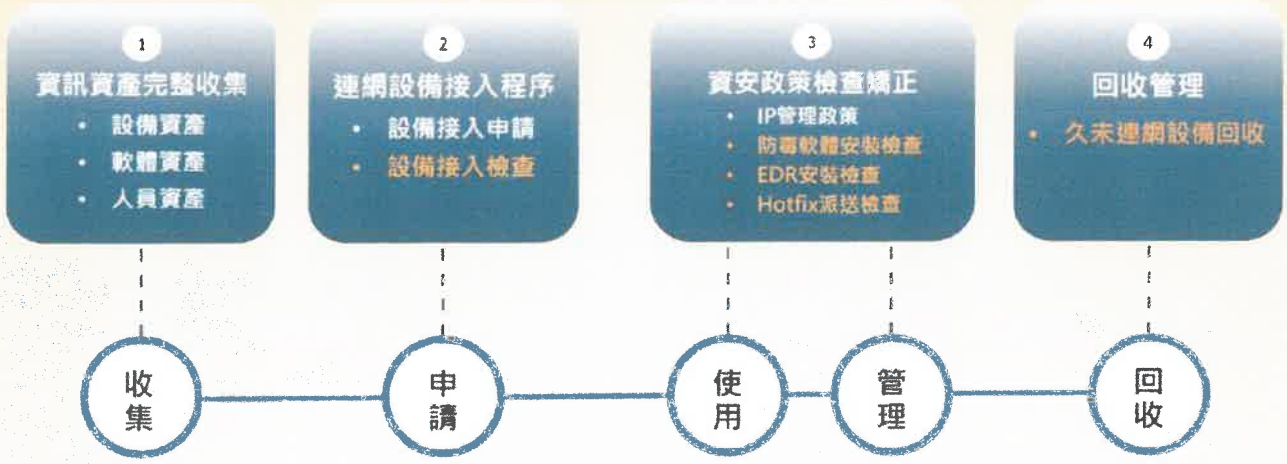
資安聯合防禦

- 與防火牆、IPS 及SIEM 等資安產品進行整合，達到內、外網資安系統協防運作模式，提升主動防禦力。
- 操作簡易、容易部署、主動防禦，降低管理員單台設定負擔。

Dr. IP IP資源管理系統

連網設備全面盤點及自動化管理

最完整的IP生命週期控管流程，採用旁路式及Agentless架構，可自動偵測所有連網裝置，並透過多種的設備識別技術掌握各種設備類型(Windows、Linux、Switch、IoT Device、中國廠牌設備等)，將外來設備全面納管，建構完整的網路存取控制流程。提供多種IP/MAC資安管理政策，配合資安法規落實管理，可產出超過80種資安報表，提升管理效益。



數位身份資產管理系統

使用者及設備資訊整合及權限異動告警

Agentless及最小權限的架構，可完整的掌握設備本機的資訊，分析異常資訊行為並告警，例如重要權限變動、異常時間登入等，再搭配整合Windows 網域系統(AD)機制 ，更達到設備實名化管理，大幅簡化管理作業，提早發現風險。

- Windows設備網域符規檢查
- AD帳號登出入稽核軌跡
- 本機人員帳號/最高權限帳號盤點
- 分享資料夾啟用及權限盤點
- SID重複稽核
- GPO套用檢查
- 本機提權告警

資訊資產風險評鑑系統

跨平台軟體資安弱點通報，快速因應及矯正

- 支援Windows、Linux 及 MacOS 進行設備軟體資產盤點。
- 排程定時更新外部 CVE 情資資料庫，保持取得最新漏洞資訊。
- 自建軟體漏洞通報機制(VANS)，節省手動繁鎖轉換步驟，VANS系統軟體資產直接上傳。
- 依據不同角度(設備、軟體、CVE)產出漏洞報表

GCB/FCB 檢核系統

GCB/FCB 組態稽核，盤點、修正、備份

依據「國家資通安全研究院或F-ISAC公告GCB及FCB範本」，檢核包含 Windows, Linux, Office, 瀏覽器及網通設備的GCB/FCB 有效性，並對於不合格的組態項目提供一鍵修正，確保設備符合安全規範，簡化管理者查核作業，提高GCB/FCB套用完整性。

- 內建所有GCB設定，定時自動檢測，避免漏網設備。
- 可依需求建立設備組態檢核群組，並依各自檢核群組進行組態盤點及修正。
- 支援手動/自動建立設備組態備份還原點，在GCB 套用過程有誤時，可還原至最初環境或備份點。

Smart AD網域組態盤點管理系統

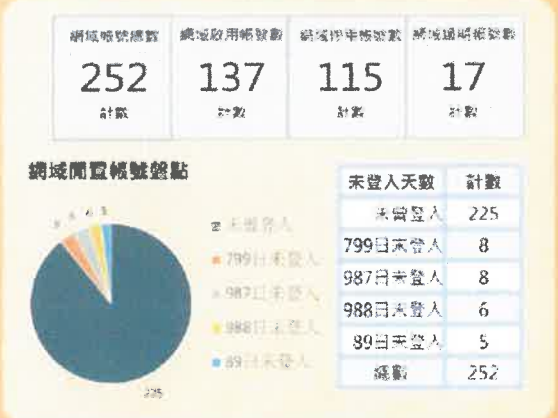
網域物件盤點、稽核及異動分析

整合Windows 網域系統(AD)，強化企業Windows 設備端點管理，透過Agentless及最小權限的架構，進行Windows 網域及設備資料收集。除了可取得使用人員帳號達到設備實名化管理，並能夠有效的收集設備本機的資安稽核相關項目之資料，簡化管理者作業。

- 網域帳號及權限群組盤點查核
- 網域帳號生命週期管理查核
- 網域帳號異動查核
- 網域帳號提權告警
- 網域群組原則異動告警

✓ 重點追蹤項目

- 離職員工網域帳號盤點
- 高權限群組離職管理者盤點
- 異常鎖定網域帳號盤點
- 閒置網域帳號盤點
- 本機預設高權限帳號盤點
- 未定期變更密碼帳號盤點
- 閒置本機帳號盤點

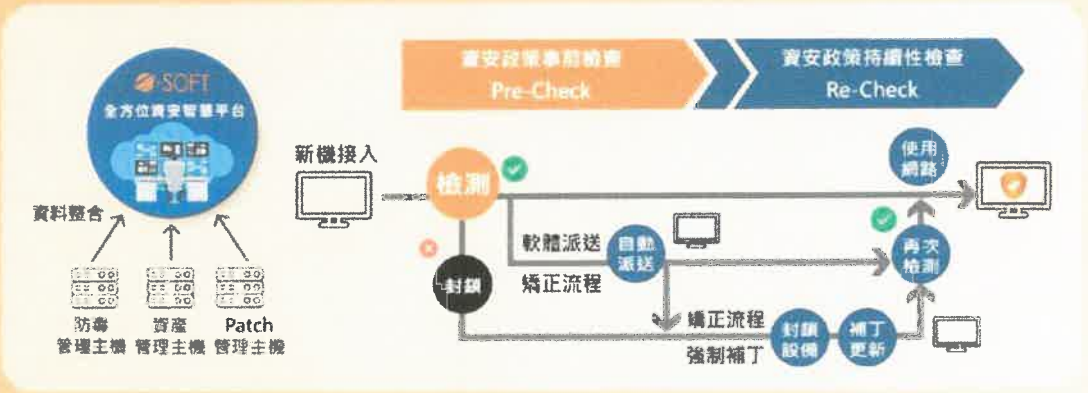


NAC++ 資安智慧部署管理系統

Pre-Check及Re-Check 自動矯正流程

整合至少40種以上的資安管理系統，包含防毒軟體、DLP軟體、資產管理軟體、EDR軟體等，協助企業打造完整及有效的資安檢查覆核機制，透過NAC++協同防禦管理，讓資安防護更完善。

- 資安管理KPI指標檢核。
- 產出ISO27001:2002(ISMS)，各類的國際資安稽核報表。
- 建立設備進機健康檢查流程，重要事件自動告警。
- 零信任網路下的設備健康檢查(信任推斷)。
- 部署完整性：全面監控企業內部電腦是否都依公司規範安裝Agent。
- 部署有效性：管理者輕鬆掌握資安軟體部署率與政策執行落實度，大量節省人員檢核工作時間。
- 自動化矯正方案：橫向整合矯正機制，整合資產軟體達成自動派發矯正。

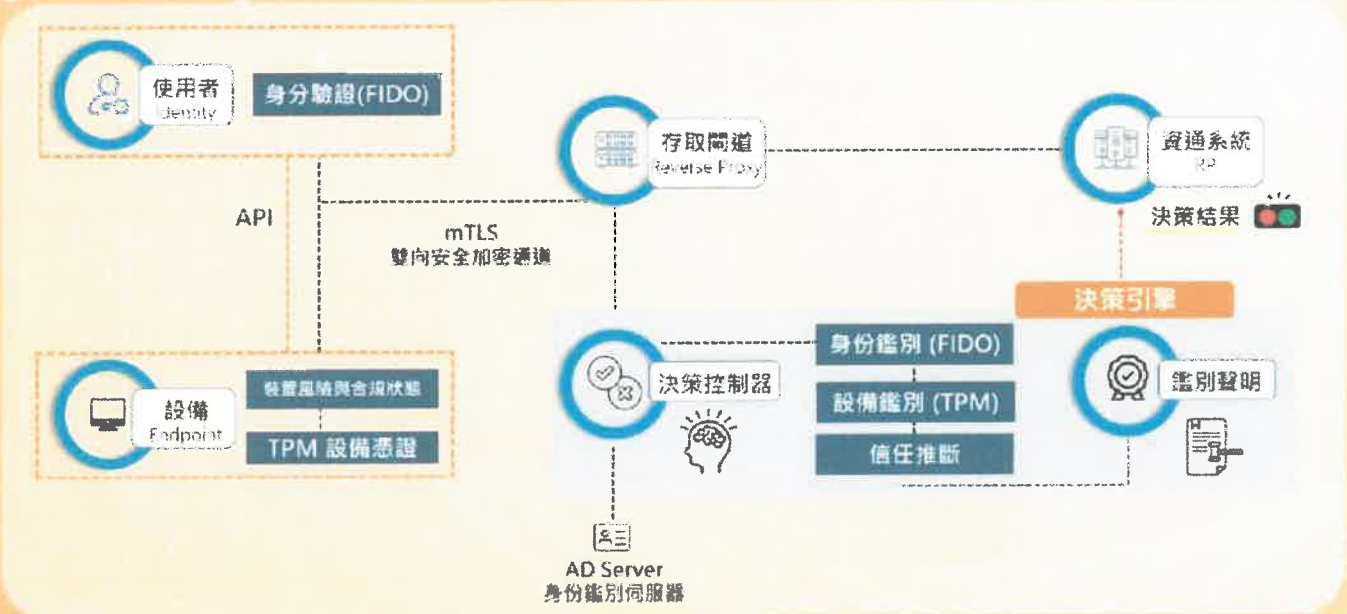


ZTA 零信任管理系統

持續驗證，全方位保護網路安全

零信任管理系統擴充基於國家資通安全研究院推動之零信任架構三大核心架構，提供企業可針對重要關鍵應用服務建立零信任存取流程，於服務連線開通前，有效識別用戶端及確認設備健康檢查合規狀況。

- 支援建構Web Portal Connection Base的零信任存取架構
- 身分識別採用AD認證並提供 FIDO無密碼驗證機制
- 設備鑑別採用TPM硬體晶片識別及軟體金鑰識別的技術
- 提供Score-Base 評分機制，有效檢查用戶端設備之合規狀況



看得到風險，才能管理風險

- **風險可視**：改善內網連網設備可視性
- **風險透明**：掌握高風險設備，挖掘企業資安管理安全點
- **資安落實**：落實資安軟體部署率
- **快速反應**：設備快速定位，縮短資安事件反應時間
- **化被動為主動**：由被動反應轉化為主動預防
- **零信任架構**：完整IP週期控管，零信任資安框架支援整合

e-SOFT
曜祥網技

TEL：(02)2712-2195
e-mail：sales@e-soft.com.tw
https://www.e-soft.com.tw