What's UPAS

NETWORK OPERATIONS CENTER

超越想像的資安管理效益

核心價值

確保每台接入網路的設備都是安全的

對於嘗試存取網路的設備，自動進行入網前安全檢查與修補，包含：登入網域、Patch更新、防毒軟體安裝、病毒碼更新、應裝軟體安裝、禁用軟體使用，軟體漏洞修補，GPO套用等檢查項目。

建立內網邊界防護

全面盤查資訊資產，未經允許的外來設備不得接入網路，避免私接設備造成風險

IoT資產盤點統計

100%盤點連線設備，並自動蒐集名稱、屬性、OS、廠牌、使用時間等詳細資訊

完善IP管理流程

提供IP申請、預約、保留、保護、例外、回收等功能，和IP使用紀錄、配置列表、開關機統計等報表

完善軟體管理政策

提供設備安裝軟體總表，檢查Patch、防毒、應裝軟體更新，並控管禁用、版權軟體

完善設備管理政策

提供硬體安裝資訊，並能進行USB管理、遠端桌面、軟體派送、軟體移除、訊息推送、檔案加密等功能

建立員工與訪客管理流程

提供員工BYOD、企業設備、和訪客身分驗證自動化流程，可限制使用權限並保留紀錄

符合法規與供應鏈查核

提供最全面的資安報表，協助組織通過資安法、NIST CSF、ISO27001、SEMI E187等各項法規稽核

NAC · ITAM

VANS · GCB

Why UPAS

NETWORK OPERATIONS CENTER

安全穩定便捷．內網管理領導品牌

98%

多項符規指標

- AD完善率
- 補丁更新率
- Agent安裝更新率
- 防毒軟體安裝更新率
- 應裝軟體安裝率

UPAS NOC 導入效益

- 確保網路正常運作
- 防止機密資料外洩
- 符合供應鏈查核
- 防止勒索病毒

系統部署簡易

使用專利技術，安裝建置容易，網路設備不須支援802.1X協定、不用安裝代理程式，彈性適應環境。

無痛安裝設定

內建系統設定精靈，快速安裝不須繁瑣操作，導入環境後政策設定一鍵完成。

智能化自動化系統設計

包括自動加入白名單，自動分群，自動派送Agent，自動套用群組政策進行合規檢查，自動隔離修補不合規設備，修補後自動恢復設備連線，輕鬆達成效率管理。

99% 資訊收集完善率

能完整辨識與紀錄設備資訊，包括設備屬性，電腦名稱，Agent部署率，終端設備合規檢查率，都可以達到99%的收集完善率。

99% 設備異動維持率

可於設備資訊如屬性、名稱、Agent狀態、OS、S/W Port更動時，自動即時更新於管理頁面，不須管理人員手動更新，達到99%的異動維持率。

友善的UI UX設計

NOC首頁可自訂顯示資訊，協助管理者有效掌握網路動態，並提供Agent UI/重導頁面/MSG訊息/訊息推送等多種告警功能，增加使用者資訊可視性。

大幅提高Agent部署率

透過全面盤點資產，建立Windows設備清單，再透過AD主機派送Agent，若AD派送失敗可再透過WMI推送進行精準再派發，將管理黑數補齊，達到98% Agent部署率。

豐富產業報表

系統內安控中心和資產統計儀表板可以整合所有內網資料，產生共計55種圖表及198項內網安全統計分析項目，並可依據產業稽核需求任意組合報表項目，例如金管會法規、ISO27001等。

風險管理與系統保全機制

系統停止運作時，不影響網路連線；系統保全機制可偵測人為與非人為的異常行為，自動轉換為監視模式，避免誤擋造成損害。