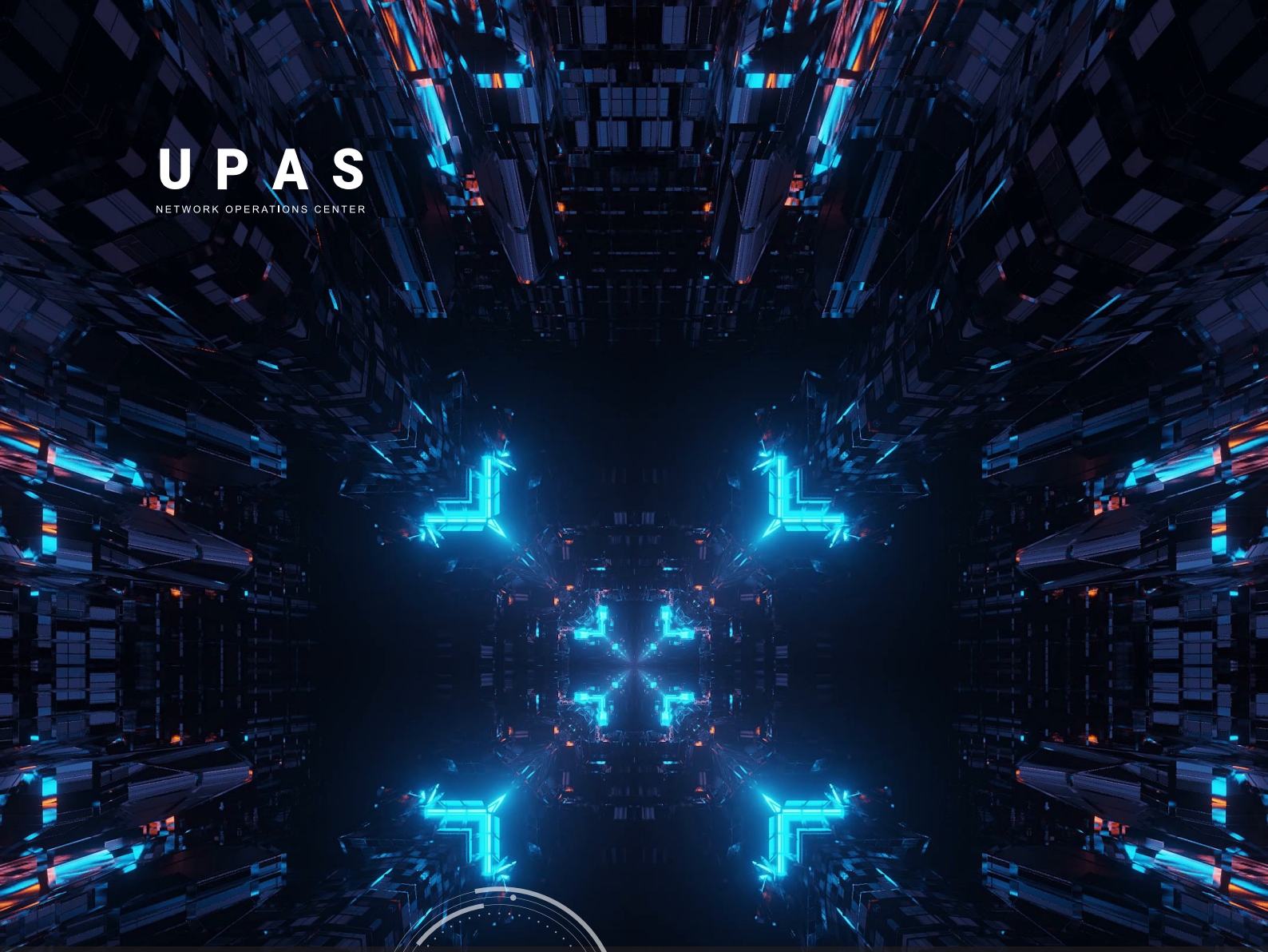

UPAS
NETWORK OPERATIONS CENTER

防禦勒索軟體

UPAS NOC
構築零信任防禦網

UPAS NOC在內網管理的層面可以說是面面俱到，其中多項功能都可以有效地將勒索軟體阻擋於內網之外。UPAS NOC以**零信任架構**將安全性漏洞所產生的影響降至最低，並可在駭客展開目標式滲透時，於多個環節即時發現異常。

面對勒索軟體及駭客事件
UPAS NOC
如何部署防禦機制

UPAS NOC 防禦機制

查找弱點設備

資產盤點：無未控管設備

- 設備白名單（NAC）
- 開關機報表

設備合規檢查：無安全漏洞

- WSUS納管
- AD帳號納管
- 防毒軟體安裝/更新
- 資產軟體安裝/更新

入侵設備

數據流量監控：無異常流量

- 監控不該連線時段
- 正常時段連線數異常

取得高權限

AD使用紀錄：無最高權限帳號變動

- 電腦設備本機登入
- 遠端登入
- 高權限使用者
- RDP連線設備

大量組態異動

設備組態行為檢查：無異常行為

- 新增非法軟體
- GPO政策變動
- 開啟高權限之資料夾分享
- 其他異常行為

惡意攻擊！

UPAS NOC
防禦機制

全面性資產盤點！
98% 業界最高設備納管率

資產盤點與管理為一切資訊安全的源頭，只有將全部連網設備都納入管理才能達到最安全的內網環境。UPAS可以做到業界最高的98%設備納管率，管理內網上的所有設備，並以此為基石加上獨特的設備白名單與合規檢查方式查找弱點設備，達到持續性的防禦與管理，讓勒索軟體無機可趁。

開關機報表
迅速掌握內網設備概況

UPAS可以產出電腦設備的開關機資訊報表，讓管理者可以透過報表內容了解設備的大致狀況。除了設備開關機報表，還有提供其餘55種報表與198項分析項目，協助管理者更加了解內網設備狀態。

- **設備久未開機**：OS Patch、防毒軟體及病毒碼未更新造成安全性漏洞。
- **非正常時段開機**：可能成為駭客攻擊目標。
- **設備異常開關機告警**：可監測異常活動如安裝惡意程式等。

整合多重伺服器
設備合規檢查無死角

過去設備合規檢查總是有道難以越過的難關，因設備數量與狀態的不清楚，導致無法有效率地確認設備是否更新到了最新的版本，UPAS透過98%的設備納管率解決了這項問題。

資產清單與設備狀態圖表，詳盡的顯示內網內設備所使用的系統與版本，同時可以介接WSUS伺服器，查找是否有最新的版本應更新並強迫設備進行更新。

UPAS的補丁管理同時可以做到防毒軟體與資產管理軟體安裝與更新的功能，確保病毒碼維持在最新的版本。並可以檢查應裝軟體是否正確安裝，是否安裝非法、盜版軟體，減少使用盜版軟體所造成設備資安事件的發生。

AD管理
完成最小權限帳號管理！

本機帳號的控管是一項對防禦勒索軟體很重要的事情，最小權限的帳號管理可避免駭客透過本機帳號的權限進行破壞。

UPAS的AD管理可以限制使用者只能以AD帳號登入使用，無法使用本機帳號登入，防止駭客安裝惡意軟體對內網造成危害。同時提供AD登入/登出時間紀錄，以管理內網中閒置設備或者使用RDP連線的設備，降低被駭客攻擊的機會。

數據流量監控
設備異常無所遁形

受到駭客控制的設備通常都會有異常的流量，UPAS能對網路使用狀況進行監測，控管終端設備網路使用行為。提供網路流量資訊，產生相關流量報告。並且提供網路攻擊分析，透過歷史紀錄分析可疑的網路攻擊。

組態行為檢查
及時告警．即刻防禦

當駭客已經取得權限且要派送勒索軟體至各設備時，UPAS可以及時告警組態的異常行為，如新增非法軟體、GPO政策的更動、開啟最高權限之資料夾分享等，讓企業可以及時阻止軟體的安裝與運作，降低損失的金額。