UPAS NOC
公部門產業方案

建立零信任安全架構杜絕資安風險

資安即國安

政府機關若發生資安事件，將面臨國安級威脅，根據iThome資料顯示，2019年有超過兩成以上的企業遭遇50次以上資安事件，其中更有四成的資安事件使服務中斷，六成的行動是資料盜竊，之所以有將近三成政府機關與學校視資訊安全項目為首要IT重點投資。2020年Q1的調查也提及勒索軟體事件比去年同期提升48%，完善資安防護刻不容緩，政府機關該如何有效因應呢？

UPAS 協助政府組織建立內網防護

01

資產數量不清、設備狀態無法掌握

現今的網路環境，除了OA區域的終端設備需要管理外，散佈在各處的監視器、刷卡機、網路印表機等IoT設備，也是資訊安全管理的重點。常見的終端管理方法為在每台設備安裝Agent，以監控各項設備，然而多數IoT設備、BYOD設備與訪客設備並不方便安裝Agent，如此便無法有效掌握環境內的資產屬性、軟硬體設備狀態，不僅造成管理困難，也讓內網環境的安全性留下疑慮。

02

疏忽外來人員的管理，造成資安漏洞

政府機關有許多訪客，不論是外賓、洽公市民或是委外廠商，相關人員時常需要接入網路，若讓管理人員逐一進行接入允許與權限設置不但耗時費工，且無法對接入設備進行有效的安全性檢查；也必須在相關業務處理完的時候手動卸離網路使用權限。以上步驟若有缺失，容易造成網路環境出現安全漏洞，導致惡意程式入侵、資料竊取等資安事件發生。

03

IPv6將全面取代IPv4，政府機關該如何因應

台灣政府機關已全面IPv6化，民間IPv6的使用率也來到全球第6名，代表未來幾年內，使用IPv6接入網路的使用者將會逐漸增多。在現今IPv4、IPv6並行的環境下，如何同時對兩種協定進行有效率的管理，成為政府機關須立即解決的問題。

04

法律規範之下，該如何選擇合適的資安防護

在《資通安全管理法》與其子法的規範下，相關機關應於規定時間內通過ISO 27001認證或NIST CSF，並完成GCB的導入與檢視資通系統防護基準之措施。《個人資料保護法》則要求公務機關應採取適當措施，防止個人資料遭到竊取、毀損。

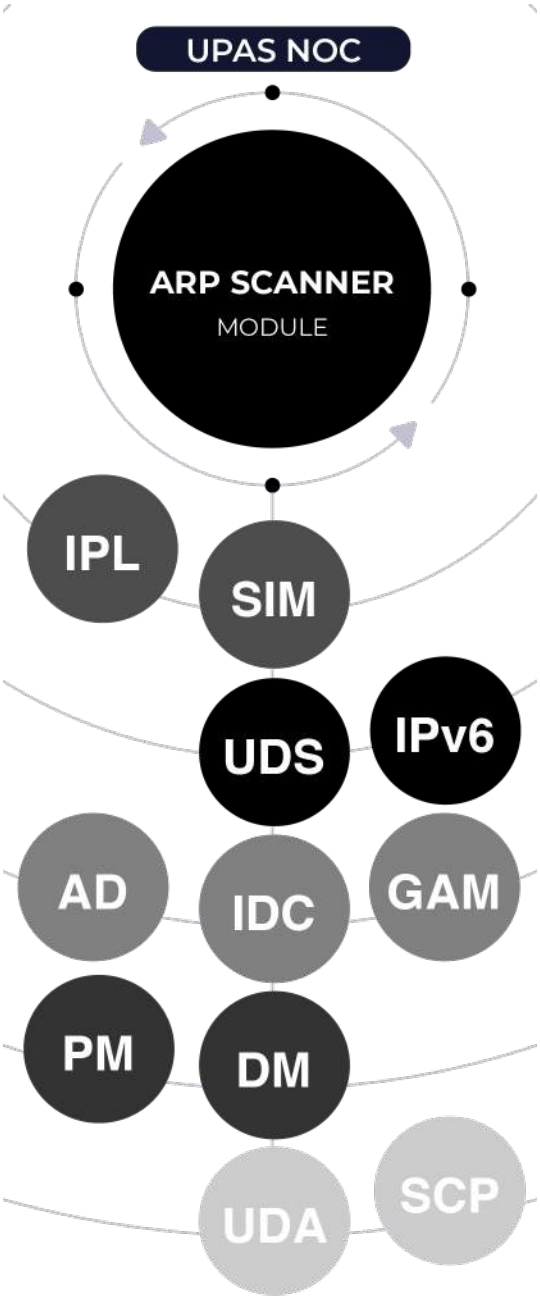
於2019年就發生過某政府部會遭木馬程式入侵，因而外洩數萬筆公務人員個資的事件，外洩的內容包含了國安人員的個人資料，不僅讓這些同仁陷入危險，也對國家安全造成嚴重的影響。

在資安預算有限的狀況下，要如何建立符合ISO 27001標準的ISMS系統，或是採用 NIST CSF，並同時遵守其他法律的規範，對相關單位都是一項挑戰。

UPAS NOC
內網管理中心

運用專利ARP技術，達成內網全面管理

UPAS NOC採用專利ARP技術讀取網路封包，獲取上線設備資訊，自動建置完整內網連線設備詳細清單。



四大內網需求，UPAS一手掌握

UPAS NOC具備**網路存取控制(NAC)**的端點管理、**IP位址管理(IPAM)**、**身分識別管理(IAM)**以及**IT資產管理(ITAM)**等功能，能有效提升企業的整體網路安全，透過高整合系統大幅減低管理人員的工作負擔，一手掌握您的內網大小事。

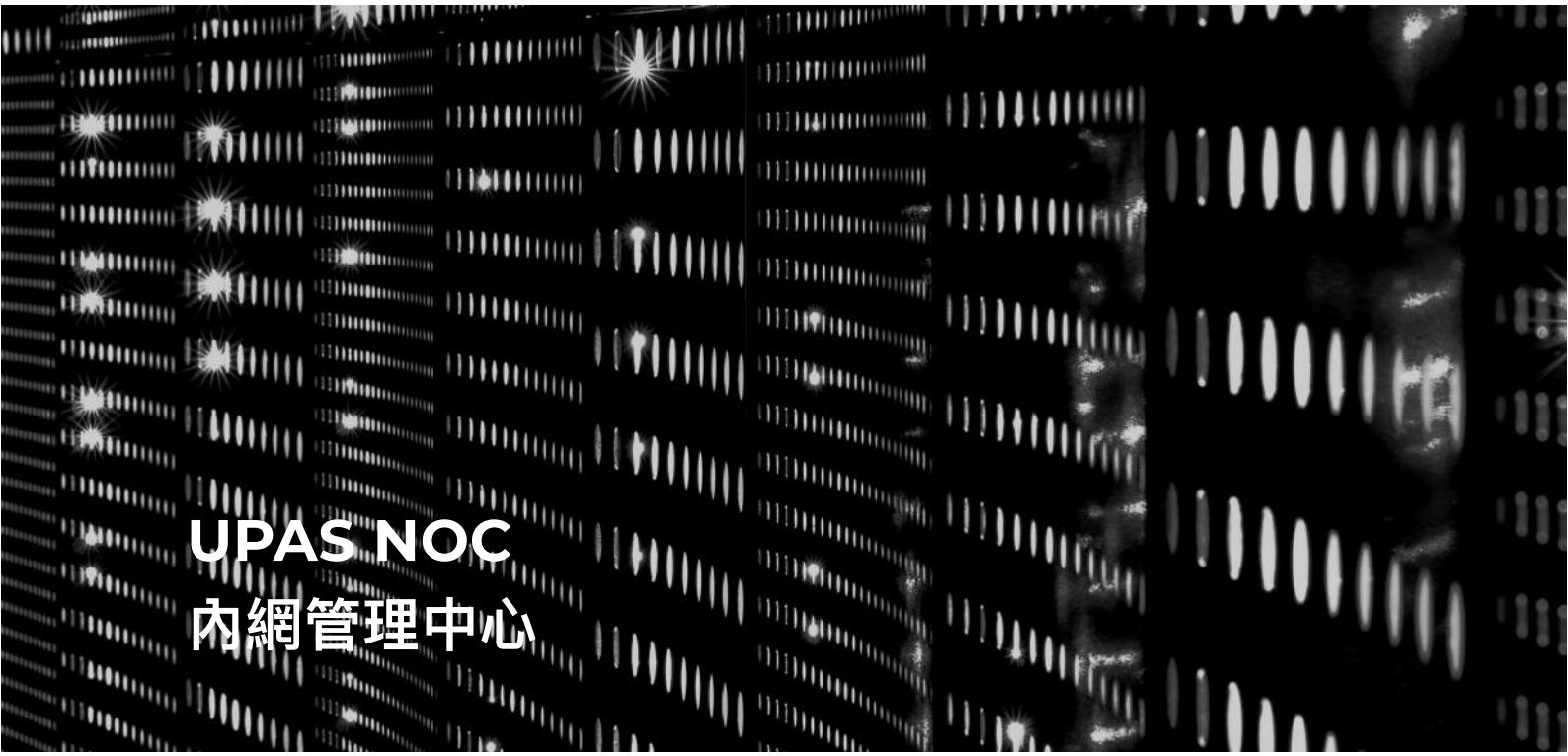
採用Agentless方案，適合各種網路環境

核心功能無須安裝任何Agent就能蒐集、辨識網路連線設備，可彈性適應各種環境。

非802.1X的管理方法，不用改變軟硬體設定，無須對企業環境進行軟體及硬體架構的重新佈署及升級，減少建置上人力與時間成本的耗損。

三層式管理架構，輕鬆解決跨國管理需求

採階層式架構，分為主Console系統串流暨管理平台，子Console系統管理平台，Sensor系統偵測器及Gatherer資料收集器。透過Sensor與Core Switch連接，可即時監測所屬內部網路，僅需使用Console介面進行管理。若有跨國、跨區域管理需求，可設定SCP主Console對各區域的Console進行資料整合以及統一管理。

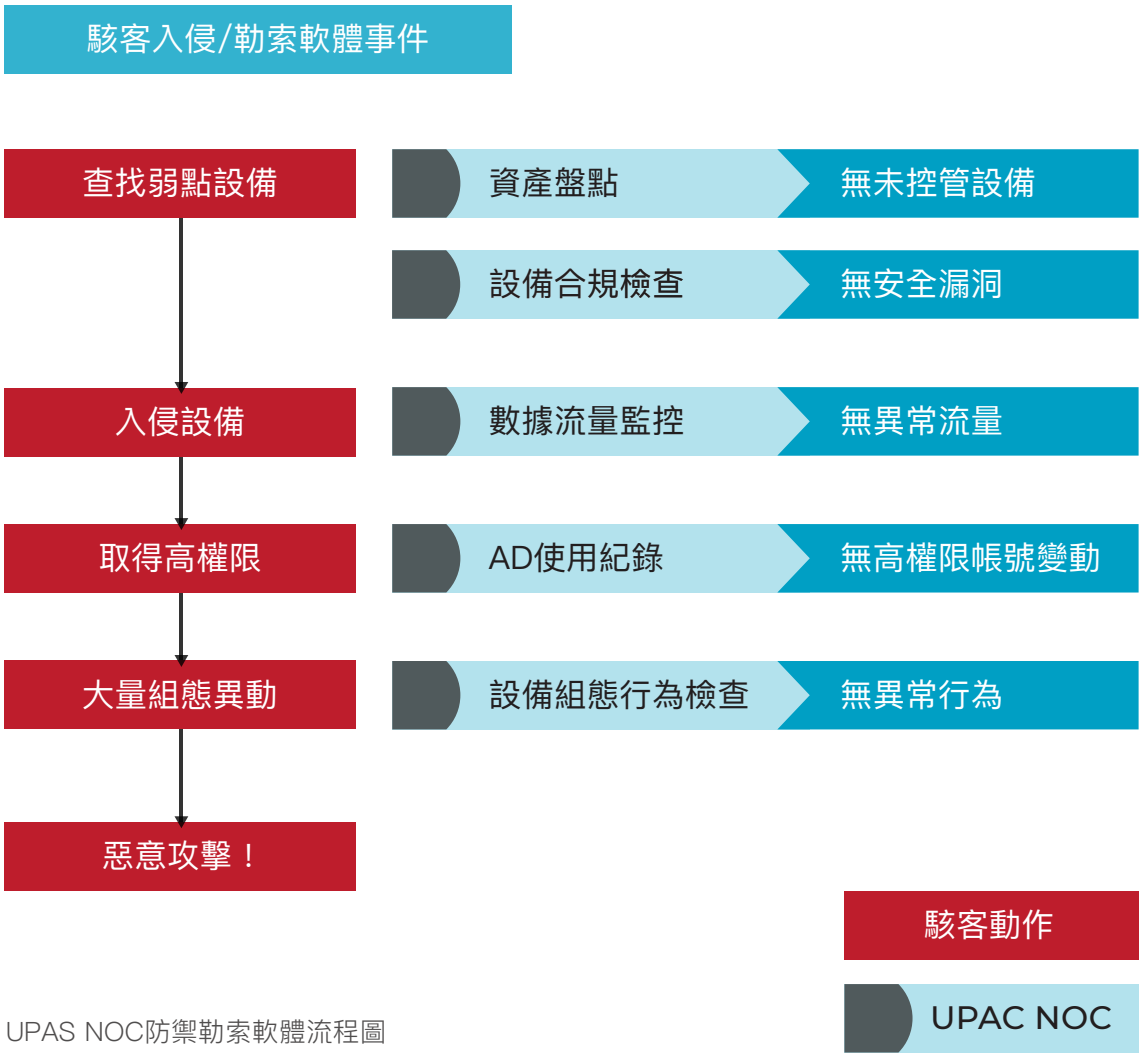


防禦勒索軟體

UPAS NOC 構築零信任防禦網

2017年肆虐全球的勒索軟體 —「WannaCry」，在150個國家造成超過40億美元的損失 ，以色列資安業者Check Point更指出，勒索軟體攻擊在2020年第三季大幅增加了50%；台灣尤其是駭客的攻擊熱點，光是2020年第四季，就有逾10家台灣上市櫃企業遭駭客入侵、勒索，不斷飆升的攻擊頻率和動輒上億台幣的贖金，讓勒索病毒防禦成為現代企業不可忽視的資安重點。

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，在攻擊發生前檢視高風險可疑活動，防範勒索事件於未然；UPAS NOC 透過設備白名單、合規檢查方式查找弱點設備，以此達到持續性的防禦與管理，其中設備合規檢查涵蓋WSUS納管、AD帳號納管、防毒軟體安裝/更新、病毒碼更新，將漏洞可能性降至最低；而異常行為報表及告警可協助管理者察覺入侵行為，即時修補防止損失的擴大。



UPAS NOC防禦勒索軟體流程圖

VANS (Vulnerability Alert and Notification System)

政府機關資安弱點通報機制

由行政院國家資通安全會報技服中心所打造的**VANS系統**可以將各級機關所提供的軟體資產報表與**NVD** (NIST弱點資料庫)比對，找出各機關的資安弱點，即時通知該單位以便在第一時間修補漏洞、消除資安風險，強化政府部門的軟體資產管理。並於**《資通安全管理法》**在各級政府機關應辦事項中明文規定，資安責任等級**A級機關**，**110年度**必須全部導入VANS系統，**B、C級機關111年度**也必須跟進。

導入VANS系統有以下三項程序：一、**盤點軟體資產**；二、轉換資產清單成**CPE格式** (Common Platform Enumeration)；三、**上傳VANS系統**進行比對；此三項程序難以手動作業，各單位都需要建置**第三方資產管理軟體**輔助執行，以下羅列UPAS NOC提供的解決方案和一般資產管理軟體效益對照表：

當前環境	尚未購置資產管理軟體	已購買資產管理軟體	
解決方案	UPAS NOC **PM補丁管理模組**	第三方資產管理軟體 +UPAS NOC **SIM安全整合模組**	只使用 **第三方資產管理軟體**
是否安裝 UPAS Agent	是	否	
終端設備盤點	使用UPAS NOC的專利ARP封包解析技術，免安裝Agent即可輕鬆**盤點環境中所有上線設備**，並能自動辨識資產屬性等詳細資料，確保設備**100%納管**，大幅提升環境中設備的可視性		**缺乏終端設備盤點措施**，大多透過AD主機直接派送Agent，無法確保所有終端設備部署成功
軟體資產盤點 CPE格式轉換	可持續盤點所有軟體資產，**自動轉換CPE格式**，並針對應裝軟體、禁用軟體和版權數量進行管理	**介接第三方資產管理軟體資料庫**，藉由比對完整的監測清單，毫無遺漏地找出未部署或未更新第三方資產管理軟體Agent的設備	Agent部署率、更新率不足，**業界平均終端設備納管率只有80%**，導致軟體資產盤點不全面，產生漏洞
上傳VANS系統軟體漏洞修補	可將CPE軟體資產清單**一鍵上傳VANS系統**，進行弱點比對，並可以高安全性的網路阻斷機制，引導不合規的設備進行**弱點修補**，協助單位消除內網安全漏洞	確保第三方資產管理軟體納管所有終端設備，**確實的盤點軟體資產**並上傳至 VANS，通過全面的軟體漏洞檢查和網路阻斷機制，有效消除資安風險	**終端設備納管率不足，軟體資產盤點不全面**，CPE軟體資產清單上傳VANS也無法比對出所有軟體漏洞，使單位暴露在**高度資安風險**下；且對軟體資產不合規的終端設備缺乏控制性

UPAS NOC 透過全面的資產盤點，同步將軟體資產盤查達到 98% 以上的完善率，並針對不同客戶的需求，提供兩種 VANS 系統解決方案：

01

尚未購置可協助導入 VANS 的第三方資產管理軟體需安裝 UPAS Agent

UPAS NOC PM 補丁管理模組可在終端設備全面盤點的基礎上，進一步盤點所有軟體資產，自動產出 CPE 格式軟體總表、一鍵上傳 VANS，輕鬆符合《資通安全管理法》對公部門的要求，並確保不遺漏任何終端設備的軟體漏洞。

該模組需要在終端設備安裝 UPAS Agent，除了可協助公家單位導入 VANS 之外，還可進行多項合規檢查，包含終端設備的 Windows 版號、防毒軟體、應裝軟體、禁用軟體和版權數量等，再透過 UPAS NOC 存取控制功能強制不合規設備修補漏洞。

02

已購置第三方資產管理軟體協助導入 VANS 不需額外安裝 UPAS Agent

若您已經購置第三方廠商的資產管理系統，並完成該廠商 Agent 的部署，可將軟體資產轉換成 CPE 格式並上傳 VANS 系統，UPAS NOC 為您提供進階的解決方案，徹底消弭安全性漏洞。

業界平均的 Agent 部署率及更新率僅有 80%，導致軟體資產盤點的不全面，造成嚴重的漏洞無法被察覺，使單位暴露在高度資安風險下。這些問題最根本的原因是在，第三方廠商多是採用 AD 主機直接派送 Agent，而若派送失敗或後續沒有正常更新，將導致該終端設備的資產軟體無法被確實盤點。

UPAS NOC 使用專利 ARP 封包解析技術，可大幅提升環境中設備的可視性，輕鬆盤點所有連網的終端設備；在高度可視的基礎上，UPAS NOC SIM 安全整合模組介接資產管理軟體資料庫，藉由比對完整的監測清單，即可毫無遺漏地找出未部署及未更新的設備，而針對不合規設備，以高安全性的阻斷網路機制強迫修補漏洞。

我們提供的進階解決方案，可以在不需額外安裝 UPAS Agent 的前提下，確保資產管理系統納管所有終端設備，確實的盤點軟體資產上傳至 VANS，通過更為全面的軟體漏洞檢查來有效消除資安風險。

12 大模組概述

IP

IP/MAC管理模組

可自動化更新白名單，辨識設備屬性，顯示所有設備的IP/MAC資訊，並可將所有資訊轉換成圖表，內建儀表板更可清晰呈現多種設備與事件統計數據。

PM

補丁管理模組

透過在終端部署Agent，檢查設備OS版本、防毒版本和病毒碼更新、應裝/禁用軟體是否安裝、和版權數量等資訊，如不符合安全規範則強制斷網並要求修補。

SIM

安全整合管理模組

採用Agentless方式介接其他安全系統，整合多種防毒軟體、資產管理軟體和WSUS主機，達到有效統一管理，全面性檢查與修補不合規設備。

DM

資產管理模組

能進行完整的USB存取管理，搭配PM模組蒐集軟體及硬體的資訊，以及針對設備管理有線與無線網路的連線。

IPL

IP位址解析模組

使用SNMP協定自動建立上下Switch串接之關聯性，識別IP之實體位址，並提供MAC/IP/Switch/Port/VLAN ID的狀態等信息。

AD

AD進階管理模組

強制所有電腦須遵循企業規範使用AD帳號登入。此外將AD帳號與設備資訊整合，提供完整的設備資訊，協助管理人員控管所有應加入AD網域的設備。

12 大模組概述

IDC

身分驗證模組

利用AD/LDAP/POP3/RADIUS伺服器進行員工自攜設備之身份驗證，支援雙因子認證，能快速識別設備並管理連線許可，確保沒有可疑人員及非法設備入侵。

UDS

DHCP派發模組

具備完整DHCP功能，透過單一介面完成派發設定，並提供IPv4及IPv6的派發功能，可配合訪客管理模組，進一步區隔訪客與內部員工使用的IP區段。

GAM

訪客管理模組

當訪客的外來設備進入企業網路時，透過自動化訪客預約申請、現場申請流程，可設定使用時效，限制訪客存取內外網之權限與時間，並記錄訪客申請所填資訊。

UDA

資料分析模組

結合Tableau數據分析軟體，根據不同產業客戶、不同管理或法規稽核需求，客製化產出99種報表，顯示198種內網統計分析項目，以多種角度視覺化分析內網數據。

IPv6

IPv6管理模組

支援IPv6管理，偵測並阻擋使用IPv6的外來設備，並提供即時資訊與歷史紀錄，協助管理員完整掌握內網IP使用狀況。

SCP

系統中樞平台

提供跨國、跨區域大型企業於總部設置SCP Console，透過三層式架構統一管理其他區域子Console，即時查看各地區設備存取狀況。

為什麼選擇 UPAS NOC

獨家ARP單播技術、完善資產盤點及IP管理流程，透過Agentless機制快速建置內網防護！

01

完整的資產盤點、掌握全面的設備狀態

據研究指出，90%以上的IoT設備無法安裝Agent，讓傳統的設備辨識技術難以發揮。UPAS NOC運用專利ARP技術，能夠以Agentless的方式自動辨識近30種連網設備屬性：

- OA區域：電腦設備、移動裝置、印表機、IoT設備
- 機房基礎架構：虛擬機、伺服器、其他虛擬機及網路設備組件
- 常見網路設備：路由器、交換器、防火牆、無線存取裝置和控制器

除了資產盤點之外，設備資訊的統計也是一大問題：OS版本、防毒軟體是否為最新版本、病毒碼是否更新、軟體使用狀況等，若其中一項出現問題，就可能導致整個網路環境陷入危險中。UPAS NOC可以介接WSUS主機、多款防毒軟體和資產管理軟體資料庫，並配合Tableau建立視覺化圖表，讓設備資訊清晰瞭然。

02

外來人員自動化管理，解決安全漏洞

在管理內網時，常會面臨外來人員需要暫時性的網路存取權限，相比嚴謹周密的外網防護，進入到內網的外來設備若未納入管理、劃分其使用權限，將可能會成為高風險的安全漏洞。UPAS NOC對外來人員提供以下解決方案：

1. 提供訪客內網連線認證，包含現場申請及預約申請兩種方式，可自動化審核訪客身分、給予相對應權限並留下完整紀錄，減少管理負擔。

2. 隔離訪客於特定網段，對於需要使用內網的訪客，UPAS NOC可以分割出訪客網段，限制訪客能存取的資料；若訪客網段發生資安事件，也可以將災害控制在該網段內，減少損失。

3. 限制訪客對內外網的存取權限與時效，到期即自動卸離白名單，藉由對存取權限與時效的管控，避免因忘記回收訪客權限而造成資安漏洞。

03

透過全面的IPv6管理，解決IP管理問題

雙協定並行下常見的問題有：IPv4、IPv6位址混雜；過去使用IPv4進行的IP派發、網段管理，切換成IPv6後須重新進行編制。以上兩種情況造成管理不易，增加相關人員負擔。UPAS NOC提供了以下IPv6的管理功能：

1. IPv6白名單管制功能。能夠自動將使用IPv6位址的合規設備納入系統白名單中，准許其使用內網。並且能夠自動化生成詳細清單，清楚詳列各IP的使用狀況。

2. 自動派發含IPv4尾碼的IPv6位址。延續過往網段建置的成果，在轉換協定時不需再重新進行額外設定，減少管理人員負擔。

3. 自動化生成IPv4與IPv6對應表。在採用雙協定的網路環境下，UPAS NOC可以自動生成雙協定的IP位址對應表，使各終端所使用的兩種IP位址一目了然。

04

協助政府機關建置ISMS系統，遵循法規要求

1. 在《資安法》的要求下，機關被要求建置可以通過ISO 27001驗證的ISMS系統與檢視資通系統防護基準。UPAS NOC符合多項ISO 27001控制項與資通系統防護機準的要求，減少通過驗證時所需花費的成本。

2. GCB的合規導入常常使管理人員頭痛，繁複的設定與眾多的電腦設備，使導入的過程極為繁瑣，更有許多原因會造成導入失敗。UPAS NOC提供完善的GPO功能可用來幫助管理者瞭解在網域中的設備GPO、GCB套用狀況，查找沒有符合規定套用GCB、GPO之端點設備。

3. UPAS NOC提供設備違規的即時告警與完整的系統軌跡記錄，這兩項功能對於個資的保護至關重要；當設備在進行違規操作時 (如跨VLAN、竄改IP)，通過即時告警，能夠在事件發生的當下立刻阻斷違規設備的連網能力，阻止災害擴大；而完整的軌跡記錄則是資安事件發生後在法律上最有力的證據。

4. NIST CSF為近期最為熱門的資安框架，相較於ISO 27001繁瑣的建置與驗證，CSF強調循序漸進的改善資安系統。根據《IThome 2020資安大調查》有一成以上的政府機關有意願導入CSF資安框架，可見對於預算有限的政府機關，CSF不失為一項良好的選擇。UPAS NOC符合多項CSF控制項，讓單位在導入時可針對需求彈性選購模組，減少建置成本。

協助政府組織
盡快完善內網管理

UPAS提供最全方位的解決方案，讓您快速建置內網安全，打造零信任安全架構，符合資安法內網相關規範。欲了解更完整的內網管理資訊，請查看下方資訊：

UPAS官方網站
了解更多關於UPAS的內網管理方法，包含NAC、IPAM、IAM、ITAM等內網重點管理事項。

UPAS Medium
訂閱UPAS Medium獲取更多內網安全最新即時資訊、相關資安新聞，以及UPAS產品資訊。

下載更多UPAS相關手冊
閱讀UPAS相關產品手冊，提供稽核、企業建議書等多樣內容。

申請POC測試
體驗UPAS NOC解決方案，專人與您進行需求評估，提供您最佳的內網管理方案。

UPAS NOC 內網管理中心

內網安全，一手掌握

立即聯絡我們，守護您的內網

WEBSITE MEDIUM FACEBOOK

UPAS
NETWORK OPERATIONS CENTER

UPAS 優倍司股份有限公司
https://www.upas-corp.com/

總部：台北市信義區基隆路二段51號9樓之8
TEL：02-27393226 / 02-77180425
FAX：02-27392836

研發中心：高雄市前鎮區民權二路6號18樓之3
TEL： 07-9700229
FAX： 07-9700225