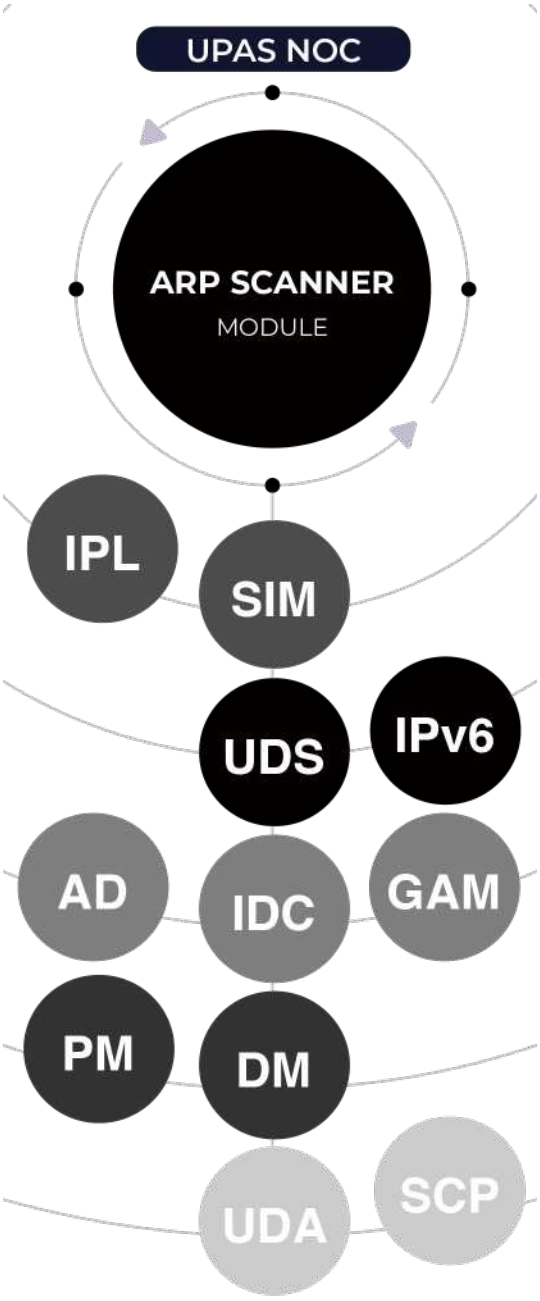
UPAS NOC
常見稽核標準
符規一覽

ISO 27001: 2013

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。

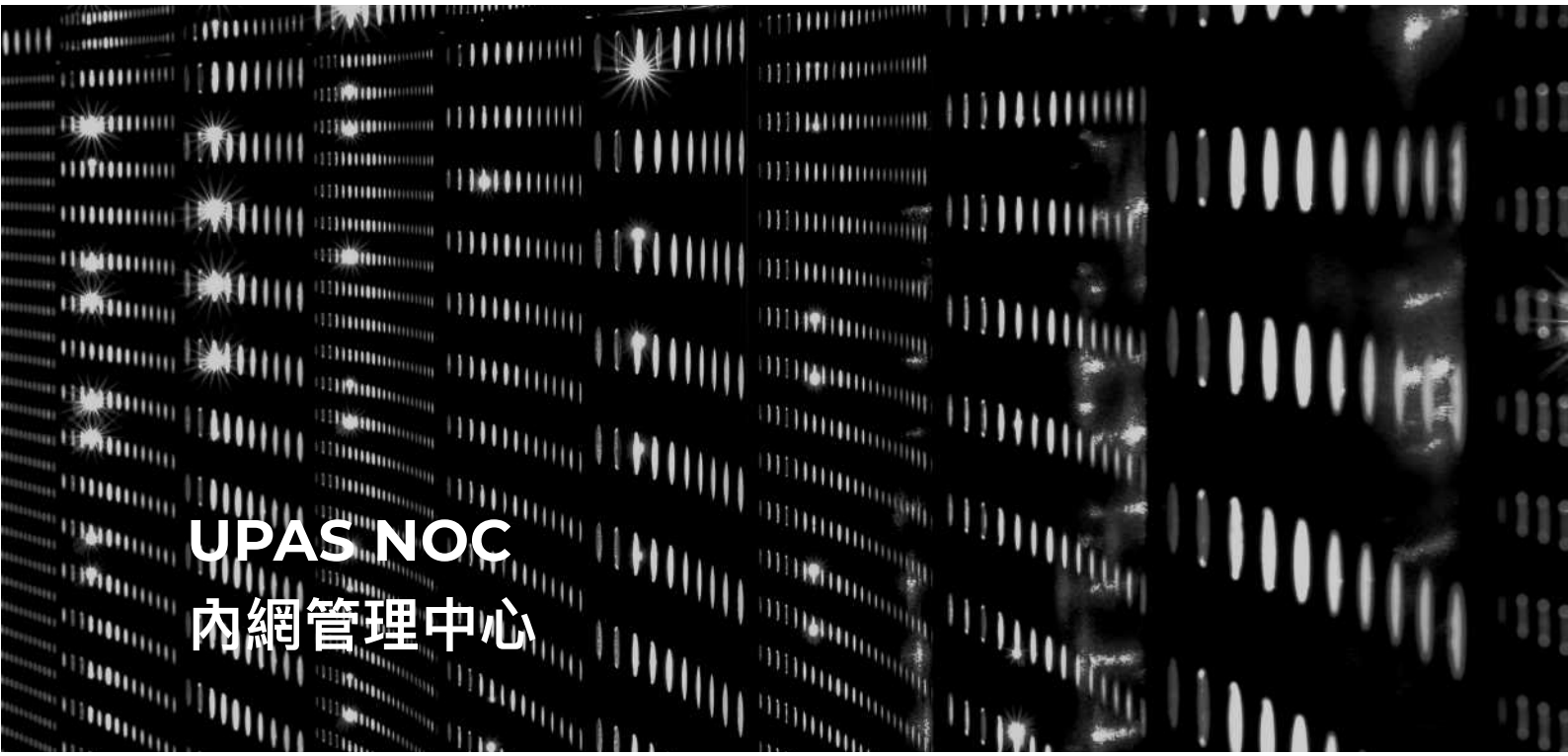
採用Agentless方案，適合各種網路環境

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。



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。

ISO 27001: 2013

ISO 27001: 2013為**國際標準組織**所制定，旨在建立、實施、維護與持續改進資訊安全管理系統 (Information Security Management System, ISMS)的一套國際通用資安管理工具和制度 (於2013年改版)；透過對管理面、制度面與技術面的規範保護組織資訊資產的機密性、可用性與完整性。

ISO 27001為主流的資訊安全管理制度

ISO 27001自2013年改版後，全球通過認證數不斷上升，2017年時總認證數達到39501，雖然2018年有下降的情況，但可以發現ISO 27001為目前國際上最廣泛採用之資訊安全管理制度標準規範，為建立完善的資訊安全管理制度提供一個良好的起點。

01

通過ISO 27001的益處

ISO 27001提醒在建構及管理資訊安全系統時，不可忽略的細節，並藉由審查機制、事件的回饋及內部稽核，預防發生資訊安全事件的風險與降低損失；通過ISO 27001驗證使企業在提升資安管理技術的同時，還可以證明企業對資訊安全的承諾，增進電子商務往來的信用度，並且符合相關法律的規範。

02

ISO 27001適用於各種行業

ISO的年度報告中列舉了通過驗證的135個國家中的39種不同行業，在各國對個人隱私資料的重視度不斷提高的時刻，資訊安全已是一個不分行業皆須重視的重要政策。通過ISO 27001驗證、建構妥善的資訊安全管理制度為刻不容緩的事項。

03

UPAS NOC與ISO 27001

UPAS符合多項ISO 27001:2013技術面的控制項，能協助企業在導入ISO 27001時減少所需耗費的資源。且UPAS系統導入快速、無須安裝任何Agent，大幅度降低導入所需耗費的人力資源和成本，能夠以最快的速度建立全面的內網安全管理系統。

ISO 27001內網安全重點項目

ISO 27001架構中的內網項目

ISO 27001控制項中，總共有41的控制項規範內網安全，涵蓋的章節為：

- A.6 資訊安全的組織
- A.8 資產管理
- A.9 存取控制
- A.10 密碼
- A.12 作業安全
- A.13 通訊安全
- A.14 資訊系統獲取、開發及維護
- A.15 供應商關係

UPAS NOC能完善24項內網安全控制項

UPAS NOC在A.9存取控制的部分達到近90%的合規比率，在A.8資產管理章節更是擁有100%合規率；UPAS NOC內網安全管理系統，於ISO 27001中無法符合的項目多數為硬體設備的建置、人員制度架構以及設備對外連線的通訊控管，如A.7人力資源安全中包含了人員聘用與教育訓練等內容，和A.12包含了部分的系統開發、測試、備份等控制項目。

四大解決方案，協助建立ISO 27001標準

- NAC網路存取控制技術，協助企業收集設備的詳細資訊、建立白名單、禁止非法設備存取網路、全面納管外來設備，並產出相關報表，保護企業內部網路安全。
- IAM的多種身分驗證機制，符合ISO 27001當中多項使用者與網路存取要求，加強內網使用者的身分認證功能。
- IPAM的IP管理功能，提供管理人員詳細的網路設備資訊，使管理更加容易。
- ITAM提供軟硬體管理與OS管理，解決ISO 27001中對系統與城市管理的要求。

UPAS系統導入快速、無須安裝任何Agent，大幅度降低導入所需耗費的人力資源與成本，能夠以最快的速度提供全面的內網安全管理。

資訊安全的組織

此為第六章節要求資訊安全組織的成立，並定義其組織架構、運作流程與責任歸屬。

A.6.1.1 資訊安全的角色與責任

- 所有的資訊安全責任應予明訂與分配。

透過UPAS NOC的帳號及權限劃分，可以對使用者設定不同的管理項目(分為管理者、使用者、觀察者等不同的操作權限)，並限制觀察者只能查看系統資訊、無法操作。

A.6.1.2 職務的區隔

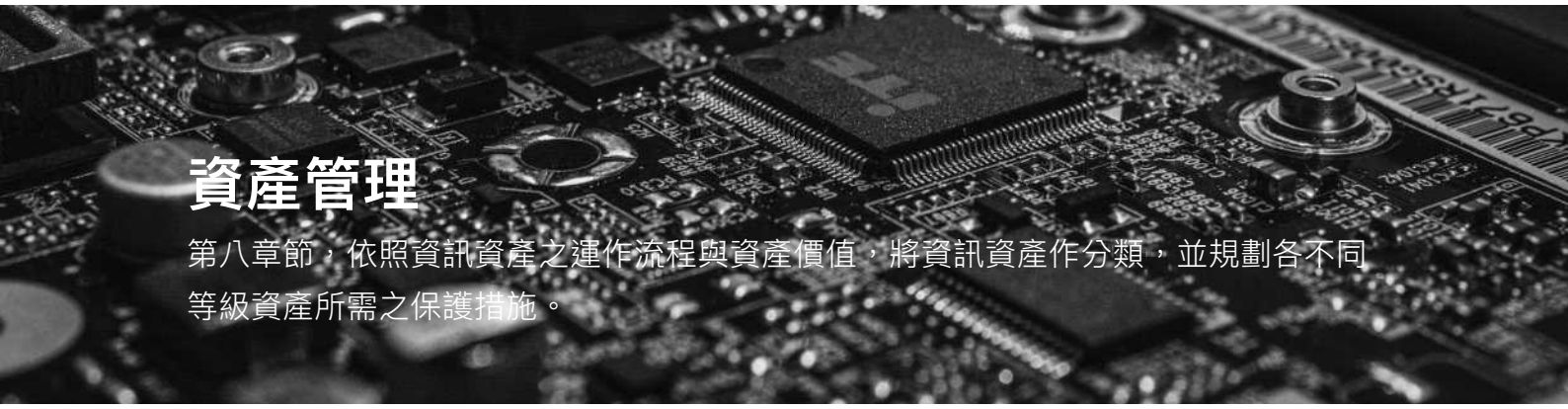
- 相互衝突的職務與責任領域應加以區隔，以降低組織資產遭未經授權或非故意的修改或誤用之機會。

UPAS NOC透過UDS及GAM模組，可以在同一VLAN下劃分子網段，進一步區隔訪客與內部使用的IP位置與存取權限，提供訪客與內部員工使用網段區分功能。

A.6.2.1 行動設備的政策

- 應採取適當政策與輔助的安全措施，以管理使用行動設備所導致的風險。

UPAS NOC使用專利技術蒐集設備的IP/MAC/電腦名稱/設備屬性等資訊，阻擋不明設備進入內網；透過IDC模組，提供BYOD設備管理，利用AD/LDAP/POP3/RADIUS sever對行動設備進行身分認證，確保非法設備不能進入內網。



資產管理

第八章節，依照資訊資產之運作流程與資產價值，將資訊資產作分類，並規劃各不同等級資產所需之保護措施。

A.8.1.1 資產清冊

- 應識別與資訊和資訊處理設施相關的資產，且應制訂與維持這些資產的清冊。

UPAS NOC可自動偵測近30種資產屬性，並根據MAC位址建立資產清冊。此外透過自動蒐集所有線上設備的IP/MAC/資產屬性/設備名稱，以建立資產屬性統計表。

A.8.2.1 資訊分類

- 資訊應依法規要求、價值、危害性與對未經授權的揭露或修改之敏感性觀點予以分類。

UPAS NOC提供IP管理、AD管理功能，設備屬性辨識，可依照設備之權限、狀態、違規種類予以分類。

A.8.2.2 資訊標示

- 應依照組織所採用的分類法，發展與實施一套適當的資訊標示程序。

UPAS NOC會自動蒐集各項系統操作紀錄、IP使用紀錄、上下線資訊、AD登入/登出紀錄、違規紀錄...等多項內容，產生軌跡資料並加密保存。

A.8.2.3 資產處置

- 應依照組織所採用的分類法，發展與實施資產處置程序。

UPAS NOC可以將IP/MAC/電腦名稱/資產屬性綁定，避免重要主機IP位址遭偽冒，導致資料遺失、毀壞、偽造或竄改。

A.8.3.1 可攜式媒體的管理

- 應依照組織所採用的分類法，實施可攜式媒體管理之程序。

A.8.3.2 媒體的處理

- 應保護含有資訊的媒體在傳送期間，不受未經授權的存取、誤用或毀損。

A.8.3.3 實體媒體的傳送

- 應依照組織所採用的分類法，發展與實施一套適當的資訊標示程序。

UPAS NOC會自動蒐集各項系統操作紀錄、IP使用紀錄、開關機紀錄、上下線資訊、AD登入/登出紀錄、違規紀錄...等多項內容，產生軌跡資料並加密保存。

存取控制

第九章節，使用者權限之設定應依使用者工作職權而給予，以降低未經授權存取系統資源之風險。

A.9.1.1 存取控制政策

- 應基於營運與資訊安全要求，建立、文件化及審查存取控制政策。

UPAS NOC使用專利技術蒐集設備的IP/MAC/電腦名稱/設備屬性等資訊，建立白名單，阻擋不明設備進入內網。

A.9.1.2 網路與網路服務的存取

- 應僅提供使用者經特定授權可存取使用的網路與網路服務。

UPAS NOC可蒐集設備的IP/MAC/電腦名稱/設備屬性等資訊，阻擋不明設備進入內網；透過IDC模組，利用AD/LDAP/POP3/RADIUS sever進行行動設備的身分認證，確保非法設備不能進入內網。對於訪客等其他內網使用者也可使用GAM模組，可以使訪客透過預約/即刻申請等方式獲得網路存取權限。

A.9.2.1 使用者登錄與註銷

- 應實施一個正式的使用者登錄與註銷登錄程序，以使所指派的存取權限可行。

A.9.2.2 使用者的存取配置

- 應實施一個正式的使用者存取權限配置程序，以對所有系統與服務的全部使用者類型分配和撤銷存取權限。

UPAS　NOC使用AD模組，可以強迫只能使用AD帳號登入設備，納入AD管理；透過IDC模組，利用AD/LDAP/POP3/RADIUS　sever進行行動設備的身分認證，確保非法設備不能進入內網。對於訪客等其他內網使用者也可使用GAM模組，可以使訪客透過預約/即刻申請等方式獲得網路存取權限。

A.9.2.3 特權的管理

- 應限制與控制特權存取權限的配置與使用。

UPAS NOC透過AD模組，限制設備只能使用特定AD帳號登入，不能使用本機登入。

A.9.2.4 使用者的機密授權資訊之管理

- 機密授權資訊的配置，應透過一個正式的管理過程加以控制。

白名單管理能透過電腦名稱/資產屬性/OUI等資訊自動加入白名單；AD模組則可以強迫只能使用特定AD帳號登入設備，納入AD管理。

A.9.2.5 使用者存取權限的審查

- 應定期審查使用者的存取權限。

UPAS NOC 透過AD模組則可以強迫只能使用特定AD帳號登入設備，納入AD管理，並在AD操作異常時即時告警。對於未加網域或私退網域的AD帳號進行管理，並設定內網/外網的權限。

A.9.2.6 存取權限的移除或調整

- 所有的員工與外部團體使用者對資訊與資訊處理設施的存取權限，在其聘僱、契約或協定的終止後應移除之，或是在變更後作調整。

UPAS NOC提供設備卸離功能，可在員工離職時將其從白名單中移除；GAM模組可以設定存取期限，在到期時自動移除使用權限。

A.9.3.1 機密授權資訊的使用

- 在機密授權資訊的使用，使用者必須遵循組織的安全作法。

UPAS NOC 提供詳細操作紀錄，清楚了解誰在什麼時刻進行了何種操作，以及是否有遵守相關規範。

A.9.4.1 資訊存取限制

- 應根據存取控制政策，限制資訊與應用系統功能的存取。

A.9.4.2 安全之登入程序

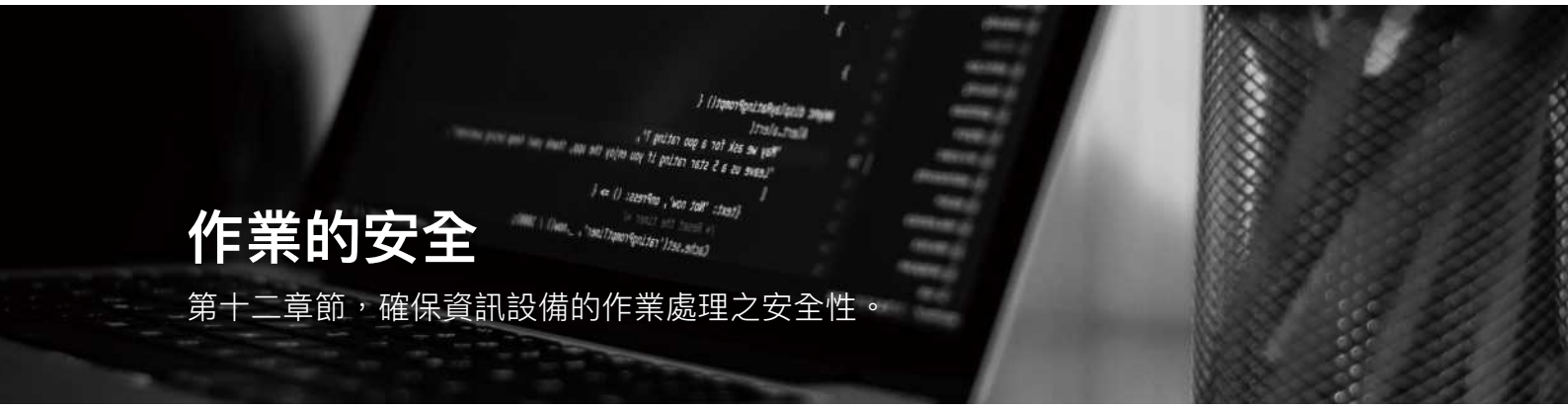
- 在存取控制政策的要求下，應由安全的登入程序控制系統與應用系統的存取。

透過UPAS　NOC內的帳號及權限設定，可以對使用者設定不同的管理項目，並限制觀察者只能查看系統資訊、無法操作。

A.9.4.4 特權的公用程式之使用

- 應限制與嚴密控制可能篡改系統與應用控制措施的公用程式之使用。

UPAS NOC 透過SIM模組可以介接資產管理系統，了解各設備軟體安裝及使用的狀況；PM模組則可以直接蒐集各設備的軟體安裝資訊，並透過違規斷網的措施限制軟體的使用。



作業的安全

第十二章節，確保資訊設備的作業處理之安全性。

A.12.4.1 事件存錄

- 事件日誌係紀錄使用者活動、異常、錯誤及資訊安全事件，應產生、保留並定期審查。

A.12.4.2 日誌資訊的保護

- 應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。

A.12.4.3 管理者與操作者日誌

- 系統管理者與操作者的活動應加以存錄、保護並定期審查。

UPAS NOC會自動蒐集各項系統操作紀錄、IP使用紀錄、開關機紀錄、上下線資訊、AD登入/登出紀錄、違規紀錄...等多項內容，產生軌跡資料並加密保存。

A.12.5.1 作業系統上軟體的安裝

- 應實施程序，以控制作業系統上軟體的安裝。

A.12.6.2 軟體安裝的限制

- 應建立與實施管理使用者之軟體安裝的規則。

UPAS NOC可偵測是否安裝應裝軟體、非法/盜版軟體，若違規則透過斷網與重導頁面要求修補；使用SIM模組可以介接資產管理系統，了解各設備軟體安裝及使用的狀況；PM模組則可直接蒐集各設備的軟體安裝資訊，並透過違規斷網限制軟體的使用。

通訊安全

第十三章節，確保通訊作業處理之安全性。

A.13.1.1 網路控制措施

- 網路應加以管理與控制，以保護系統與應用系統的資訊。

A.13.1.2 網路服務的安全

- 應識別所有網路服務的安全機制、服務水準及管理要求並納入網路服務協議中，不論此等服務是由內部或委外所提供。

UPAS NOC蒐集設備的IP/MAC/電腦名稱/設備屬性等資訊，建立白名單，阻擋不明設備進入內網。透過IP/MAC/電腦名稱/資產屬性綁定，保護重要主機不會因遭受IP衝突等事件，造成服務中斷。

A.13.1.3 網路區隔

- 應將資訊服務、使用者及資訊系統各群組使用的網路加以區隔。

UPAS NOC 透過UDS模組可以設定DHCP派發區段，並結合GAM模組，可以在同一VLAN下劃分子網段，進一步區隔訪客與內部使用的IP位置與存取權限。

供應商關係

第十五章節，確保供應商可存取之組織資產的保護 ，維持議定等級之資訊安全及服務交付，並能與供應商協議一致。

A.15.1.1 供應商關係的資訊安全政策

- 應與供應商協議資訊安全要求，以減少供應商對組織資產存取的風險並加以文件化。

UPAS NOC透過UDS及GAM模組，提供訪客與內部員工使用網段區分功能，減少訪客存取資產的風險。可以在同一VLAN下劃分子網段，進一步區隔訪客與內部使用的IP位置與存取權限。

協助企業及政府
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