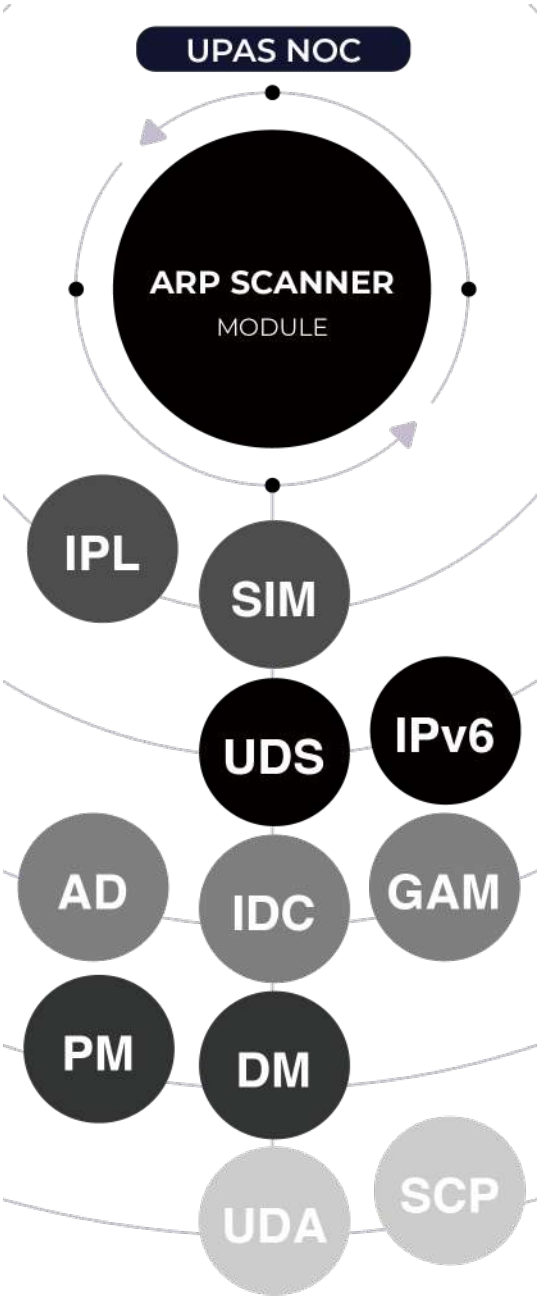
UPAS NOC
常見稽核標準
符規一覽

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。

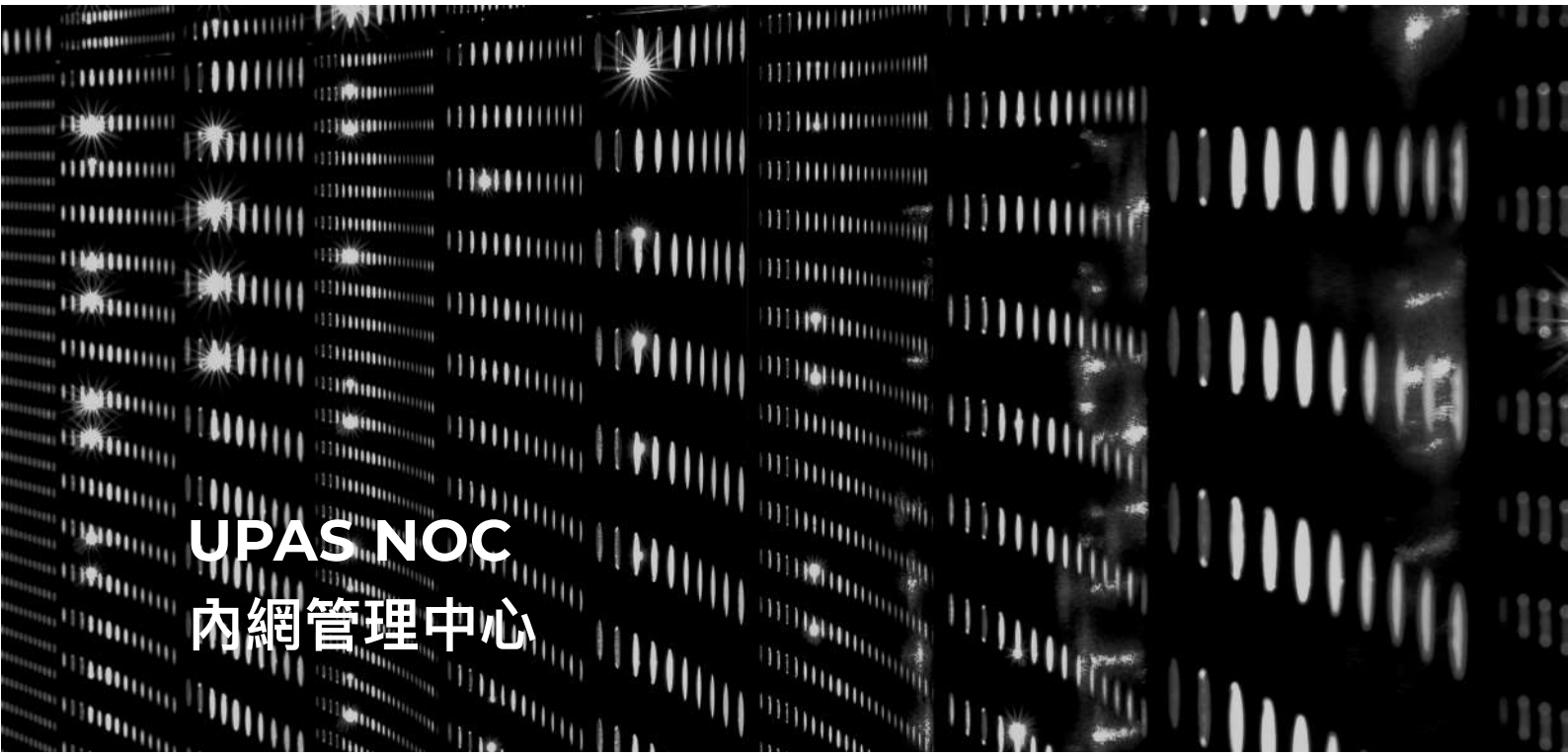
採用Agentless方案，適合各種網路環境

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

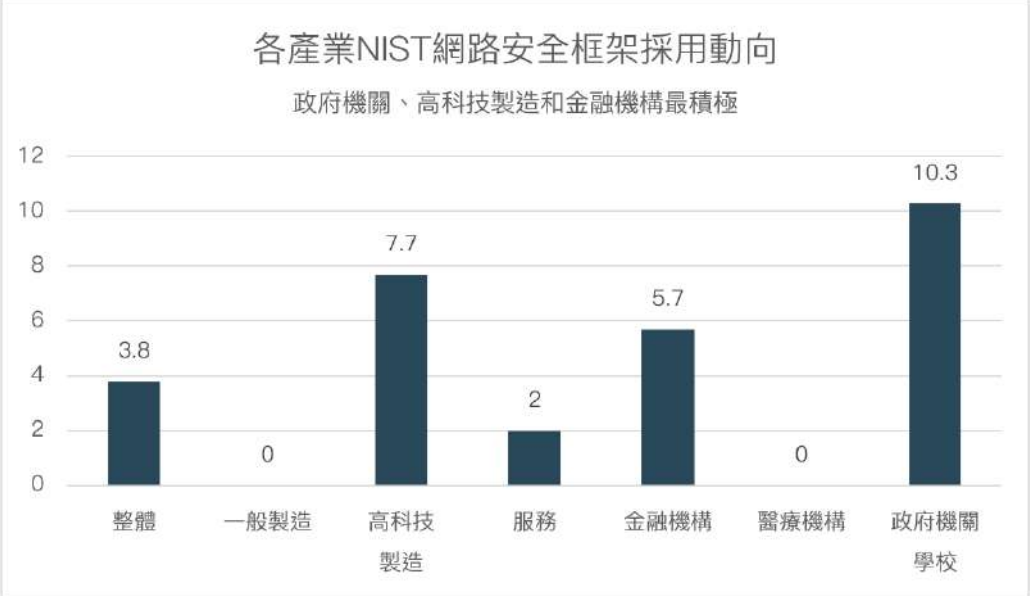
提供跨國、跨區域大型企業於總部設置SCP Console，透過三層式架構統一管理其他區域子Console，即時查看各地區設備存取狀況。

Cybersecurity Framework (CSF) V1.1

資訊安全框架的黑馬

為了改善政府和關鍵基礎設施的網路安全，2013年時任美國總統歐巴馬下令**國家標準暨技術研究院**（NIST)訂立一套通用的資安框架，於是在2014年NIST發布《網路安全框架》(Cybersecurity Framework, CSF) 1.0正式版，接著在2017年，美國頒布新的行政命令，要求聯邦政府必須全面導入CSF；雖然當初CSF所適用的對象是美國政府和關鍵基礎設施，此框架同樣適用一般企業環境；權威資訊顧問公司Gartner預估，2020年會有一半的美國企業採用CSF管理資安風險，不只美國，英國、義大利、以色列、日本等國的公部門與企業，也逐步導入CSF。

根據《iThome 2020 資安大調查》，在台灣有高達一成的政府機關與學校機構預計採用CSF，另也有7.7%的高科技製造業有在考慮導入。相較於ISO 27001的高建置成本，容易上手又涵蓋完整的CSF成為資安預算有限的機構的最佳選擇。

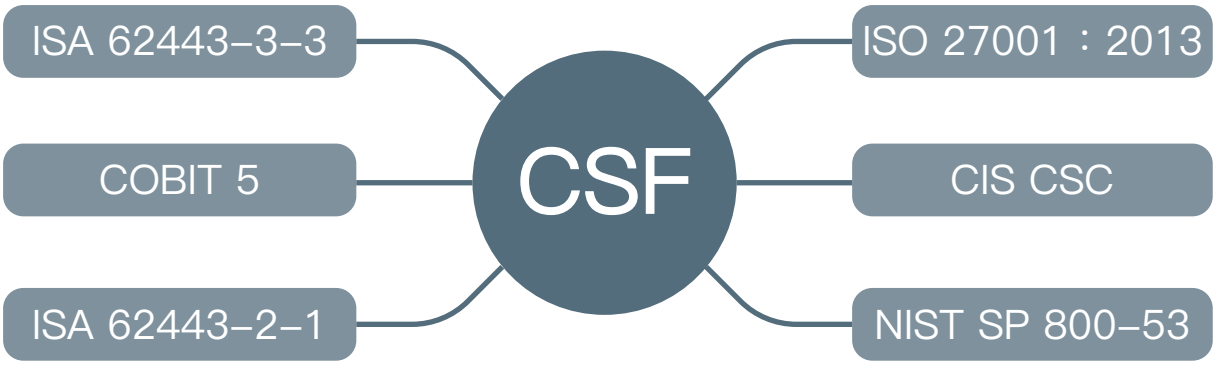


CSF與 6 大資安標準

NIST CSF的制定參考世界上具指標性的資安標準：

- ISO/IEC 27001：2013
- CIS CSC
- NIST SP 800–53 Rev. 4
- ISA 62443–2–1：2009
- ISA 62443–3–3：2013
- COBIT 5

CSF在檢核別列出了所參考的資訊，讓使用者能清楚了解該項目是對應到不同標準的哪一個控制項，體現出CSF與其他資安架構的互通性。



5 大功能落實網路安全

NIST於2018年推出CSF 1.1版，在五大功能(識別、保護、偵測、回應、復原)下定義出23個類別與108項子類別。企業可以根據這108項子類別與自身業務營運相符合的目標進行檢視與落實。

- Identify識別：建立組織規則以管理系統、人員、資產、資料和功能的網路安全風險
- Protect保護：建立和實施適當的安全措施以確保重要服務的運行
- Detect偵測：制定並實施適當的作為以識別網路安全事件的發生
- Respond回應：對偵測到的網路安全事件，規劃並實施適當的行動
- Recover復原：制定並實施適當的措施以修復因網路安全事件受損的功能和服務

UPAS NOC協助符合NIST CSF規範

NIST CSF架構中的內網項目

NIST CSF被具備多種資安規範，如：內網安全、人員管理、制度建立、系統維護等。NIST CSF的控制項中，共有51項為規範內網安全項目，涵蓋的三大功能，分別為Identify、Protect、Detect。

UPAS NOC能完善21項內網安全控制項

- Identify有 7 項符合
- Protect有 13 項符合
- Detect有 1 項符合

Identify中符合的項目為資產管理與風險管理策略等兩類別；而Protect中則是身分管理與准入控制、資料安全、資訊保護的流程、保護技術等四項類別；在Detect中的類別則是持續性的安全監測。

UPAS NOC為網路安全管理系統，於NIST CSF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Respond中的求各人員(員工、利益相關者)在災害發生時需要了解他們的職責並作出相對應的行動；Recovery中則是要確定復原計畫有依照計畫執行並且有作出相對應的更新。

UPAS NOC快速協助建立CSF標準

UPAS NOC與CSF的識別、保護等兩大功能展現了高度的適配性，能協助企業在導入CSF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與成本，能夠以最快的速度提供全面的內網安全管理。

UPAS NOC符合NIST CSF的對應項目

UPAS符合CSF Identify功能中之類別

- ID.AM (Asset Management)：依據組織的目標與風險策略，對資料、人員、設備、系統和設施進行識別和管理。
- ID.RM (Risk Management Strategy)：建立組織的優先級別、風險容忍度，以協助風險決策。

NIST CSF		UPAS NOC
ID.AM–1	Physical devices and systems within the organization are inventoried	UPAS可以自動蒐集所有連上網路設備的IP/MAC/資產屬性/設備名稱，並建立資產屬性統計清單、圖表。
ID.AM–2	Software platforms and applications within the organization are inventoried	SIM模組可介接資產管理系統，了解各設備軟體安裝及使用的狀況。 PM模組可直接蒐集各設備的軟體安裝資訊、建立統計圖表，並透過違規斷網限制其使用。
ID.AM–3	Organizational communication and data flows are mapped	UPAS系統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，自動產生軌跡資料並加密保存。
ID.AM–5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	UPAS系統提供IP管理、AD管理、設備屬性辨識等功能，並能依照設備之權限、狀態、違規種類予以分類。
ID.RM–1	Risk management processes are established, managed, and agreed to by organizational stakeholders	UPAS系統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，自動產生軌跡資料並加密保存。
ID.RM–2	Organizational risk tolerance is determined and clearly expressed	
ID.RM–3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	

UPAS符合CSF Protect功能中之類別

- PR.AC (Identity Management and Access Control)：對物理和邏輯資產及相關設施的訪問僅限於授權用戶、流程和設備，並評估的未經授權的訪問和交易的風險。
- PR.DS (Data Security)：資料的管理與組織的風險策略一致，以保護資料的機密性，完整性和可用性。
- PR.IP (Information Protection Processes and Procedures)：維護資安策略（包含目的，範圍，角色，職責，管理承諾以及組織間的合作），流程和過程，並用於管理資訊系統和資產的保護。
- PR.PT (Protective Technology)：對技術安全解決方案進行管理，以確保系統和資產的安全性和彈性，並與相關的策略、過程和協議保持一致。

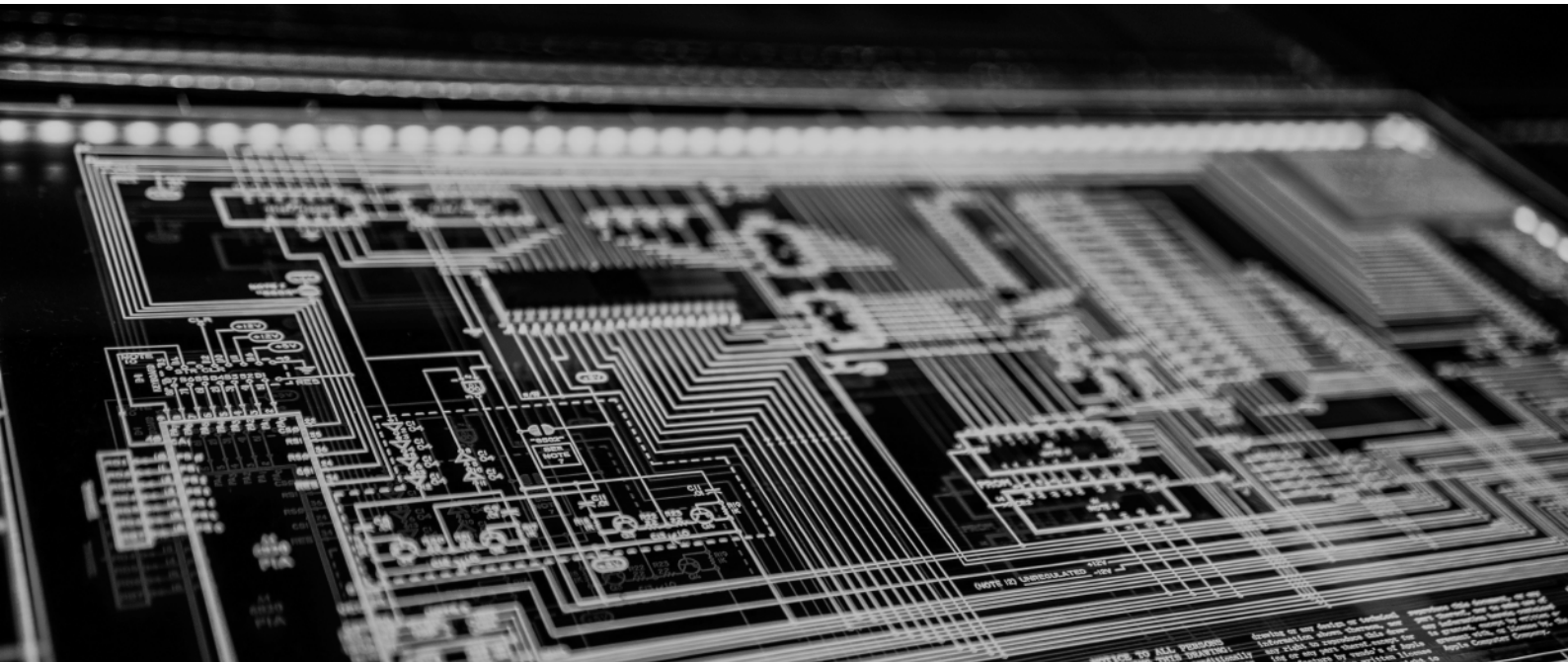
NIST CSF		UPAS NOC
PR.AC–1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	UPAS使用專利技術蒐集設備的IP/MAC/電腦名稱/設備屬性等資訊，阻擋不明設備進入內網。 AD模組可強迫使用AD帳號登入指定設備，將所有設備納入AD管理。 IDC模組利用AD/LDAP/POP3/RADIUS Sever 進行行動設備的身分認證，確保非法設備不能進入內網。 GAM模組可使訪客透過預約/即刻申請等方式獲得網路存取權限。 UPAS系統更提供100多種的系統報表，全方位掌握網路安全事件。
PR.AC–6	Identities are proofed and bound to credentials and asserted in interactions	
PR.AC–7	Users, devices, and other assets are authenticated (e.g., single–factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	
PR.AC–5	Network integrity is protected (e.g., network segregation, network segmentation)	UDS模組提供自動化分配網段功能，依照設備屬性/工作區域/身分性質提供不同網段，並在設備試圖更換網段時即時告警。
PR.DS–1	Data–at–rest is protected	透過IP/MAC/電腦名稱/資產屬性綁定，避免外來設備偽冒MAC，偽裝為內部網路設備，進行機密資料竊取、毀壞或竄改。
PR.DS–2	Data–in–transit is protected	UPAS系統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，自動產生軌跡資料並加密保存。

NIST CSF		UPAS NOC
PR.DS–3	Assets are formally managed throughout removal, transfers, and disposition	透過IP/MAC/電腦名稱/資產屬性綁定，避免外來設備偽冒MAC，偽裝為內網路設備，進行機密資料竊取、毀壞或竄改。 UPAS系統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，自動產生軌跡資料並加密保存。
PR.DS–5	Protections against data leaks are implemented	透過IP/MAC/電腦名稱/資產屬性綁定，避免外來設備偽冒MAC，偽裝為內網路設備，進行機密資料竊取、毀壞或竄改。 使用PM模組可以要求各設備安裝DLP軟體，防止資料外洩的事件發生。
PR.DS–6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	SIM模組可介接資產管理系統，了解各設備軟體安裝及使用的狀況。 PM模組可直接蒐集各設備的軟體安裝資訊，並透過違規斷網與重導頁面限制軟體的使用。 UPAS的准入技術可確保網域內的設備安全性，與自動蒐集系統操作、事件紀錄，確保訊息完整性。 AD模組可強迫使用AD帳號登入指定設備，將所有設備納入AD管理。 IDC模組利用AD/LDAP/POP3/RADI–US Sever 進行行動設備的身分認證，確保非法設備不能進入內網。 GAM模組可使訪客透過預約/即刻申請等方式獲得網路存取權限。
PR.IP–6	Data is destroyed according to policy	UPAS系統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，自動產生軌跡資料並加密保存。
PR.PT–1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	
PR.PT–2	Removable media is protected and its use restricted according to policy	透過IP/MAC/電腦名稱/資產屬性綁定，避免外來設備偽冒MAC，偽裝為內部網路設備，進行機密資料竊取、毀壞或竄改。 UPAS系統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，自動產生軌跡資料並加密保存。

UPAS符合CSF Detect功能中之類別

- DE.CM(Security Continuous Monitoring)：監視信息系統和資產以識別網絡安全事件並驗證保護措施的有效性。

NIST CSF		UPAS NOC
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	UPAS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。 SIM模組可介接資產管理系統，了解各設備軟體安裝及使用的狀況。 PM模組可直接蒐集各設備的軟體安裝資訊，監控盜版、禁用軟體，並透過違規斷網與重導頁面限制軟體的使用。



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