UPAS

ZERO TRUST ARCHITECTURE

全方位零信任資安解決方案

ZERO TRUST · TRUST UPAS

— 產 品 型 錄 —

- APAC CIO Outlook -

TOP 5 / TOP 10
Cyber Security Solutions Provider
in Taiwan / APAC


ZERO TRUST
TRUST UPAS















UPAS

內網安控系統領導品牌

UPAS 成立於1993年，為內網安控系統的開拓者與領導者，從研發 IP 管理與 NAC 網路存取控制系統產品開始，多年來在資訊安全及網路管理的領域深耕，協助客戶建立全方位內網安控系統，協助提升企業內網安全與管理效率，減少管理成本、強化資安韌性。

專業赤誠為您服務

UPAS 致力於為客戶提供內網安全最佳解決方案，我們的使命為協助客戶建立堅實邊界防護，確保內網的端點設備皆安全且符規，防止勒索病毒入侵及機密資料外洩。

團隊在政府、關鍵基礎設施、科技業、製造業、金融業、醫療單位、教育研究單位與一般企業皆有豐富實績。我們將持續傾聽客戶的聲音，持續因應客戶需求優化產品，在資訊安全的路上與客戶一同前進。

技術領航跨足國際

UPAS 服務據點跨足臺灣、中國大陸、日本與東南亞，無論您是大型的跨國企業、海外品牌或國際品牌， UPAS 的專業技術，都能夠為您的需求提供完善的解決方案、零信任安全架構以及堅實的內網安全防護。

您的內網環境 可能正面臨以下風險



- 環境設備未完整盤點，駭客有機可乘
- 違規設備非法接入，形成潛在危機
- IoT 設備數量劇增，無法使用 Agent 管理



- Windows Patch 未更新，設備出現漏洞
- 病毒碼未更新，新型病毒將恣意入侵
- 終端設備軟體漏洞，管理人員無法即時修復
- GPO 不合規



- 重要檔案遭到外洩
- 員工自攜設備私自進入內網存取資料
- 員工使用個人 USB 存取重要資訊



- 員工私接 Hub、IP 分享器，影響公司內部網路
- 外部訪客未經驗證逕自使用內部網路
- 終端設備私退網域



- 行動裝置將機密資訊拍照、截圖外流
- 行動裝置任意安裝非法應用程式

多種風險防禦，多樣設備管理不需多套軟體

UPAS ZTA 給您最堅實的內網安全解決方案

UPAS 5S 關鍵優勢

ZERO TRUST ARCHITECTURE

Simple

- 使用 NAP 專利技術，具備簡易佈署架構，安裝及建置容易
- 具備彈性佈署功能，同時適用於雲端與地端建置
- 模組化架構，可自由靈活應用，兼具高 CP 值
- 高度兼容支援各種品牌的 Switch、防毒軟體及網路架構
- 精美的 UI 設計，友善的 UX 設計，系統安裝與設定採用一頁式管理，減少頁面轉換，使用更加方便

Support

- ZTA 系統，單一平台、單一 Agent，一套搞定 NAC、ITAM、IAM、IPAM、MDM 等
- Agent 支援 Windows / Linux / macOS / Android / iOS 等作業系統管理
- 支援更新 Patch、安裝防毒軟體、應用程式安裝、禁用軟體、USB 管理、軟體弱點更新、GPO 修補等多項功能，並全面自動化
- 提供整合性功能，支援 syslog、API 等
- NOC 首頁清晰數據圖表分析，設備資訊高度可視化
- 提供多元且豐富的報表功能，自動化生成各類報表

Smart

- 完善率、維持率、屬性辨識、Agent 部署率、終端設備合規檢查率等，皆可達到 98% 以上，保障系統安全性
- 智慧化及自動化設計，包括自動加入白名單、自動分群、自動派送 Agent、自動依群組政策合規檢查、自動隔離修補、自動恢復連線等，節省人力與時間

Safe

- 具故障 ByPass、防錯設計等高安全機制

Stable

- 高穩定效能卓越，備受滿意信賴

5 大資安解決方案 20 大功能模組

全方位實踐零信任架構．永不信任且持續驗證

網路存取控制 NAC
Network Access Control

主模組

ARP IP / MAC 管理模組
ARP Scanner 存取控制

DAM 設備鑑別模組
Device Authentication Management



IT 資產管理 ITAM
IT Asset Management

PM 補丁管理模組
Patch Management

DM 設備管理模組
Device Management

ROM 遠程運維模組
Remote Operations Management

TIM 信任推斷模組
Trust Inference Management

GPO GPO 管理模組
GPO Management

VANS 漏洞警報和通知系統
Vulnerability Alert and Notification System



身分驗證管理 IAM
Identity and Access Management

AD AD 管理模組
ADVantage

ZERO TRUST ARCHITECTURE

為 IT 人員、MIS 人員量身打造的專業管理工具

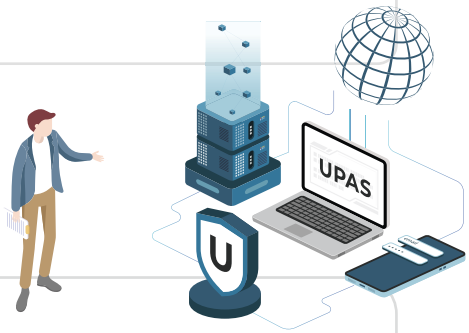
IP 位址管理 IPAM
IP Address Management

ARP IP / MAC 管理模組
ARP Scanner　IP管理

行動裝置管理 MDM
Mobile Device Management

MDM 行動裝置模組
Mobile Device Management

其他加值管理解決方案
Other Value-Added Functions



SIM 安全整合管理模組
Security Integration Management

IPL IP 地址解析模組
IP Locator

IPv6 IPv6 管理模組
IPv6 Management

IPAF IP 申請表單功能
IP Application Form Functionality

DHCP DHCP Server 整合功能
DHCP Server Integration Functionality

IPLI IP 使用記錄整合功能
IP Usage Log Integration Functionality

IDC 身分驗證模組
ID Checker

GAM 訪客管理模組
Guest Access Management

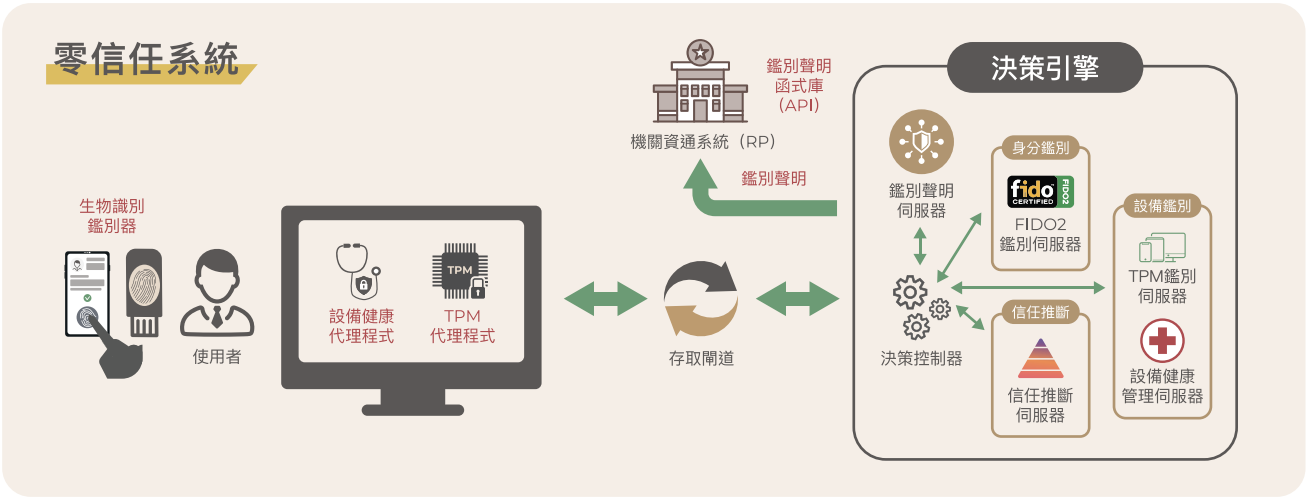
SCP 系統中樞平台
SCP Console

APP 行動管理 APP
UPAS Management App

UPAS ZTA 全方位實踐零信任架構

2020年美國國家標準技術研究院（NIST）頒布了標準文件「NIST SP 800-207」，根據「NIST SP 800-207」列出的零信任原則中提到：「企業應該要盡可能收集有關資產、網路基礎架構與通訊的資訊現況，並用這些資訊來增進安全狀態。」而UPAS能夠協助先進行內網連線設備的資產及健康度檢查，再進行設備鑑別以實現防止偽冒設備入侵內網的可能性。

▼ 零信任架構



第一階段 身分鑑別

以FIDO進行無密碼的雙因子身份認證。

第二階段 設備鑑別

基於設備的信任平台模組（TPM）驗證設備，並進行設備健康管理。

第三階段 信任推斷

依據使用者情境及設備健康狀態，動態決定資源存取結果。

UPAS ZTA 模組介紹

建立在零信任架構之下，UPAS的5大解決方案由1個主要模組，以及20個不同功能的模組所組成，您可以自由選擇功能模組與主模組搭配，建立專屬於您的最佳解決方案。

UPAS自主研發技術已獲得數個國內外專利，有效協助阻斷非法設備連接內網，並實時監控內網安全。具備各種告警機制、使用者友善之操作介面、多種豐富報表，協助您有效達成端點安全防護以及內網安全管控。



1+20 單一平台・單一Agent 功能模組自由組合

ARP IP / MAC 管理模組

ARP Scanner　存取控制

以ARP專利封包解析技術，無須安裝Agent即可進行資料搜集、設備辨識和高強度存取控制。能夠進行100%資產盤點，進而達到IP / MAC管理、設備接入管理（網路存取控制）和網路阻斷。

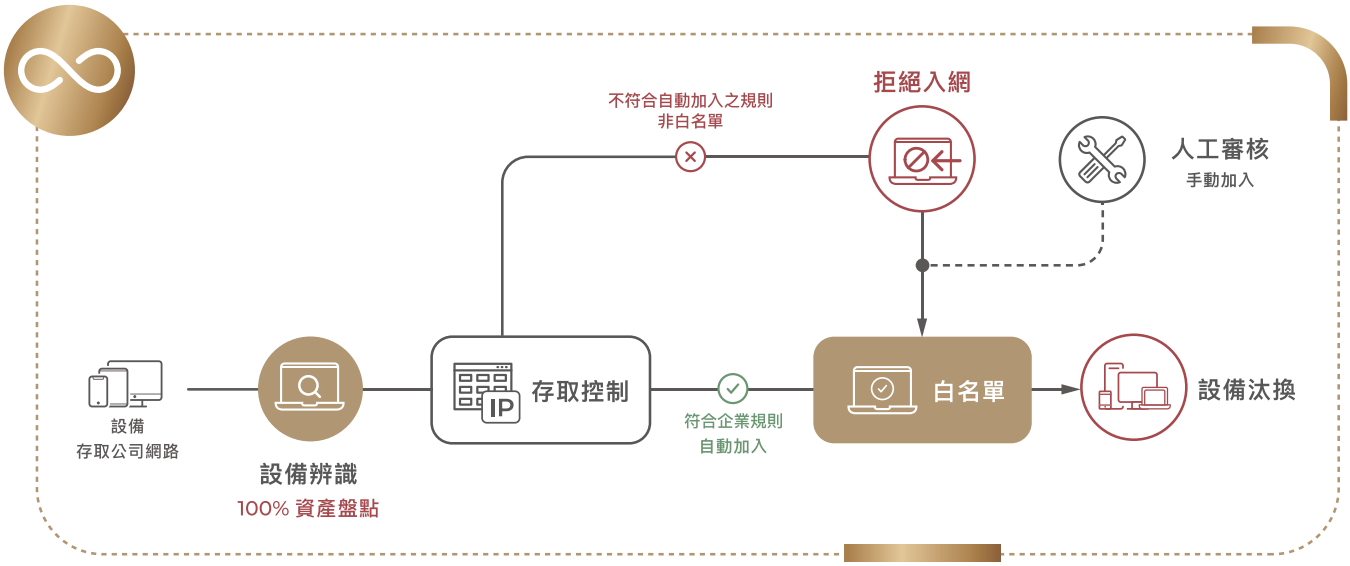
管理者可依需求制訂接入規則，UPAS系統即可自動建立設備白名單，只讓符合安全政策的設備入網，並禁止未經允許的外來設備接入，同時提供重導頁面、Agent UI、MSG等告警機制，從根本確保內網安全。

DAM 設備鑑別模組

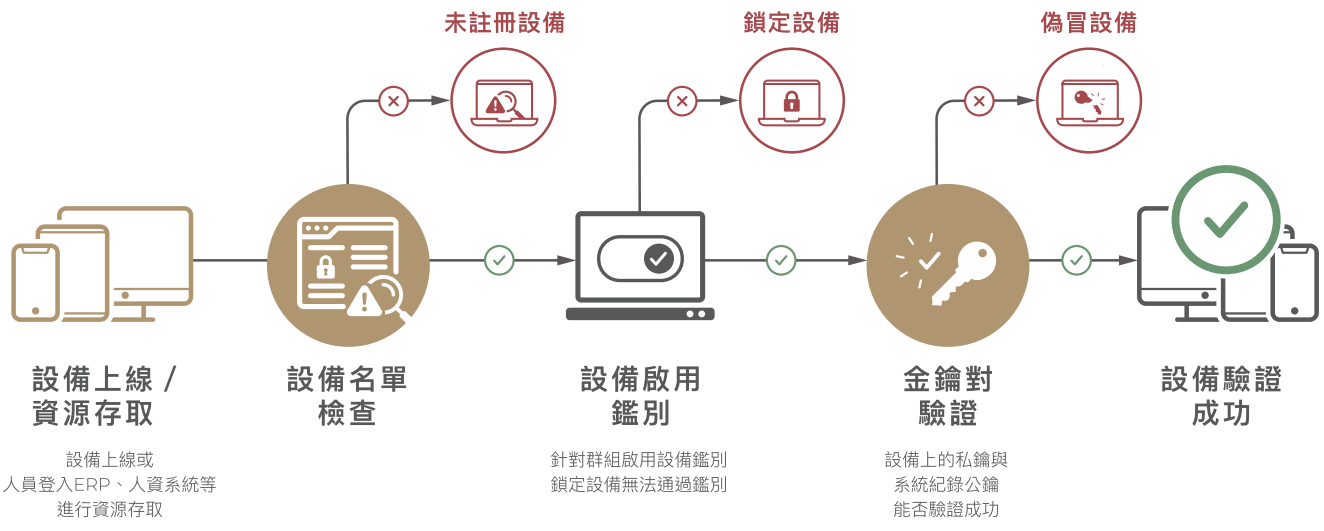
Device Authentication Management

DAM設備鑑別模組透過在終端設備部署的Agent，可以針對設備進行硬體或軟體的保護等級檢查。不僅可在設備上線時驗證連網設備為可信任設備，亦可應用於資源存取場景。透過與身分鑑別廠商的整合，提供全面的安全防護措施。

此模組提供管理設備功能如新增、鎖定、刪除，同時具備設備健康度資訊、儀錶板統計數據及鑑別歷史紀錄查詢功能，並於鑑別失敗時產生事件以通知管理者。



▲ ARP Scanner – IP / MAC 管理流程（存取控制）



▼ DAM – 設備鑑別模組運作流程

PM 補丁管理模組
Patch Management

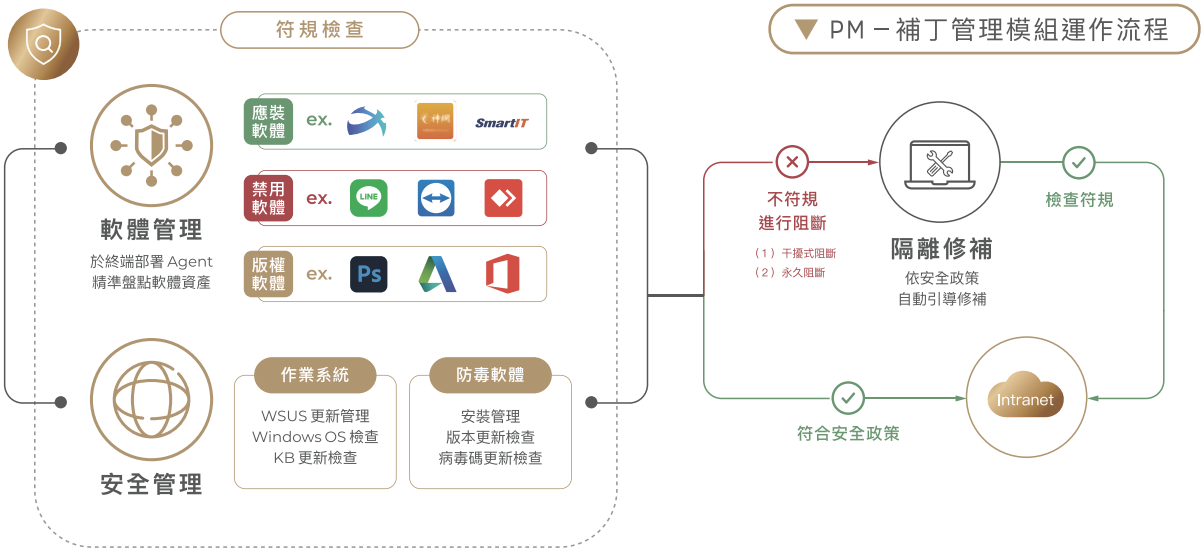
透過在終端設備部署Agent，可定時掃描並獲得內網連線設備的軟體總表、Windows作業系統版號 / KB、防毒軟體資訊與病毒碼版本；藉由軟體總表之搜集，還可進行以下檢查：應裝軟體、禁用軟體、軟體使用版權數量、軟體版本、是否回報WSUS Server等。

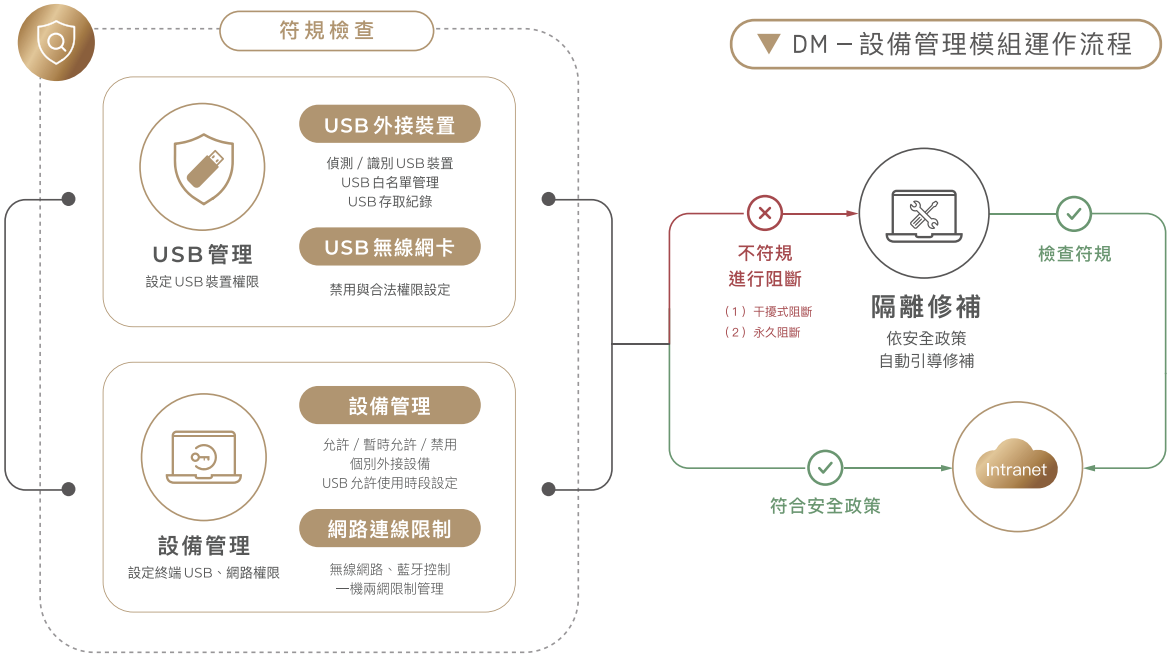
若有不符規事件（應安裝未安裝、不該裝卻安裝、使用盜版軟體、應更新未更新、WSUS未回報）可斷網已重導頁面告知被管制原因，可設定不同程度權限，以利設備穩定運行並引導修補至符合安全政策。另可與ROM模組進行連動，讓管理者協助設備進行自動軟體修補。

DM 設備管理模組
Device Management

透過在終端設備部署Agent，能夠識別並控管USB儲存設備、記憶卡、行動裝置、USB網路卡及光碟機等USB外接裝置，可設定電腦對於接入裝置的權限，像是可否接入裝置和有無權限修改，避免機敏資料外洩。也可建立USB儲存裝置白名單，防止未經驗證的不明USB儲存裝置進行資料傳輸與存取。

另外，可偵測並禁止設備使用無線網路或藍牙，防止繞過企業網路使用私人網路傳輸機敏資料。





ROM 遠程運維模組
Remote Operations Management

在終端設備部署Agent，搜集設備各項軟硬體型號與規格等資訊，並進行遠程運維管理。

具備遠端桌面管理功能及檔案派送、軟體刪除功能。搭配參數指令，可實施檔案靜默安裝。並提供訊息推送及群組廣播功能，讓管理人員便於對終端設備進行管控、維護。

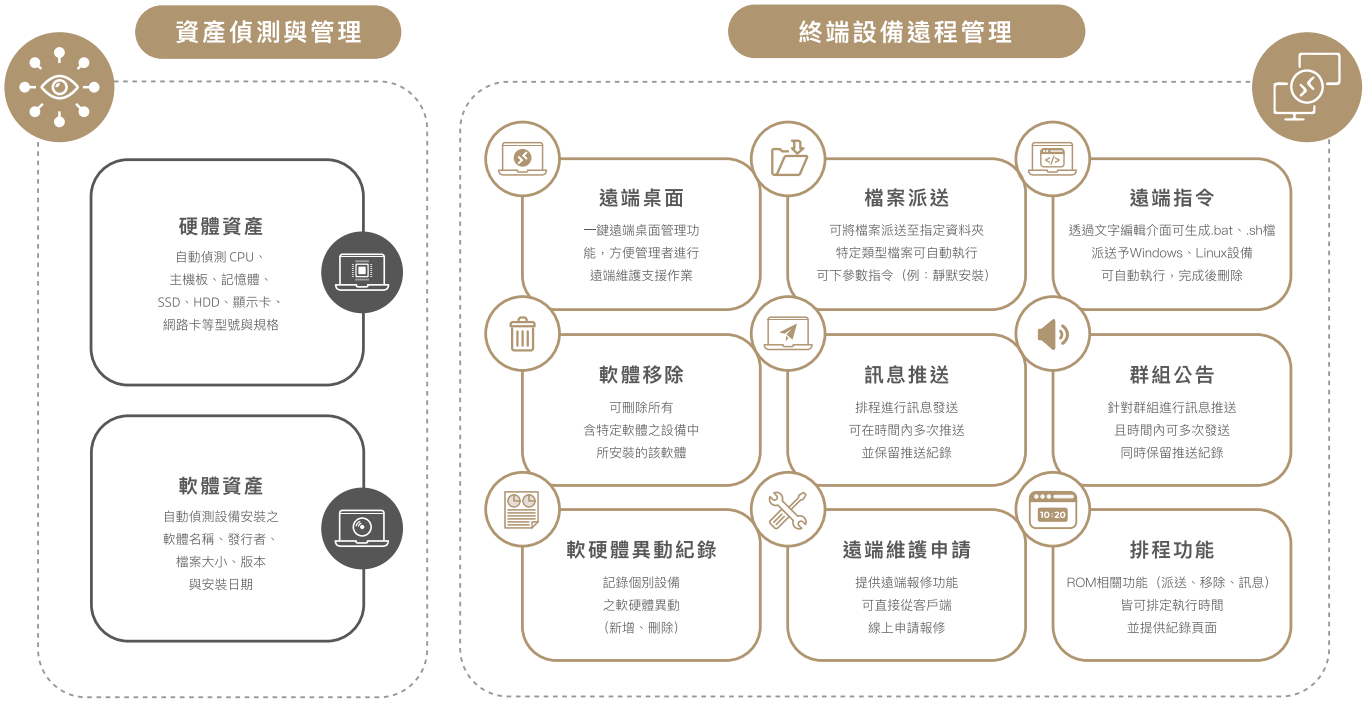
使用者也可以自行向管理人員發出遠端桌面需求，透過Agent UI說明問題，讓管理人員及時協助處理。

TIM 信任推斷模組
Trust Inference Management

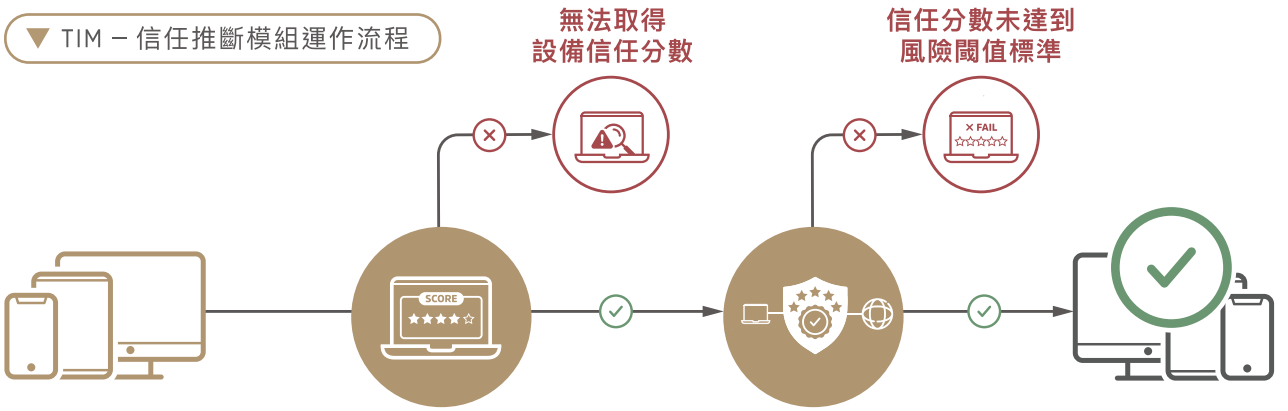
TIM信任推斷模組透過盤點設備資訊（包括OS、防毒、安裝軟體以及潛在風險漏洞），作為設備安全性評估的依據。

收集的安全性資料結合身分鑑別、設備鑑別，能作為於資源存取時信任分數評估之標準，並由決策控制器決定存取結果。此模組功能包含設備安全性檢視、信任分數資訊、儀表板統計數據以及歷史紀錄。

▼ ROM – 遠程運維模組功能說明



▼ TIM – 信任推斷模組運作流程



GPO 管理模組
GPO Management

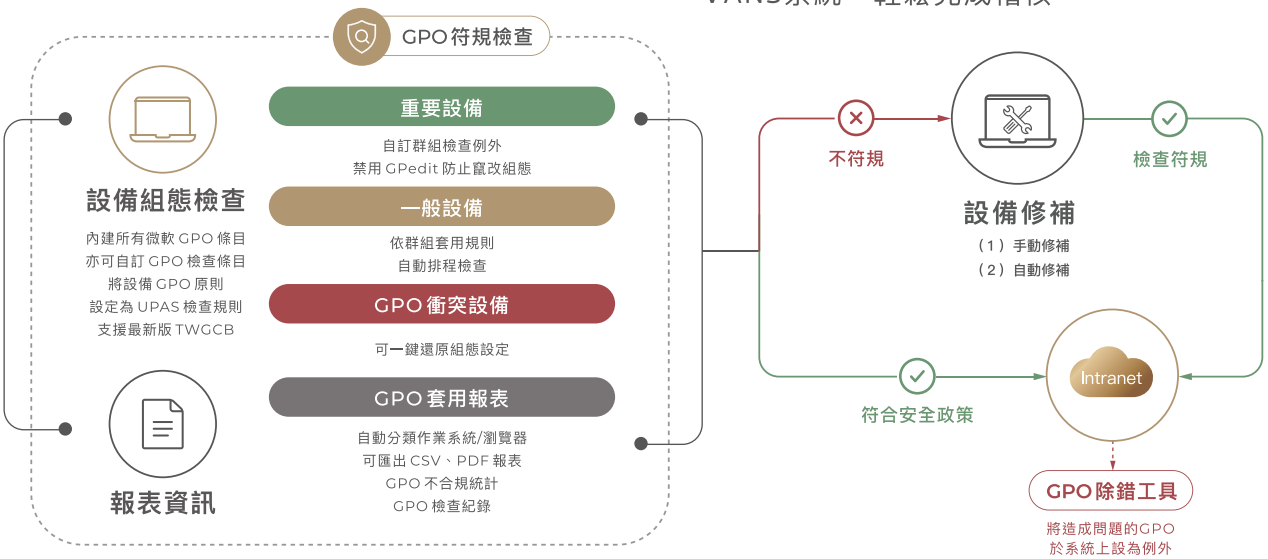
GPO管理模組支援最新版本的TWGCB，在高完成度的資產盤點下，不需要擁有WMI網域最高權限，即可對網域內設備進行GPO套用檢測，針對GPO不合規設備可進行自動修補或手動修補，並自動回報套用結果、提供修補紀錄。

具備組態一鍵還原功能，能將設備還原至套用GPO之前的組態，以免設備套用GPO後無法正常運作。

漏洞警報和通知系統
Vulnerability Alert and Notification System

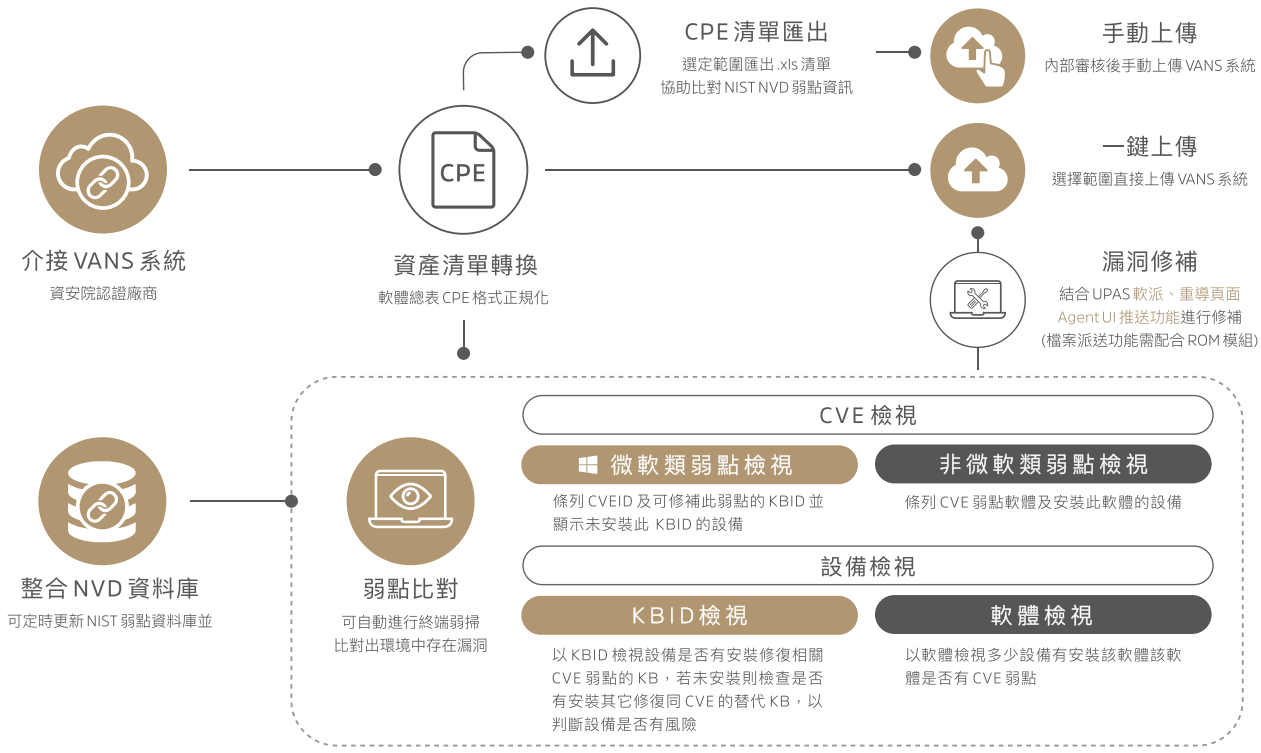
整合NVD弱點資料庫，自動比對環境內電腦軟體資產弱點，統一查詢企業電腦軟體資產是否有NVD公布之CVE漏洞。

可由CVE檢視微軟類弱點以及非微軟類弱點，或是由設備KBID檢視設備是否有安裝修復相關CVE弱點的KB、由設備軟體檢視有多少設備安裝具有CVE漏洞的軟體，透過軟體更新檢查、軟體派送、Agent UI、重導頁面等方式修補漏洞。並支援CPE清單匯出，一鍵上傳資安院VANS系統，輕鬆完成稽核。



▲ GPO－GPO 管理模組運作流程

▼ VANS－漏洞警報和通知系統運作流程



AD 管理模組
ADVantage

可透過分別綁定AD帳號和電腦、禁止本機登入、禁止私退網域等方式，強制所有電腦遵循企業安全政策，使用特定AD帳號登入特定PC，安全政策及管理涵蓋所有Windows設備，整合超過20個以上AD資訊與設備資訊，提供帳號使用紀錄。

針對共用資料夾可偵測檔案及異動。可偵測SID重複事件、產出特權帳號登入登出紀錄和本機帳號等資訊，協助管理人員發現異常行為、控管所有應加入AD網域的設備。

IP / MAC 管理模組
ARP Scanner　IP管理

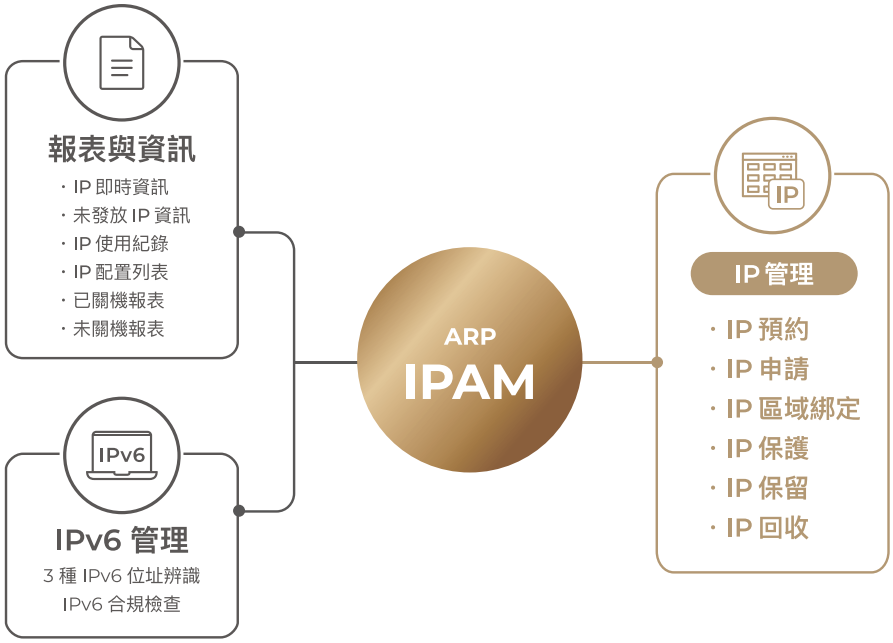
可對所有連線設備進行IP / MAC / DHCP區段 / 電腦名稱 / 硬體指紋（UUID）之間的多重綁定，以達到IP保護、IP保留、IP回收、防止IP衝突、防止MAC偽冒等功能。

UPAS同時能產出：未分配IP列表、IP配置列表、IP使用記錄、未關機報表、未開機報表等多種內網統計清單，幫助管理者完全掌握內網資產和IP使用情況，且相關設定可以一頁搞定，協助管理人員及時輕鬆管理內網IP資源與設備。



▲ AD－AD 管理模組運作流程

▼ ARP Scanner－IP / MAC 管理流程（IP 管理）

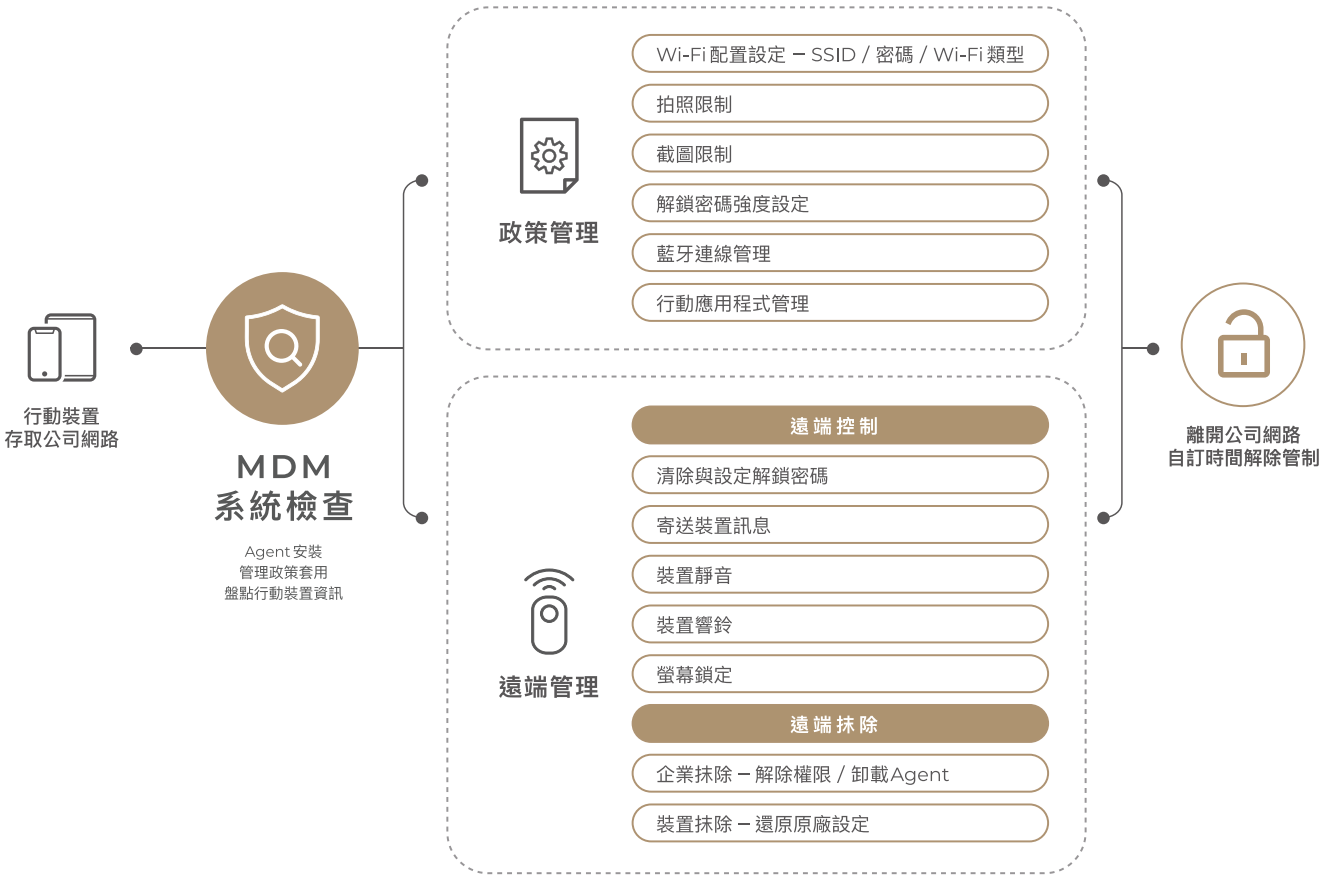


MDM 行動裝置管理模組
Mobile Device Management

透過在Android設備部署Agent，或是建立iOS MDM Server，即可搜集IP / MAC / 帳號 / 手機型號 / OS詳細版本 / 製造商 / 漫遊狀態 / 上次連線時間等資訊，並執行Wi-Fi連線與藍牙連線管理、設定解鎖密碼強度、限制拍照與螢幕截圖、應用程式管理，以及遠端進入螢幕鎖定、清除解鎖、重設解鎖密碼功能。

可根據不同廠區 / 工作區域設置各自的管理政策，依照其OS版本 / 使用的IP區段等資訊自動分配所屬群組並套用群組的安全政策，減少管理人員工作負擔。

針對Android更增加資料恢復原廠設定、開啟靜音模式、設備響鈴、寄送訊息等遠端功能，並提供定位離線輔助判斷，確保行動裝置離開管制區域後，才予以解除管控，避免員工假裝離開管制區域而脫離管控，進而竊取機敏資料。



▲ MDM – 行動裝置管理模組運作流程

SIM 安全整合管理模組
Security Integration Management

不需在終端設備安裝Agent，即可介接WSUS主機、多種防毒軟體（Symantec / Trend Micro / McAfee / 卡巴斯基 / 360衛士）與資產管理軟體（神網 / WinMartix / X-Fort / IP-guard / SmartIT / Ivanti / SCOM / SCCM）達到整合性的管理，進行多項符規檢查，藉由斷網及重導頁面強制使用者修補至符規，不符規設備可設定不同程度的權限限制。

運用IP / MAC系統可達到近100% WSUS納管率、防毒軟體安裝更新率與資產管理軟體安裝更新率，使終端設備符合企業安全策略。

IPL IP地址解析模組
IP Locator

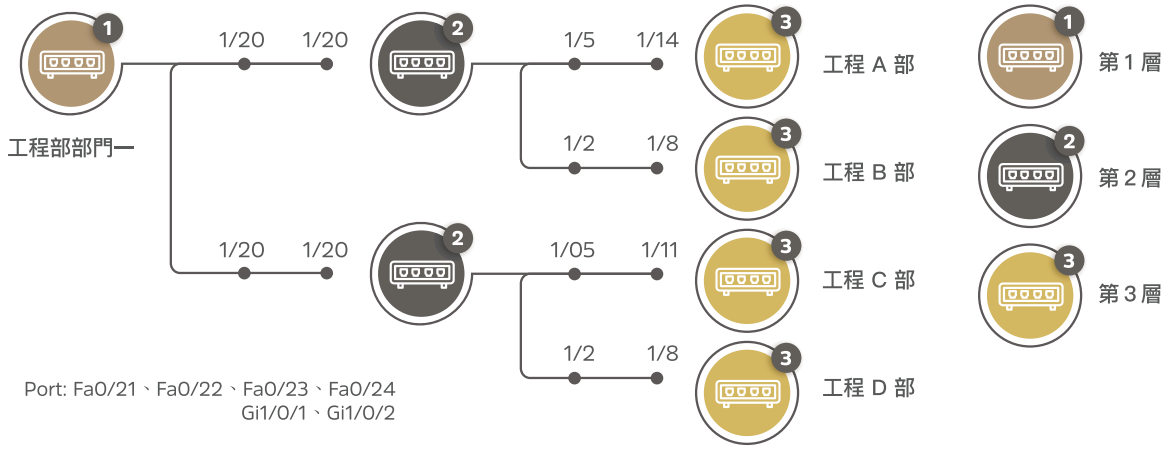
使用SNMP協定自動建立上下Switch串接之關聯性，識別設備IP實體位址，自動產生網路拓樸圖，並提供MAC / IP / Switch / Port / VLAN ID之歷史紀錄，支援市面上絕大多數品牌之Switch，可取得Windows / Linux / macOS / Android / iOS等多平台設備資訊。

協助管理人員盤點與統計資產，可建立單一Port多MAC清單或設定MAC / Port綁定，若發生任何私接設備事件，系統會自動告警並跳出修正提示，確保內網安全與網路正常運行。

▼ SIM－安全整合管理模組說明



▼ IPL－IP地址解析模組架構示意



IPv6 IPv6管理模組
IPv6 Management

不需安裝Agent，即可支援全面的IPv6管理，可偵測單點播送、多點播送、任一傳播三種IPv6位址，對IPv6設備進行符規檢查，阻擋使用IPv6的外來設備。

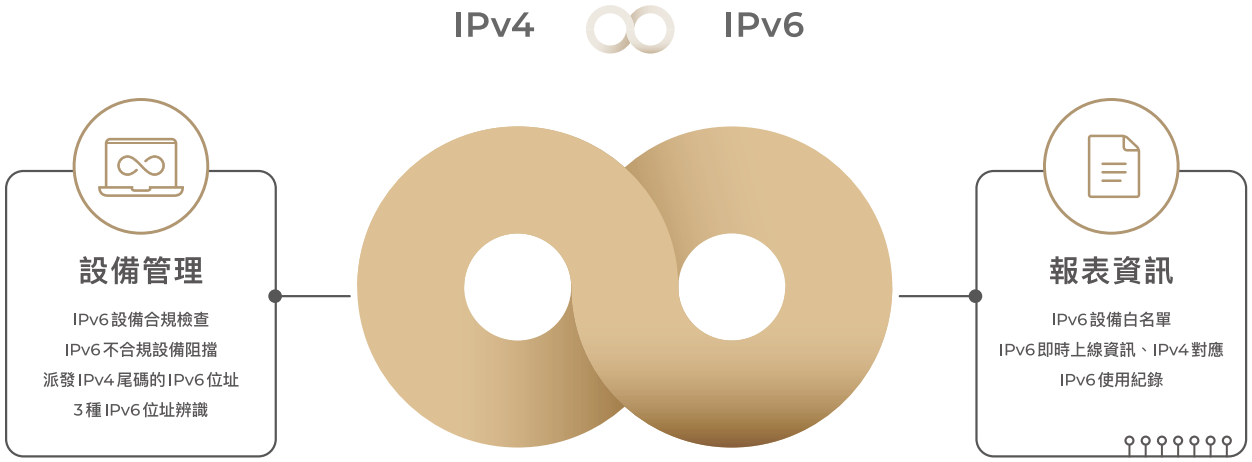
具備自動建置IPv6白名單功能，提供暫時性及永久性IPv6白名單，並可匯入或匯出IPv6設備清單。可依照IPv6管理需求，針對不同管理情境進行白名單設定，並提供多重IPv6及MAC位址綁定功能。

另外，提供IPv6即時資訊、歷史紀錄及IPv4位址的對應列表。

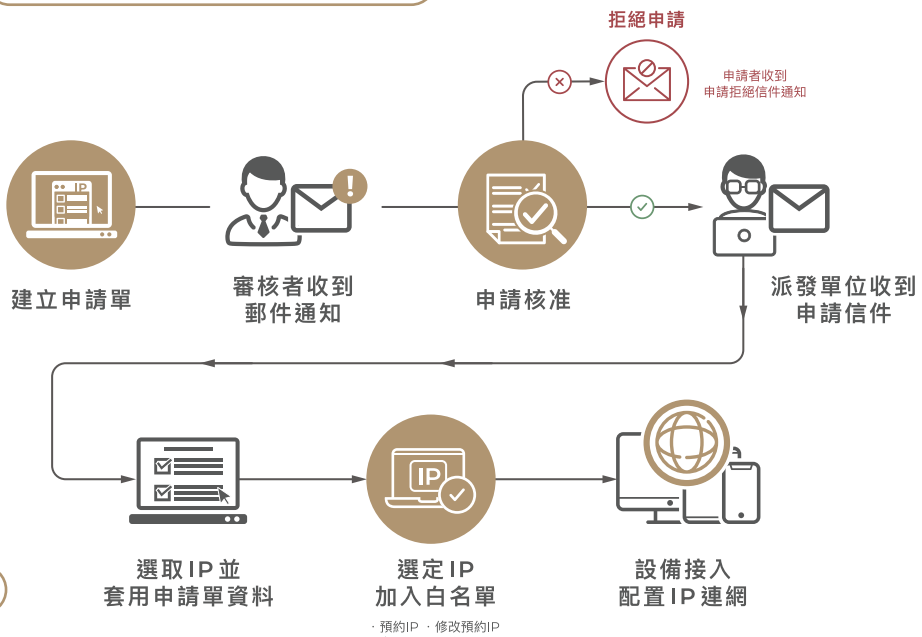
IPAF IP申請表單功能
IP Application Form Functionality

透過自定義線上的IP申請表單，使各單位的申請者能夠輕鬆完成IP申請，同時省去繁瑣的紙本簽核流程，實現全面的電子化操作。此外，可在IP頁面使用搜尋功能，讓使用者能夠在同一個頁面上迅速查詢可用的IP。

一旦使用者確認了欲使用的IP，系統將帶入相關的IP申請單資訊，且申請者可以輕鬆追蹤申請進度，並在需要時查閱所有操作狀態，這些紀錄都將同步記錄於申請紀錄頁面。同時提供匯出功能，使申請者能將所有相關的申請資訊匯出，供備存和查詢之用。不僅確保了資料的安全性，也為未來的審查和管理更加方便。



▲ IPv6 – IPv6 管理模組運作流程



IPAF – IP 申請表單功能運作流程 ▶

DHCP DHCP Server整合功能

DHCP Server Integration Functionality

可透過白名單指定IP與MAC同步DHCP保留區派送。建立白名單後同步至DHCP伺服器，透過系統自動將該白名單中的IP與MAC組合同步至DHCP伺服器的保留區中。當從白名單中移除IP時，系統也會自動將相應的IP與MAC從DHCP伺服器的保留區中刪除。

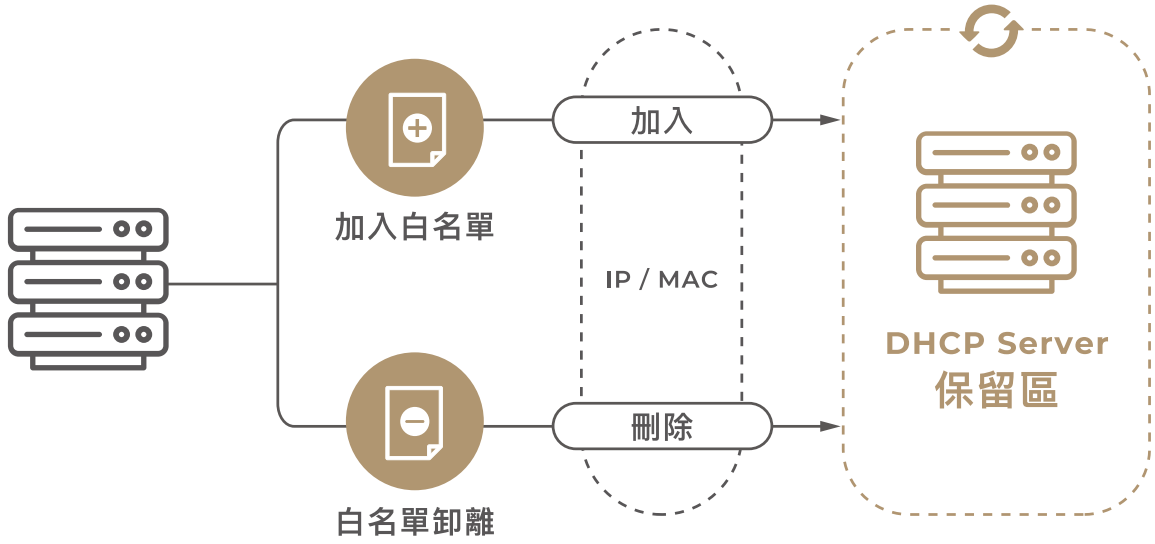
定期比對白名單中的IP與MAC，若發現IP相同但MAC不同的情況，系統會自動將DHCP伺服器保留區中該IP對應的MAC更改為白名單中的MAC地址，以保持一致性。存在DHCP伺服器保留區但不在白名單中的IP與MAC組合，系統會將其從保留區中刪除，以確保保留區中僅保留白名單中設定的IP與MAC地址對應關係。

IPLI IP使用記錄整合功能

IP Usage Log Integration Functionality

UPAS能夠將上下線IP的使用資訊和紀錄同步至指定的Syslog主機，意即可以即時追蹤和監控網路上的IP活動。此功能將助於確保網路安全，並提供更完整的監控和分析工具，以優化網路運作和管理。透過將資訊同步至Syslog主機，也可以方便地保存和檢索歷史數據，以進行風險評估、調查事件和遵循合規要求。

▼ DHCP – DHCP Server整合功能運作流程



IPLI – IP使用記錄整合功能運作流程 ▶



IDC 身分驗證模組
ID Checker

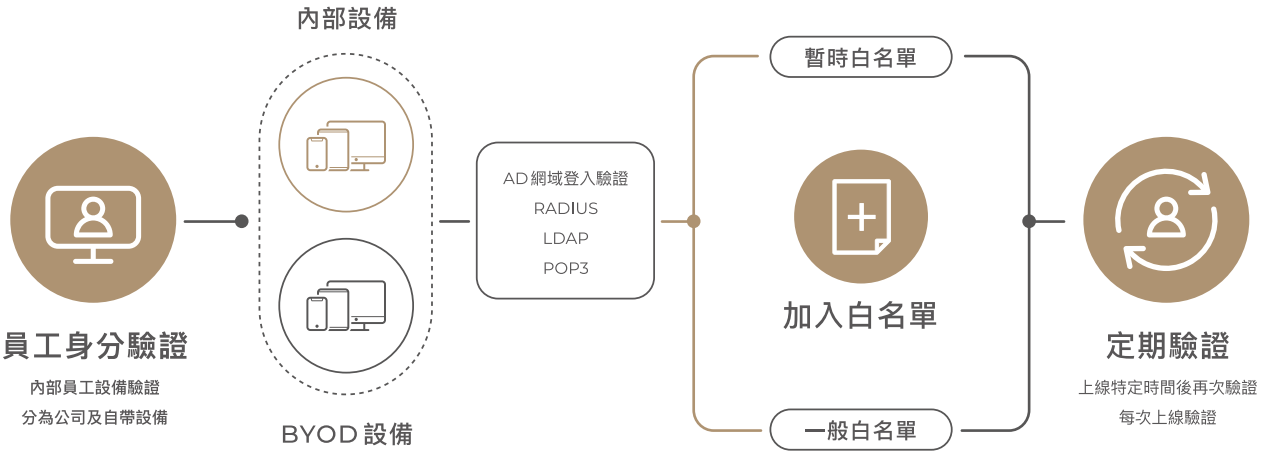
利用AD / LDAP / POP3 / RADIUS伺服器進行人員自攜設備（BYOD）之身分驗證，快速識別設備並管理連線許可，建立人員與設備方面的零信任安全。

人員進入企業或政府網路後，系統即會已重導網頁引導進行認證，依據企業安全政策驗證身份後，系統自動授予人員相對應存取權限（外網 / 內網 / 特定網段）及有效時效，也可要求設備每經固定時間進行定期驗證。

GAM 訪客管理模組
Guest Access Management

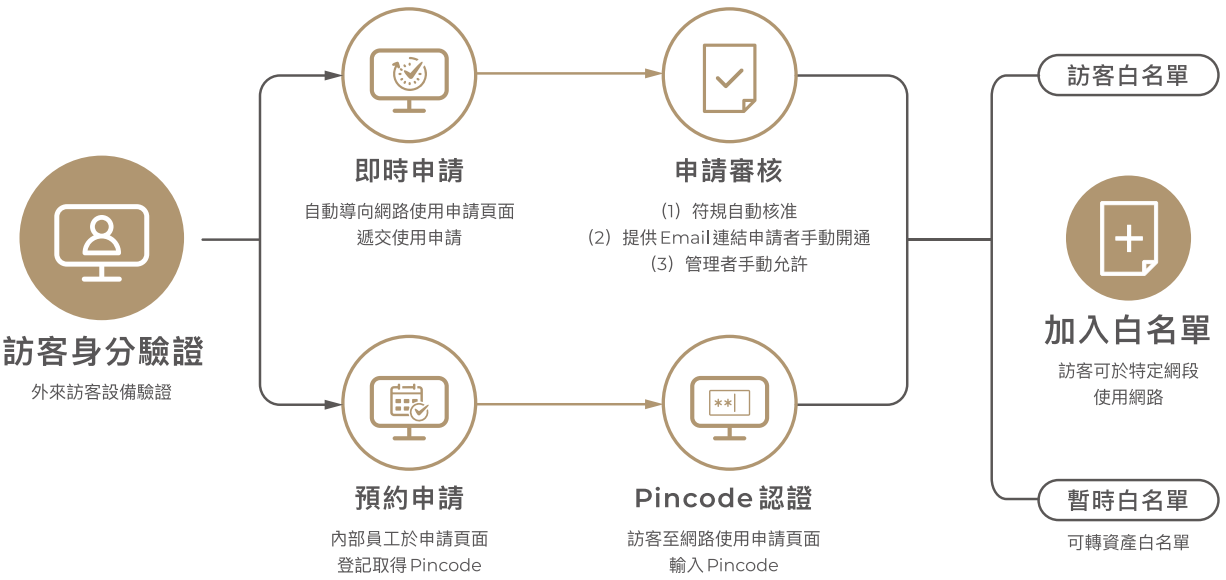
當訪客的外來設備進入企業網路時，訪客管理模組可提供自動化訪客預約申請，透過自動允許、手動允許、受訪者允許開通網路。

使用預約申請的訪客會預先取得Pin Code，進入企業網路後，於申請連線頁面輸入Pin Code即可開通網路，所有訪客皆可設定對內網、外網的存取權限和存取時效，時限到期系統會自動回收權限，自動化機制方便界定與管理訪客，並可產出詳細記錄報表以供稽查。



▲ IDC – 身分驗證模組運作流程

▼ GAM – 訪客管理模組運作流程



SCP 系統中樞平台
SCP Console

可協助超過5,000組IP / MAC的大型企業完成跨國跨區管理，於總部設置SCP Console / 子Console / Sensor統一管理其他區域，防止各地 Console連線異常，並可即時查看各地區內網狀況，統整全球內部數據，協助管理者分析各地事件趨勢及安全管理政策。

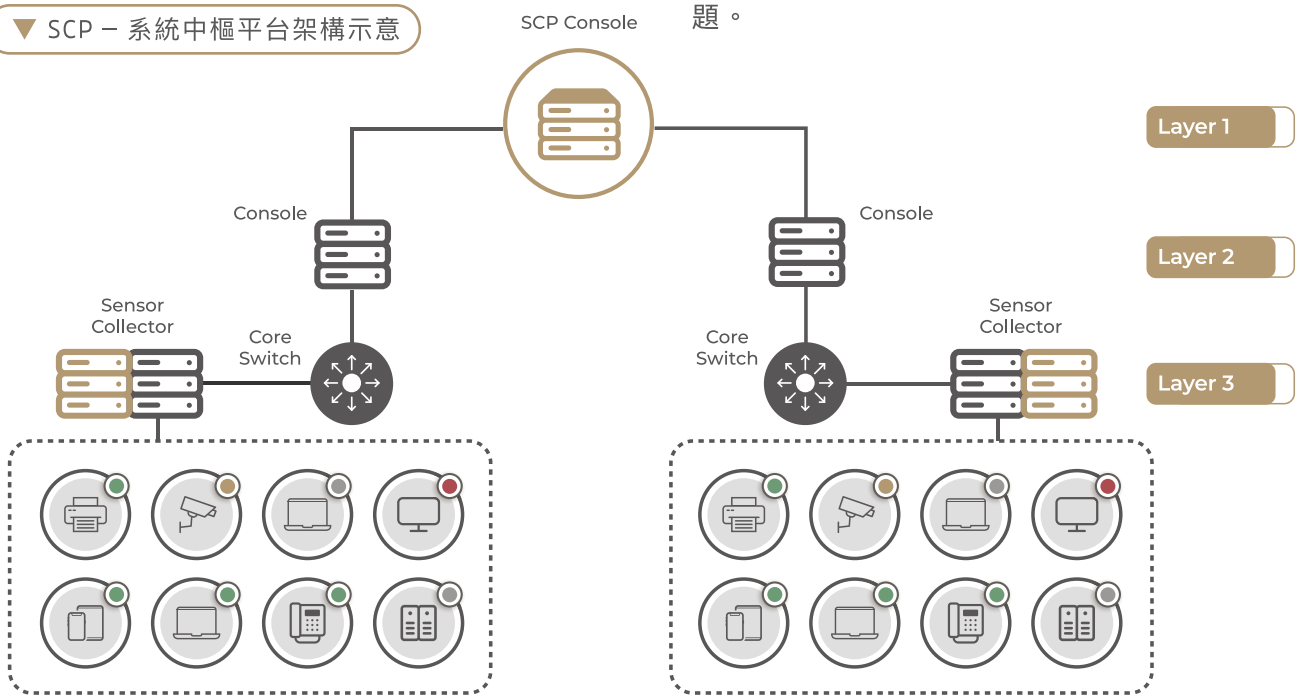
也可即時同步白名單設備資訊及出差白名單至各地子Console，簡化差旅人員權限管理，保持全球同步更新。

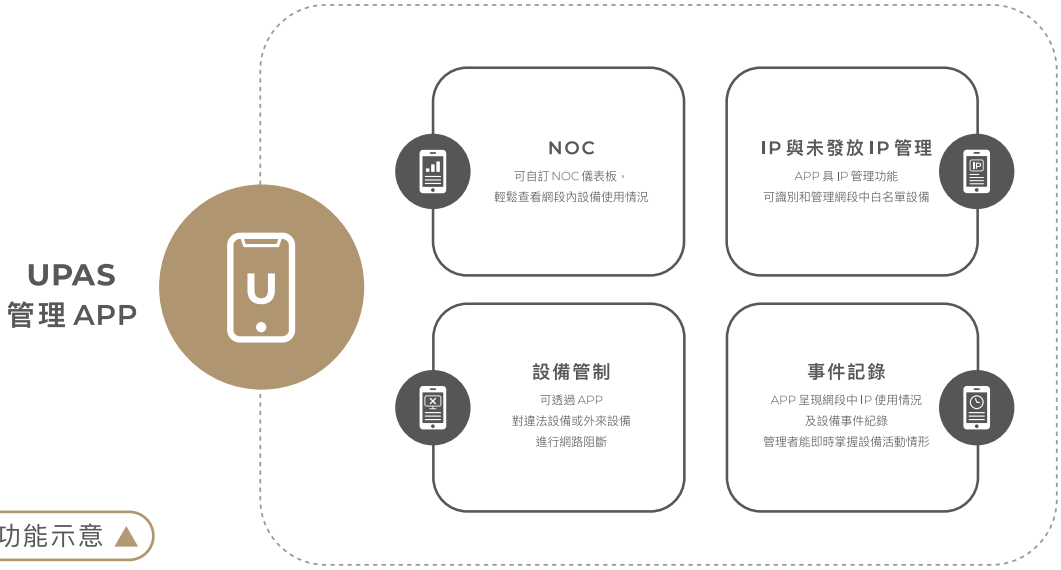
APP 行動管理 APP
UPAS Management App

行動管理APP彙整了UPAS上的實用功能，讓管理者可以隨時隨地掌握企業網段及設備的使用狀況。透過自訂的NOC儀表板，可以輕鬆查看網段內設備的使用情況。

此外，APP提供了IP管理功能，能夠輕鬆識別和管理網段中的白名單設備。並透過設備管制功能，可以有效地對違法設備或外來設備進行網路阻斷。同時，APP也呈現了網段中的IP使用情況及設備的事件紀錄，讓管理者能夠全面掌握每個設備的活動狀況，及時應對潛在問題。

▼ SCP – 系統中樞平台架構示意



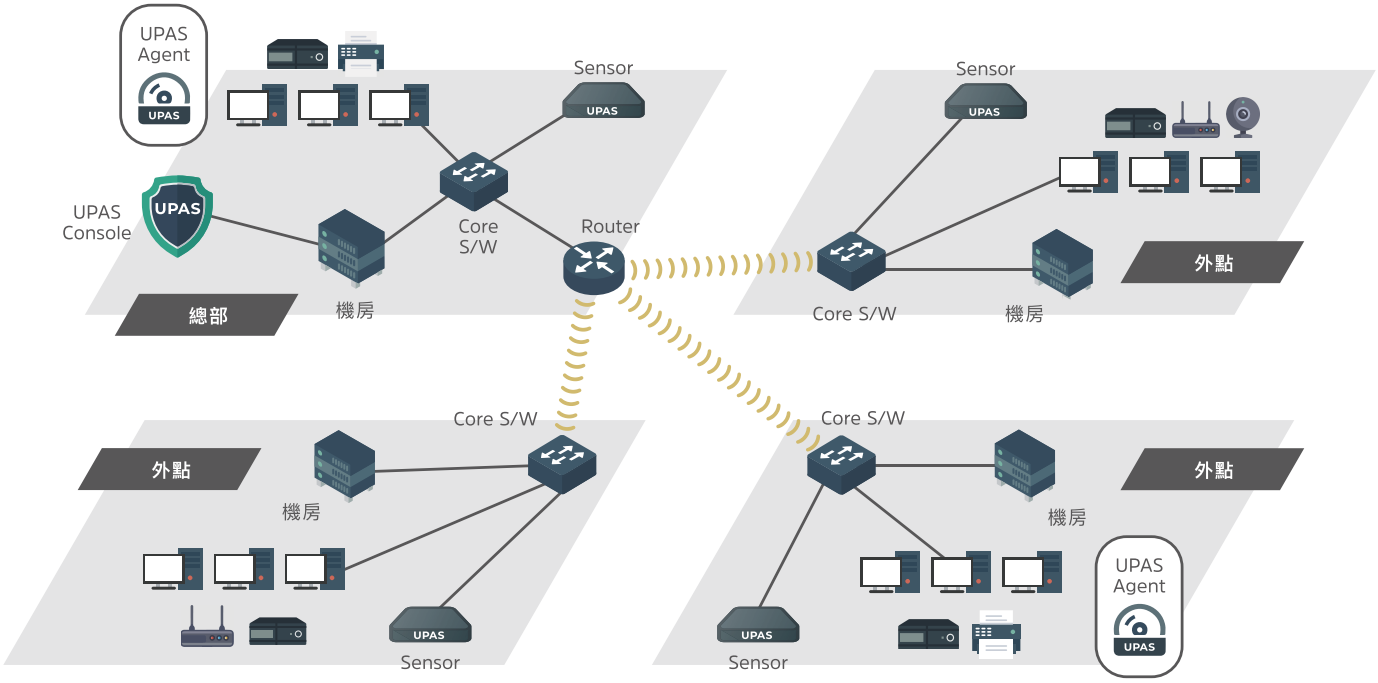


APP – 行動管理 APP 功能示意 ▲

UPAS 主要系統架構 - Console + Sensor (+Agent)

採取旁聽式部署，不須改變客戶端網路架構，不論無線或有線的網路環境皆適用，只要將Sensor連接上客戶環境的Core S/W，即可透過Trunk Port收取網路封包，盤點所有上線設備，並透過Console對其進行身分認證和網路存取控制。

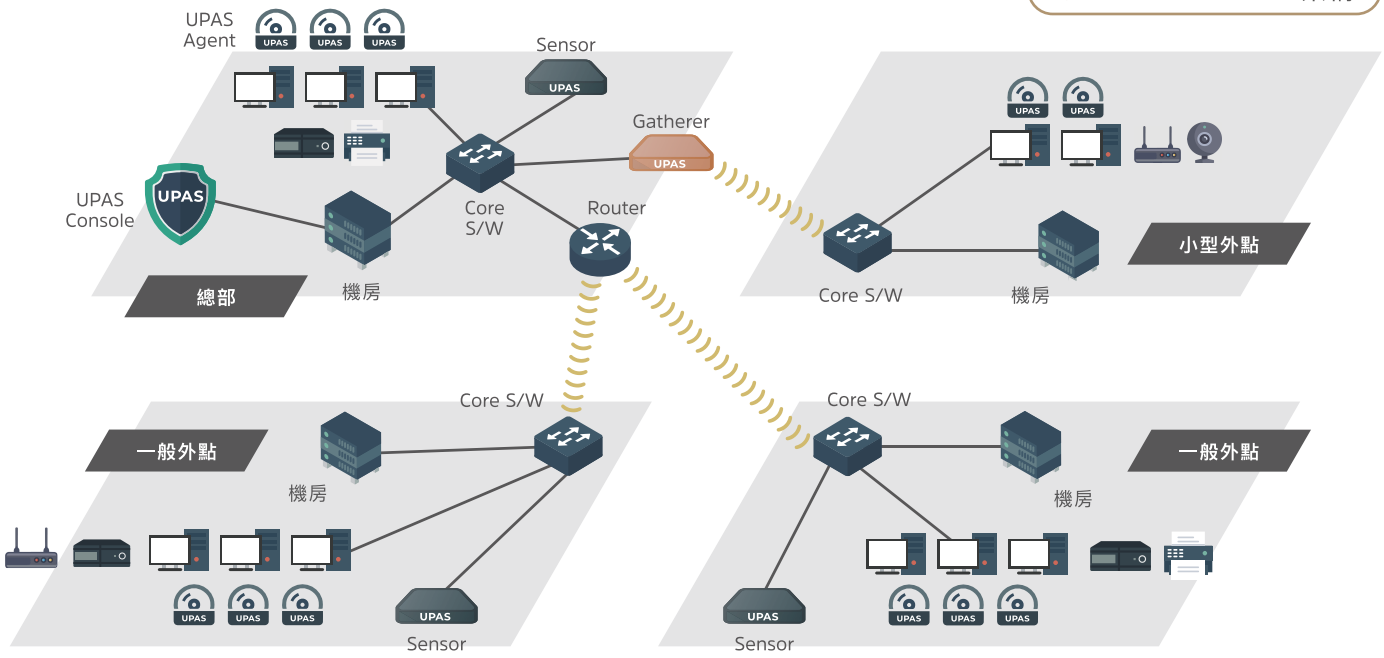
▼ UPAS主要系統架構 – Console+Sensor



Gatherer 架構

Sensor + Gatherer混和方案可同時滿足存取控制和進階資產管理需求；特別是對於外點數量特多的環境，只要在總部建置Gatherer，即可跨Router、Firewall進行管理，顯著降低系統建置成本。

▼ Sensor+Gatherer架構



UPAS ZTA 跨平台支援各大作業系統



ZERO TRUST ARCHITECTURE

- 版權軟體管理
- 安裝軟體總表
- 檔案/指令派送
- 禁用軟體與程式檢查
- USB外接裝置管理
- 軟體移除
- 應裝軟體與版本檢查
- USB白名單
- 遠端桌面
- 設備軟體異動紀錄
- 無線網路管理
- 使用者發起遠端服務需求
- 自動修補
- 軟硬體資產資訊蒐集
- 訊息推送/群組廣播

UPAS ZTA 建議規格

	Console		Sensor	
CPU	< 1,000 U 1,000 ~ 3,000 U 3,000 ~ 5,000 U	4C8T 8C16T 12C24T	BOX: <500 BOXi7: <1,000 1U: 2,000	J3160 (4C4T) i7-8550U (4C8T) E3-12XX (4C8T)
RAM	< 1,000 U 1,000~3,000 U 3,000~5,000 U	8 GB 16 GB 32 GB	BOX: <500 BOXi7: <1,000 1U: 2,000	4 GB 8 GB 8 GB
HDD	< 1,000 U 1,000~3,000 U 3,000~5,000 U	250 GB SSD X4 Raid5 250 GB SSD X4 Raid5 250 GB SSD X5 Raid10	BOX: <500 BOXi7: <1,000 1U: 2,000	250 GB SSD X1 250 GB SSD X1 250 GB SSD X1
備註	5000 U 以上請另行確認		單網卡 2000 U / 20 個 VLAN / 20 個網段限制	

UPAS ZTA 5 大資安解決方案

為您的管理需求量身打造
常見使用情境一次看

針對企業面臨的主要內網資安與管理問題，UPAS提供五大解決方案，整合UPAS ZTA的20個強大模組功能。



NAC 網路存取控制

為您確保內網無非法設備接入 ARP DAM

使用情境

隨著存取網路的裝置類型與數量大幅成長，企業與政府須考量到這些裝置的安全風險。

1. 企業如何在不需安裝Agent的情況下實現全面的設備盤點與內網存取控制，並保證網路的安全性？
2. 需要根據安全政策自動建立設備白名單，禁止不符合規定的設備接入內網。
3. 希望能夠在設備上線時進行可信任設備驗證，同時提供全面的設備安全防護。

解決方案

- UPAS的NAC系統使用ARP專利封包解析技術實現無Agent的資料搜集、設備辨識和高強度存取控制，達到100%的資產盤點，包括IP/MAC管理和網路存取控制。
- UPAS系統根據需求制定接入規則，自動建立符合安全政策的設備白名單，禁止未經允許的外來設備接入。同時提供重導頁面、Agent UI、MSG等告警機制，確保內網安全。
- DAM設備鑑別模組可進行硬體或軟體的保護等級檢查，包括設備健康度資訊和鑑別歷史紀錄查詢功能。在鑑別失敗時，系統會產生事件通知管理者。



ITAM IT 資產管理

為您全面防禦病毒、修補漏洞
合規沒煩惱、確保設備健康度

PM DM ROM TIM GPO VANS

使用情境

安裝代理軟體的終端安全方案仍存在死角，多數企業環境內，無法完善安裝的裝置數量在持續增長：

1. 企業內部許多在線裝置常因未定期更新版本，容易形成外部入侵的節點，如何確保企業防毒軟體及應用程式能如實運作？
2. 不明的外接設備（如：USB）進行資料存取，造成極大的機密資料外洩及勒索風險。
3. 如何確保企業及單位內部設備符合政府規範，同時也針對其健康度來把控？

解決方案

- UPAS具備全面的資產管理與安全監控，自動掃描終端設備，收集軟體及系統資訊，包括裝載軟體、安全補丁狀態等。監控USB及外接設備，設定權限以防止資料外洩。整合弱點資料庫，自動識別及修補系統漏洞，提升系統安全性。
- 便捷的遠端運維和管理，提供遠程桌面管理和檔案派送功能，方便管理者進行遠端操作和維護，提供訊息推送和群組廣播功能，以有效管控和維護設備。
- 強化的信任評估與存取控制，根據設備安全性資料及身分鑑別，評估存取時的信任分數，決定存取權限。提供設備安全性檢視、信任分數資訊和存取歷史紀錄，協助管理者做出適當的存取決策。

IAM 身分識別管理

確保設備人員身分皆通過驗證 AD

使用情境

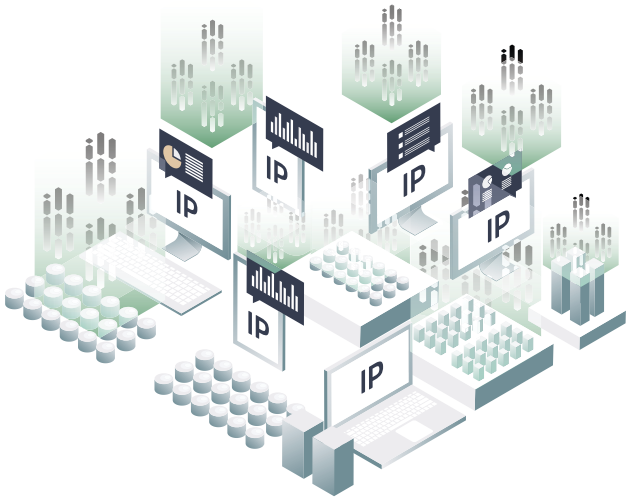
進入內部網路的設備必須被識別身分及管理，根據身分授予其最小化的權限，提供管理者對數位身分的可視性。

1. 企業希望可以強制所有電腦遵循企業安全政策，包括使用特定AD帳號登入特定PC，並控管所有Windows設備等。
2. 企業需要監控共用資料夾中的檔案異動，並偵測潛在的安全風險和異常行為。



解決方案

- UPAS可透過AD帳號和電腦綁定、禁止本機登入、禁止私退網域等方式，強制所有電腦遵循企業安全政策，確保使用特定AD帳號登入特定PC，並整合AD資訊與設備資訊，提供帳號使用紀錄。
- 針對共用資料夾，能夠監控檔案異動，包括新增、修改和刪除等操作，並及時偵測潛在的安全風險，以保護企業資料的安全性。
- 透過偵測SID重複事件、特權帳號的登入和登出紀錄以及本機帳號等資訊，協助管理人員發現並應對異常行為，並控管所有應加入AD網域的設備。



IPAM IP 位址管理

讓您管理 IP 更加輕鬆方便 ARP

使用情境

隨著企業與政府組織規模擴大，擁有的龐雜網路資源亟待被有效管理與應用。

1. IP位址混亂造成的管理困擾，除影響正常營運外，也大幅增加管理人員在基礎維護的耗時。
2. 當事件發生時，MIS人員查找問題費時、費力，錯失最佳救援時機。

解決方案

- IPAM可以自動辨識設備屬性、顯示IP/MAC資訊，同時具多重綁定功能，可對所有連線設備進行IP/MAC/DHCP區段/電腦名稱/硬體指紋（UUID）之間的多重綁定，實現IP保護、保留、回收，同時防止IP衝突和MAC偽冒。
- UPAS在設定上可一頁式管理相關功能，並能產出多種內網統計清單，幫助管理者完全掌握內網資產和IP使用情況，協助管理人員及時管理內網IP資源與設備。

MDM 行動裝置管理

為您確保行動裝置與機敏資料安全 MDM

使用情境

智慧型手機、平板電腦等裝置普及，網路環境使用權限應更受關注。

1. 行動裝置的系統開放性、應用程式開發便利性，無嚴謹規範將使資安風險拉警報，提升資料外洩風險。
2. BYOD/COPE如何制定管理規範？

解決方案

- MDM結合網路存取控制技術，於行動裝置進入組織網路時，進行符規檢查與身分識別後根據群組設定套用管制政策，嚴格保護組織資訊安全。
- 管理者可依場域制定管理政策，管制項目包含Wi-Fi連線設定、禁用相機、解鎖密碼強度設定、禁用截圖設定等，管理介面亦可遠端(ROM)控制裝置鎖定螢幕、卸載代理程式、初始化設定、設定與清除解鎖密碼、響鈴靜音與訊息推送。
- 支援iOS / Android作業系統。



ZERO TRUST

TRUST UPAS

UPAS 導入效益



NAC ー 建立內網邊界防護

有效降低安全與營運風險。防止私接設備造成的風險，包括資料外漏與病毒木馬入侵。



資產盤點 ー 強化設備可視性

建立 IoT 資產清單，強化設備可視性，避免閒置設備。且辨識設備屬性、OS、所在位置、使用者資訊等內網設備資料。



合規檢查 ー 提高內網符規率

AD 管理完善率
Windows Patch 更新率
防毒軟體安裝率更新率
應裝軟體安裝率更新率



完善軟硬體管理政策

透過控管禁用軟體，非法版權查核，防止非法版權被原廠求償；設備管理可控管 USB 外接設備、限制 Wi-Fi 使用、並防止一機兩網之行為。



完善 IP 管理流程

IP 回收、IP 保留、IP保護、IP 使用記錄、IP 配置清單、已關機報表、未關機報表。



協助通過法規與資安稽查

符合《ISO27001》、《NIST CSF》、《資通安全管理法》、供應鏈安全檢查等稽查標準。

立足台灣・跨足國際
豐富實績・好評見證



30 年

台灣原廠

專業自主研發經驗

7 大

產業應用

政府｜科技｜製造｜金融｜醫療
教育｜一般企業｜關鍵基礎建設

3800+

客戶見證

100+

10000 IP以上
大型企業

榮獲美國矽谷期刊《APAC CIO Outlook》

2023 TOP5 Cyber Security Solutions Provider in Taiwan 台灣資安解決方案
2023 TOP10 Cyber Security Solutions Provider in APAC 亞太資安解決方案

UPAS

ZERO TRUST ARCHITECTURE

了解更多專屬於您的最佳安全管理解決方案

Website Facebook LINE Medium LinkedIn