

# UPAS

ZERO TRUST ARCHITECTURE

## 內網零信任安全解決方案

連網設備全面可視化

打造校園網路安全環境

以單一締造第一 · 內網管理首選

# UPAS

ZERO TRUST ARCHITECTURE

ZERO TRUST · TRUST UPAS

## 目錄

- 關於UPAS
- 盤點校園設備管理需求
- 成功案例網路環境
- 首創！NAC+ITAM2合1
- 教育單位資安解決方案
- 系統管理流程
- 全方位整合內網安全資訊
- 導入效益

# UPAS

永不信任 · 持續驗證

## 全方位內網安全管理系統

---

### 關於UPAS

# UPAS

30年

台灣原廠

專業自主研發經驗

7大

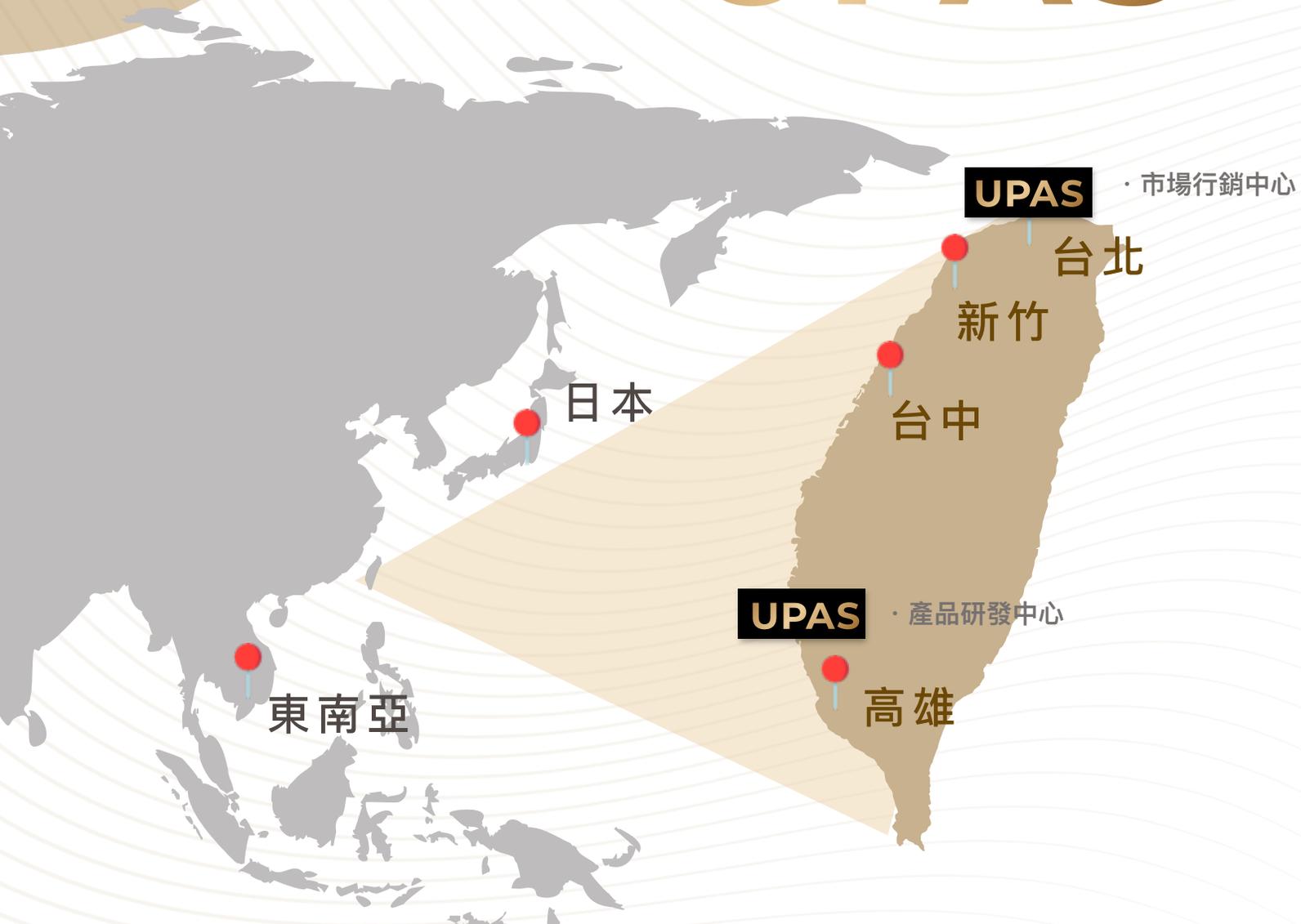
產業應用

政府 | 科技 | 製造 | 金融 | 醫療  
教育 | 一般企業 | 關鍵基礎建設

3800+

客戶見證與信賴

4





## 資安整合服務平台

上架資安產品



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



## 資訊安全能量登錄

NOC | AD管理 | IAM

GCB | VANS | OT系統防護

## 資訊服務能量登陸

IPAM (IP管理系統)

## 《資通安全管理法》 採購指引懶人包

資安弱點通報機制  
(VANS)

導入參考廠商

廠商名稱 (以筆劃排序)
ForeScout
中華數位科技股份有限公司
中華龍網股份有限公司
日月晶耀股份有限公司
旭辰資訊股份有限公司
捷睿智能股份有限公司
瑞思資訊股份有限公司
誠雲科技股份有限公司
達燭科技股份有限公司
睿明知通股份有限公司
精品科技股份有限公司
精誠資訊股份有限公司
優倍司股份有限公司
耀祥網科技股份有限公司



Since 1993

# UPAS

內網安全管理領導品牌



# UPAS

永不信任 · 持續驗證

## 全方位內網安全管理系統

---

### 盤點校園設備管理需求

# 盤點校園設備管理需求

以下僅為示意圖，非實際案例環境

## 教室、研究室、圖書館

1. 學生自帶設備管理
2. 電腦教室設備：
  - 使用者驗證
  - 使用記錄

## 行政網路、OA

1. 教師及行政人員：
  - IP/MAC綁定
  - IP保護
2. 資產盤點
3. 外來設備入網控管

# 終端設備主要的安全威脅



## 防漏困境

- 邊界防護
- AD管理
- USB禁用



## 防駭困境

- 重要KB未更新
- 防毒軟體未安裝、更新
- EDR軟體未安裝
- 軟體禁用
- 組態設定不符合GCB
- 安裝軟體高風險CVE



## 運維困境

- 軟硬體資訊收集
- 軟體派送、移除
- 遠端桌面
- 版權檢查
- 訊息推送
- IP管理
- 財產管理

# UPAS

永不信任 · 持續驗證

## 全方位內網安全管理系統

---

### 成功案例網路環境

# 成功案例網路環境

客戶：國內科技大學

網路環境：約3,000台終端設備 / 9台Sensor

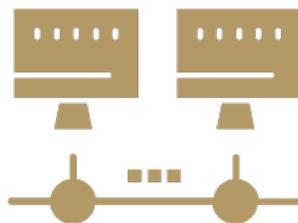
**管理需求：終端設備盤點、外來設備入網控管、針對設備漏洞進行修補檢查**

UPAS 提供此客戶的解決方案



100% 資產盤點

自動辨識連網設備資產屬性



外來設備管理

入網設備完整上線資訊



一鍵上傳VANS弱點比對

GPO套用檢測 不合規設備修補

# UPAS

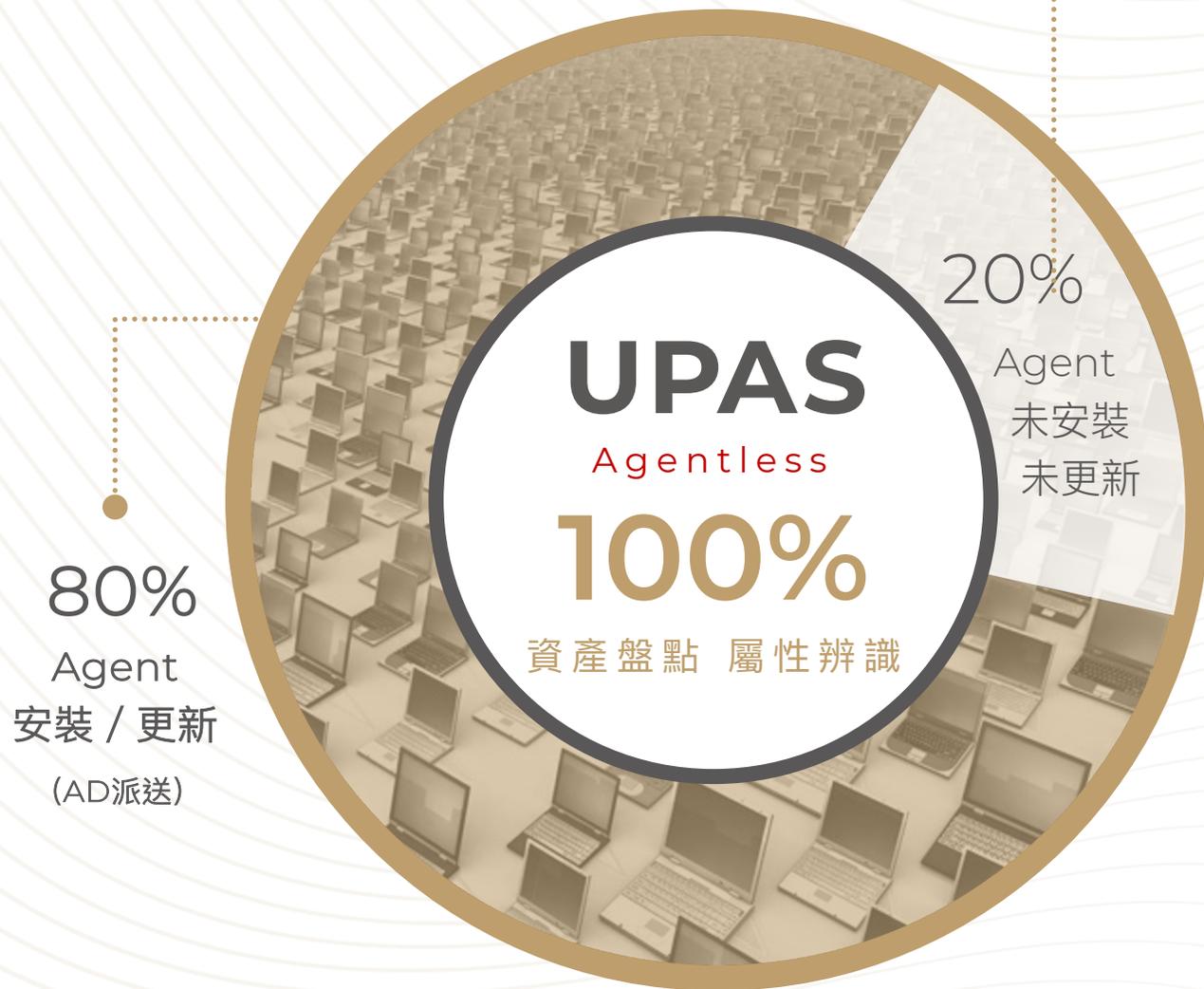
永不信任 · 持續驗證

---

## 首創！NAC+ITAM2合1

網路存取+資產管理 邊界防護再升級！

# 為什麼企業需要 98% Agent ?



強化Agent-Based設備資產管理，  
查找出環境內未安裝、未更新的設備

## 漏洞修補技術

WMI推送 | 重導網頁

完善Agent安裝 / 更新

整體Agent成功部署率

達 **98%** 以上



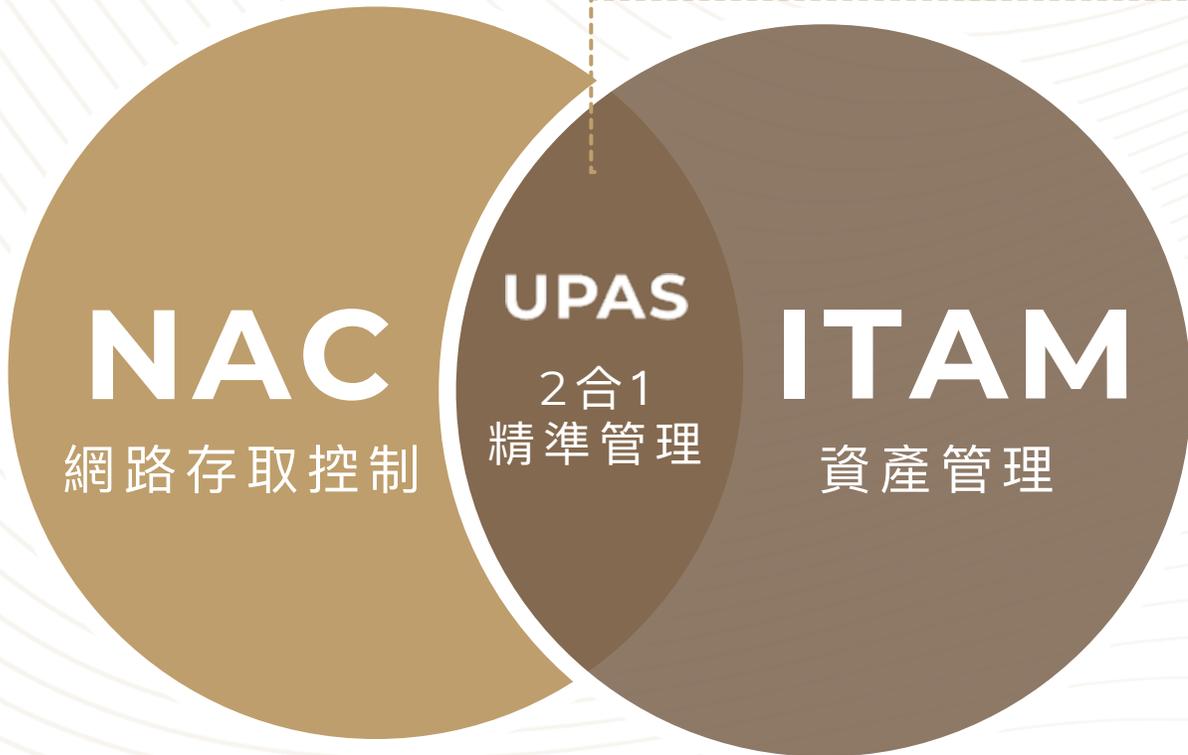
KB、防毒軟體更新率  
防毒、應裝軟體安裝率  
GPO套用、VANS修補  
軟硬體資訊收集完整性等

全面提升 

# UPAS

## 網路存取 + 資產管理 2合1

- ✓ 自動
- ✓ 安全
- ✓ 資料正確



環境內設備



+1

自動安裝agent  
重導網頁/WMI推送

-1

軟體總表-1  
版權檢查-1

高風險設備 → 阻斷、引導修補

精準管理  
設備納管率

98% ↑

# 內網安全管理零死角

傳統的管理方式

NAC、ITAM兩套軟體分別執行

UPAS首創! 新世代管理趨勢

NAC+ITAM一套軟體 整合管理

上線設備  
未安裝agent

無法掌握

精準管理

安全

上線設備  
agent無回應

無法掌握

精準管理

安全

設備離線及卸離

無法掌握

精準管理

方便

管理成本

高  
多套軟體 耗時費力

低  
單一平台 整合各項內網資訊

自動化

設備納管率

80% ↓

98% ↑

資料  
正確

VS

# UPAS ZTA 三重防線

## 防漏

機敏資料不外流

## 防駭

防範駭客入侵

## 運維

全面設備運維

全方位提升校園內網環境安全，協助資訊部門確保終端設備正常運行、輕鬆應對資安標準稽查、資產妥善分配及使用

# UPAS

永不信任 · 持續驗證

## 全方位內網安全管理系統

---

## 教育單位資安解決方案

# UPAS 全方位內網安全管理系統

單一平台·一套搞定 教育單位解決方案

ZERO TRUST ARCHITECTURE 零信任架構



NAC

網路存取控制

100%資產盤點  
納管連網設備



IPAM

IP位址管理

管理內網  
IP資源及設備



IAM

身分識別管理

識別連網設備  
使用者身分



ITAM

IT資產管理

軟硬體設備管理  
合規沒問題

永不信任 · 持續驗證

# 全方位內網安全管理系統

---

## UPAS ZTA

系統管理流程

# UPAS ZTA 設備安全檢查流程



## NAC 網路存取控制

### 解決要點

#### 設備入網第一道辨識 納管連網設備

- ARP專利封包解析技術
- agentless 100%資產盤點
- 快速定位IP實體位址
- 掌握設備財產編號 以利財產統計分析



# 自動辨識20種以上內網設備資產屬性



100%  
設備可視性

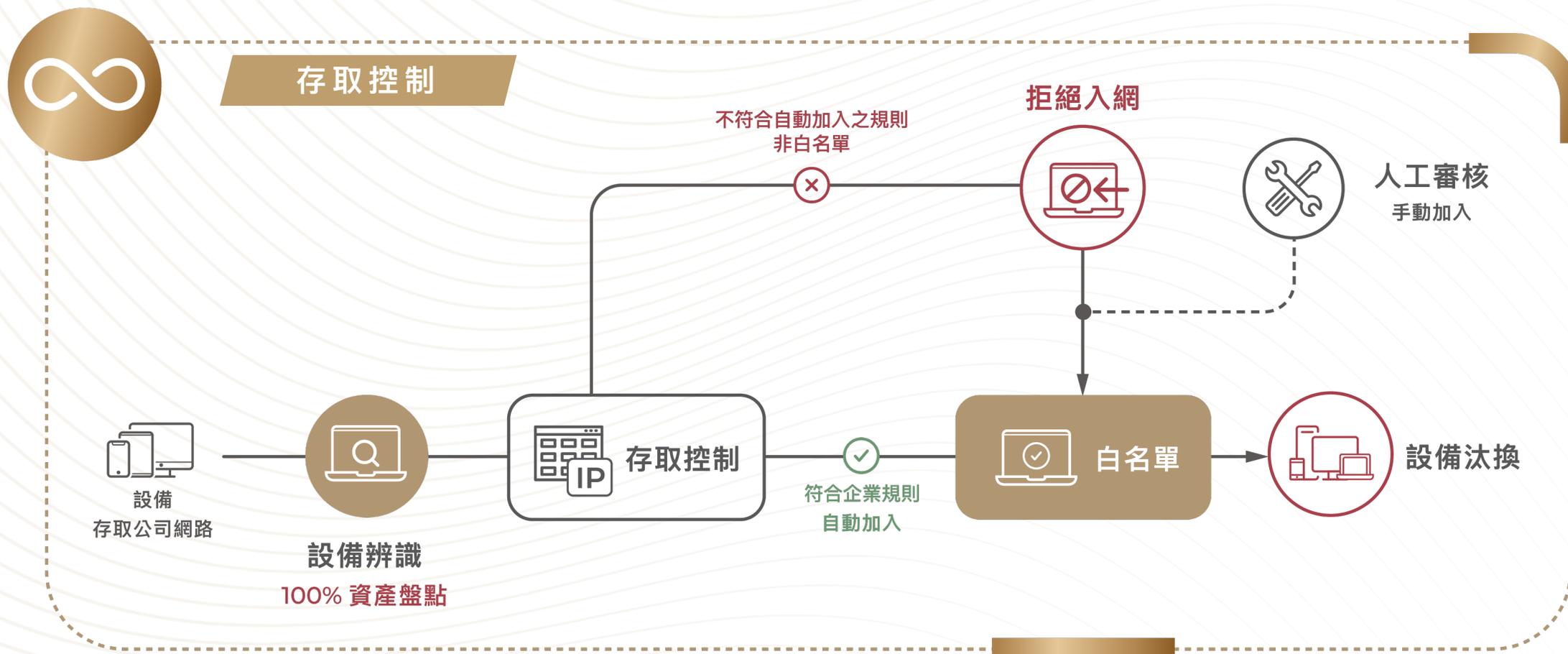
- 電腦設備
- Switch
- 伺服器
- 網路攝影機
- 防火牆
- 負載平衡器
- 路由器
- 儲存設備
- 影像工作站
- 傳真機
- 電話交換器
- 手持裝置
- 網路印表機
- 虛擬機
- 網路電話
- 集線器
- 電源及安全設備
- 錄音設備
- 視訊會議系統
- 門禁設備
- Bloomberg主機
- 數位錄影機

## 資產屬性辨識技術

- Nmap
- SNMP
- OUI
- WSUS
- DHCP 封包
- Server 網段
- AD Server
- WMI
- Plugin DB
- Uagent

# IP/MAC管理 確保入網設備皆安全符規

- 依需求制定接入規則 → 自動加白名單
- 不符規設備 → 產生事件並阻斷設備



# 快速鎖定威脅位址！



當環境設備發生安全威脅  
不易查找事件位置

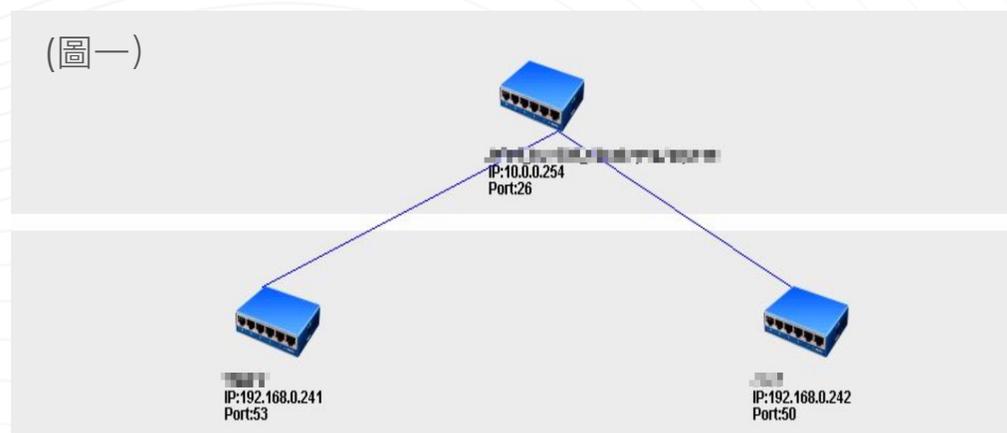
透過IP位址僅能得知設備虛擬位址，需要花費大量時間找尋設備實際位址。

## 導入IP位址解析模組

快速!! 定位IP實際位址

- 新增Collector，自動生成Switch拓樸圖 (圖一)
- 管理各Switch Port使用狀況
- 綁定MAC/Port，阻止其他設備使用該Switch Port
- 任何私接設備事件，系統自動告警跳出修正提示
- 透過單一Port多MAC查找，快速辨識IP實際位址

(圖一)

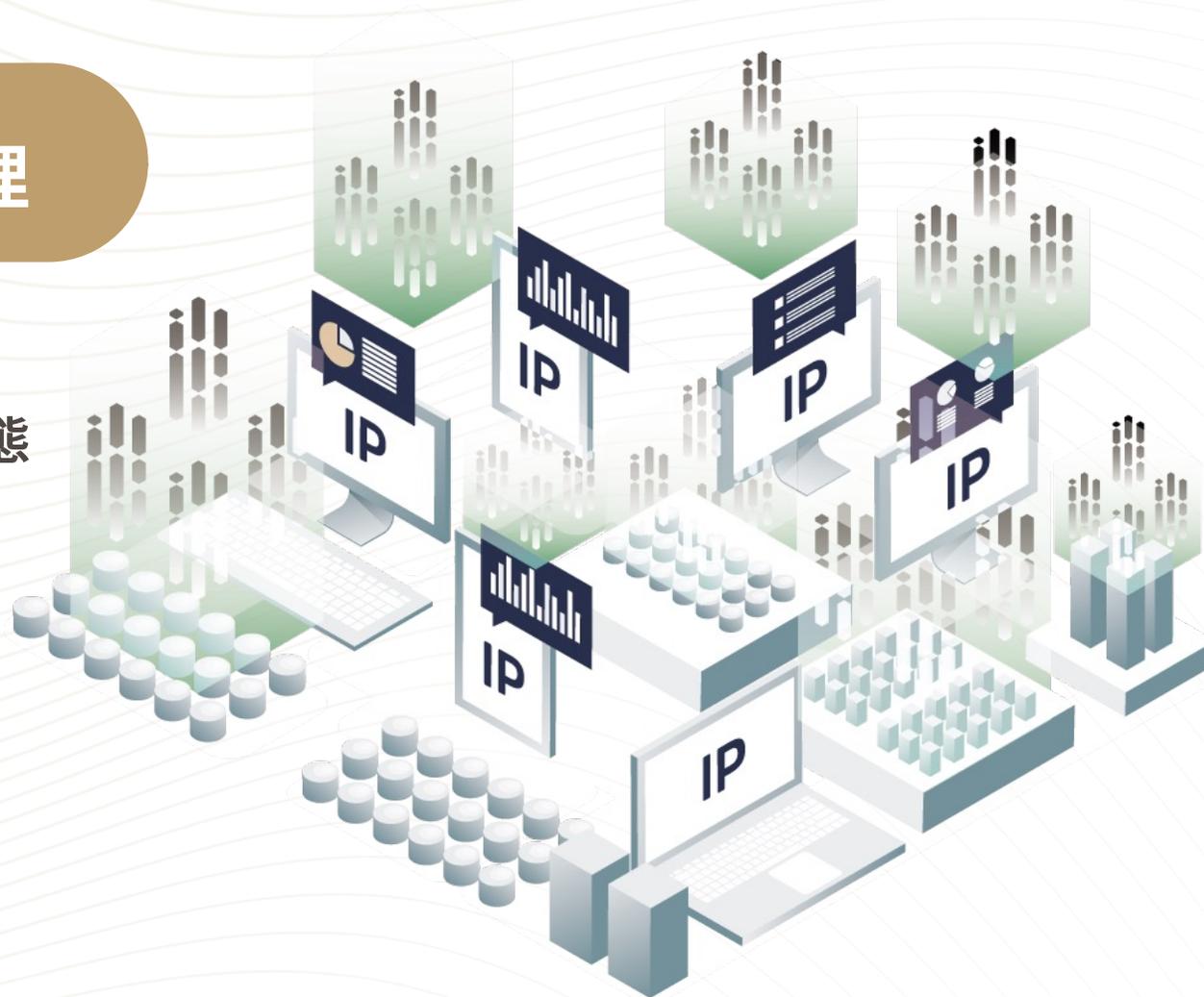


## IPAM IP位址管理

### 解決要點

#### 即時掌握內網所有IP動態

- 完善IP管理流程
- 掌握IP即時狀態
- 多種IP管理報表



# 完善IP管理、保護重要IP 確保產線不中斷

- IP申請
- 查詢可用IP
- IP預約
- IP發放
- IP回收
- IP保留
- IP綁定
- IP保護

申請類型

新設備申請  舊設備汰換

申請設備

資產屬性 -- ▾

選擇群組 ▾

MAC

電腦名稱

清除 新增

IP申請

IP管理

快速查詢

未發放IP  預約IP  白名單IP  不可用IP  外來設備

10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9
10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9	10.15.227.9

查詢可用IP

新增規則  刪除

IP保留規則

全選

10.0.0.0 ~ 10.0.0.255

10.0.10.0 ~ 10.0.10.255

10.0.20.0 ~ 10.0.20.255

10.0.30.0 ~ 10.0.30.255

IP保留

# IP 報表資訊 即時掌握所有連網設備動態

- IP 即時資訊
- VM 設備資訊
- 開關機報表
- IP 使用紀錄
- IP 配置列表

UPAS NETWORK OPERATIONS CENTER

NOC 即時資訊 報表管理 系統管理

IP即時資訊 全部設備 終端設備(Windows) 終端設備(macOS) 伺服器(Windows) 伺服器(Linux) 行動裝置(Android) 行動裝置(iOS)

Q 查詢

狀態: 全部 (選中) 上線中 離線中

收集來源: 全部 (選中) Sensor Gatherer

群組: -- (選中) 資產白名單 lancetest sensor\_0 10 20 server 分支白名單

其他查詢項目: 全部 (選中) IP使用區段 自訂IPv4區段 目前停機設備 24hr管停機設備 違規與否 白名單類型 IP類型 資產屬性 MAC位址 IP位址 電腦名稱 網卡廠牌 Switch IP

IP	MAC	名稱	種類	資產屬性	OS	設備不停機	白名單類型	IP類型	群組
10.0.0.0~10.0.0.255									
10.0.0.50	D8-5E-D3-4E-59-...		1	電腦裝置	Linux	不需設定	資產	S	sensor_0
10.0.0.101	00-F1-F3-A0-12-...	TOP-1T3QS78	1	電腦裝置	Windows 10	不需設定	資產	S	sensor_0
10.0.0.102	00-F1-F3-A0-12-3C	DESKTOP-IK1V9EH	1	電腦裝置	Windows 10	不需設定	資產	S	sensor_0
10.0.0.161	B4-2E-99-24-97-EF		1	電腦裝置	Linux	不需設定	未納入管理	S	
10.0.0.166	68-ED-A4-00-92-CD		1	電腦裝置	Linux	不需設定	未納入管理	S	
10.0.0.210	D8-5E-D3-4B-C9-11		1	電腦裝置	Linux	不需設定	未納入管理	S	
10.0.0.254	00-23-AC-3C-2F-4B			交換器		不需設定	MAC管制例外	S	sensor_0
10.0.10.0~10.0.10.255									
10.0.10.161	00-F1-F3-A0-12-06		1	電腦裝置	Linux	不需設定	未納入管理	S	
10.0.10.166	68-ED-A4-00-92-CD		1	電腦裝置	Linux	不需設定	未納入管理	S	
10.0.10.210	D8-5E-D3-4B-C9-11		1	電腦裝置	Linux	不需設定	未納入管理	S	
10.0.10.254	00-23-AC-3C-2F-4B			交換器		不需設定	MAC管制例外	S	10
10.0.20.0~10.0.20.255									
10.0.20.161	00-F1-F3-A0-11-EF		1	電腦裝置	Linux	不需設定	未納入管理	S	

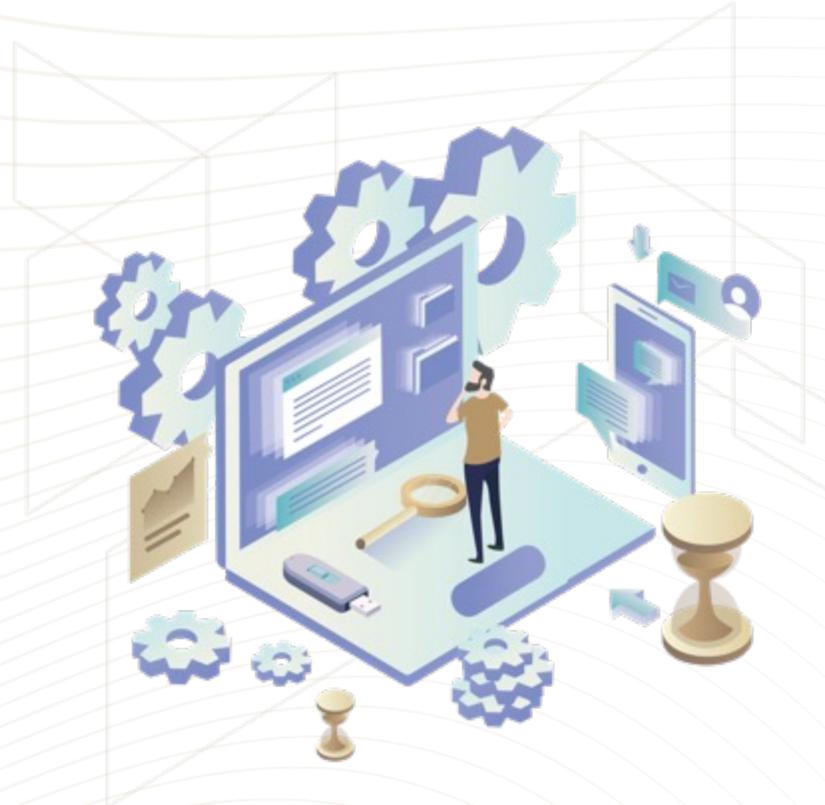
教育單位解決方案

## ITAM IT資產管理

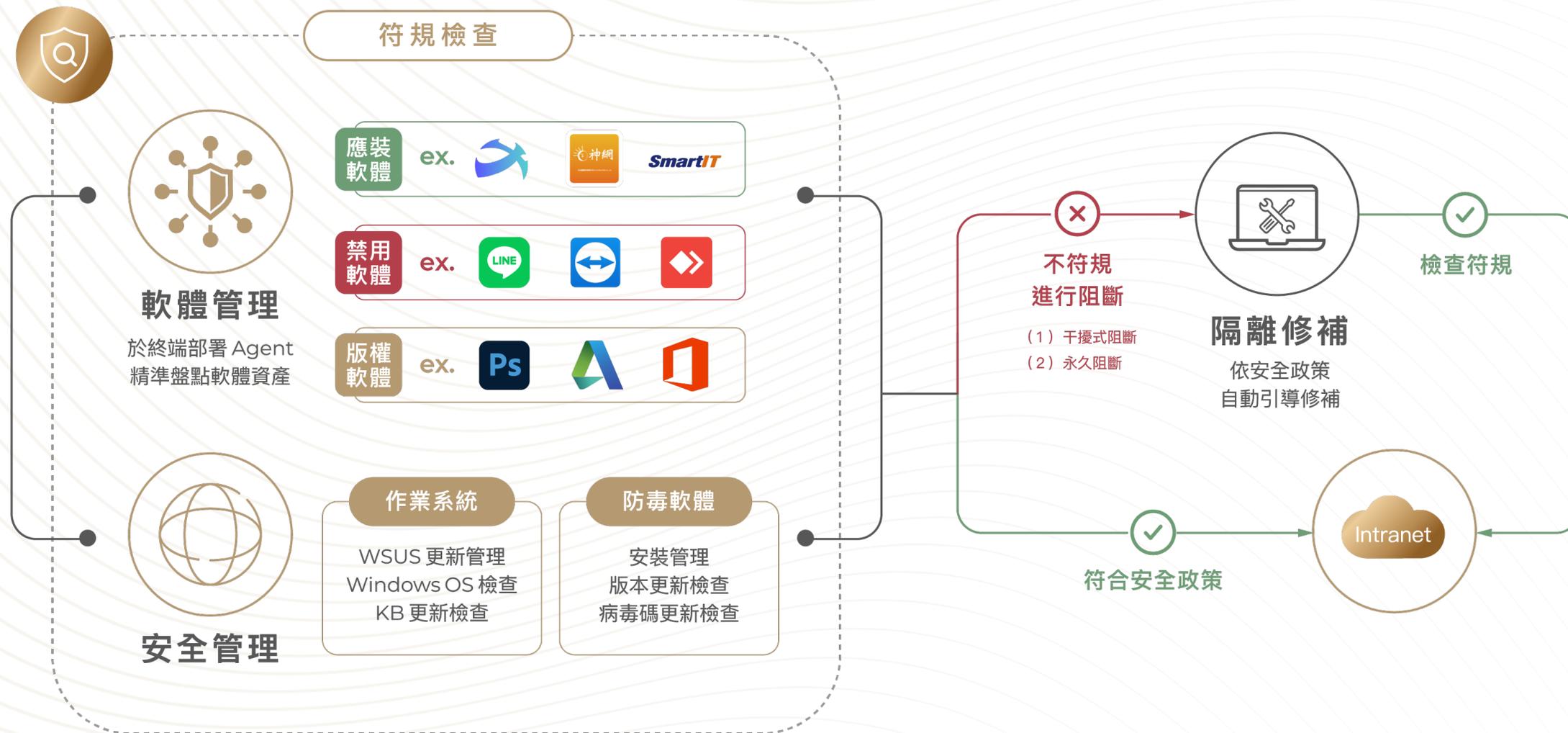
### 解決要點

#### 軟硬體資產管理 合規沒問題

- 補丁管理：終端設備軟體符規檢查
- 漏洞警報及通知系統：修補漏洞
- 遠程維運：檔案派送、遠端指令
- 限制USB及外接設備存取
- 零信任管理：設備鑑別、信任推斷



# 補丁管理 終端設備軟體符規檢查



# 遠程維運管理 檔案派送、遠端指令

## 資產偵測與管理



### 硬體資產

自動偵測 CPU、  
主機板、記憶體、  
SSD、HDD、顯示卡、  
網路卡等型號與規格



### 軟體資產

自動偵測設備安裝之  
軟體名稱、發行者、  
檔案大小、版本  
與安裝日期



## 終端設備遠程管理



### 遠端桌面

一鍵遠端桌面管理功  
能，方便管理者進行  
遠端維護支援作業



### 檔案派送

可將檔案派送至指定資料夾  
特定類型檔案可自動執行  
可下參數指令 (例：靜默安裝)



### 遠端指令

透過文字編輯介面可生成.bat、.sh檔  
派送予Windows、Linux設備  
可自動執行，完成後刪除



### 軟體移除

可刪除所有  
含特定軟體之設備中  
所安裝的該軟體



### 訊息推送

排程進行訊息發送  
可在時間內多次推送  
並保留推送紀錄



### 群組公告

針對群組進行訊息推送  
且時間內可多次發送  
同時保留推送紀錄



### 軟硬體異動紀錄

記錄個別設備  
之軟硬體異動  
(新增、刪除)



### 遠端維護申請

提供遠端報修功能  
可直接從客戶端  
線上申請報修

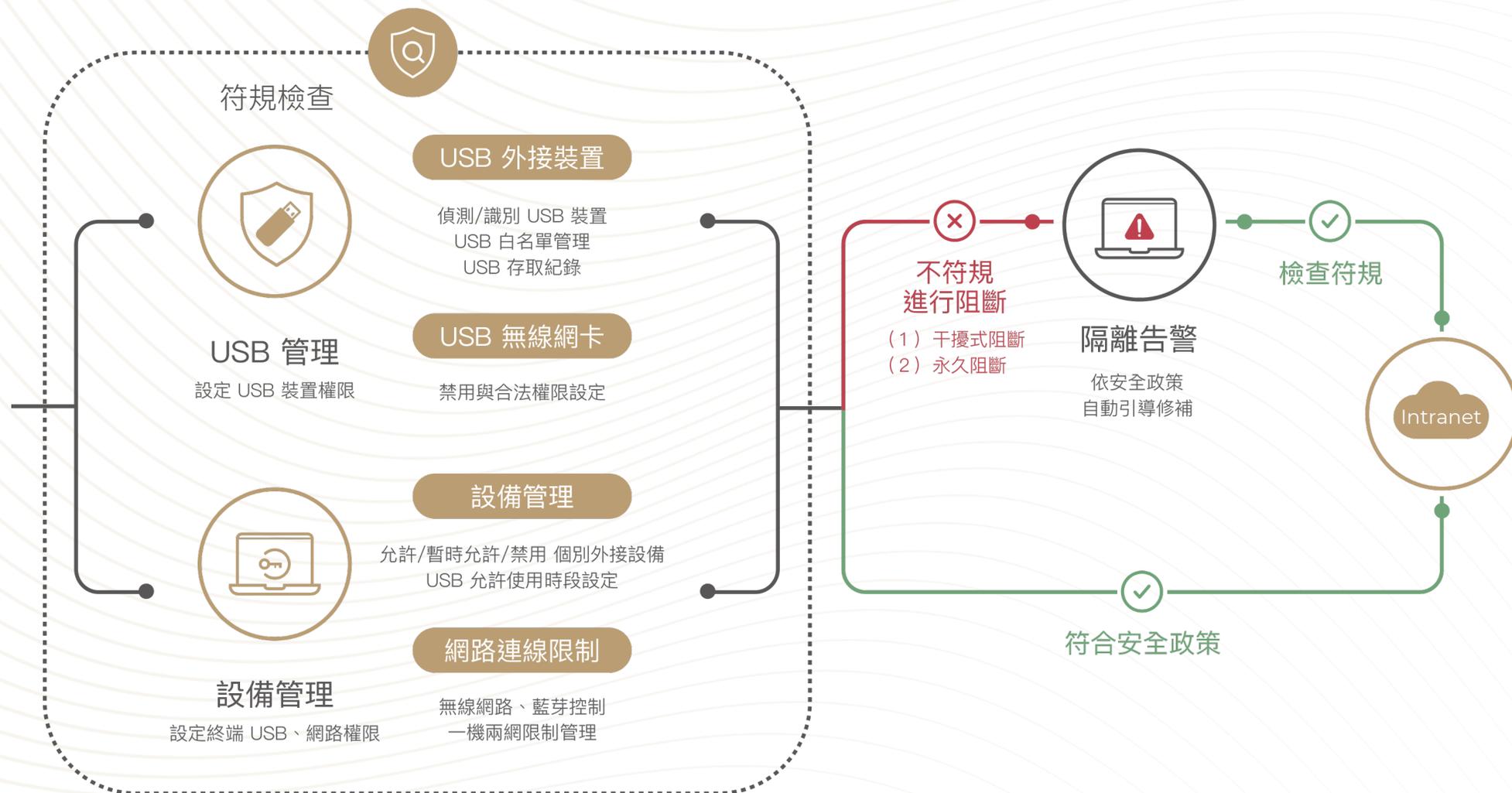


### 排程功能

ROM相關功能 (派送、移除、訊息)  
皆可排定執行時間  
並提供紀錄頁面



# 設備管理 管理外接設備及網路連線



# 協助公部門導入VANS

- 支援 VANS 1.0+2.0
- 支援NVD弱點資料庫比對
- CVE、CPE、終端設備多角度檢視，分權管理

**UPAS**  
ZERO TRUST ARCHITECTURE

VS

他牌資產管理軟體

## 終端設備盤點

免安裝agent  
掌握環境內連網設備

缺乏終端設備盤點措施  
透過AD主機派送agent  
無法確保設備部署成功

## 軟體資產管理

持續盤點軟體資產  
自動轉換CPE格式  
應裝、禁用、版權軟體管理

Agent部署率不足  
軟體資產缺乏控制性  
容易產生漏洞

## 軟體修補漏洞

一鍵上傳VANS弱點比對  
藉由重導頁面、Agent  
UI等進行弱點修補

無法管制和漏洞修補未安裝  
或更新agent終端設備，  
導致資安風險

# GPO支援TWGCB、組態一鍵還原

- GPO自動檢查套用
- GPO修補及還原
- GPO除錯工具
- GPO統計功能

The screenshot displays the UPAS (Network Operations Center) interface for GPO management. The navigation menu includes NOC, 即時資訊, 報表管理, and 系統管理. The current view is 'GPO管理 | GPO設定'. Under '自動檢查規則', 'Windows 7' is selected, and a '新增規則' button is visible. A list of rules is shown on the left, with '尚未設定' highlighted. The main area shows the configuration for 'DefaultGCB' under 'Windows 7'. It includes a search bar and a table of GPO settings.

檢視環境內安裝Agent設備GPO檢查結果，  
得出該設備的合規性

TWGCB-ID	規則類別	GPO名稱	檢查	修補	GPO設定值	備註
TWGCB-01-001-0001	Win7AccountPolicy	密碼最短使用期限	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> GCB原則 <input checked="" type="radio"/> 1	
TWGCB-01-001-0002	Win7AccountPolicy	密碼最長使用期限	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> GCB原則 <input checked="" type="radio"/> 90	

# UPAS ZTA

永不信任 · 持續驗證

---

**UPAS 單一平台  
全方位整合內網安全資訊**

# UPAS 全方位內網安全管理系統

省去多套軟體

單一平台 單一Agent

清楚掌握環境內所有連網設備狀態

有效管理內網安全

✓ 自動化管理

✓ 零信任架構

✓ 資料正確

✓ 高可視性



# 多樣化報表 協助稽查標準合規要求

## 事件紀錄

- 事件紀錄報表
- Sensor 事件報表
- 停機事件報表
- IP 衝突事件報表

## MAC 配置列表

- IP 配置列表

## 未發放IP

- 未發放IP資訊報表

## 資產清單

- 資產清單

## 開關機報表

- 已關機報表
- 未關機報表

## 白名單

- 白名單到期報表
- 新增白名單報表

## Agent 部署率

- Agent 部署率報表

## 系統操作記錄

- 系統操作記錄報表

## AD 管理

- 網域設備報表
- 電腦登入報表
- AD 帳號登入報表
- 共用資料夾報表
- SID 重複報表
- 本機登入報表
- 本機帳號報表

## GPO 部署率

- GPO 部署率報表

## VANS 報表

- CVE 弱點報表

## 補丁管理

- Window Patch 更新報表
- 防毒更新報表
- 應裝軟體報表
- 禁用軟體報表
- 版權軟體報表
- 軟體報表

## 安全整合管理

- Window Patch 更新報表
- 防毒更新報表
- 資產管理軟體報表

# UPAS

永不信任 · 持續驗證

---

## 導入效益

# 全方位內網安全管理解決方案



# 建立零信任架構

ZERO TRUST ARCHITECTURE

# UPAS

ZERO TRUST ARCHITECTURE

NAC | ITAM | IAM | IPAM | MDM

## 優倍司股份有限公司

台北市信義區基隆路二段51號樓之8  
高雄市前鎮區民權二路6號18樓之3



Website



Facebook



LINE



Linkedin



Medium