UPAS NOC
金融產業方案

實現真正安全的金融業營運環境

金融業發生資安事件將蒙受鉅額損失，根據iThome資料顯示發生內部資安事件的企業約二成五為金融產業，而內部攻擊中約六成是資料盜竊。隨著近年資安防護觀念的成熟，公部門對金融機構的檢核日益嚴謹，金融機構該如何有效因應呢？

從零打造金融內網安全

金融產業高度重視外部資安威脅的防禦，透過加強防火牆、防毒軟體等，防止惡意攻擊侵入企業網路，然而當上述所提的風險源於內部，常常有難以察覺的情形；內部威脅具有下列幾種先天優勢：

- 在企業日常作業的過程中，內部攻擊者已經取得合法的存取權限
- 內部攻擊者得知重要資料存放位置，也熟悉公司內部的防護機制

金融組織面對內部威脅時，若缺乏偵測或預防機制，危害便難以控制，唯有透過內外網聯合防禦，快速建立**「零信任」(Zero Trust)** 的資安管理架構：藉由提高的內網可視性及控制性，強化內外聯防的資安政策，完善金融網路環境。

UPAS 協助金融產業建立內網防護

01

特權帳號疏於管理，導致嚴重的資安危機

特權帳號擁有較高的存取權限，放任特權帳號的使用可能導致有心員工竊取資料，且無法追蹤其使用軌跡，甚至在資安事件發生後難以將其定罪；若駭客取得特權帳號，短時間就可能讓整個內網淪陷；如何管理特權帳號，是所有金融業者當務之急的工作。

02

如何滿足外來人員網路使用需求，同時保護重要主機？

金融業者大多有許多分行，分別採取不同網段進行管理，有些人員如稽核團隊，會自帶設備到各個分行作業，因此需要經常修改權限，才能讓這些差旅同仁有網路可用；這些修改都必須由管理人員手動操作，登入交換機內敲下指令，不僅增加管理人員負擔，且若因疏忽而忘記移除設備使用權限，將造成嚴重的資安漏洞。

金融業提供許多重要的線上服務，若提供服務的主機連線異常，便會造成嚴重後果，輕則服務中斷，重則導致金融資料遺失或被竄改，不僅會有相關法律問題，對企業形象也會造成影響。

03

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是在每台設備安裝Agent，以監控各項資訊，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設備的資產屬性、軟硬體狀態，不僅管理困難，也讓內網環境的安全性留下疑慮。

04

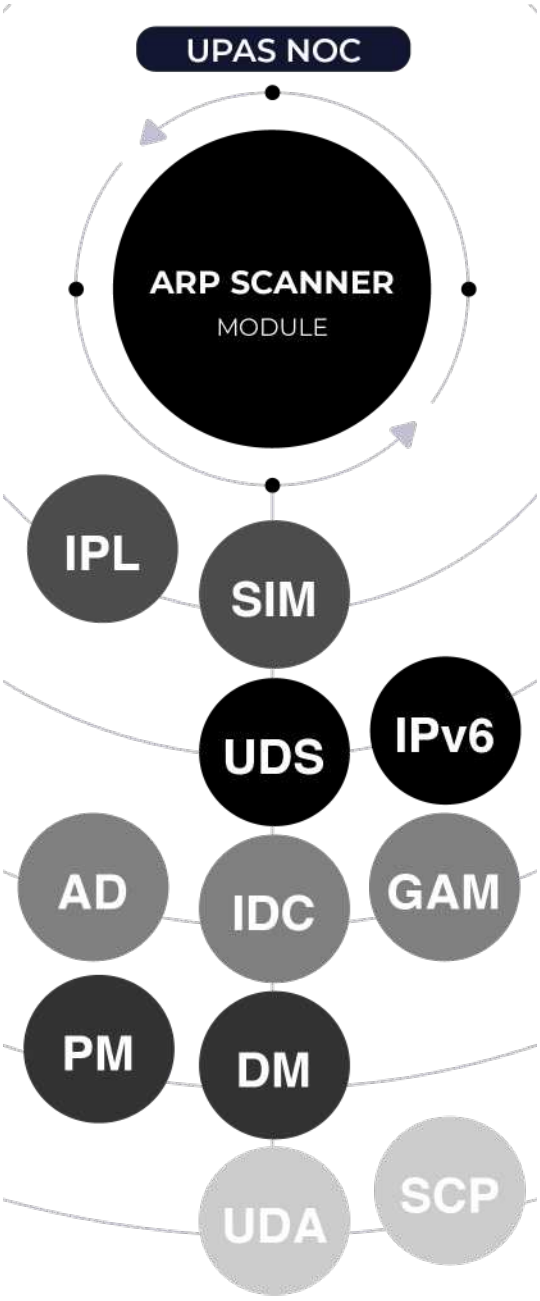
如何建置合格的資訊安全管理系統，以符合相關規範

資安事件發生的頻率逐年上升，法律對於資訊安全的要求也愈加嚴謹。除了規範個人資料的保護外，主管機關也不斷地增加內/外部稽核的內容，更加重視ISMS系統的建置；近年來有越來越多的金融企業通過ISO 27001的認證，便是基於ISO 27001對於資訊安全系統的建置有完善的建議。通過ISO27001認證，對金融企業來說除了可以降低資安事件的發生機率之外，對外也能提升客戶信心、有效提升企業對外的形象。

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。

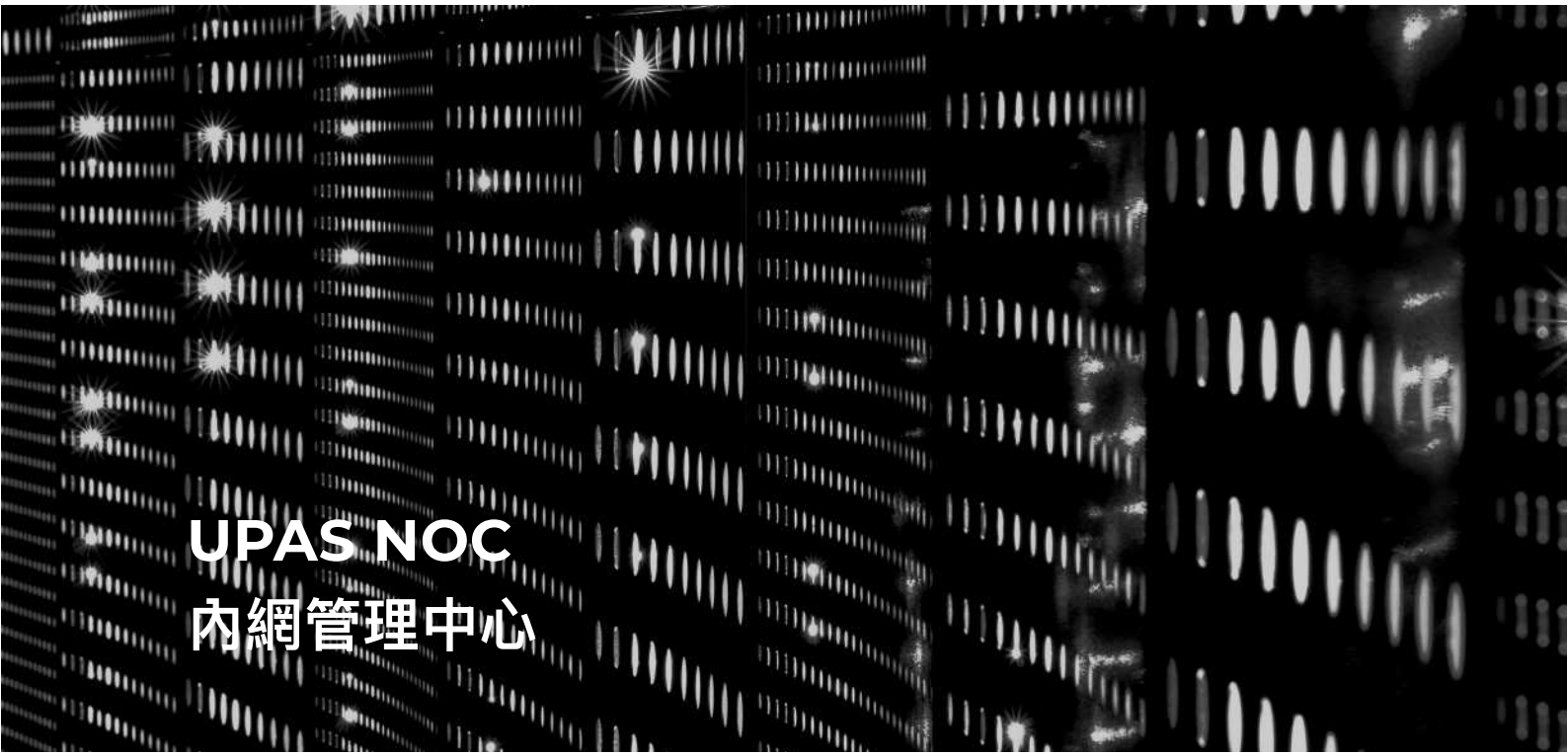
採用Agentless方案，適合各種網路環境

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

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

透過在終端部屬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

01

AD帳號的全面管理，避免特權帳號的濫用

UPAS NOC 提供AD進階管理方案解決特權帳號的使用問題。過去AD帳號登入電腦，僅會針對帳號本身權限而非使用者進行核對。若企業無監督會對特權帳號進行管理，則非法活動便可以透過獲得帳號權限進而對企業進行攻擊。UPAS NOC 透過以下幾種方法進行AD帳號管理：

1. 可強制要求電腦設備必須使用特定AD帳號登入，若偵測到私退AD網域或未加入網域設備，則可自動阻斷並要求其加入網域。

2.避免員工任意退出AD網域，在無法監管的情況下使用電腦設備。

3. AD帳號與電腦名稱綁定，非指定帳號無法登入。

4. 整合員工資訊，提供「加入/退出」AD網域、「登入/登出」AD帳號的日期、時間和次數。

02

系統化管理外部人員，提供完整IP保護措施

面對稽核團隊的連網需求，UPAS NOC在不影響公司其他設備的連線之下，提供了下列解決方案：

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. UPAS NOC可對連網設備設定卸離時間，到期時自動移除設備連網能力，減少人工操作失誤的事件發生。

3. 提供IP保護功能，透過多種IP綁定機制，避免因IP衝突、外部搶IP等事件導致企業重要主機連線中斷、服務停止。

03

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。

04

與ISO 27001高度合適性，降低建置成本

1. UPAS NOC符合多項ISO 27001控制項的要求，減少通過驗證時所需花費的成本。詳細對應項請參照ISO 27001法規對照手冊。

2. 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。

協助金融產業
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