Openfind 零信任 (ZTA)
解決方案

網擎資訊

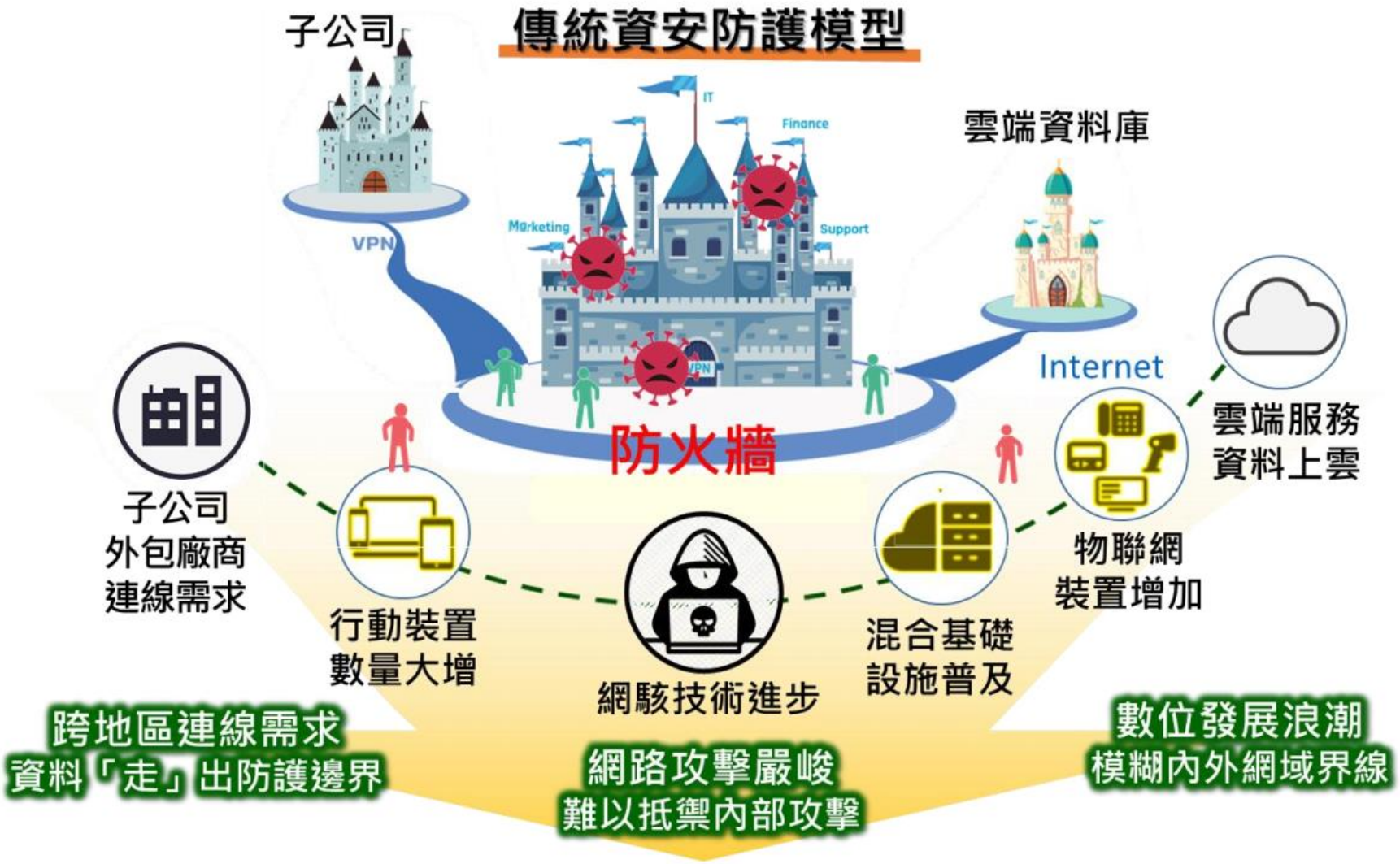
Openfind

首先，什麼是零信任？

從不信任，總是驗證

即使裝置已經連接到經許可的網路(通常是內部網路)
並且之前已通過驗證，仍不應預設信任裝置。

為什麼我們需要零信任架構？



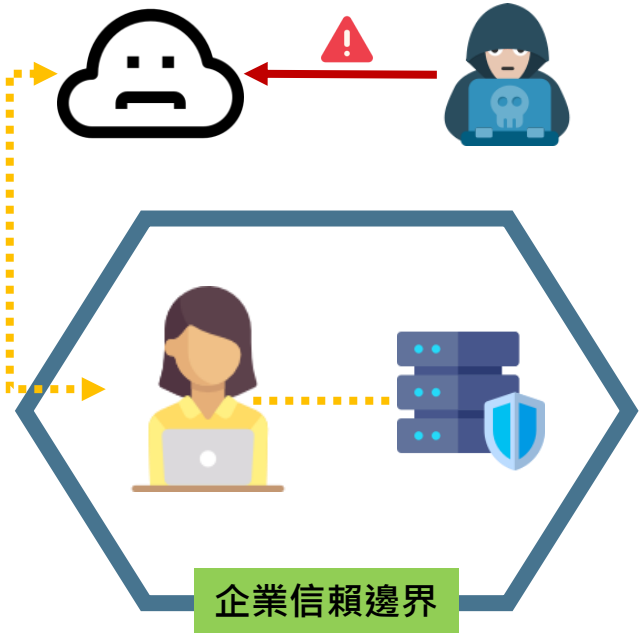
資料來源：行政院國家資通安全會報技術服務中心

為什麼我們需要零信任架構？

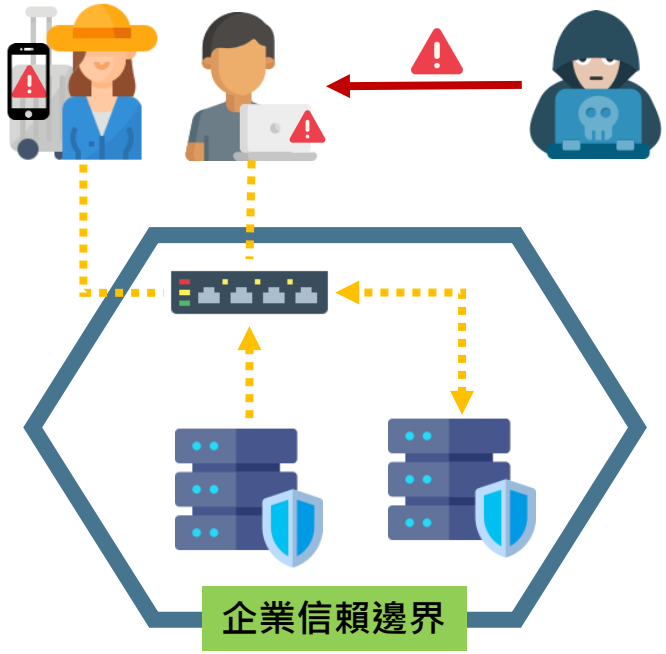
隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型 (常見的內外網隔離) 已現資安窘境，難以滿足新形態工作需求。

存取設備多元化 BYOD

使用非企業指定之雲端服務



居家、遠距辦公

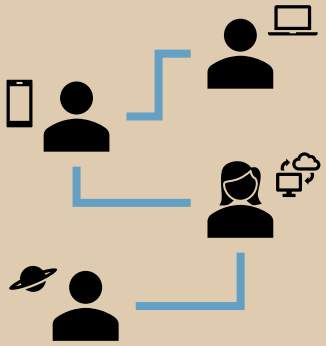


零信任的主要精神

- ✓ 從保護網路存取 → 改為聚焦 **保護資料/應用存取**
- ✓ 不再有具體邊界的概念，因為使用者/設備與資料/應用隨處都在
- ✓ 任何資料存取都要「**從不信任**」且「**總是驗證**」

以前，
有護城河
守住城河就好

導入
零信任



現在，沒有邊界
從不信任，總是驗證

NIST 零信任推動建議

- 2020 年美國國家標準技術研究院 (NIST) 正式頒布標準文件 SP800-207 零信任架構 (Zero Trust Architecture, ZTA)，成為各界採用基礎，其說明：
  - 零信任網路以決策引擎為核心，包含**「身分鑑別」**、**「設備鑑別」**及**「信任推斷」** 3 大關鍵技術

實施零信任會是**一段過程**，而不是一次大規模替換基礎架構，且與傳統模式會同時混合運作。

NIST 零信任3 大關鍵技術

① 身分鑑別

多因子身分鑑別
與鑑別聲明

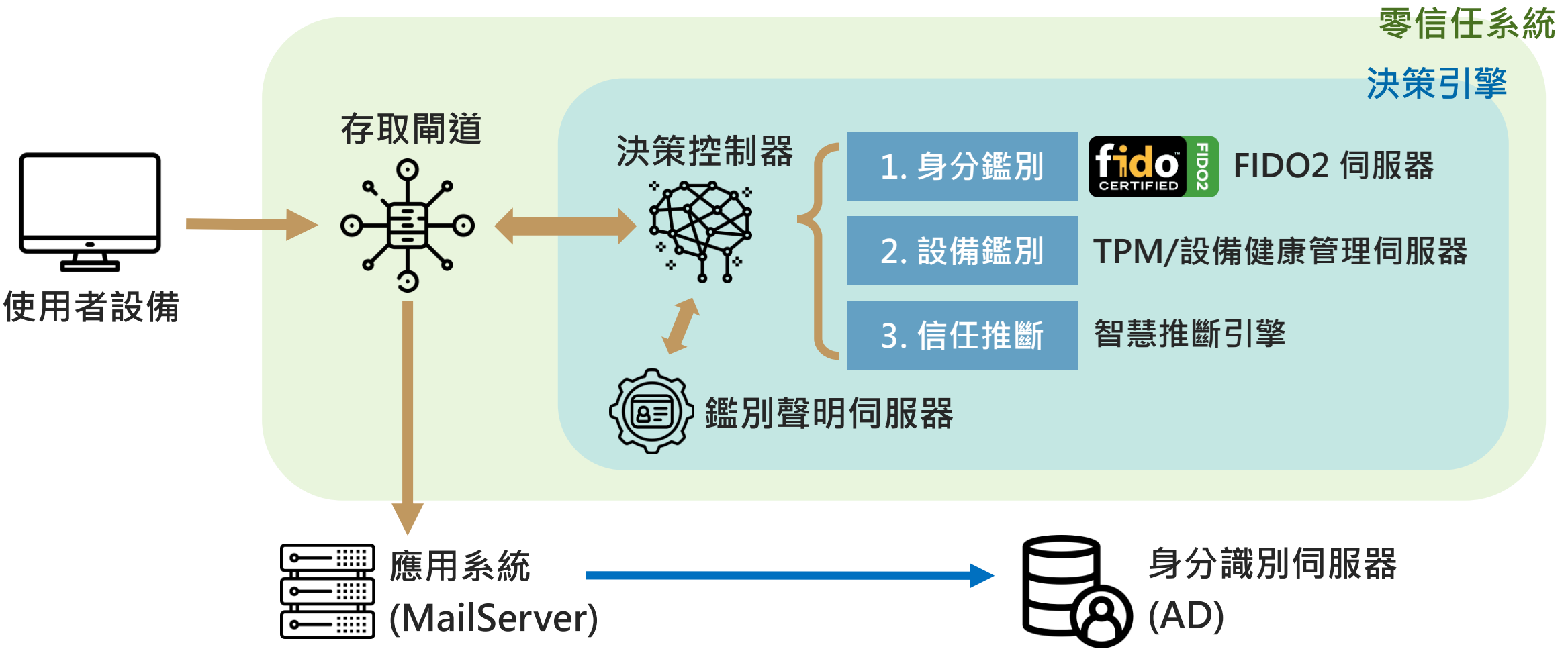
② 設備鑑別

設備鑑別
與設備健康管理

③ 信任推斷

使用者情境
信任推斷機制

台灣政府推廣之零信任架構



整合支援 零信任網路身分鑑別系統

- 配合政府推動期程，整合「零信任網路身分鑑別系統」

  身分鑑別 (登入 / 驗證鑑別聲明)

  信任推斷 (權限檢查)

  行為回饋 (視系統要求而定)

政府零信任網路身分鑑別功能符合性驗證通過名單 (更新至 112.1.30)

項次	廠商名稱	產品名稱
1.	全景軟體股份有限公司	零信任網路身分鑑別系統
2.	安碁 powered by AuthenTrend	零信任網路身分鑑別系統
3.	臺灣網路認證股份有限公司	零信任網路身分鑑別系統
4.	來毅數位科技股份有限公司	Keypasco 零信任網路身分鑑別系統
5.	偉康科技股份有限公司	零信任網路身分鑑別系統
6.	中華資安國際股份有限公司	中華資安國際 ZTNA

Openfind 已有部署經驗，可彈性在地對應、快速整合！

政府機關 x 零信任

政府機關為什麼需要零信任？

全球政經趨勢

- **美國國防部**
  計畫於2027年完成零信任部署
- **日本數位廳**
  去年6月30日針對政府資訊系統，發布零信任架構適用方針
- **新加坡**
  前年10月發布「網路安全戰略2021」，指出零信任策略是未來五年發展重點

資通法 & 政策指引

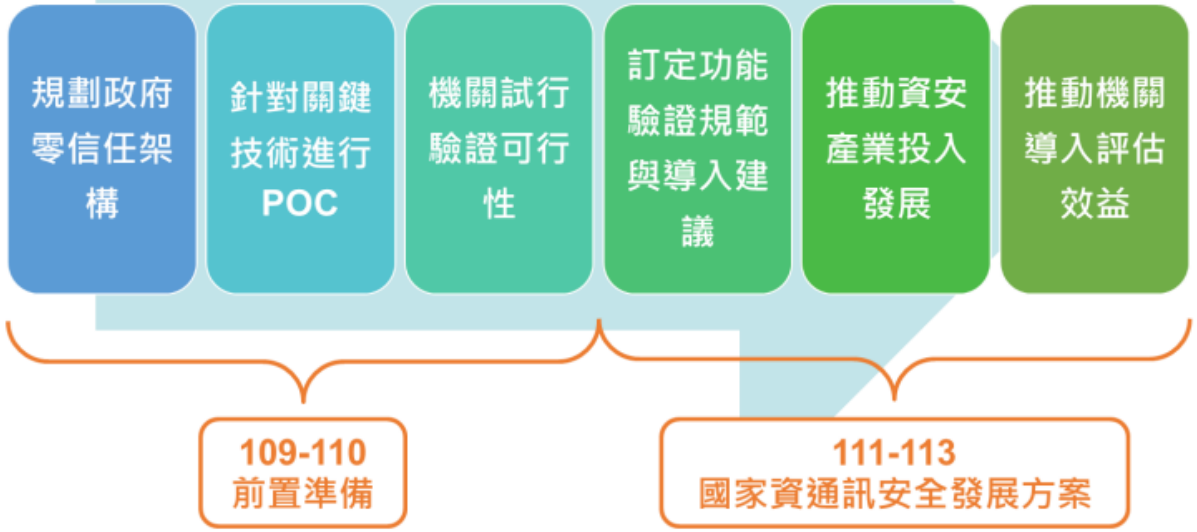
- **資通法**明確規定
- **數位發展部**部長唐鳳近期亦表示，推動零信任架構為**今年 9 大施政重點之一**

防範威脅及攻擊

- 針對政府機構的**駭客攻擊**、**社交工程**日漸嚴重
- 政府機構的**敏感數據資料**有可能因此被盜取
- 提高安全性，應對威脅，確保政府機構的**運營和服務的持續性**

台灣政府 零信任 推動規劃

導入零信任架構為政府強化資安防護之既定政策，數位發展部部長唐鳳近期亦表示，推動零信任架構為今年 9 大施政重點之一，1 年內 A 級機關導入「零信任」架構



資料來源：行政院國家資通安全會報技術服務中心

台灣政府 零信任 推動規劃

- 依據「**國家資通安全發展方案**(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任網路資安防護環境，推動政府機關導入零信任網路，完善政府網際服務網防禦深廣度。

- 政府在 2023 年明確指引機關、企業須推動零信任網路架構，資通安全責任等級的 **A 級公務機關**優先導入，並預計在三年內，分階段逐年導入零信任網路的 3 大核心機制：**身分鑑別**、**設備鑑別**，以及**信任推斷**。因此，2023 年的重點，無疑將是 **導入身分鑑別**。

身分鑑別

- NIST SP 800-63-3依註冊、鑑別及聲明 3 階段將身分鑑別分為身分保證等級(IAL)、鑑別保證等級(AAL)及聯邦保證等級(FAL)3個類別，各類別定義3個等級
- 政府機關導入零信任網路應至少達到 IAL2/AAL3/FAL2 等級

	身分保證等級(IAL) Identity Assurance Level	鑑別保證等級(AAL) Authenticator Assurance Level	聯邦保證等級(FAL) Federation Assurance Level
說明	使用者用來證明自己身分之強度	鑑別過程之防護強度	身分鑑別者(IdP)傳遞給服務提供者(RP)之身分鑑別聲明(Assertion)之防護強度
等級1	自己宣稱之身分便具有效力	至少需要單因子身分鑑別	身分鑑別聲明須經過IdP簽章
等級2	需親自提供證據進行身分證明	• 需要2種不同之鑑別因子 • 鑑別過程之通訊，需使用加密技術	身分鑑別聲明須簽章與加密
等級3	需在監督下親自提供證據與生物特徵進行身分證明	• 透過密鑰(key)進行鑑別 • 需要硬體加密鑑別器	身分鑑別聲明須簽章與加密，且使用者應向RP證明，擁有與身分鑑別聲明對應之密鑰


金融業 x 零信任

金融單位為什麼需要零信任？

疫後轉型、加速資安風險

- **資安事件頻傳**，金融機構仍是攻擊者頭號目標
- 疫情調整營運作業模式，出現**利用疫情**發動的攻擊
  如偽冒客戶聯繫居家辦公同仁進行詐騙轉帳等
- **數位轉型**，也讓金融面臨更嚴峻的資安風險，如App、雲端服務、開放銀行、Open API、eKYC等新興金融數位應用

金融資安行動方案 2.0

- 金管會於2022年12月27日發表**金融資安行動方案2.0**
- 延續1.0版四大策略外，另增加了14項精進措施，包含鼓勵金融機構擁抱**零信任架構**，強化核心資料保全。

金融資安行動方案 2.0

- 金管會於2022年12月27日發表 **金融資安行動方案2.0**
- 金融資安行動方案2.0版以擴大適用、落實與深化、鼓勵前瞻為持續精進方向，訂有40項措施，**其中新增資安措施計12項**、擴大適用範圍計5項、持續性措施計23項。
- 目前零信任網路是**採鼓勵性質**，不會有裁罰，且先從金融機構開始，尚不擴及上市櫃公司。

金融資安行動方案 2.0

鼓勵零信任網路部署，強化連線驗證與授權管控：

規劃鼓勵金融機構逐步導入**身分鑑別**、**設備鑑別**及**信任推斷**等零信任網路 3 大核心機制，搭配網路及資源的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。

金融資安行動方案2.0 - 精進重點

項次	推動措施	擴大適用	落實深化	鼓勵前瞻
1	擴大資安長設置，定期召開**資安長聯繫會議**	V	V	◎
2	因應數位轉型及及網路服務開放，增修訂自律規範		V	
3	深化**核心資料保全**及營運持續演練		V	V
4	擴大導入國際資安管理標準及建置資安監控機制	V	V	
5	鼓勵資安監控與防護之**有效性評估**		V	V
6	鼓勵**零信任網路部署**，強化連線驗證與授權管控			V
7	鼓勵配置多元專長資安人才，擴大**攻防演訓**量能		V	V
8	提升資安情資分享動能，增進資安聯防運作效能		V	
9	辦理資安攻防演練，規劃**重大資安事件支援演訓**		V	

Openfind 的零信任對應功能

① 身分鑑別

- 鑑別聲明 (session-key) 驗證
- FIDO 整合

② 設備鑑別

- 信任裝置
- 裝置綁定

③ 信任推斷

- 異常登入 IP 警示
- 異常行為分析
  登入 IP 限制
- Session 綁 IP or Browser
- MailMDR 情資
- 等級權限設定、管理權限設定

Openfind 的零信任「3A」

認證
Authentication

整合FIDO及生物辨識，並與零信任認證廠商進行整合

授權
Authorization

則透過產品細緻的權限設計，達到最小範圍的存取與控制

紀錄
Accounting

提供多樣的使用及管理紀錄，清楚留下行為軌跡

零信任架構 + 3A 安全防護

為什麼 Openfind 可以符合零信任架構？

整合經驗多！
在地法規對應、彈性整合

1. 配合法規推動期程，整合「零信任網路身分鑑別系統」
2. 系統功能可符合零信任網路的 3 大核心機制精神

身分鑑別 **設備鑑別** **信任推斷**

3. Openfind 3A 安全防護，安全機制從內到外滴水不漏！

認證	授權	紀錄
Authentication	Authorization	Accounting

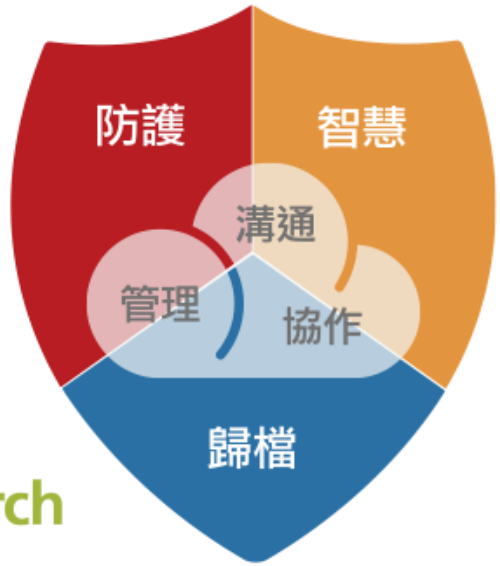
Thank you

MailGates
郵件防護系統

Secure
雲端資安服務

MailAudit
郵件稽核系統

Mail2000
電子郵件系統



MailCloud
企業雲端服務

Pro
SecuShare
企業雲端儲存平台

MailCloud Messenger
企業溝通平台

Enterprise Search
企業搜尋探勘系統

MailBase
郵件歸檔系統

Email : info@openfind.com URL : www.openfind.com

Contact
聯絡我們

網擎資訊
info@openfind.com
www.openfind.com