



推動證券商導入金融零信任說明會

—網路安全

資誠智能風險諮詢管理有限公司
2025. 7

Agenda

項次	內容
1	實作參考原則分級解析-網路安全
2	零信任架構導入常見問題-網路安全



實作參考原則分級解析- 網路安全

零信任架構實作參考原則分級-5大支柱

Identity



身分

是指唯一描述特定使用者或實體（包括非個人實體）的屬性或屬性集。

Devices



設備

是指任何可連接到網路的資產（包括其硬體、軟體、韌體等），包括伺服器、桌上型電腦和筆記型電腦、印表機、行動電話、物聯網設備、網路設備等。

Networks



網路

是指開放的通訊介質，包括典型通道（例如機構內部網路、無線網路），以及其他潛在通道（例如用於蜂巢式網路和應用程式層級通道）。

Applications



應用程式

包括在本機、行動裝置和雲端環境中執行的資通系統、程式和服務。

Data



資料

包括正在訪問或曾經訪問的設備、網路、應用程式、資料庫、基礎設施和備份（包括本機和虛擬環境）中的所有結構化和非結構化檔案和片段。

金融業導入零信任架構參考指引-實作參考原則

等級 I

支柱	功能
身分	身分認證
	身分互通
設備	設備合規
	供應鏈風險
網路	網路區隔
	流量加密
應用程式	存取授權
資料	外洩防護
	資料分類
	資料可用性
	資料加密

等級 II

支柱	功能
身分	身分認證
	權限存取
設備	設備合規
	資源存取
網路	網路區隔
	流量管理
應用程式	存取授權
	程式安全
資料	程式部署
	資料存取

等級 III

支柱	功能
身分	可視性分析
設備	威脅防護
	可視性分析
網路	網路韌性
	可視性分析
應用程式	威脅防護
	可視性分析
資料	外洩防護
	可視性分析

等級 IV

支柱	功能
身分	自動化治理
設備	自動化治理
網路	自動化治理
應用程式	自動化治理
資料	自動化治理

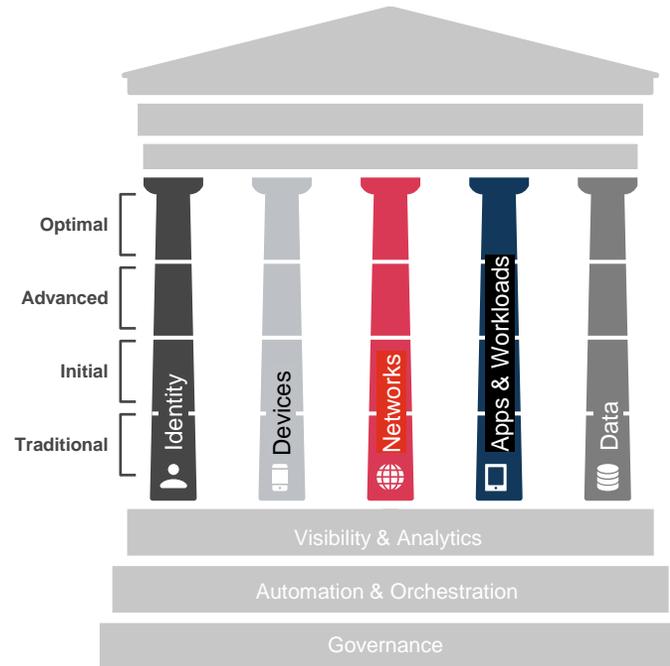
金融業導入零信任架構參考指引-實作參考原則

1 身分(7)

- 身分認證 (I*1、II*1)
- 身分互通 (I*2)
- 權限存取 (II*1)
- 可視性分析 (III*1)
- 自動化治理 (IV*1)

2 設備(7)

- 設備合規 (I*1、II*1)
- 供應鏈風險 (I*1)
- 資源存取 (II*1)
- 威脅防護 (III*1)
- 可視化分析 (III*1)
- 自動化治理 (IV*1)



3 網路(7)

- 網路區隔 (I*1、II*1)
- 流量管理 (II*1)
- 流量加密 (I*1)
- 網路韌性 (III*1)
- 可視性分析 (III*1)
- 自動化治理 (IV*1)

4 資料(8)

- 外洩防護 (I*1、III*1)
- 資料分類 (I*1)
- 資料可用性 (I*1)
- 資料存取 (II*1)
- 資料加密 (I*1)
- 可視化分析 (III*1)
- 自動化治理 (IV*1)

5 應用程式(7)

- 存取授權 (I*1、II*1)
- 威脅防護 (III*1)
- 程式安全 (II*1)
- 程式部署 (II*1)
- 可視化分析 (III*1)
- 自動化治理 (IV*1)



3. 網路

網路被切分為最小的區段，防止未授權的存取與橫向擴散

網路被切分為最小的區段，防止未授權的存取與橫向擴散

I 靜態指標

- **3-1 網路區隔：**具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。
- **3-4 流量加密：**於資源存取路徑進行資料傳輸加密(如 https 等加密協定)。

II 動態指標

- **3-2 網路區隔：**具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表。
- **3-3 流量管理：**呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。

III 即時指標

- **3-5 網路韌性：**對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。
- **3-6 可視性分析：**整合事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，並與資安監控機制整合，針對入侵指標或攻擊行為樣態進行即時的判斷與應處。

IV 整合指標

- **3-7 自動化治理：**具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。

1. 身分

2. 設備

3. 網路

4. 應用程式

5. 資料

3-1 網路區隔

I 靜態指標

具網段隔離機制，採**最小需求原則**限制存取資源之網路連線，並「**得**」限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。

3-2 網路區隔

II 動態指標

具**軟體定義網路(SDN)**或**網路微分段(Micro-Segmentation)**機制，可以依據業務需求或**動態**屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以**個別主機或個別系統**為獨立網路區隔，縮小攻擊表面。

金融業導入零信任架構參考指引-實作參考原則

	網路分段	網路微分段	軟體定義網路(SDN)
定義	將網路分成 多個獨立區域 (網段)，控制每個區域的連線。	將網路劃分為 更小的隔離區塊 (如個別主機、系統)，每個區域擁有 獨立的安全規則 ，限制彼此之間的連線。	使用軟體來 動態 管理網路設定，根據業務需求 調整 流量路徑。
指標	I 靜態指標	II 動態指標	II 動態指標
主要目的	限制網路流量，保護不同網段間的資料安全	限制感染範圍， 防止橫向擴散	提供靈活的網路配置，依需求動態調整網路配置
應用範例	辦公區域網路(LAN)劃分成內部和外部網路	金融機構將各項業務分區，防止攻擊傳播	大型企業動態控制各部門的網路流量與安全策略
技術機制	使用VLAN或傳統防火牆進行子網隔離	透過微分段技術(可在網路分段原架構下)，建立更細微隔離	使用SDN控制器管理，控制網路設備
安全優勢	將網段內部流量限制到 最小需求 ，降低攻擊面	單一主機受到攻擊時，其他主機不易受影響，減少橫向移動風險	自動化管理，提供快速配置調整能力
適用場域	所有企業	安全需求高的環境，如 金融 、醫療等敏感資料系統	需要靈活配置、集中控制動態網路的企業

金融業導入零信任架構參考指引-問答



Question:

零信任在實施網路區隔時，建議採用什麼原則來限制網路連線？

選項A

最高效能原則



不適用

選項B

最大連接數原則



不適用

選項C

最小需求原則



依需求限制存取資源之網路連線

金融業導入零信任架構參考指引-問答



Question:

根據零信任參考指引，為防止攻擊橫向擴散，建議採用什麼技術？

選項A

強化VPN通道



不適用

選項B

隨機調整內部IP



不適用

選項C

採微分段與網路區隔



將主機或個別系統為獨立網路區，縮小攻擊表面

金融業導入零信任架構參考指引-問答



Question:

零信任網路區隔強調「軟體定義網路」的主要目的為？

選項A

緩解網管人力負擔



不適用

選項B

動態調整網路邊界



可依需求或動態屬性變更路網拓樸

選項C

加速網路連線速度



不適用

3-3 流量管理

呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。

I 靜態指標

II 動態指標

III 即時指標

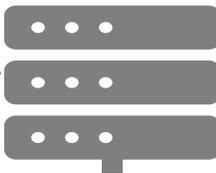
IV 整合指標

相依性關係
示意圖

DataBase



System



Device



流量監控

- 近期流量趨勢圖
- 異常警示
- 應對措施(限速或隔離)
- 事件紀錄

- ! 異常嘗試行為
- ! 高流量警示
- ! 敏感資料訪問
- ! 訪問頻率過高

單一設備檢視

- 設備名稱、IP位置
- 裝置狀態(上線、離線)
- 連接的系統與伺服器
- 防火牆設定

金融業導入零信任架構參考指引-問答



Question:

零信任流量管理對設備的狀態監控，建議應包含哪些面向？

選項A

監控單一設備



不適用

選項B

監控網路狀態、相關系統



不適用

選項C

監控設備及相關系統、端點與網路



可監控流量之網路拓樸

金融業導入零信任架構參考指引-問答



Question:

根據網路流量管理原則，以下哪項功能是正確的？

選項A

監控端點設備，不考慮系統間的連接



不適用

選項B

監控網路流量，但無法處理異常



不適用

選項C

可以從單一設備延伸查看相關系統、端點與網路的狀態，並具備異常監控及應處機制



適用

3-4 流量加密

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標



於資源存取路徑之資料傳輸加密(如採 https 等加密協定)。

加密流量概念：

- 保密性：確保資料僅供授權方存取。
- 完整性：防止資料被修改。

兩種加密方式：

- 通道加密：針對傳送的路徑。(Https/VPN/FTPS/SSH...)
- 訊息加密：端到端訊息加密。(E2E Encryption/電文加密 ...)

金融業導入零信任架構參考指引-問答



Question:

零信任在實施流量加密時，建議採用何種方式？

選項A

資料只允許在VPN內傳送



不適用

選項B

傳輸過程採用HTTPS或其他加密協定



適用

3-5 網路韌性

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。

NDR(網路偵測回應)

- **功能**：即時監控網路和設備間流量，偵測並回應潛在威脅指標(IOC)
- **操作**：發現異常活動時，NDR自動
 - (1) 發出告警
 - (2) 發出事件單
 - (3) 調整網路防護
 - (4) 消除橫向移動

名詞解釋

- IOC(威脅指標)：潛在威脅的資料點，如可疑IP地址、異常文件、可疑URL



Question:

根據網路韌性管理原則，以下哪項不屬於動態調整網路設定的方式？

選項A

切換備援路由



適用

選項B

調整資源配置



適用

選項C

調整網路防護邊界即時隔離



適用

3-6 可視性分析

整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook等)。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

1. 集中收容日誌資料至同一平台(如SIEM)
 - 確保安全事件有完整、可查的紀錄
2. 異常偵測與警告機制
 - 定期審查並監控日誌，偵測異常行為
 - 發現可疑活動，立刻觸發警示採取應對
3. 資安監控與即時回應
 - 與資安監控中心(SOC)整合，快速分析入侵指標(IOC)或攻擊行為模式(Mitre ATT&CK TTP)
 - 根據事件自動執行回應動作(如生成事件單或啟動SOAR Playbook)

名詞解釋

- **SIEM**：安全資訊事件管理系統，集中收集和分析資安日誌，即時偵測異常，協助快速應對安全威脅。
- **Mitre ATT&CK TTP**：Mitre建立的框架，描述攻擊的戰術、技術、程序(TTP)，幫助團隊識別攻擊行為。
- **SOAR Playbook**：敘述如何驗證及回應安全事件的文件。若SOAR(資安協作自動化應變系統)失效，可作為人工處理的備案。

3-7 自動化治理

可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

階段	說明
手動管理	•手動進行網路環境設置，定期整合政策及情勢變化。
部分自動	•使用部分自動化管理，根據政策與監控資料進行設置。
全面自動	•自動化變更管理方法，自動化所有網路環境配置；並自動評估風險，執行政策和安全措施。
最佳化	•網路與環境通過程式碼定義，並由自動化變更管理工具管理，實現全自動化，且能因應需求快速變動。 ***網路存取控制NAC、軟體定義邊界SDP***

2

零信任架構導入常見問題-
網路安全

零信任架構導入常見問題一覽表-網路安全(1/2)

PwC 整理常見導入零信任架構之網路安全時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
舊系統不支援SDN無法重塑，如何因應「同網段隔離」要求？	<ul style="list-style-type: none">• 透過自動化或人工方式盤點各系統關聯設備，使用VLAN/PVLAN將關聯設備分組，搭配ACL 設定禁止非相關系統的互通連線。• 或可選擇透過開啟本機防火牆設定規則進行控管。
目前已有網路流量監控機制，但尚未呈現對系統、端點與網路間連線的相依性關係，有什麼建議落實措施？	<p>旨在可即時透過任一設備掌握系統與網路的運作狀態，建議可考量：</p> <ul style="list-style-type: none">• 網路微分段機制，透過使用可視化分析模組收集傳送流量資訊及工作負載背景資訊，繪製應用系統相依性圖。• 非微分段機制，透過網路流量分析(NTA)及追蹤端點與服務間之流量，搭配可視化工具實踐、ITOM/CMDB先建立「應用系統與組件」的 CI (Configuration Items)，然後紀錄CI之間關聯性。

零信任架構導入常見問題一覽表-網路安全(2/2)

PwC 整理常見導入零信任架構之網路安全時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
舊應用、裝置或瀏覽器不支援HTTPS，建議如何調整以達到傳輸加密？	可優先更新瀏覽器或升級應用。若不可行時，可暫時採用技術性替代方案使用反向代理/應用層代理，或是透過VPN/VDI、遠端桌面登入支援HTTPS環境訪問內/外網系統。未來可擬定計劃逐步淘汰不安全的舊系統、設備，持續監控和評估安全狀況。
如何分階段推動這些措施，是否有優先建議的順序或切入點？	<ul style="list-style-type: none">• 實施基本網路區隔，建立基本的流量管理和監控系統。• 盤點資產依據業務角色將主機、服務、裝置等分類，掌握分各系統間的實際流量與連線需求。• 導入如軟體定義網路(SDN)或網路微分段等解決方案。• 整合與SIEM或SOC串接，實現告警與事件處理的自動化機制。

Q & A

pwc.tw

© 2025 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.