pwc 資誠

推動證券商導入金融零信任說明會

–設備管理

資誠智能風險諮詢管理有限公司

2025.6

Agenda

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

1

實作參考原則分級解析-設備管理

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
	程式部署
資料	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

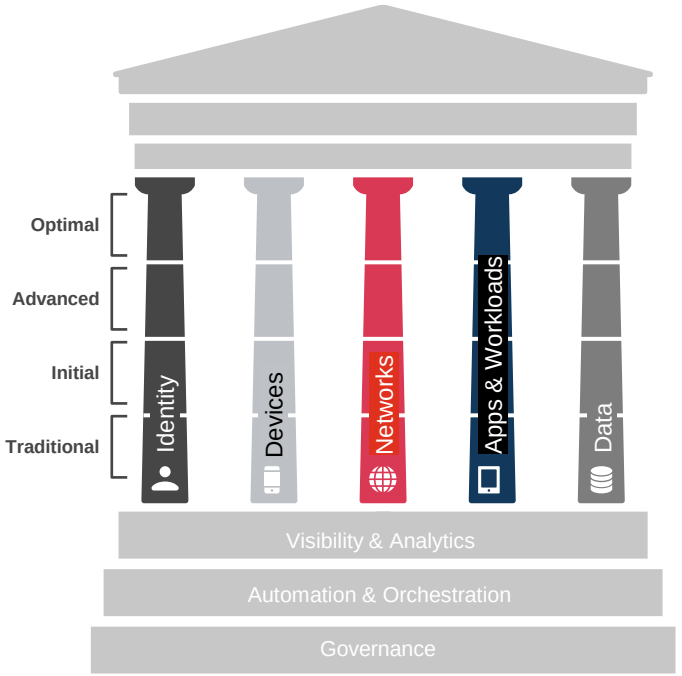
等級 IV

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（I*1、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）

5 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）

4 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）

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

2. 設備

保障連線設備的合規和安全性，確保每個設備都是可信賴的

金融業導入零信任架構參考指引-實作參考原則

保障連線設備的合規和安全性，確保每個設備都是可信賴的

I 靜態指標

- **2-1 設備合規**：具有效盤點且可唯一識別之納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。
- **2-3 供應鏈風險**：對外部設備建立不低於內部設備防護基準之管控措施，或限制透過合規中繼閘道存取。

II 動態指標

- **2-2 設備合規**：具納管設備合規檢測及弱點管理機制，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。
- **2-4 資源存取**：可將設備動態屬性納為每個工作階段之授權審核條件，動態撤銷、限縮存取或即時告警；或具備隔離機制，偵測並阻斷未合規設備之連線；或限制透過合規中繼閘道存取。

III 即時指標

- **2-5 威脅防護**：對設備活動紀錄具即時偵測及回應機制，在偵測到威脅指標時，可自動隔離或即時應處。
- **2-6 可視化分析**：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

- **2-7 自動化治理**：可依資安政策快速調適之自動化管理機制，確保設備生命週期的安全性及合規性。

金融業導入零信任架構參考指引-實作參考原則

2-1 設備合規

具有效盤點且可唯一識別(如TPM等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

1. 納管設備機制

- 設備**有效盤點**
- 設備具**唯一識別** (可理解為每個設備有自己的身分證)

  註: TPM(為安全硬體，提供設備識別碼且可協助加密)

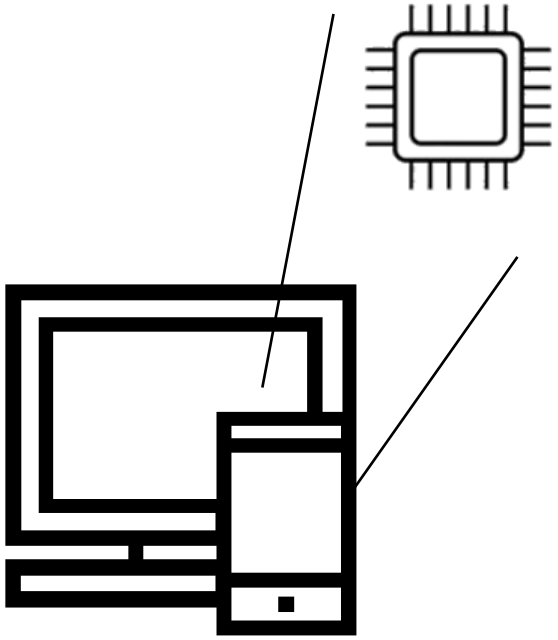
2. 安全檢查和處理

- 已納管設備：能夠判斷安全狀態(如是否更新作業系統、病毒碼等)
- 未納管設備：能即時偵測，進行風險控管

→ 強調設備具唯一識別與納管機制，並能對安全要求進行判斷和處理

2-1 設備合規

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

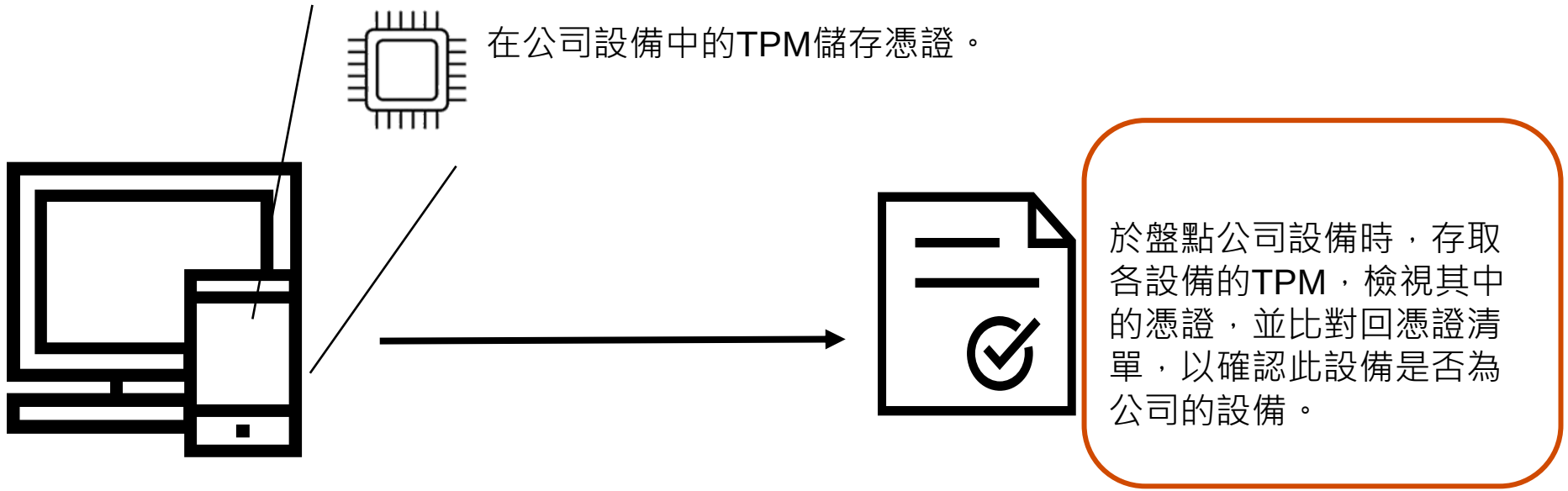


Trust platform module, TPM

信賴平台模組，一種電腦硬體零件，藉由密碼學的技術，**可以將用戶的關鍵資訊儲存在獨立的記憶體中，如憑證、金鑰等資訊**。TPM有獨立的韌體，不須依賴電腦的作業系統執行指令，**確保軟體和系統在受到攻擊時不會影響到用戶的關鍵資訊。**

2-1 設備合規

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標



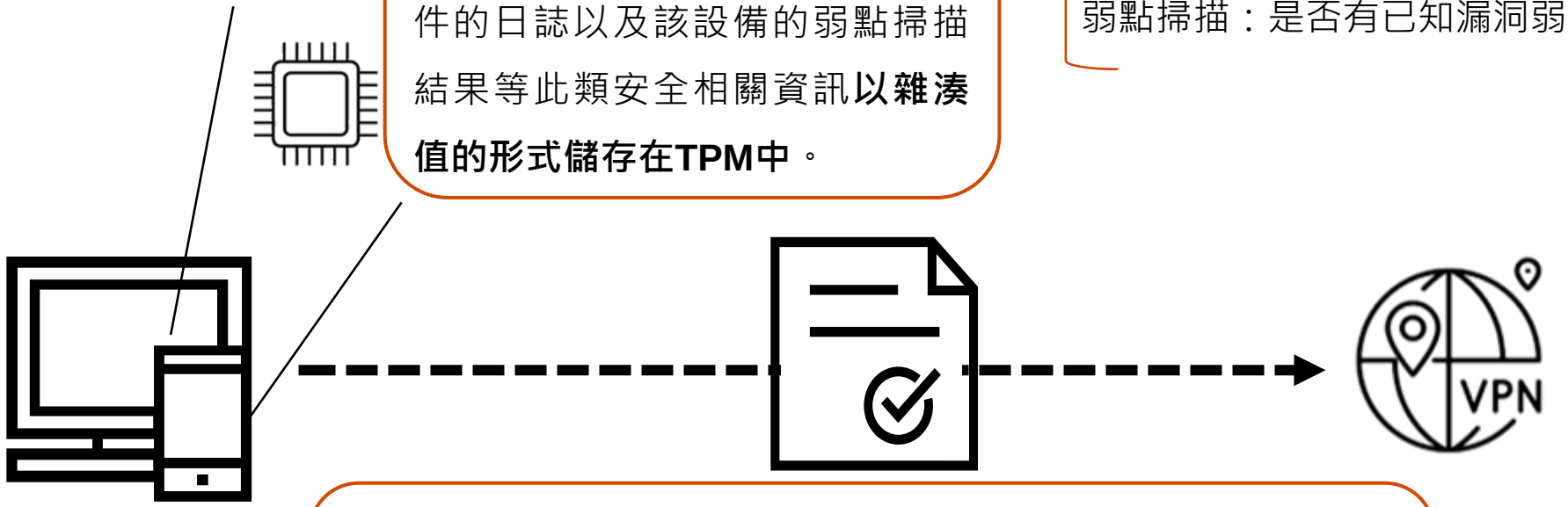
金融業導入零信任架構參考指引-實作參考原則

2-1 設備合規

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

設備是否安裝防毒軟體、EDR、此類防護機制是否捕捉到異常事件的日誌以及該設備的弱點掃描結果等此類安全相關資訊**以雜湊值的形式儲存在TPM中**。

- 合規性檢查：如該安裝的更新是否有安裝
- 健康度檢查：如檢查結果是否有告警
- 弱點掃描：是否有已知漏洞弱點



當公司需要對設備進行身分驗證時(如建立VPN連線)，會請求該設備的TPM提供相關的安全資訊，透過比對TPM中的資訊與公司的規範的標準組態模板，確認設備安全是否符合公司要求，確認安全無虞後，才可以使用公司的後續應用服務。

金融業導入零信任架構參考指引–問答

Question:
零信任要求設備必須「可唯一識別」，以下哪個技術不符合此要求？

選項A

MAC address

→ ✓ **風險可控下，可使用MAC地址識別**

選項B

IP位址

→ ✗ **不適用**

選項C

TPM 模組

→ ✓ **可將唯一識別碼存放於設備的TPM中**

金融業導入零信任架構參考指引-實作參考原則

2-2 設備合規

具納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

1. 合規性檢測

- 確保設備符合安全和管理標準

  (包括設置、軟體版本、病毒碼規範等)

2. 弱點管制

- 能檢查設備是否更新或有無資安漏洞

3. 監控不合規設備

- 能執行風險控制措施

  (如強制更新、修補漏洞、即時警告)

➡ **強調納管設備的合規性檢測和弱點管理**

金融業導入零信任架構參考指引–問答

Question:
當偵測到未納管或未合規設備存取行為，建議的處置方式分別為何？

情況一

未納管設備

→ **隔離及即時告警**

情況二

已納管但未合規之設備

→ **強制更新、修補弱點、強制隔離、即時告警**

2-3 供應鏈風險

對外部設備(如BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之合規中繼閘道(如VDI等)存取。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

1. **內、外部設備防護管控措施標準一致**
2. **設置中繼閘道，確保外部設備經由安全路徑訪問公司**

名詞解釋

- BYOD(Bring Your Own Device)：員工自己的裝置，包括電腦、手機等。
- VDI(虛擬桌面基礎設施)： 讓使用者透過網路安全使用公司桌面的技術，可在伺服器上集中管理。

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，BYOD（自攜設備）應如何處理？

選項A

禁止所有自攜設備接入

→ X 不適用

選項B

授權一次後即可長期使用

→ X 不適用

選項C

經合規中繼閘道（如:VDI）存取

→ ✓ **限制需經由VDI存取，且防護措施不等於內部設備**

金融業導入零信任架構參考指引-實作參考原則

2-4 資源存取

可將設備之動態屬性(如是否納管及合規、設備位址、或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼閘道(如VDI等)存取。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

動態授權審核條件(信賴分數)

- 根據設備屬性進行審核(是否納管、合規、位置、內部/外部)
- 實施動態撤銷或限制存取授權
- 即時警告/阻斷/隔離未合規設備連線行為

範例：

- **信賴分數高**：員工A使用納管設備自總部且通過合規、健康度檢查進行存取敏感資料
  —> **允許存取**
- **信賴分數中**：員工B使用納管設備通過合規但有尚未完整Patch進行存取敏感資料
  —> **限制存取、發出告警**
- **信賴分數低**：員工C使用自攜設備於弱點掃描存在弱點進行存取敏感資料
  —> **即時阻斷、發出告警**

金融業導入零信任架構參考指引-實作參考原則

2-5 威脅防護

對設備活動紀錄具有即時偵測及回應機制(EDR)，在偵測到威脅指標(IOC)時，可自動隔離或即時應處(如發出事件單即時追蹤處置)。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

EDR(端點偵測與回應)

- **功能**：即時監控設備活動，偵測並回應潛在威脅指標(IOC)
- **操作**：發現異常活動時，EDR自動
  - (1) 發出告警
  - (2) 開立事件單
  - (3) 追蹤處置
  - (4) 自動隔離設備

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

金融業導入零信任架構參考指引-問答

Question:
零信任要求設備之「動態屬性」納入授權條件，以下哪一項屬於動態屬性？

選項A

設備是否合規、地點位置、時間

✓ 亦可作業系統版本、更新時間、是否納管等

選項B

設備製造商品牌

X 不適用

選項C

設備購買時間

X 不適用

金融業導入零信任架構參考指引-問答

Question:
以下哪一種設備管理機制屬於即時指標（Level III）等級？

選項A

病毒碼檢測

→ X 此為靜態指標（Level I）

選項B

持續監控並強制安裝更新或隔離

→ X 此為動態指標（Level II ）

選項C

EDR部署

→ ✓ 對設備活動紀錄，具有即時偵測及回應機制

金融業導入零信任架構參考指引-實作參考原則

2-6 可視化分析

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)進行即時的判斷與應處(如事件單、SOAR Playbook)。

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。

2-7 自動化治理

可依資安政策快速調適之一致性且自動化管理機制，確保於設備生命週期之安全性及合規性。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

階段	說明
傳統	•機構手動配置、註冊、管理企業內的設備
最佳化	**•全面自動化設備和虛擬資產的配置、註冊、監控、隔離、修復和撤銷過程** Enterprise-wide***統一端點管理UEM***

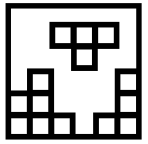
設備支柱之應用–統一管理暨分析設備健康度

傳統架構


組態管理


修補、更新


主機安全系統(HBSS)

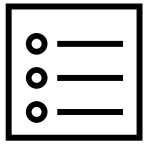

端點資安及持續性檢測解決方案

彼此孤立

零信任架構

資安政策 → SIEM → 設備控制


事件驅動


持續自動盤點偵測


設備合規檢測


動態設備更新


依信賴分數授予權限

相互整合

設備支柱之應用–統一管理暨分析設備健康度(釋例)

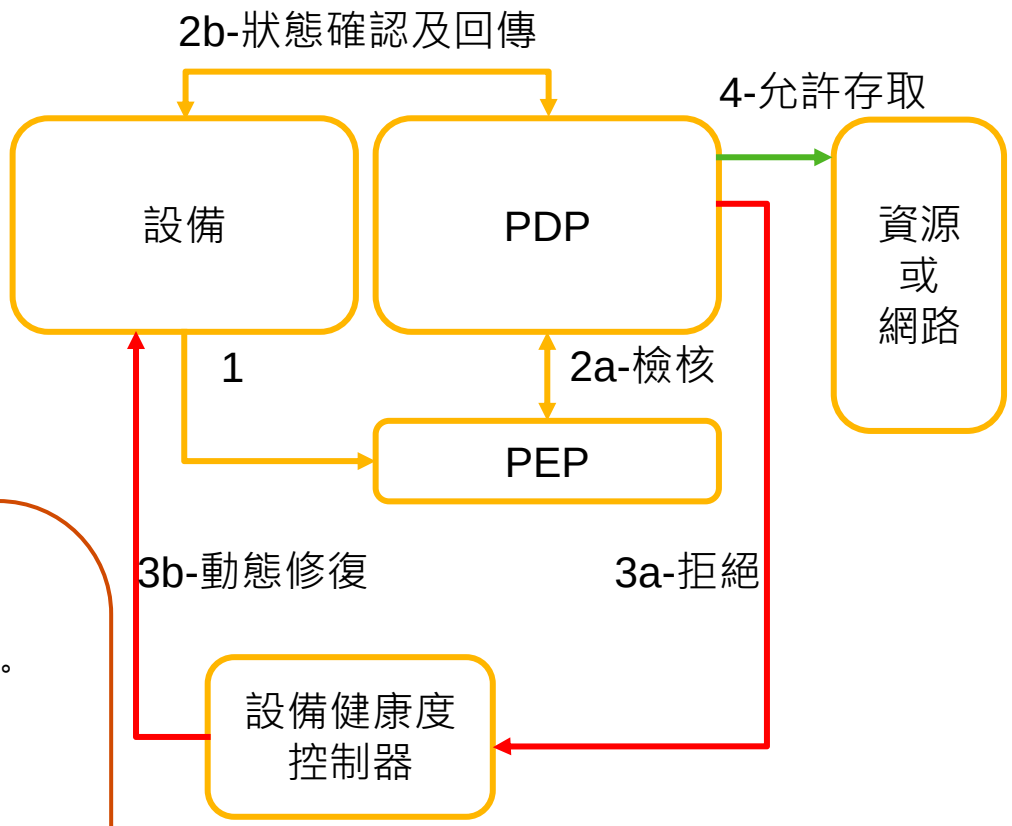
預設條件（Preconditions）

(a) 設備安全規範：會根據公司最新的規則和設備清單來更新健康度控制器。

(b) 將最新政策派送給本地端上之健康度控制器 。

(c) 設備健康度控制器從設備或代理收集配置狀態與遠端數據，並應用補丁，進行持續的背景處理。

(d) 健康度控制器更新合規政策，以確保系統狀態的同步。



設備健康度控制器

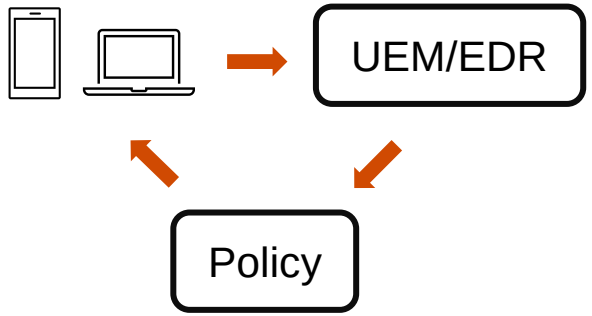
定義：管理和維護設備安全措施的系統，監控設備配置和狀態，確保符合安全狀態。

功能：

1. **收集設備狀態：**持續獲取設備或agent的狀態資訊，監控設備健康。
2. **修復與更新：**自動修補漏洞並進行版本更新。
3. **合規檢查：**控制器會將設備狀態傳遞給PDP，檢查是否符合規範。
4. **推送補救措施：**如設備未能通過檢查，會推送動態補救措施到本地設備，協助合規。

設備支柱之應用–統一管理暨分析設備健康度(應用案例)

邏輯概念：



1. UEM/EDR確認設備健康狀態
2. 檢查是否合規 (Policy)
3. 決定授權與否 (Policy)

範例：

金融業員工須透過筆電存取敏感資料庫(如交易紀錄、財報、風控模型等)

控管機制：

僅允許公司核准且合規的裝置存取(如具備加密、防毒、定期更新)

裝置狀況不良 → 封鎖存取或導引自動修復

依使用者身分、裝置屬性、時間/地點調整權限(搭配ABAC政策)

零信任評估

靜態指標：設備盤點、政策制定(含供應鏈、BYOD)

動態指標：自動檢查設備合規、自動對設備進行風險管控措施、自動管控存取

即時指標：自動偵測威脅並回應、可視化

整合指標：全自動化

2

零信任架構導入常見問題-設備管理

零信任架構導入常見問題一覽表–設備驗證(1/2)

PwC 整理常見導入零信任架構之設備支柱時，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
針對既有資產清單，想確認是否已符合指引中的資產盤點與更新標準?	因機構設備資產清單是靜態、人工手動維護的，不具備持續性更新與全面可視性，尤其常遺漏雲端資源、遠端設備與其他內/外部資產。可重新檢視盤點流程並導入具備自動盤點、可分類篩選的資產管理工具。
請問在既有已導入端點管理機制的基礎上，可調整哪些控管措施，以利貼近指引要求?	可推行自動修補、設定與合規檢查，並及時採行風險控管措施。 • 啟用代理程式可遠端執行修補與組態指令。 • 建立可持續偵測「設備合規性政策」措施，例如：病毒碼、作業系統版本、公司政策安全組態設定等。 • 對於不合規設備，能強制隔離或即時告警機制。

零信任架構導入常見問題一覽表–設備驗證(2/2)

PwC 整理常見導入零信任架構之設備支柱時，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
關於資安漏洞掃描，若已建立例行掃描機制，是否需再進行額外流程設計或整合？	可將掃描後之結果，評估風險影響，對於中高風險進行優先修復，符合可接受的安全等級，建立安全漏洞管理流程；並整合至設備管理平台作為自動處理之依據，以掌握設備的整體健康與最新安全狀態。
已部署端點偵測及回應機制(EDR)，我們可如何進一步強化其偵測與回應效能，以達到實質防護的效果？	針對端點告警進行資料分析、偵測行為模式並回饋決策，如以下幾點： • 可定期檢查是否產出異常告警與後續行動報告。 • 可整合EDR系統與SIEM或SOC串接，實現即時處置機制。 • 可定期匯報端點威脅趨勢給高階管理層或資安治理小組。

Q & A

pwc.tw