淺談零信任架構的迷思與導入策略
An overview of myths and strategies of the zero trust architecture

主講人：查士朝

國立臺灣科技大學資訊管理系 教授

國立臺灣科技大學資通安全研究與教學中心主任

國立臺灣科技大學
NATIONAL TAIWAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

今天有兩個人來分享 (誤)


神隊友援救少女
台北
資安教授 查士朝
去找出
NEWS 下載APP看直播


民視快新聞
台科大資管系副教授
查士朗
中資疑慮難解「淘寶台灣」恐禁用

今天我來的目的最重要是這個

查士朝

- 台大資管博士
- 現職 臺灣科技大學
  - 資訊管理系教授
  - 資通安全研究與教學中心主任
- 經歷
  - 曾任意藍科技股份有限公司資深技術顧問
  - 曾任資誠企業管理顧問股份有限公司協理
  - 曾任台灣大學工商管理學系兼任助理教授
- 近年來執行多項科技部與產學合作計畫
- 協助多家機構建立資訊安全管理制度
- 協助政府建立物聯網及手機應用程式安全標準
- 專長
  - 資訊安全架構
  - 資訊安全程式設計
  - 新興科技資訊安全風險分析與管理

個人擁有認證

技術

- Google Associate Android Developer
- CCDH (Developer for Apache Hadoop (CCDH)
- EMCISA
- RFID+
- MCSD.NET
- MCSE
- Sun Certified Enterprise Architect (SCEA)
- Sun Certified Java Programmer (SCEA)
- Linux Professional Institute Certification Level 1 and 2

資訊安全技術

- OSCP
- Certified Wireless Security Professional

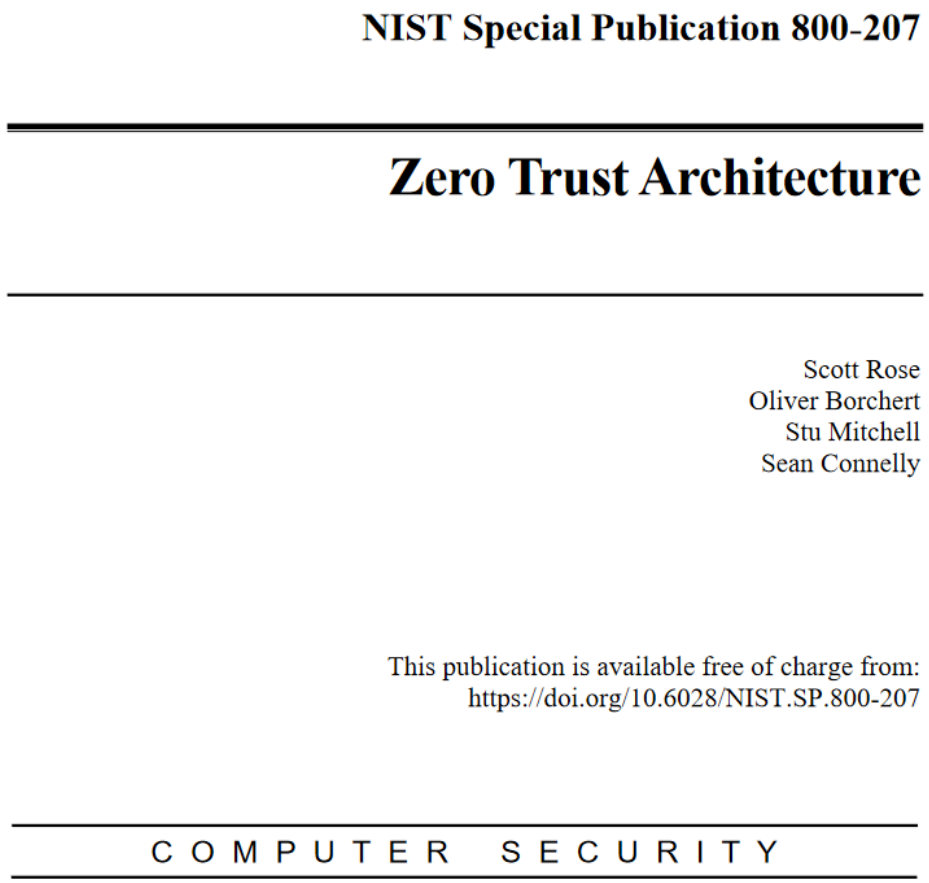
資訊安全管理

- CCFP
- CCSK (Certified Cloud Security Knowledge)
- CSSLP
- CISSP
- CISM
- BS7799 LA

管理/資訊治理

- Certified Scrum Master
- ITIL Service Manager
- PMP

這是個從名稱開始就容易讓誤解的概念



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

零信任?

你信任某個加解密演算法嗎？

你信任某個電子商務網站嗎？

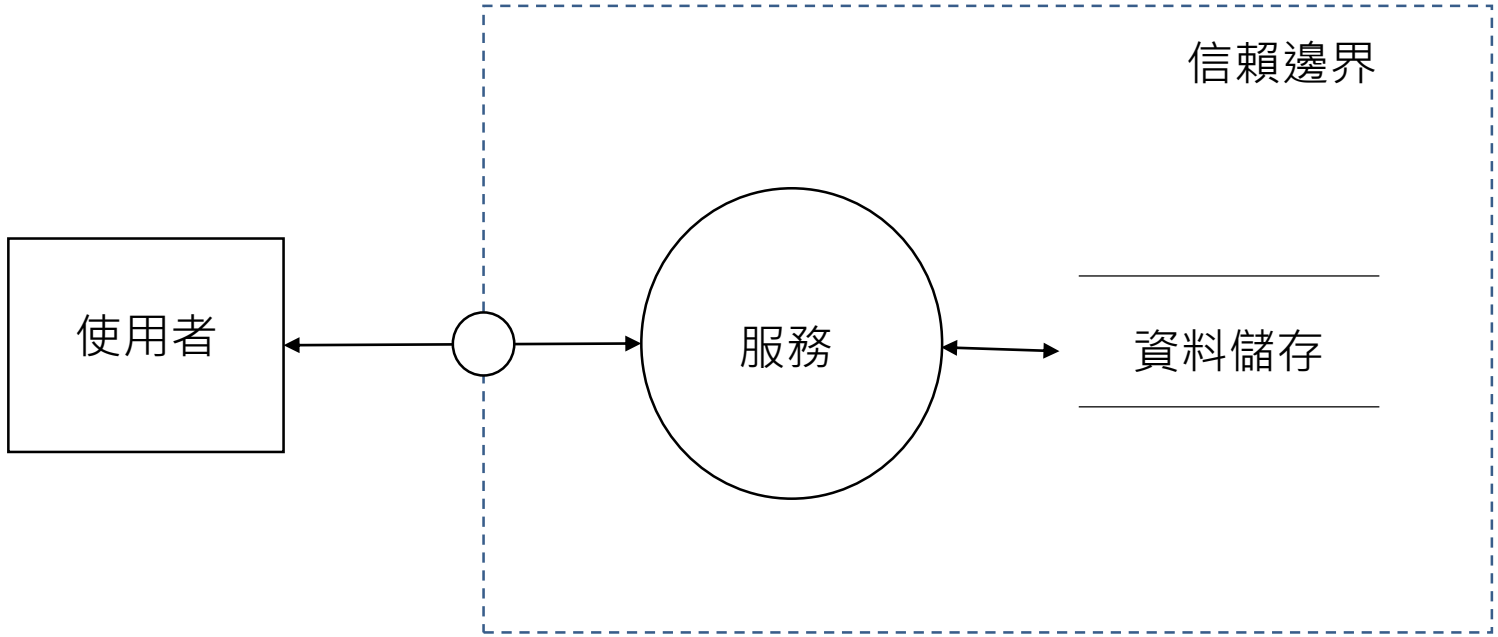
你信任某個晶片沒有被裝後門嗎？

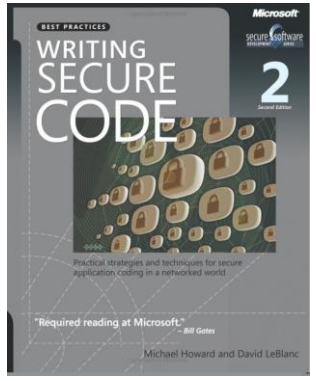
零信任?

你為何會信任某個系統或網站？

如果不信任你要怎麼辦？

威脅模型與信賴邊界





Writing Secure Code, Second Edition 2nd ed., 2003

通常會基於某種信任假設去提供資訊服務

基於對 CA 的信任而建立安全連線與簽章

基於伺服器硬體的信任而在上面佈署服務

基於對程式語言編譯器的信任而使用它來開發程式

所以零信任架構並不是「零信任」的架構

起源可能是來自於無心插柳的結果

- 傑里科論壇 (Jericho Forum) 與去周邊化 (de-perimeterization) 概念
  - 其實這概念是要消除邊界，當然在消除邊界後會有很多需要解決的資安議題
- 比較具體的概念是 2010 年由 John Kindervag 所提出
  - 裝置不再有信賴與不信賴的邊界 There are no longer a trusted and an untrusted interface on our security devices
  - 不再有信賴與不信賴的網路 There are no longer a trusted and an untrusted network
  - 不再有信賴與不信賴的使用者 There are no longer trusted and untrusted users

Jericho Forum

From Wikipedia, the free encyclopedia

The **Jericho Forum** was an international group working to define and promote de-perimeterisation. It was initiated by David Lacey from the Royal Mail, and grew out of a loose affiliation of interested corporate CISOs (Chief Information Security Officers), discussing the topic from the summer of 2003, after an initial meeting hosted by Cisco, but was officially founded in January 2004. It declared success, and merged with The Open Group industry consortium's Security Forum in 2014.[1]

https://en.wikipedia.org/wiki/Jericho_Forum

November 5, 2010

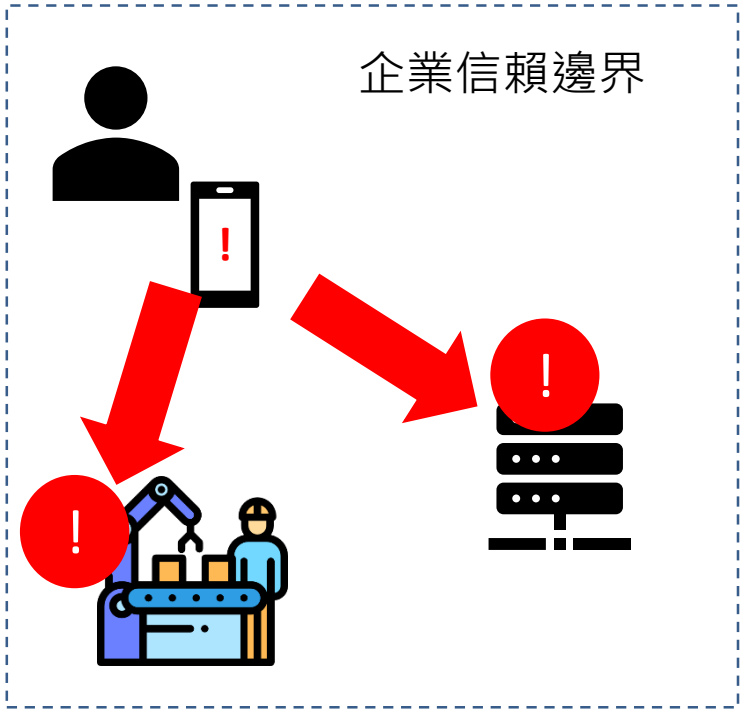
Build Security Into Your Network's DNA: The Zero Trust Network Architecture

by John Kindervag

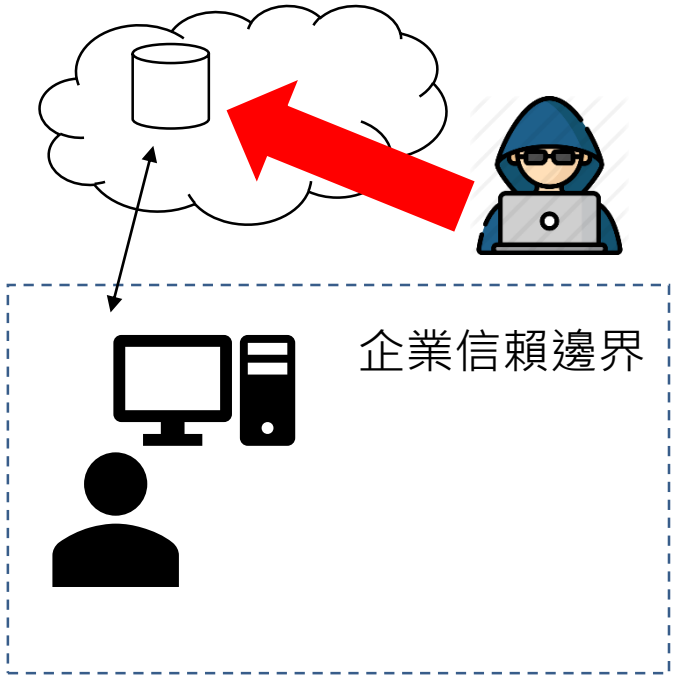
with Stephanie Balaouras and Lindsey Coit

傳統強化邊界方法在面對新興存取方式的挑戰

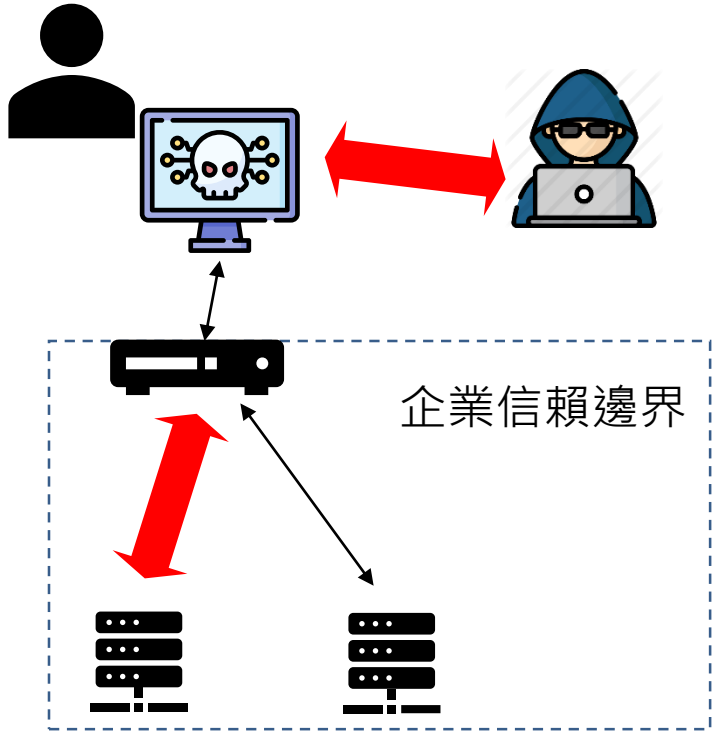
BYOD



使用雲端服務

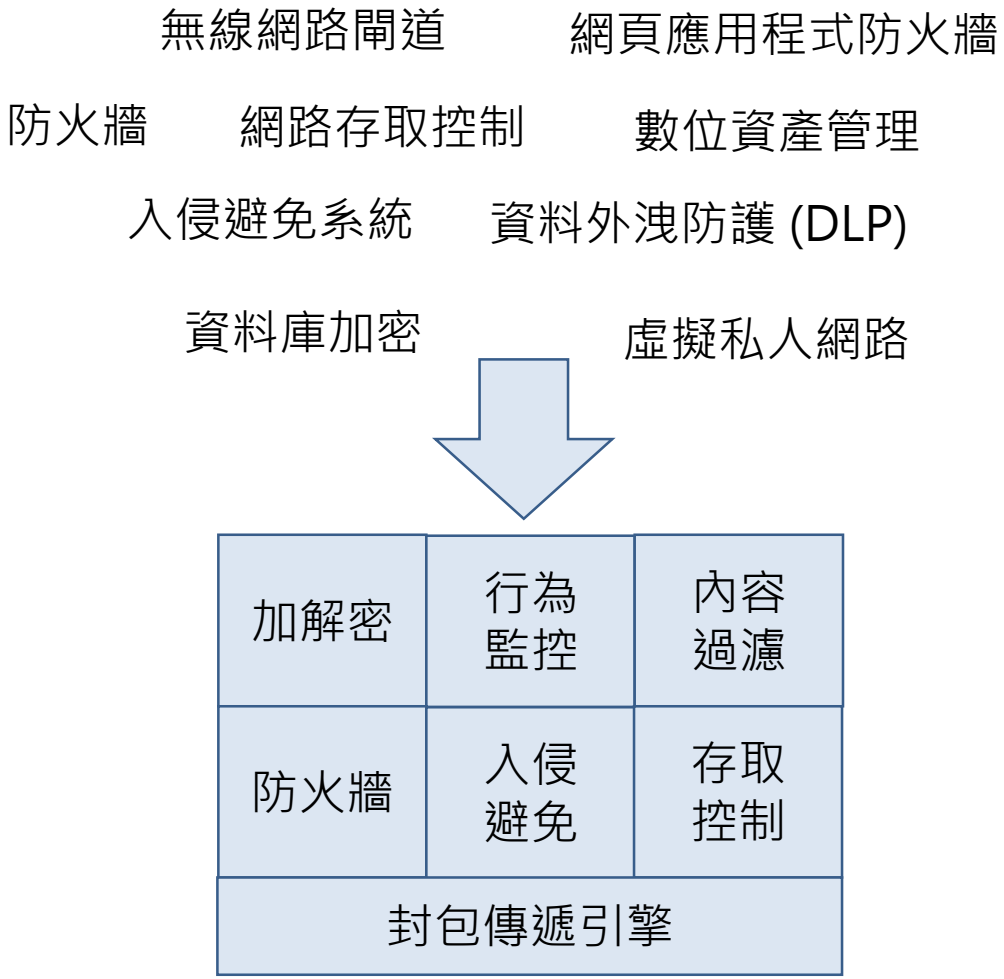


遠端工作

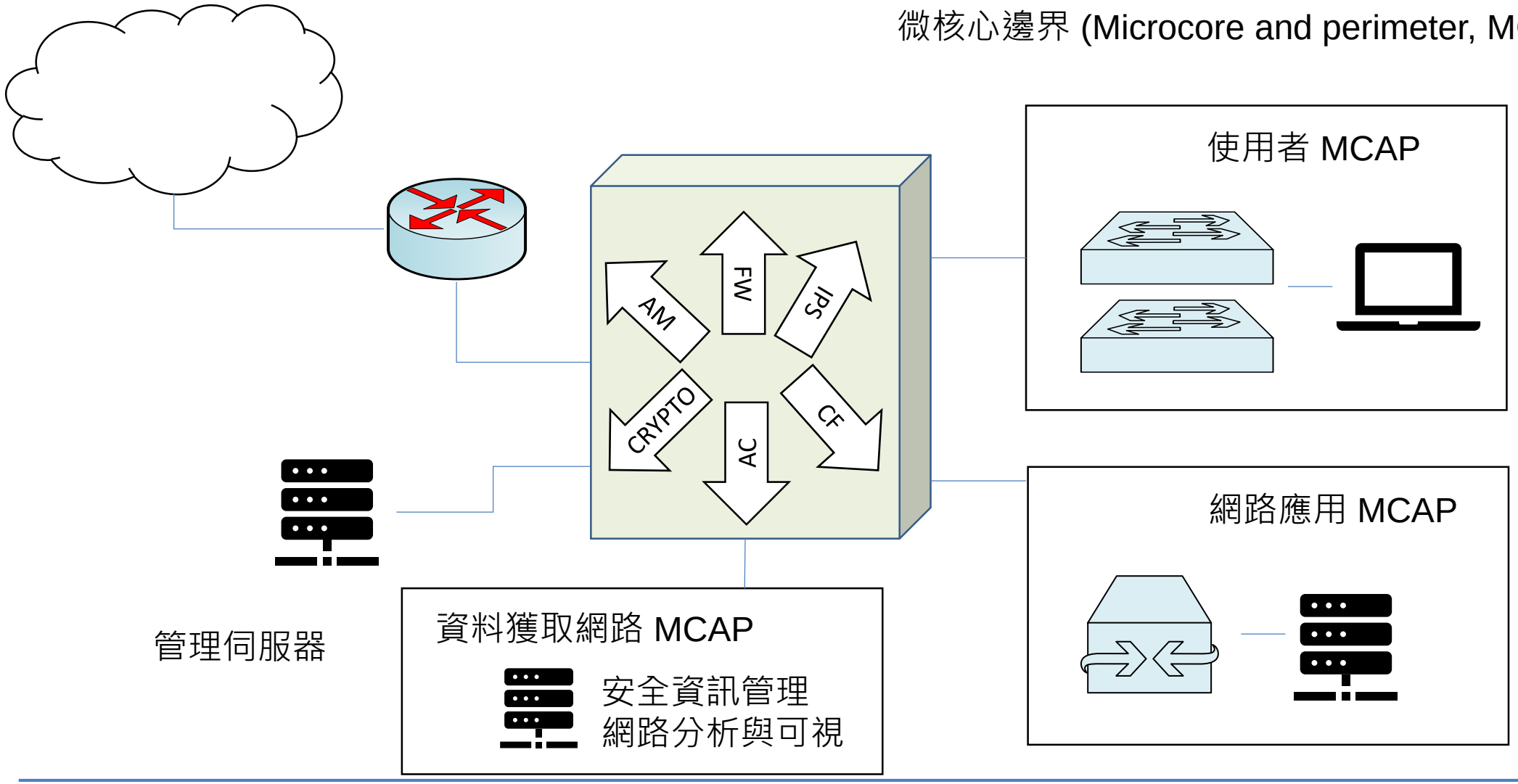


John Kindervag 的零信賴架構概念

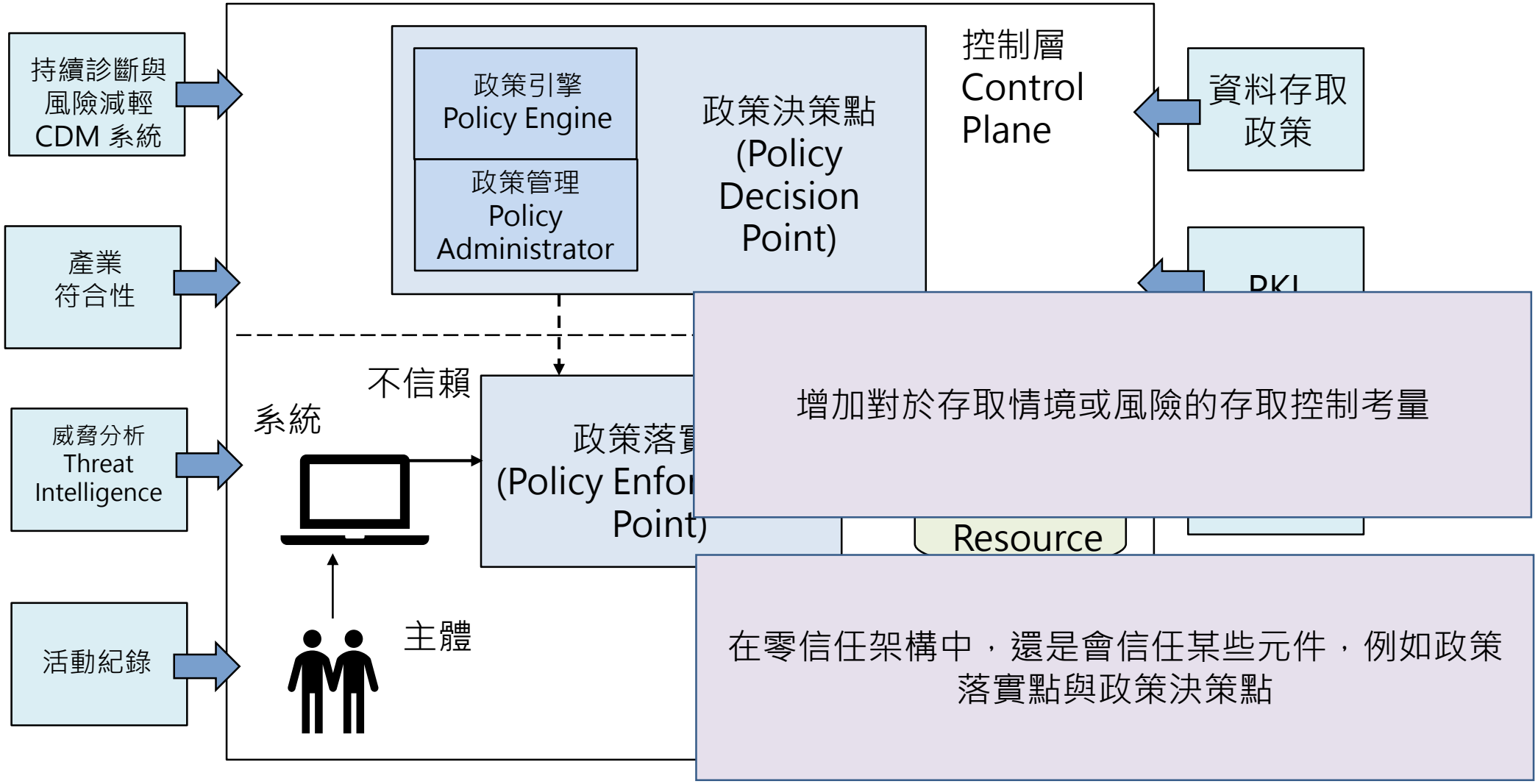
- 採用整合的分割閘道器形成網路中的核心元素 Use an integrated "segmentation gateway" as the nucleus of the network
- 建立平行的，安全的網路分隔 Create parallel, secure network segments
- 考慮到網路後台的集中管理 Think of centralized management as the network backplane.
- 建立資料取得網路以掌握網路的完整狀況 Create a data acquisition network to gain complete network visibility



微核心邊界 (Microcore and perimeter, MCAP)



在 NIST SP 800-207 中，ZTA 的核心元件



NIST SP 800-207 當中零信賴架構的教條 Tenets of Zero Trust Architecture

- 所有的資料來源與運算服務都要被當作是資源 All data sources and comp dered resources：每個網路上當作是服務或是可被存取的設備都應該被視為資 取。
- 不管是和哪個網路位置的裝置通訊，都需要確保安全 All communication network location：不要依照網路位置來決定是否信賴。
- 對於個別企業資源的存取要求，應該要以每次連線為基礎去進行許可Access to individual enterprise resources is granted on a per-session basis：要先評估要求者的可性度， 存取是以該次連線為基礎。
- 資源的存取應該要基於客戶端識別、應用服務，以及要求存取資產可觀察到的狀態，以及可能包括的行為或環境屬性去動態決定 Access to resources is determined by dynami observable state of client identity, application/service, and the requesting other behavioral and environmental attributes

識別可存取資源

連線安全

妥善存取控制

考量存取者狀態

與其說是有某一個特殊的「架構」不如說是透過一些原則去檢視安全架構

- 企業監控與衡量所有擁有與相關資訊資產的正確性與安全狀態 The enter sures the integrity and security posture of all owned and associated assets：沒有 言賴的。
- 在允許存取之前，所有的資源的身分鑑別與授權機制，都要是依監控結果 落實 All resource authentication and authorization are dynamic and strictly enf allowed
- 企業應該要儘可能收集有關資訊資產、網路架構、骨幹，與通訊的現況 安全狀態 The enterprise collects as much information as possible about the curre ork infrastructure and communications and uses it to improve its security pos

了解資源狀態

監控裝置與資源風險

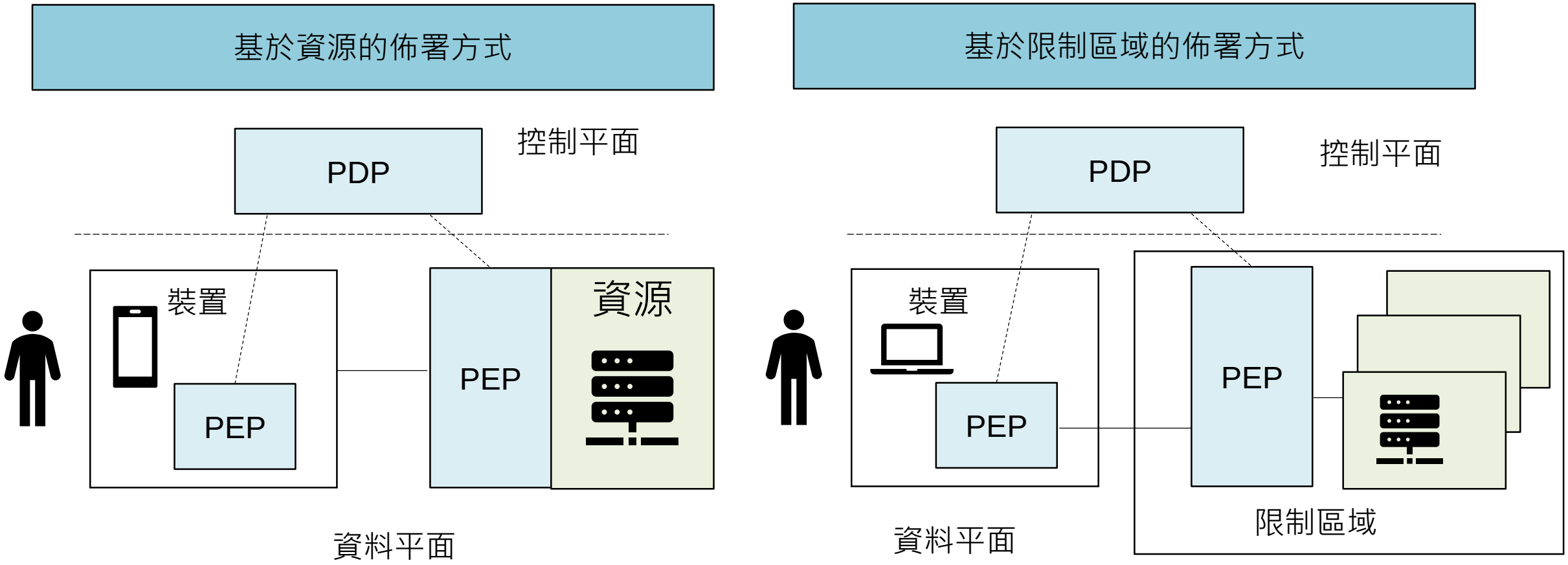
持續收集資訊與改善

可存取資源的
識別

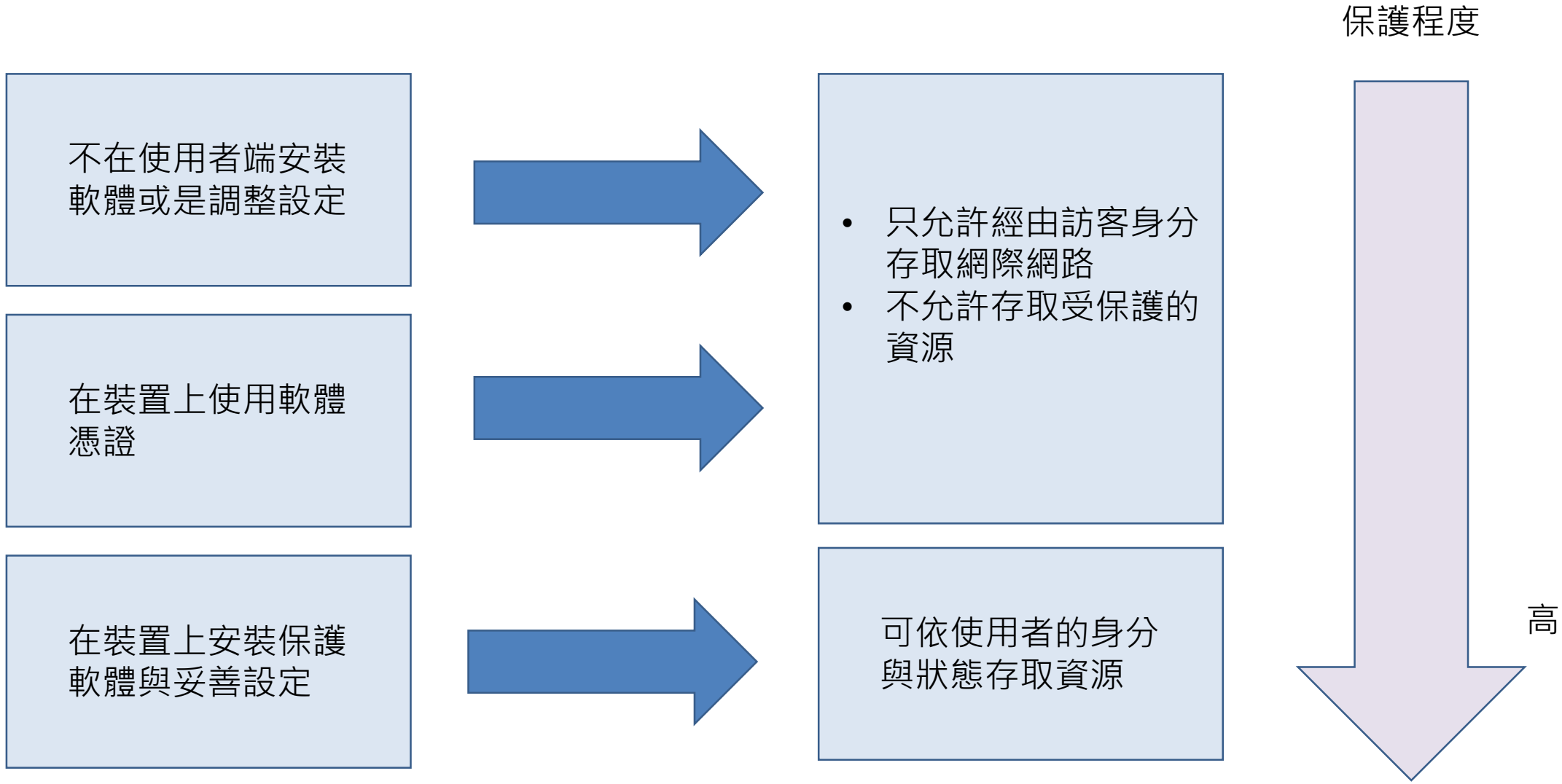
使用者層級的
存取控制

在存取控制加入
對風險的考量

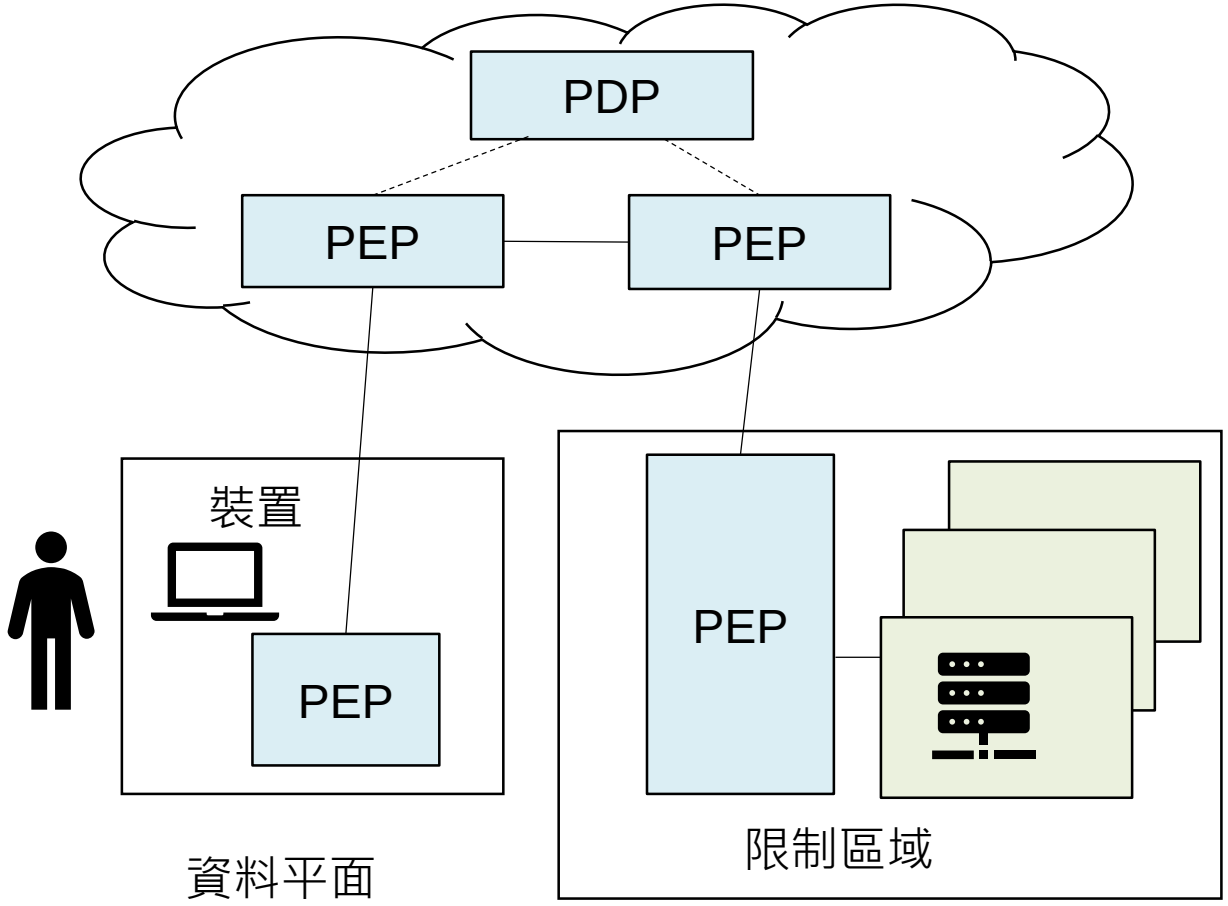
ZTA 佈署模式


基於資源的佈署方式
控制平面
PDP
裝置
PEP
PEP
資源
資料平面
基於限制區域的佈署方式
控制平面
PDP
裝置
PEP
PEP
限制區域
資料平面

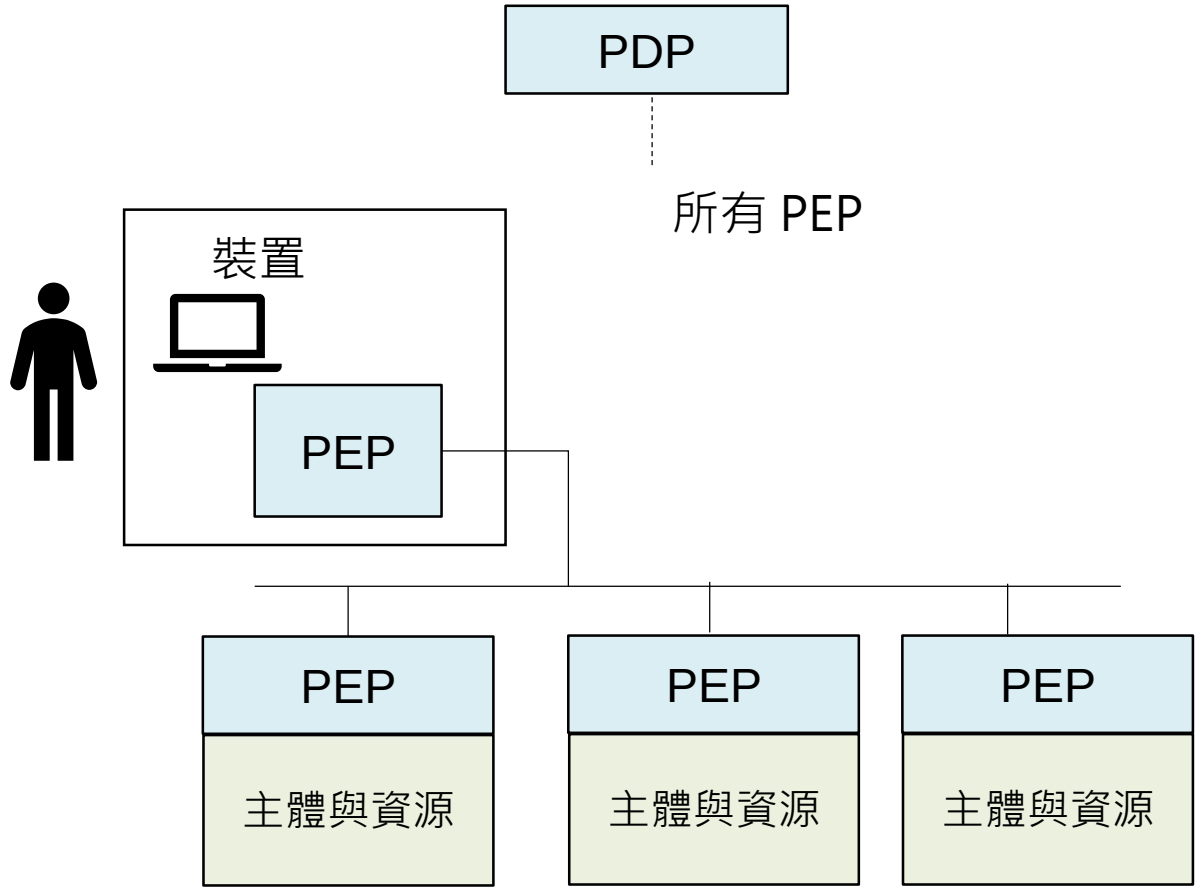
在客戶端的保護程度和權限



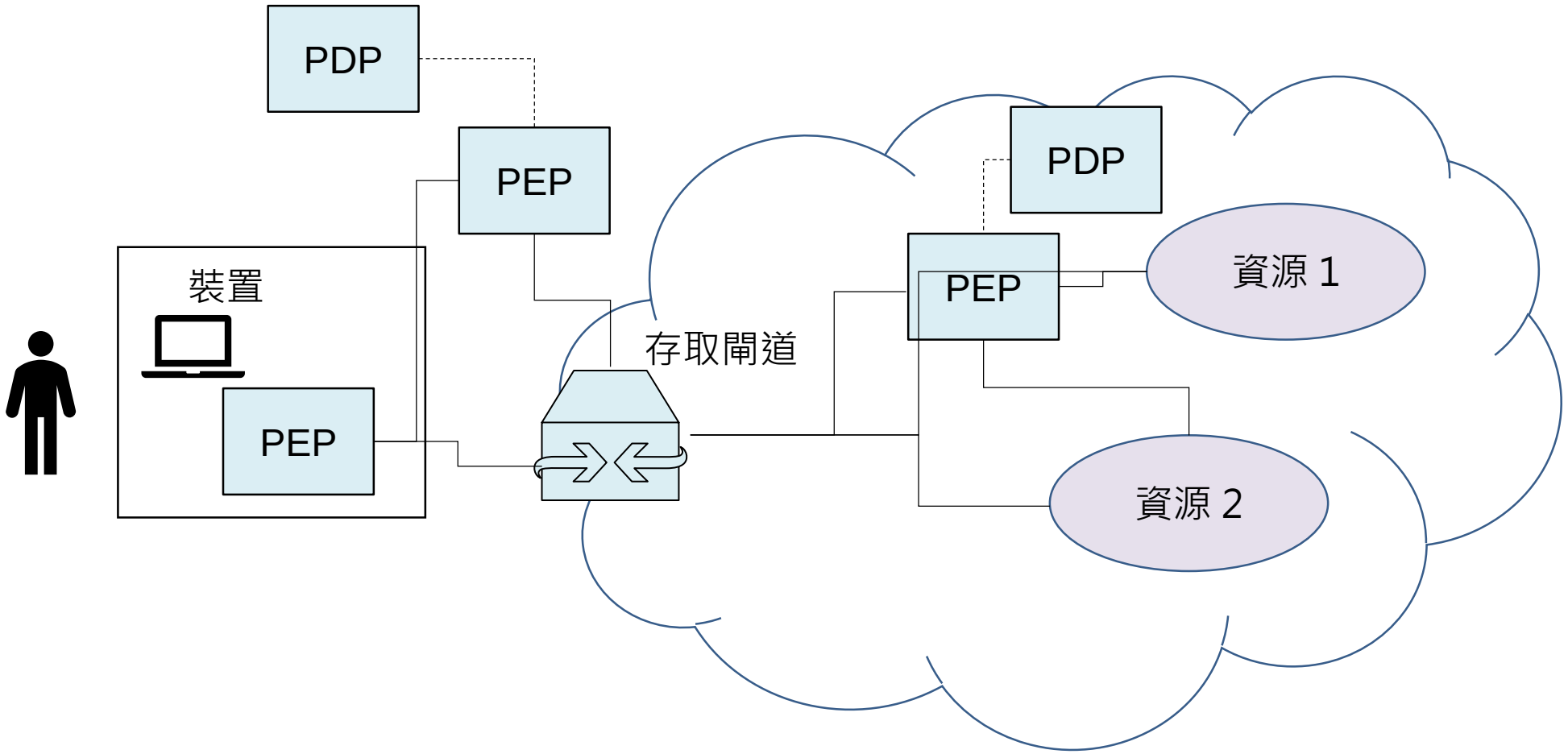
經過雲端的佈署模式



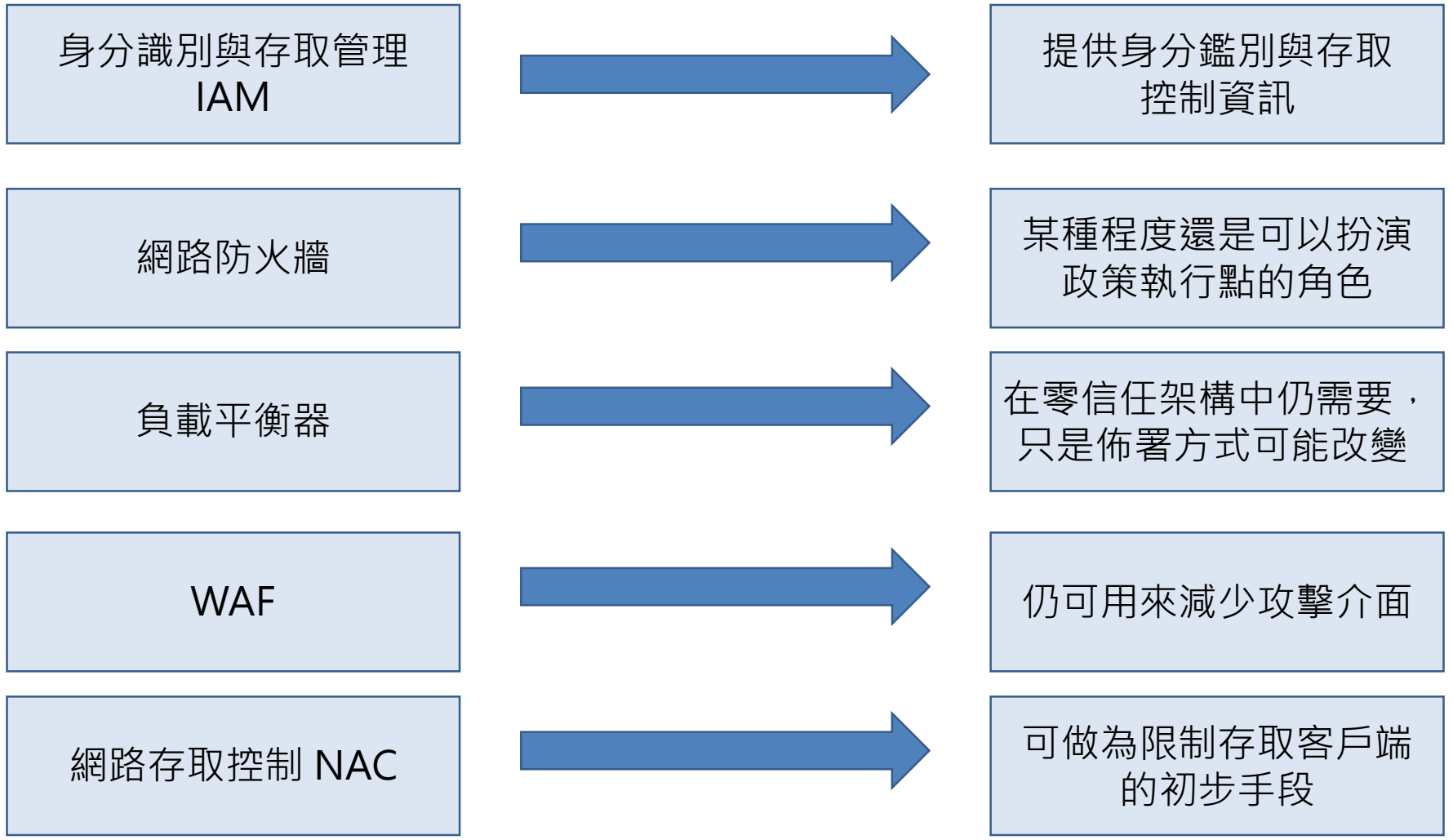
微分割佈署模式



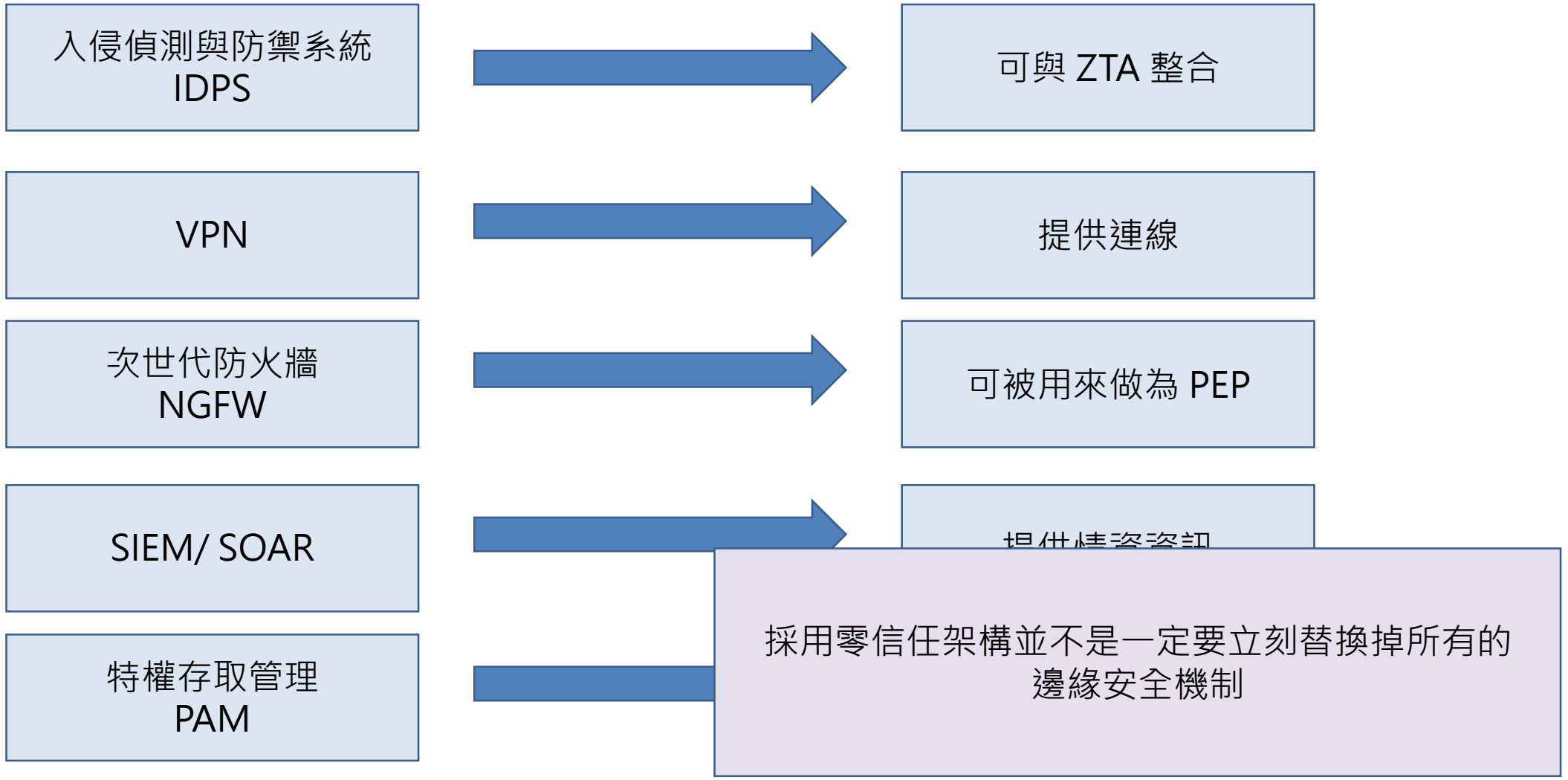
Source: Zero Trust Security: An Enterprise Guide


PDP
PEP
裝置
PEP
存取閘道
PDP
PEP
資源 1
資源 2

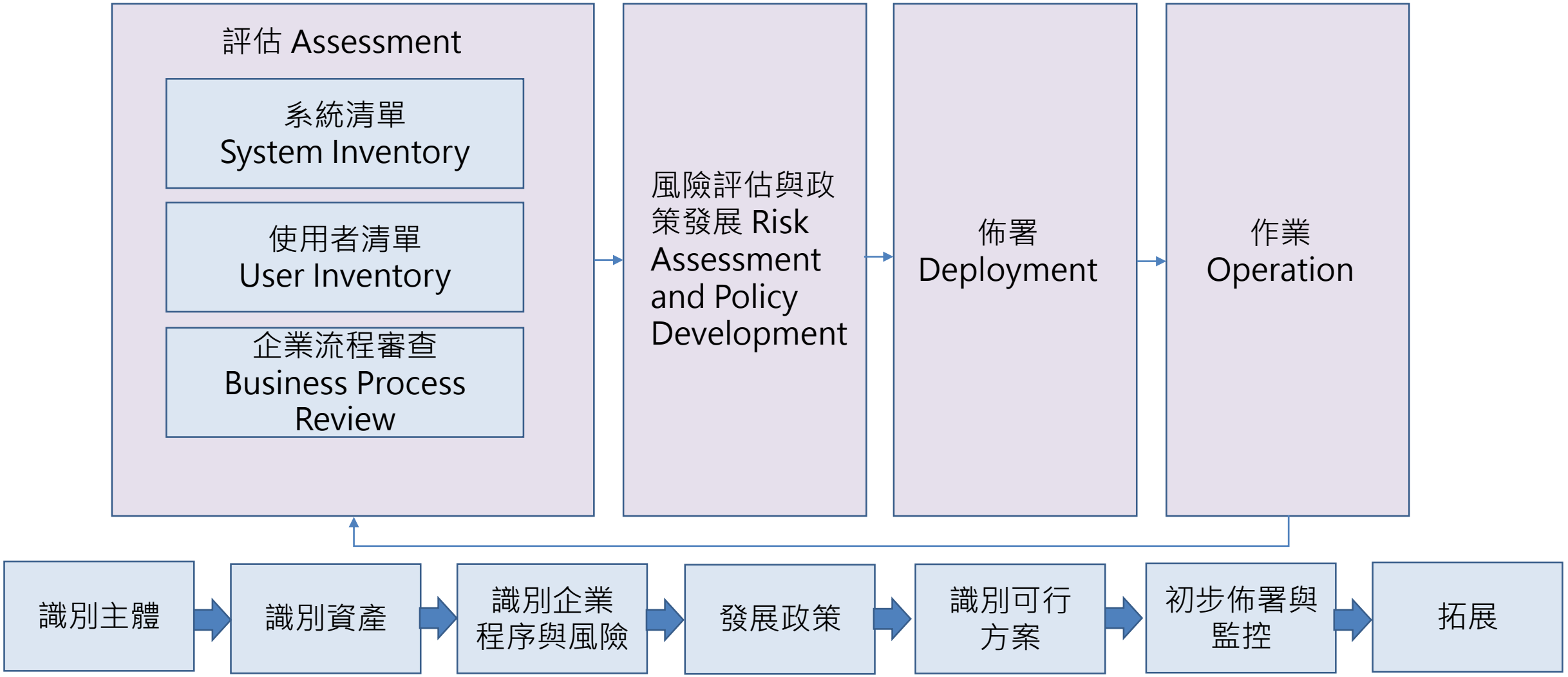
既有邊緣安全機制與零信任架構



既有邊緣安全機制與零信任架構 (續)



NIST SP 800-207 之導入零信任架構的步驟建議



階段式導入概念

先別急著花錢

掌握現況

- 盤點所有企業資源與存取情境
- 掌握既有存取控制規則
- 掌握既有安全控制措施

強化根基

- 強化存取控制措施
- 強化記錄機制
- 強化災難復原機制
- 資安檢查

深化安全

- 掌握風險資訊提前因應
- 依存取情境變更存取權限
- 持續檢討與改善

結論

- 零信任架構從名稱就引發很多誤導
  - 在零信任架構中，還是會信任某些元件
  - 與其說是有某一個特殊的「架構」不如說是安全原則
  - 並不是一定要立刻替換掉所有的邊緣安全機制
- 幾個關鍵
  - 盤點使用者與資源
  - 妥善佈署資源
  - 檢視權限並落實存取控制
  - 掌握資源與使用者狀態
- 可以考量本身的狀態，引入相關概念，並逐步強化

感謝各位的聆聽