



AWS比你想像中安全

謝博尊

中華電信國際分公司

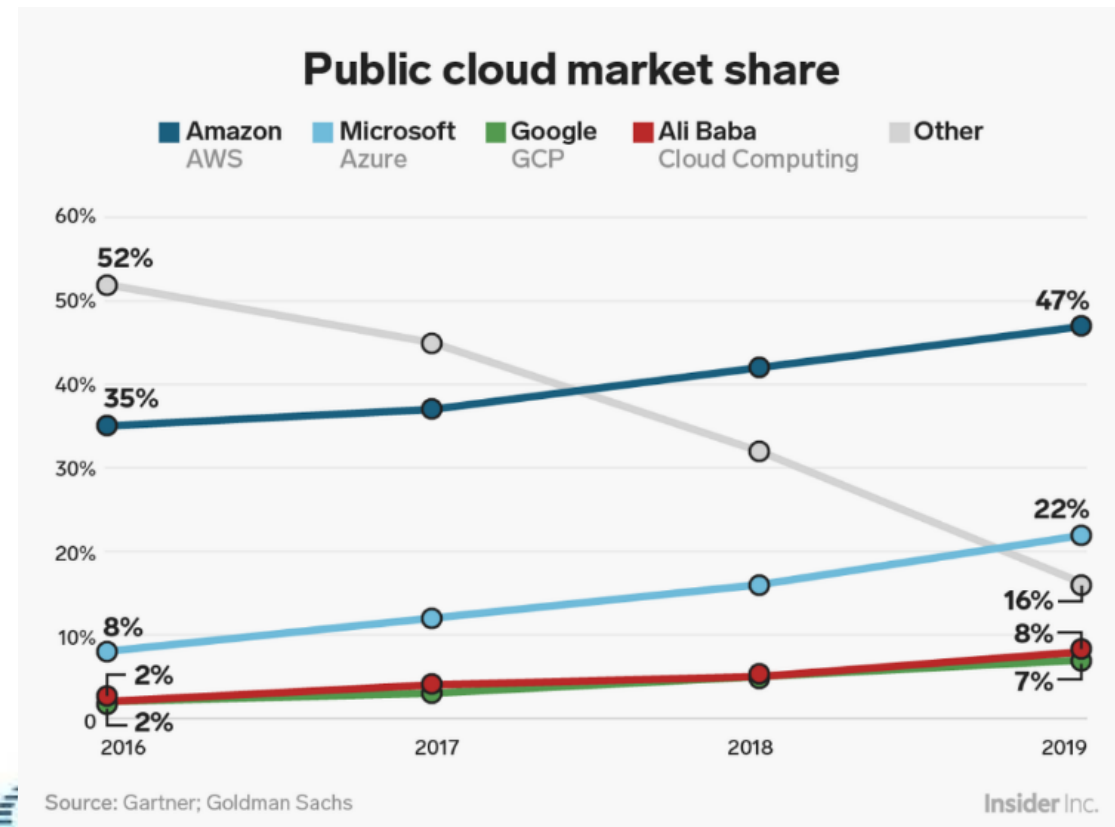
yugiohx@cht.com.tw

Who am I

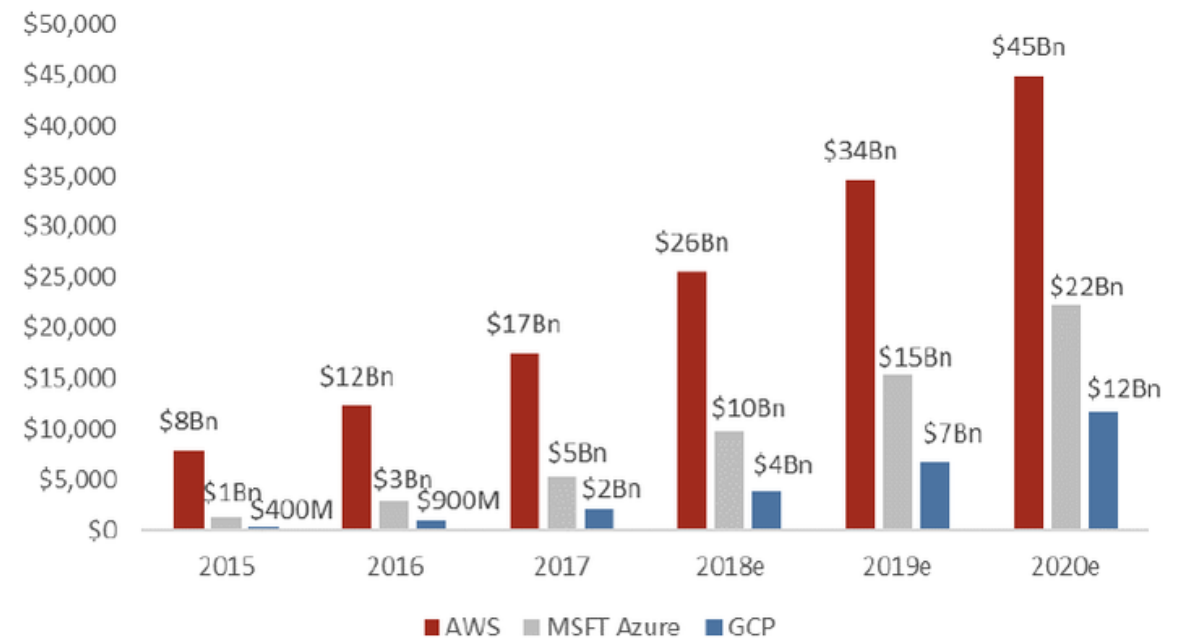
- 謝博尊 (Artsun)
- 現職：中華電信國際分公司 AWS資安架構師
- 經歷：
 - 政府單位跨國網路資安分析負責人
 - 校園國際電路DDoS防禦技術顧問
 - 中央大學管理學院電算中心網管教學組組長
- 專長：網路安全架構設計、系統解決方案設計。
- yugiohx@cht.com.tw

國際公雲市佔及趨勢分析

Amazon AWS 持續成長並**保持市場龍頭**，Microsoft Azure**成長速度居冠**，Google GCP及Alibaba保持成長，其餘公雲業者(含IBM)均**下滑非常快速**



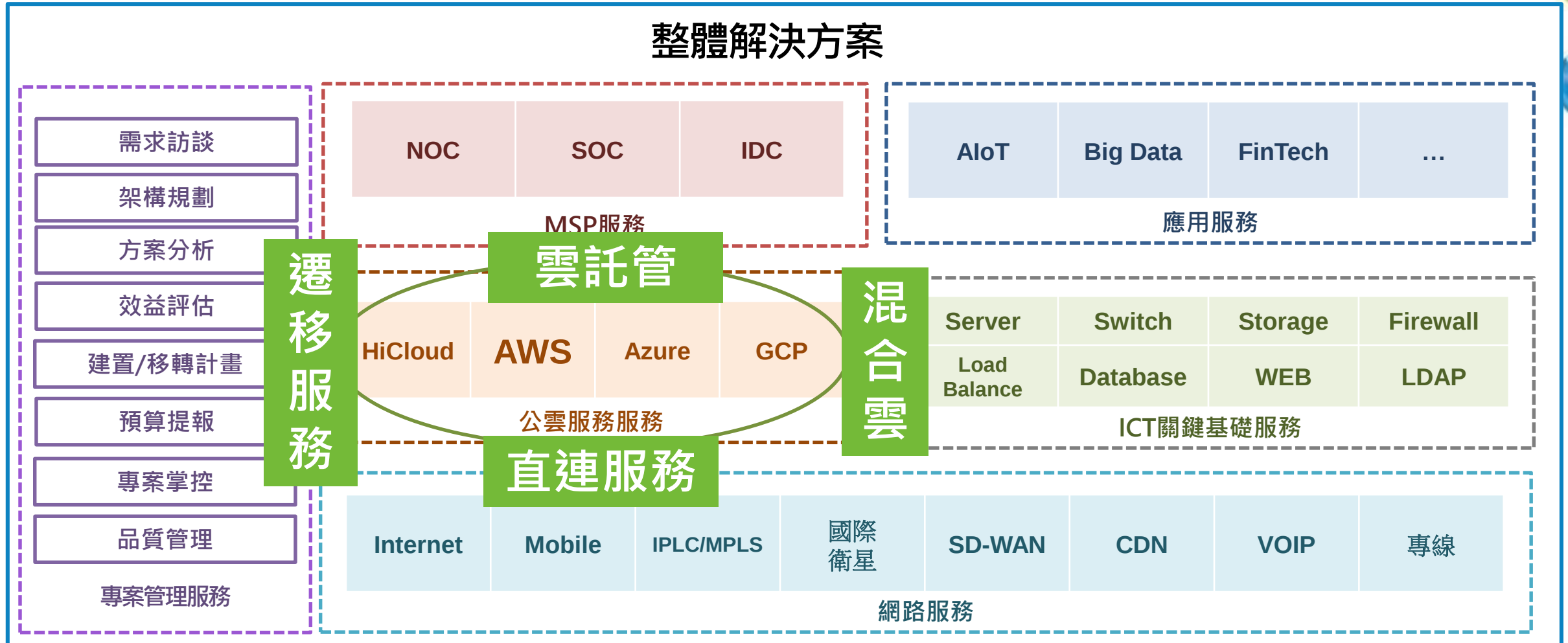
Revenue trends – AWS with a head start, Azure & GCP showing rapid growth



目前CHT全球資通訊服務

運用**公雲服務**、數據/國際網路、IDC、資安、增值應用等產品/服務，提供企業ICT整合解決方案。

整體解決方案



CHT雲網融合服務

在台灣已獲得超過百位客戶採用

aws ¹⁰⁰certified
AWS PARTNER NETWORK



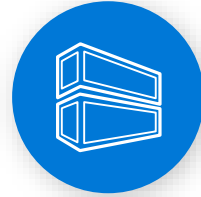
Migration

網站/資料庫
App
ERP
內部系統
..



AIoT

智慧製造
智慧交通
智慧路燈
智慧安防
..



Data analytic

客流分析
銷售預測
精準行銷
客戶標籤
購物推薦
..



DevOps

敏捷開發
版本管理
需求管理
持續交付
..



Security

網站防駭
弱點管理
稽核管理
資安代管
..



台灣唯一同時提供直
連及顧問服務公司

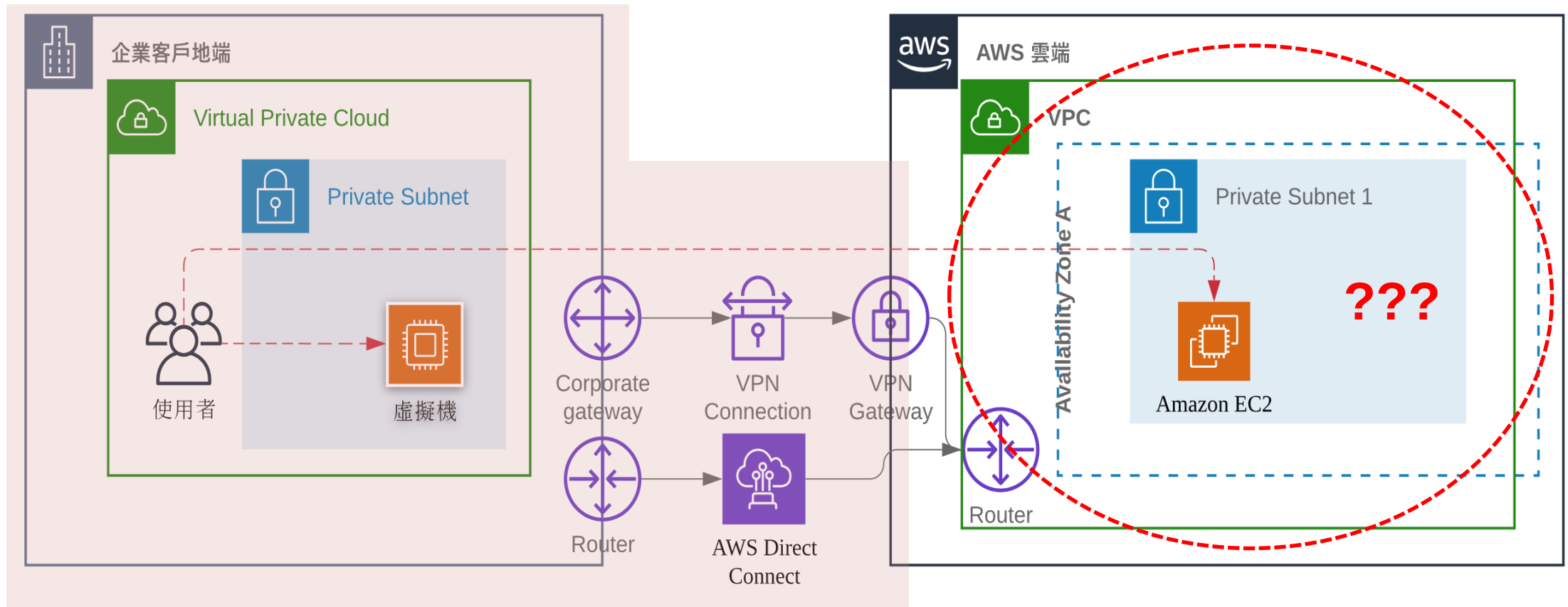
台灣唯一獲得AWS
IoT認證公司

金融、電信、產壽險、稅務、
電力、流通等領域專業分析，
具備超過100專業人力

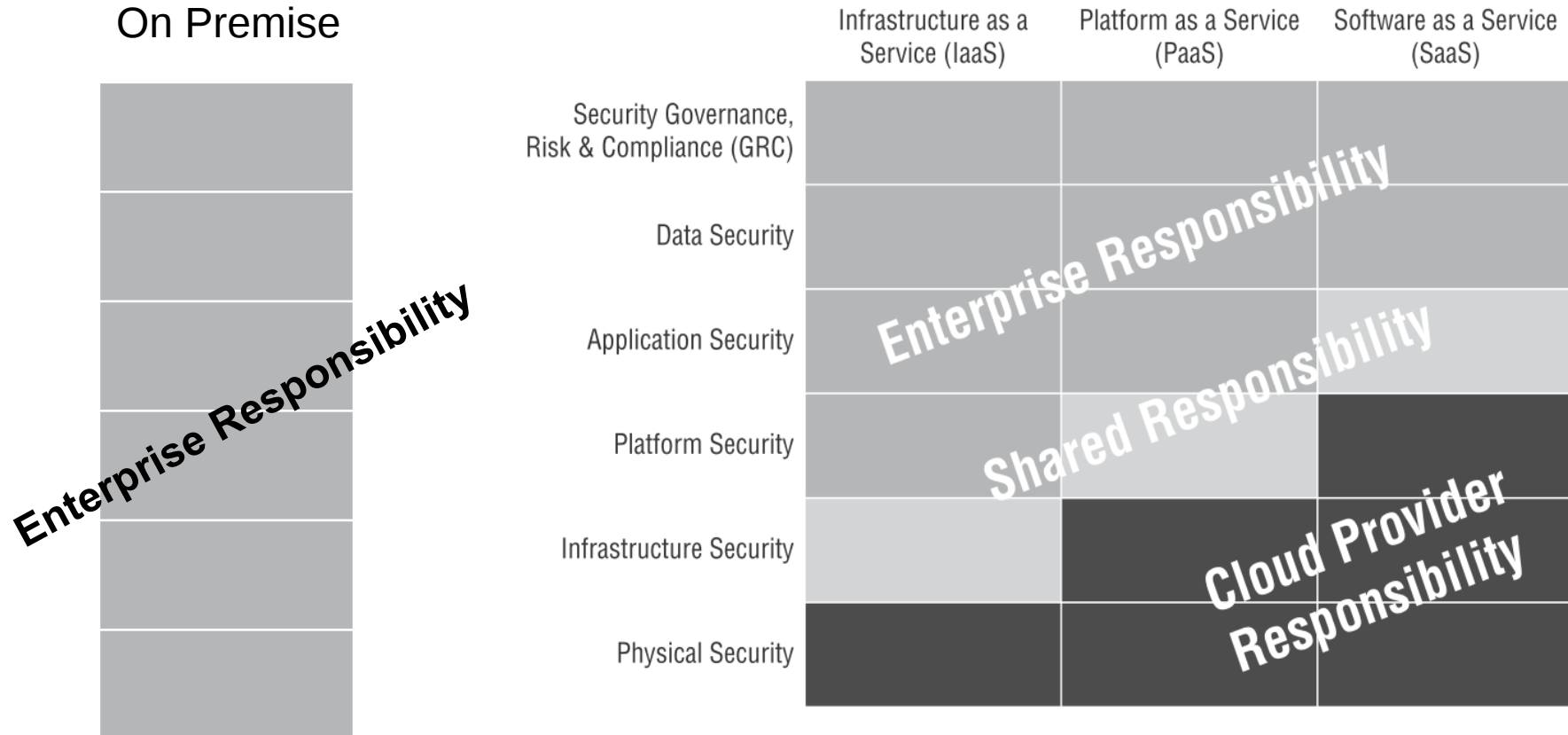
DevOps顧問團隊協助持
續整合及交付開發模式

超過100位認證架構師
協助實踐雲端最佳化

企業採用公雲後的防護邊界



共享責任模型



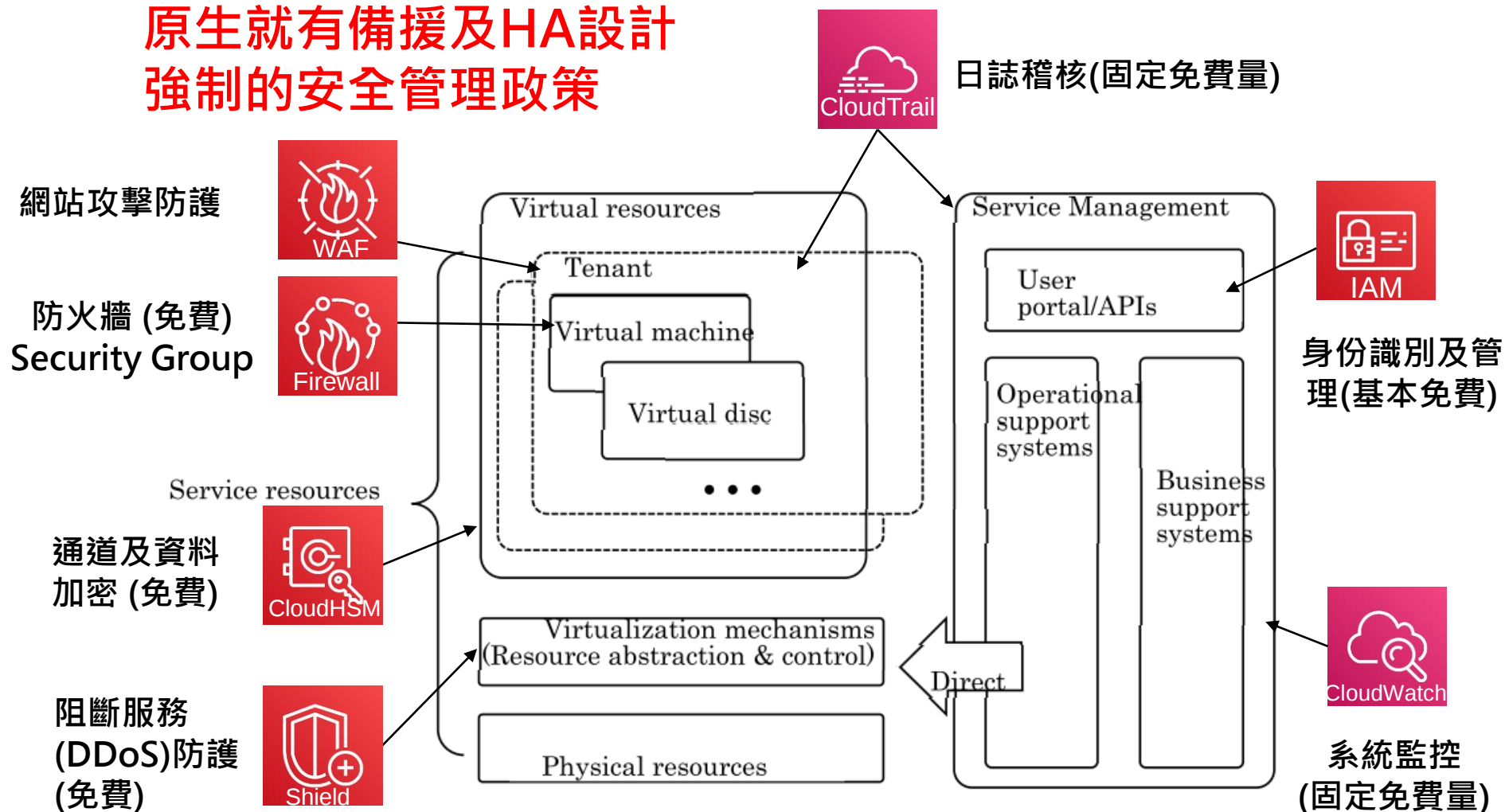
Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Azure AD, Google App Engine, Apache Stratos, OpenShift
IaaS	Amazon EC2 , Microsoft Azure VM, Google Compute Engine (GCE)

資料來源：Certified Cloud Security Professional Official Study Guide

Right to audit: ask provider for any and all audit reports you may have prepared for customers in order to satisfy your need for due diligence.

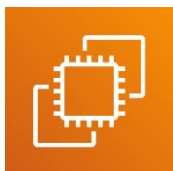
AWS用戶可直接使用的基本安全功能

原生就有備援及HA設計
強制的安全管理政策



NIST Cloud Architecture Model

AWS公雲服務資安功能



Amazon EC2 & EBS

- Guest OS run in CPU **Ring 1**
- **Firewall** (Security Groups) resides between physical and virtual NIC
- **Deny** by default
- EBS **replication**
- NIST 800-88 ("Guidelines for **Media Sanitization**")
- **Encrypted** EBS with **AES-256**



S3

- IAM Policies/ ACL
- Bucket Policies
- **Restricted** by default
- SSL encrypted endpoints
- **Encryption** at rest (exclude metadata)
- Access logs
- Data Durability and Reliability



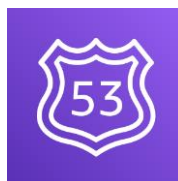
Amazon RDS

- Perform **backups**
- Handle **failover**
- **Maintain** database software
- ACL (**DB Security Groups**)
- IAM Policies



ELB

- **Encryption and decryption**
- Single point of contact
- Supports **E2E** encryption using TLS
- Having the originating client IP address



Amazon Route 53

- **Highly available**
- Scalable
- Health check for your website



CloudFront

- **Layer 3-4 Anti-DDoS**
- Support **private content**
- Access logs

And More....



AWS合規計劃

資安管理合規

全球



CSA
雲端安全聯盟控制



ISO 9001
全球品質標準



ISO 27001
安全管理控制



ISO 27017
雲端特定控制



ISO 27018
個人資料保護



PCI DSS 第 1 級
支付卡標準



SOC 1
稽核控制報告



SOC 2
：安全性、可用性和
機密性報告



SOC 3
一般控制報告

資料隱私權合規

亞太區域



澳洲資料隱私權



香港隱私權



印度資料隱私權



印尼資料隱私權



日本資料隱私權



韓國資料隱私權



馬來西亞資料隱私權



紐西蘭資料隱私權



菲律賓資料隱私權



新加坡資料隱私權



台灣資料隱私權

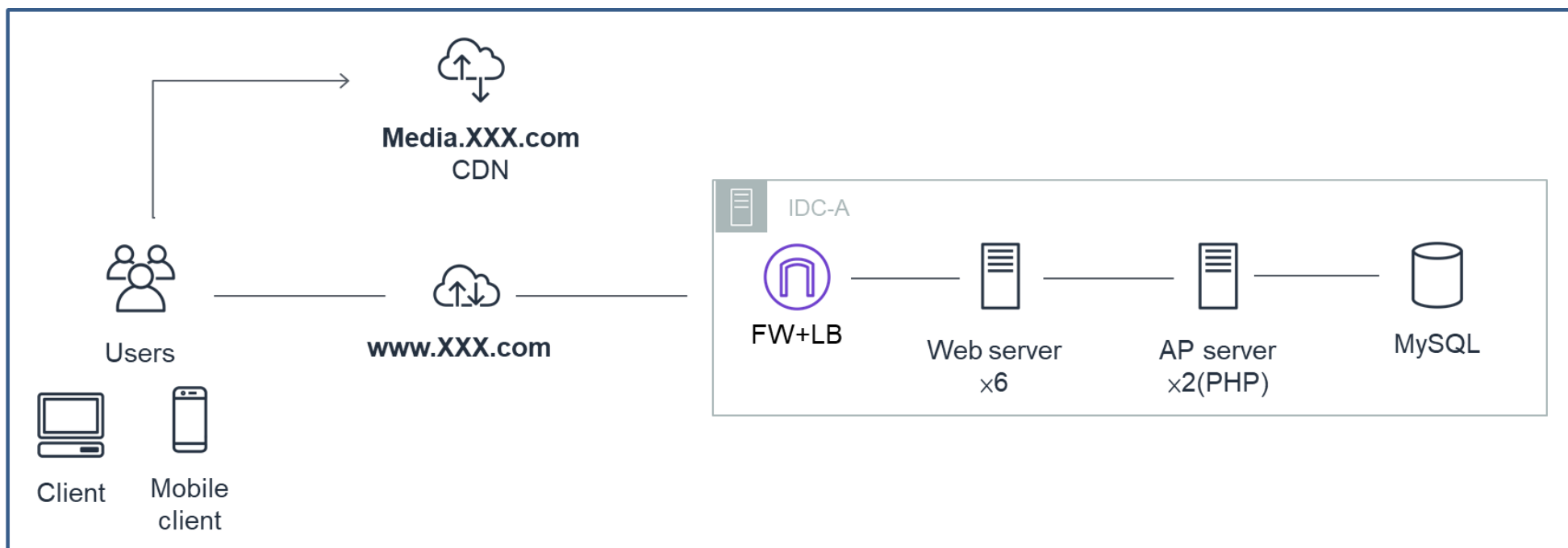


泰國資料隱私權

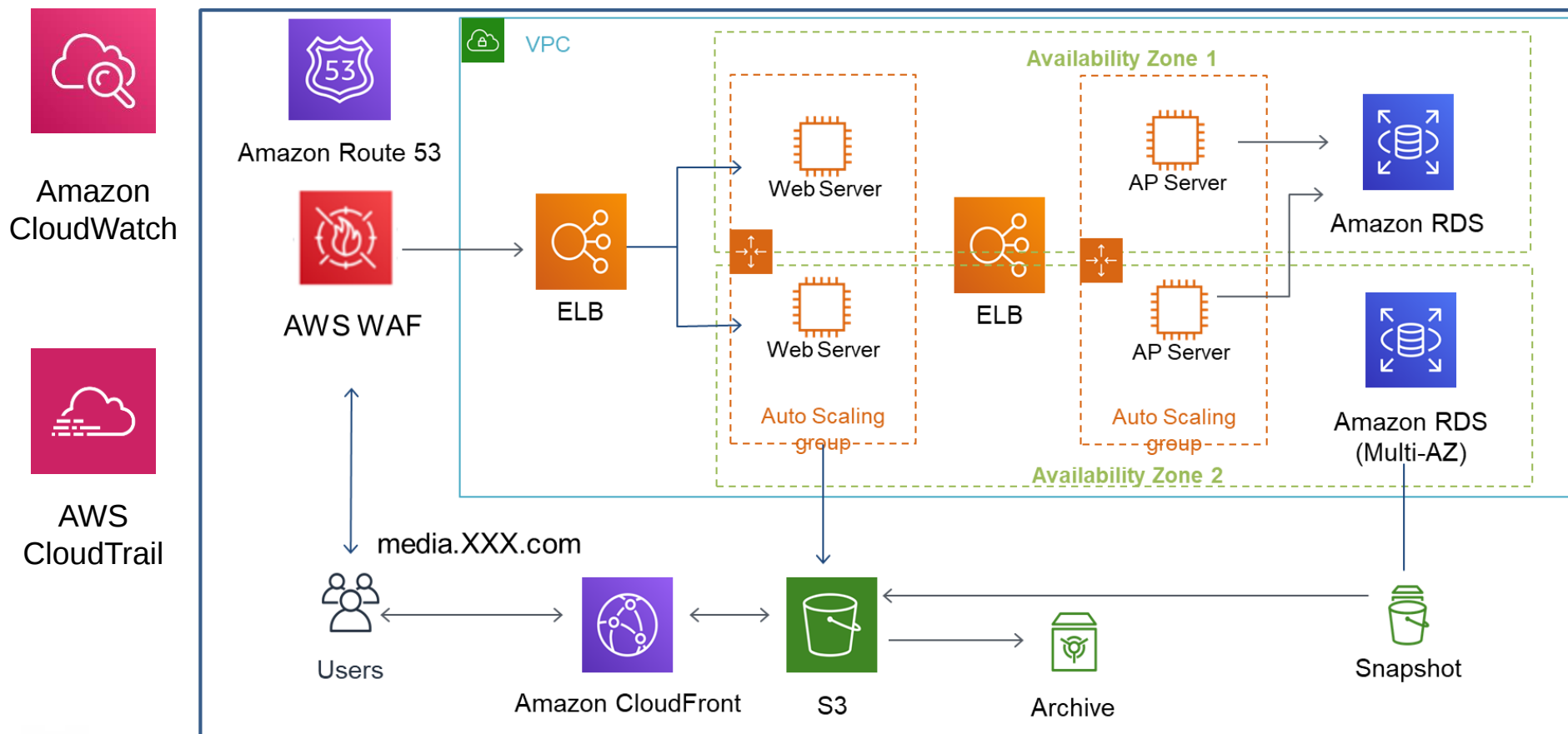
一個簡單的例子：DMZ遷移

瓶頸

- 資安攻擊頻繁
- 軟/硬體擴充一次性成本高
- 建置時程長
- 維運複雜度高

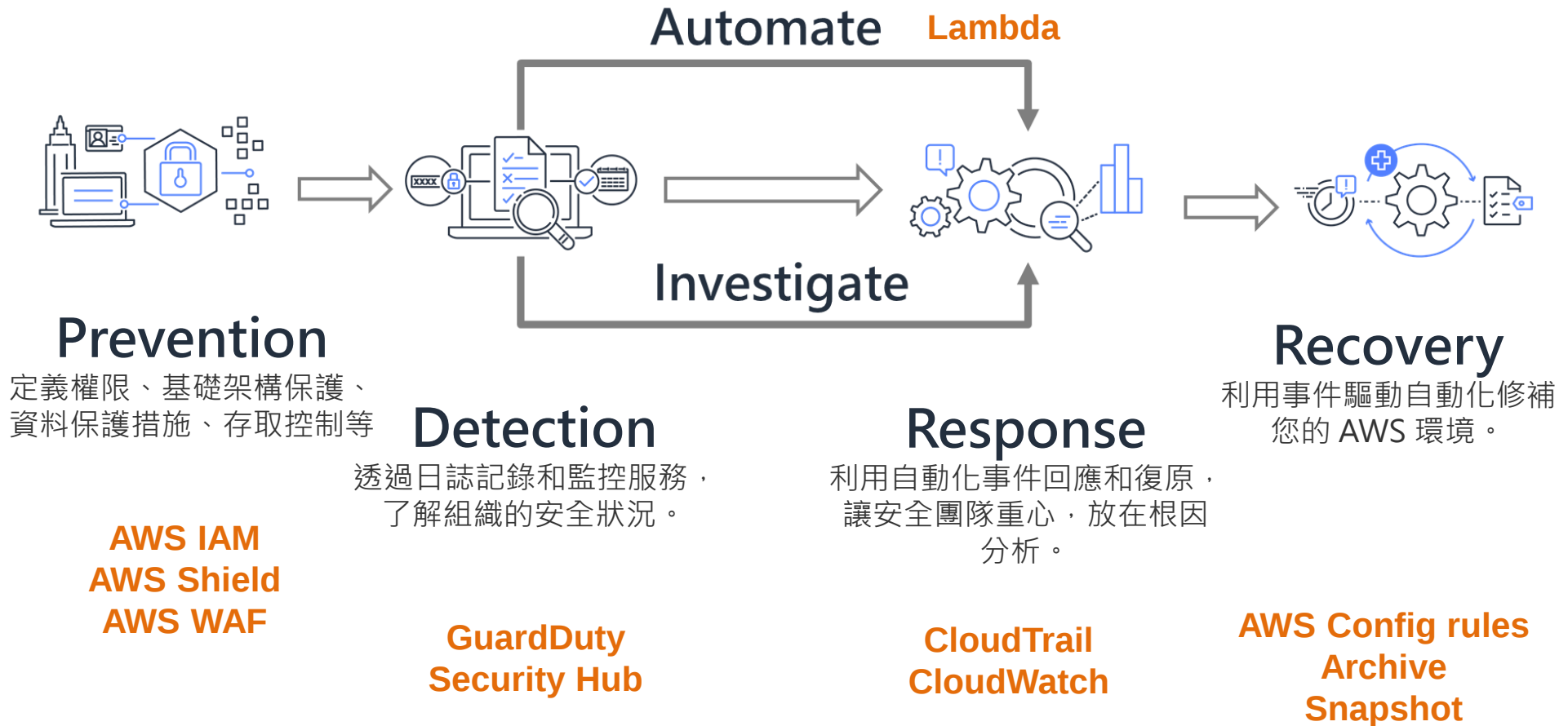


改採AWS後的DMZ架構設計



- 提升安全防護
- 可彈性擴展服務
- 降低成本
- 高可靠架構且維護工作降低60%

資安防護常用的工具



結語：AWS比大部分自建來的安全

公雲資安問題大多為Knowledge Gap

建置Landing zone

人員養成及培訓 (做中學)

資安防護、監控及事故復原自動化