永遠走在最前面
Always Ahead

混合雲應用趨勢及資安設計考量

劉順德

2019.10.31

中華電信
Chunghwa Telecom

自我介紹

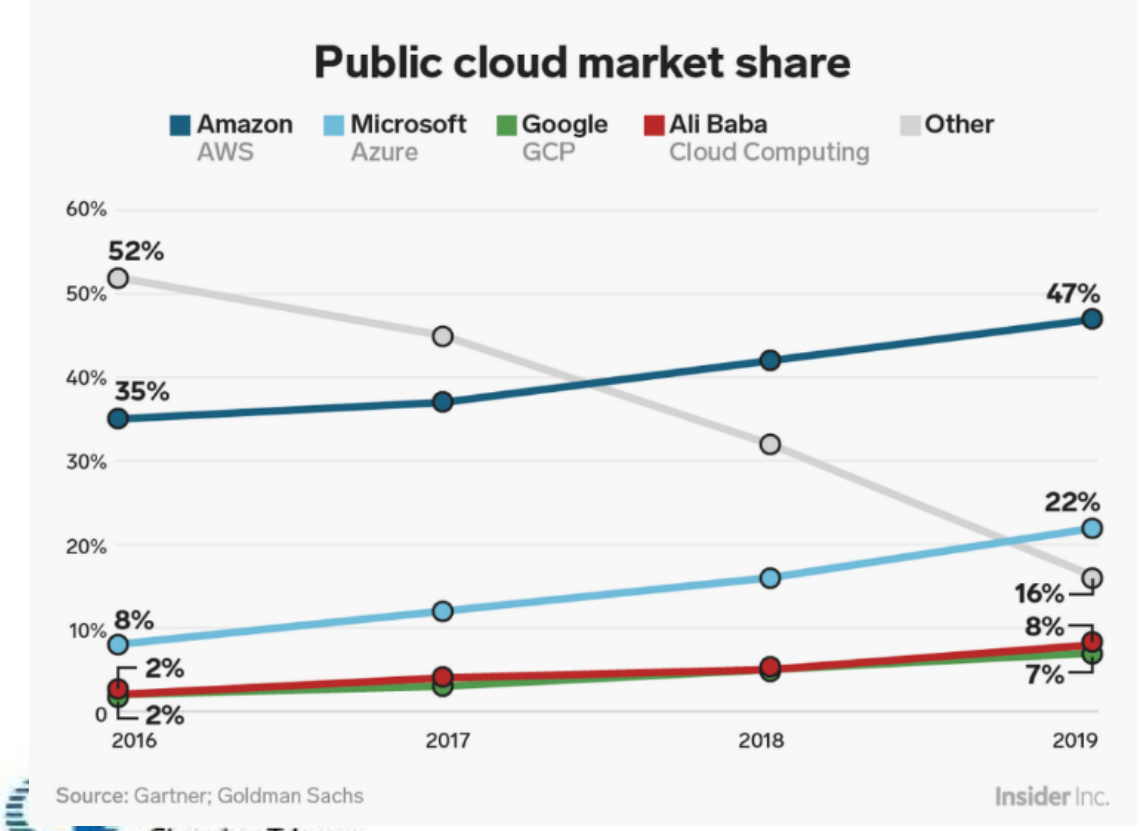
- 劉順德
- 現職：中華電信研究院資通安全研究所
- 學歷：中央大學資訊管理博士
- 經歷：
    - 中華電信大數據辦公室
    - 中華電信研究院資通安全研究所
- 專長：大數據/人工智能技術於新興資安威脅分析及資安事件分析等領域。
- 個人興趣：惡意檔案、網路攻擊偵測技術及大數據分析技術研究。
- rogerliu@cht.com.tw

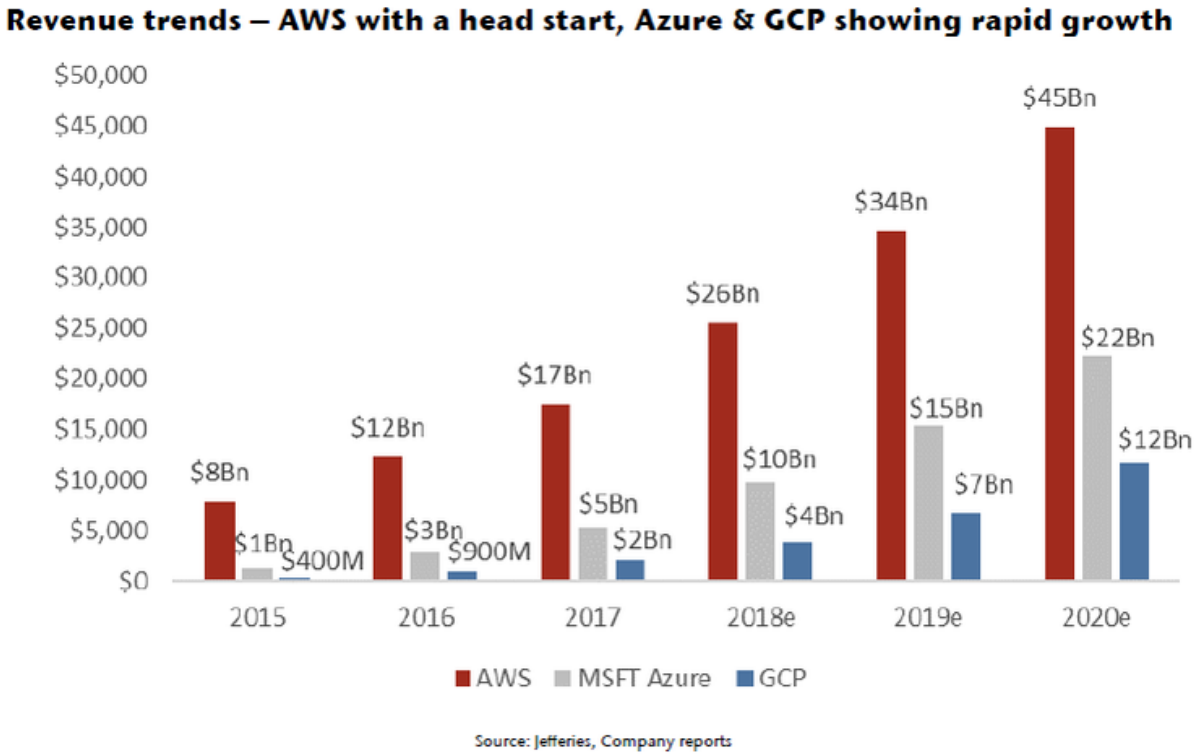
大綱

- 什麼是混合雲
- 公雲發展趨勢
- 企業為什麼使用公雲
- 混合雲架構設計考量
- 混合雲風險項目識別
- 混合雲監控架構設計
- 結語

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





2019國際技能競賽新職類：雲端運算

編號	職類名稱	職類名稱中譯
50	3D Digital Game Art	3D數位遊戲藝術
51	Freight Forwarding	船舶物流
52	Chemical Laboratory Technology	化學實驗室技術
53	Cloud Computing	雲端運算
54	Cyber Security	網路安全
55	Water Technology	水資源技術
56	Hotel Reception	旅館接待

2019年國際技能競賽新增正式職種列表。

台灣是全球資訊設備的重要供應基地之一，Amazon Web Service，Google Cloud Platform及Microsoft Azure三大公有雲供應商也視台灣為兵家必爭之地，相關人才需求也隨之上昇。但目前這個職類需要的技能，跟高中職的課程沒有交集，現有的國家技術士認證也還沒有相關的職類，全國技能競賽也還沒有對應的職類，因此，2019年台灣很難選派出選手，去參加這個新職類。

中華電信 Chunghwa Telecom

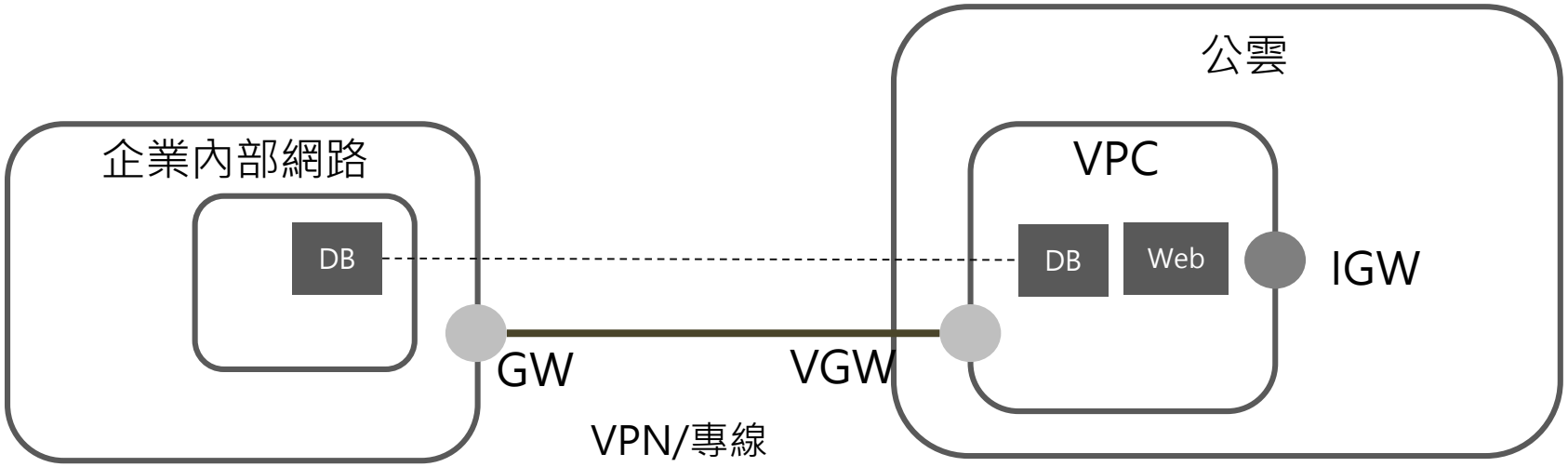
什麼是混合雲

- The cloud **infrastructure** is a composite of **two or more** distinct cloud infrastructures (Private, Community, or Public) that remain **unique** entities, but are bound together by standardized or proprietary technology that enables data and application portability

--NIST Cloud Computing Security Reference Architecture

混合雲應用場景

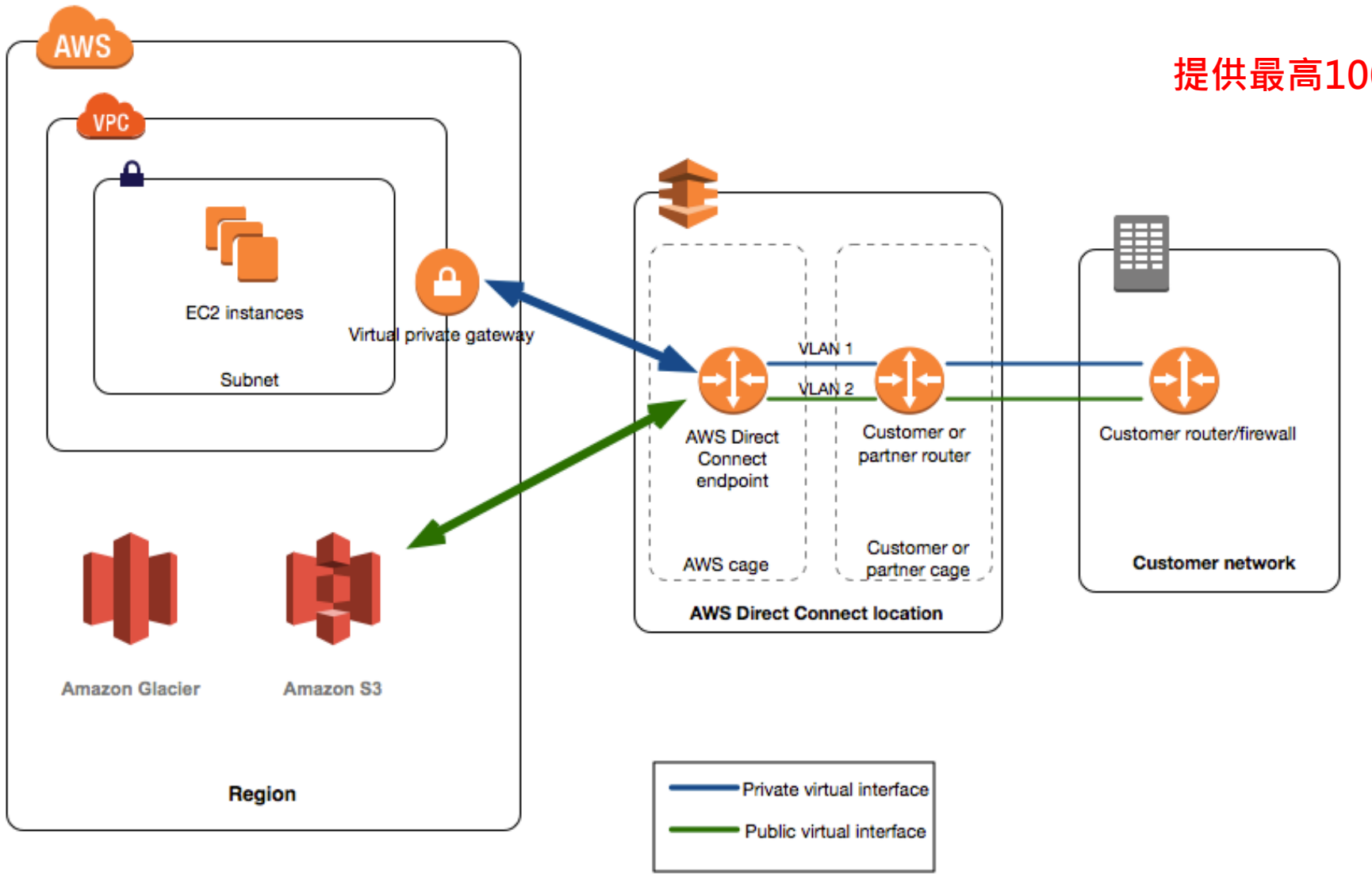
面向客戶的服務移到公雲，面向內部服務的保留在網企業內



GW: Gateway
VGW: Virtual Gateway
IGW: Internet Gateway
直連：AWS Direct Connect/ Azure Express Route/ GCP Interconnect

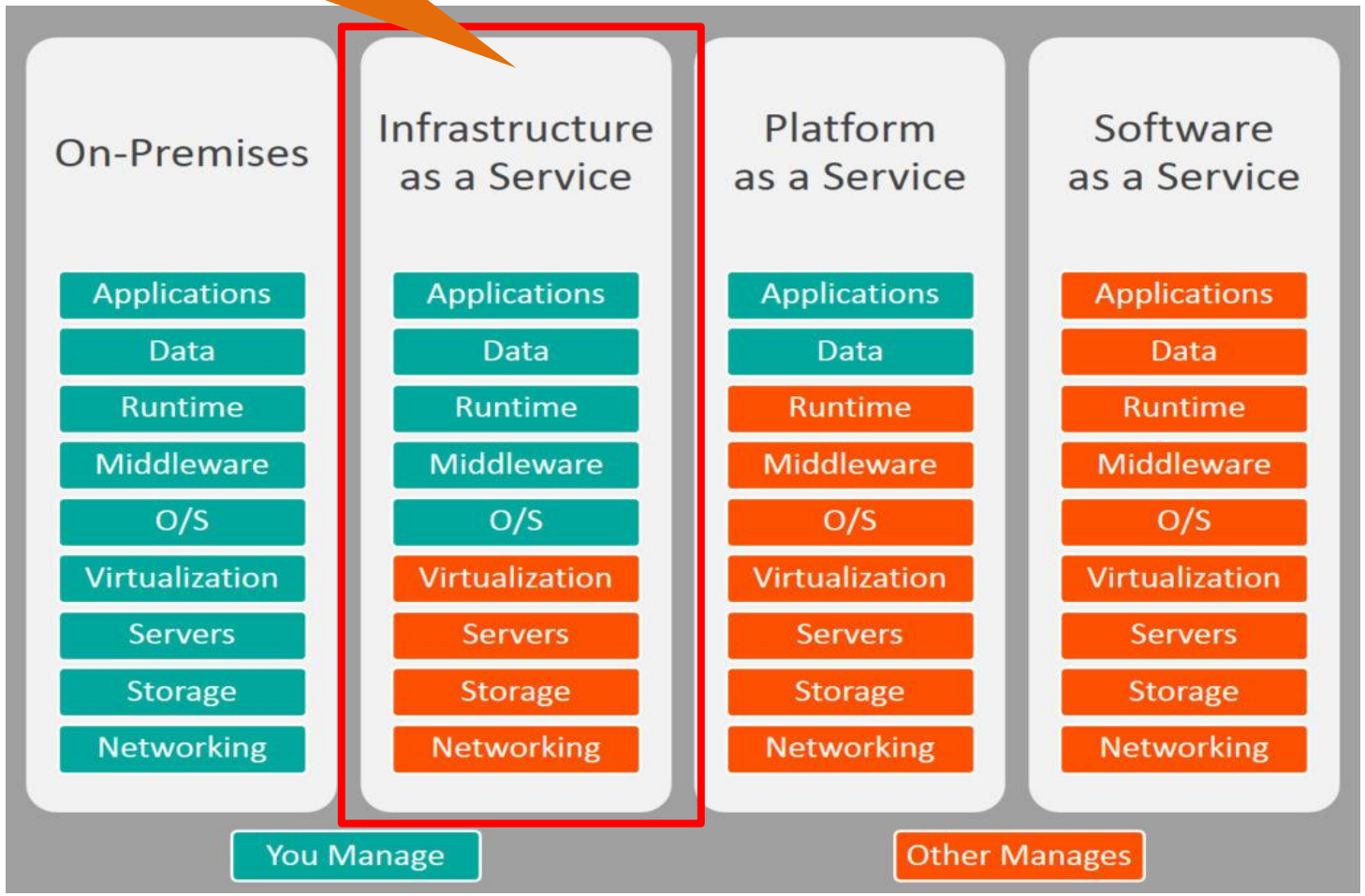
什麼是直連

提供最高100G頻寬



雲端服務類型比較

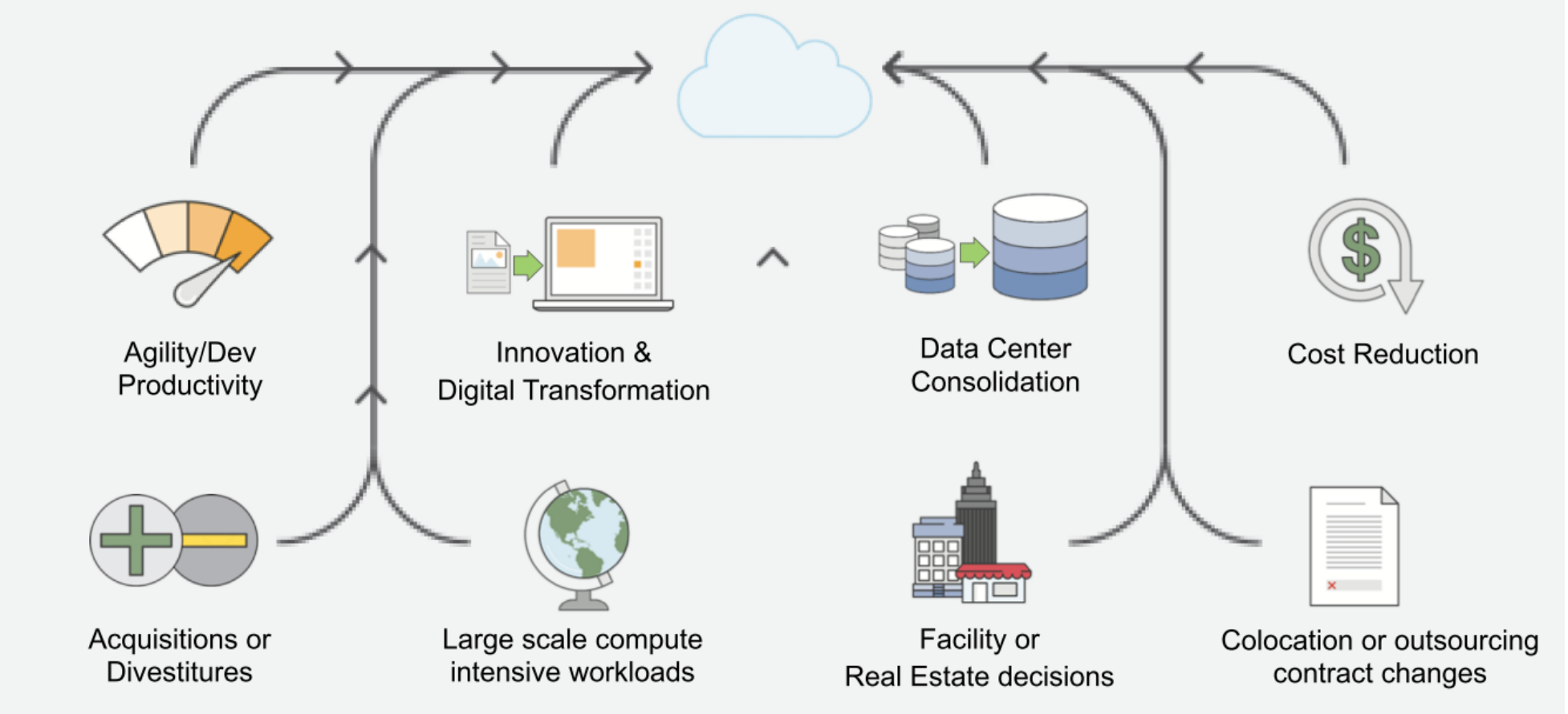
混合雲著重在IaaS



Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

資料來源：https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

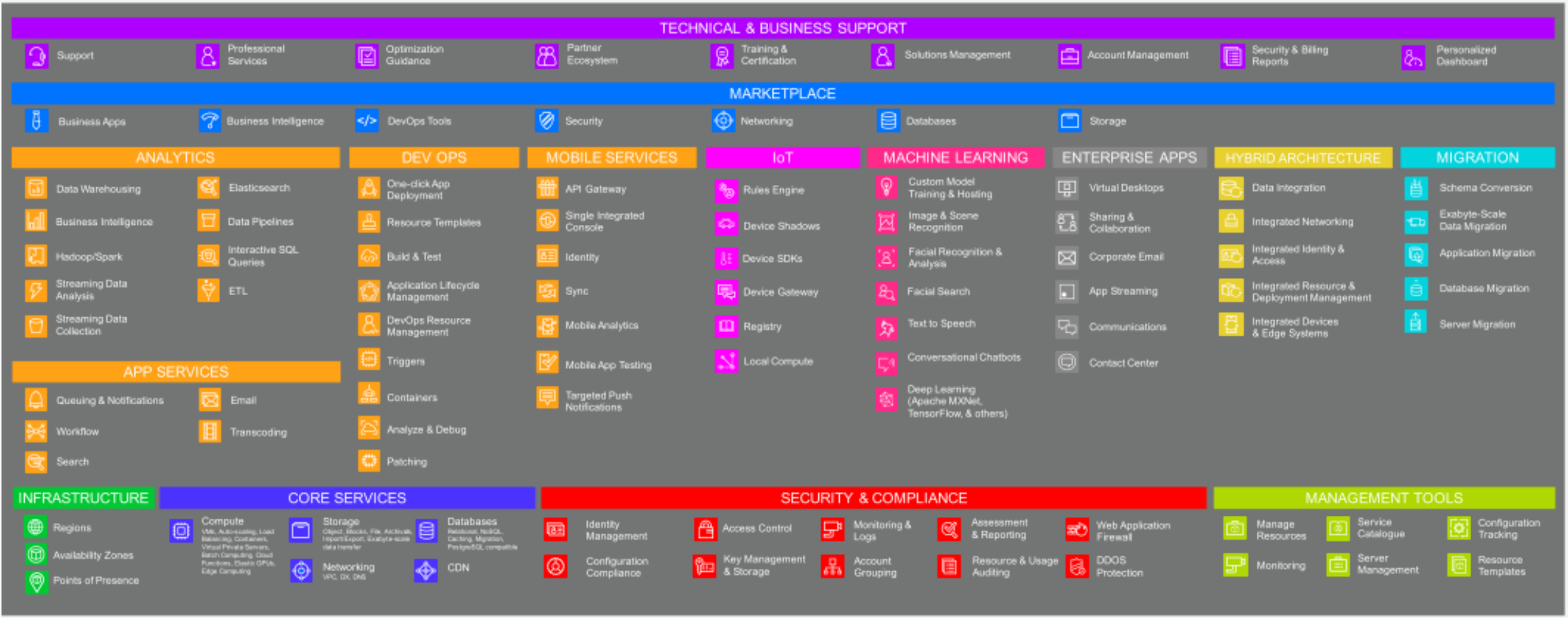
為什麼企業擁抱公雲


Agility/Dev
Productivity
Innovation &
Digital Transformation
Data Center
Consolidation
Cost Reduction
Acquisitions or
Divestitures
Large scale compute
intensive workloads
Facility or
Real Estate decisions
Colocation or outsourcing
contract changes

為什麼企業擁抱公雲-地端ICT產品在公雲都找的到

Tech Layer	On-Premise	AWS	Azure	GCP
Application	Office Exchange	WorkDoc WorkMail	Office 365	G Suite Google Map
Runtimes	IIS/Apache/Tomcat/Nginx MQ Hadoop	Lambda Beanstalk EMR	App Service CycleCloud	App Engine Cloud Pub/Sub Dataproc
Security & Integration	AD/LDAP Firewall/WAF/IDS/AV SIEM/VA/PT/IR Orchestration	IAM Cloudwatch GuardDuty System Manager	Azure AD Monitor Security Center Automation	Cloud Identity StackDriver Cloud Scanner Composer
Database	MS-SQL/PostgreSQL Hbase/MangoDB	Aurora/RDS DynamoDB	Azure SQL Cosmos DB	Cloud SQL BigTable
Server OS	Win server/Linux/..			
VMM	Vmware Docker/Kubernetes	EC2 Elastic Container	Virtual machine AKS	Compute Engine Kubernetes Engine
Virtual storage	SAN/NAS CIFS/NFS/SFTP/FTP	S3/EBS/EFS Glacier	Blob File Storage Backup	Cloud Storage Persistent Disk
Virtual network	DNS CDN Load Balance Router VPN/VLAN	Route 53 Cloudfront Elastic LB Direct Connect VPC	Azure DNS Azure CDN Load Balancer Express Route VPC	Cloud DNS Cloud CDN Cloud LB Cloud Interconnect VPC

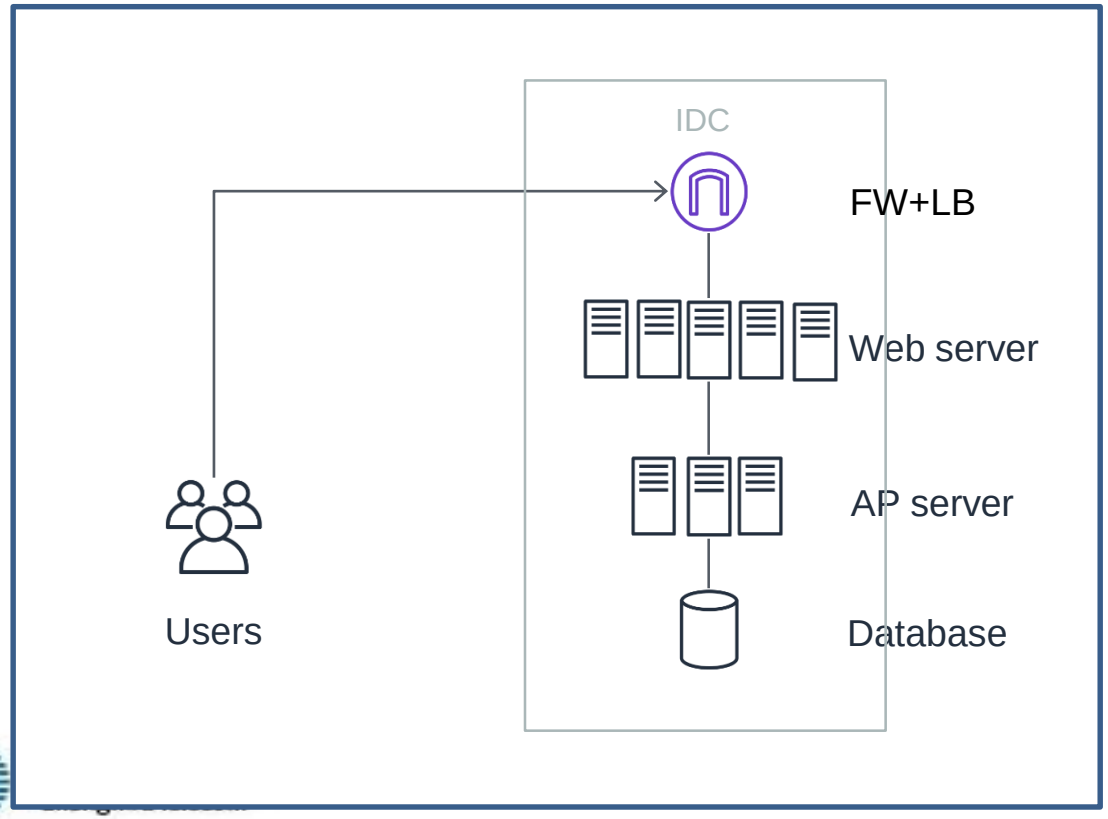
公雲的產品組合—以AWS為例



混合雲實例

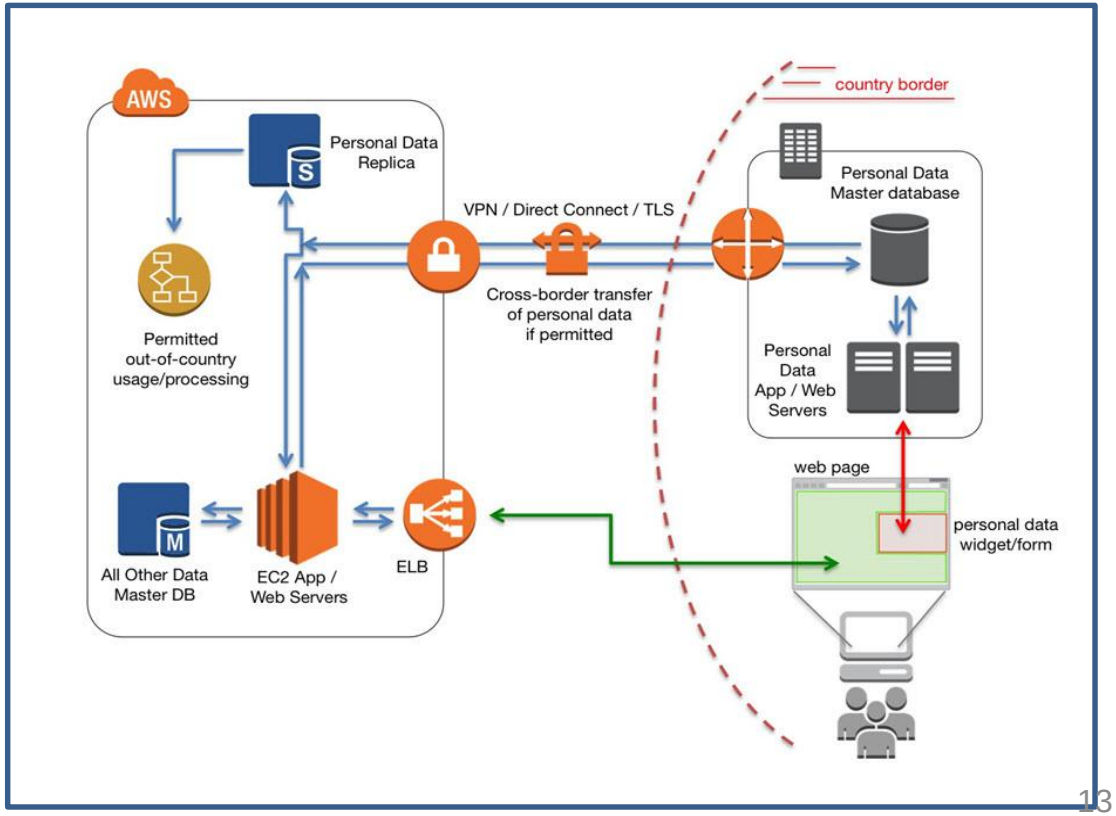
瓶頸

- 客戶流量變動無法即時滿足
- DR Site建置成本高
- 機敏資料

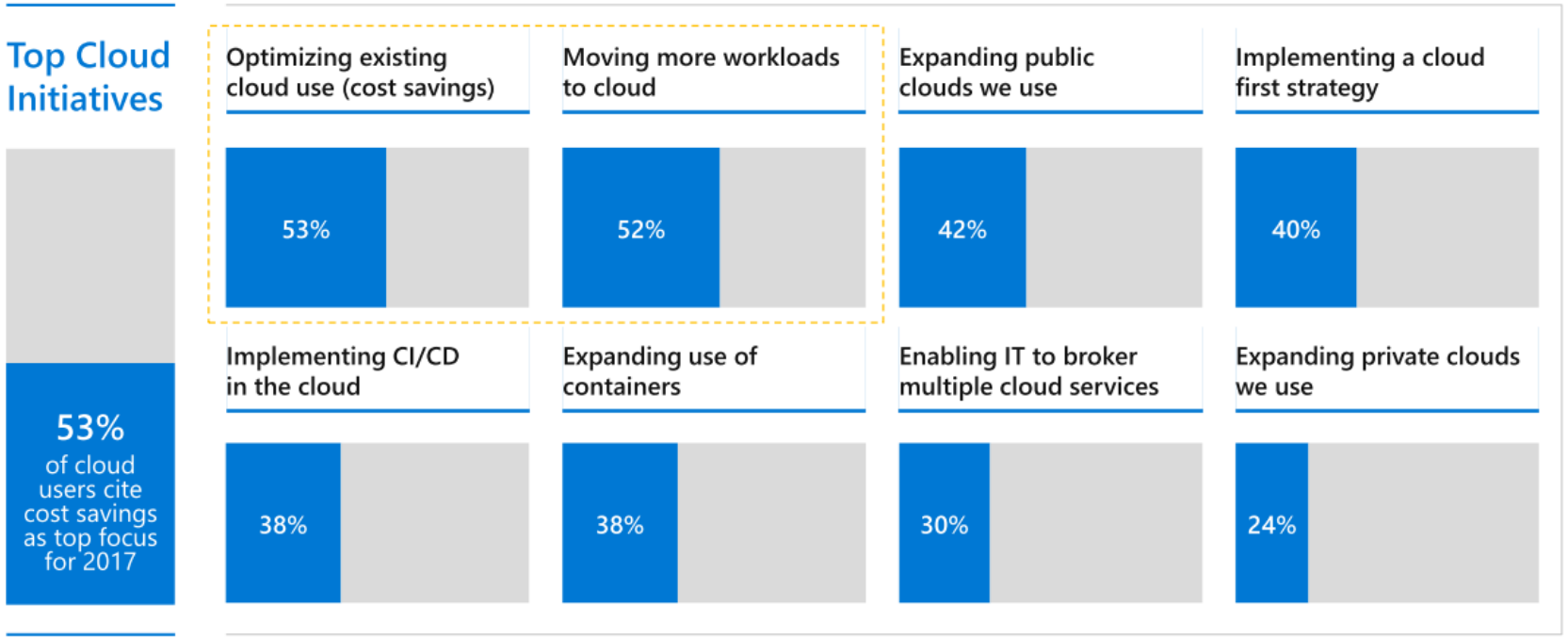


效益

- Autoscaling即時滿足所需運算資源
- 個資落地，非機敏資料上雲
- 使用Direct Connect即時備份大量資料



為什麼企業擁抱公雲-提高交付效率及降低總成本

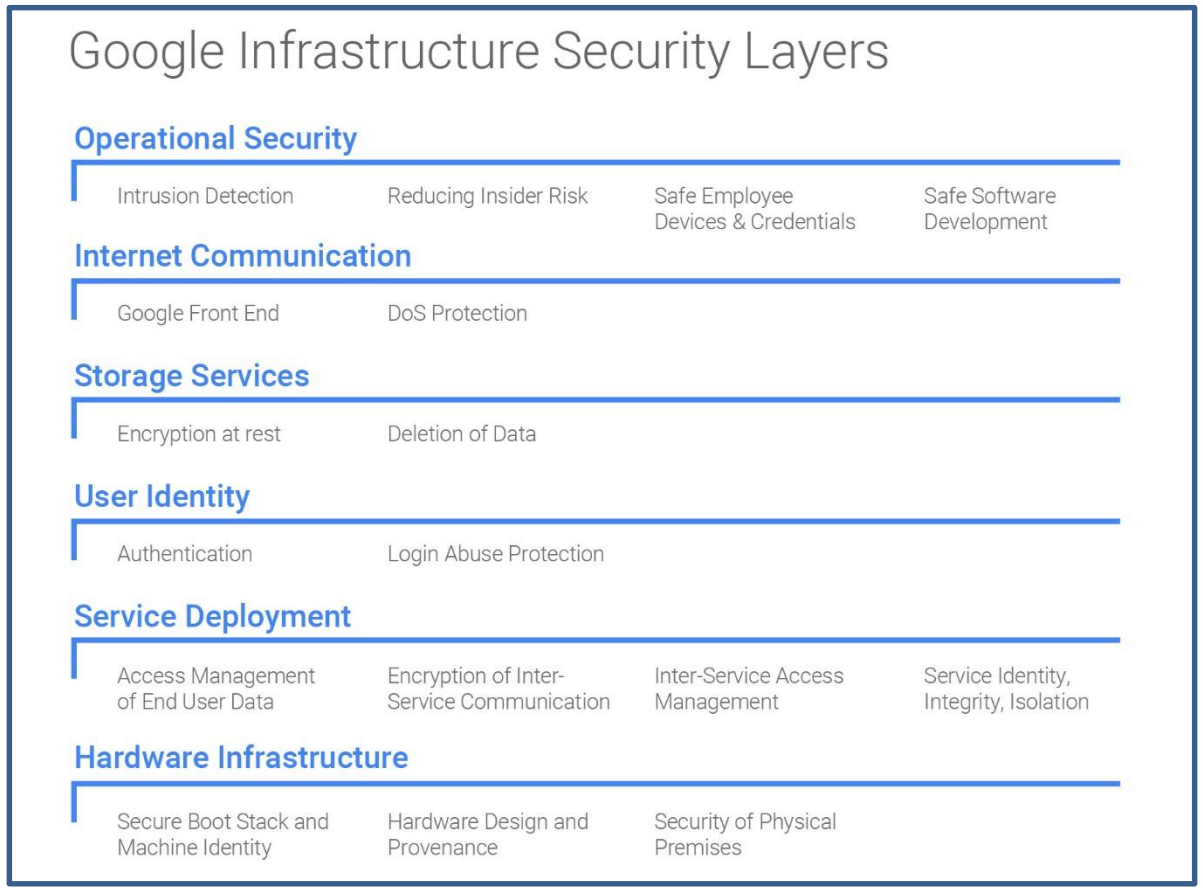


- **自建隱藏成本**
  - 安裝/維護人力
  - 電費、空間
- **雲端隱藏成本**
  - 人員訓練
  - 網路頻寬
  - 系統監測
  - 資安服務

以我們的例子，平均可降低30~50%

為什麼企業擁抱公雲-公雲比大部分自建來的安全

以GCP為例

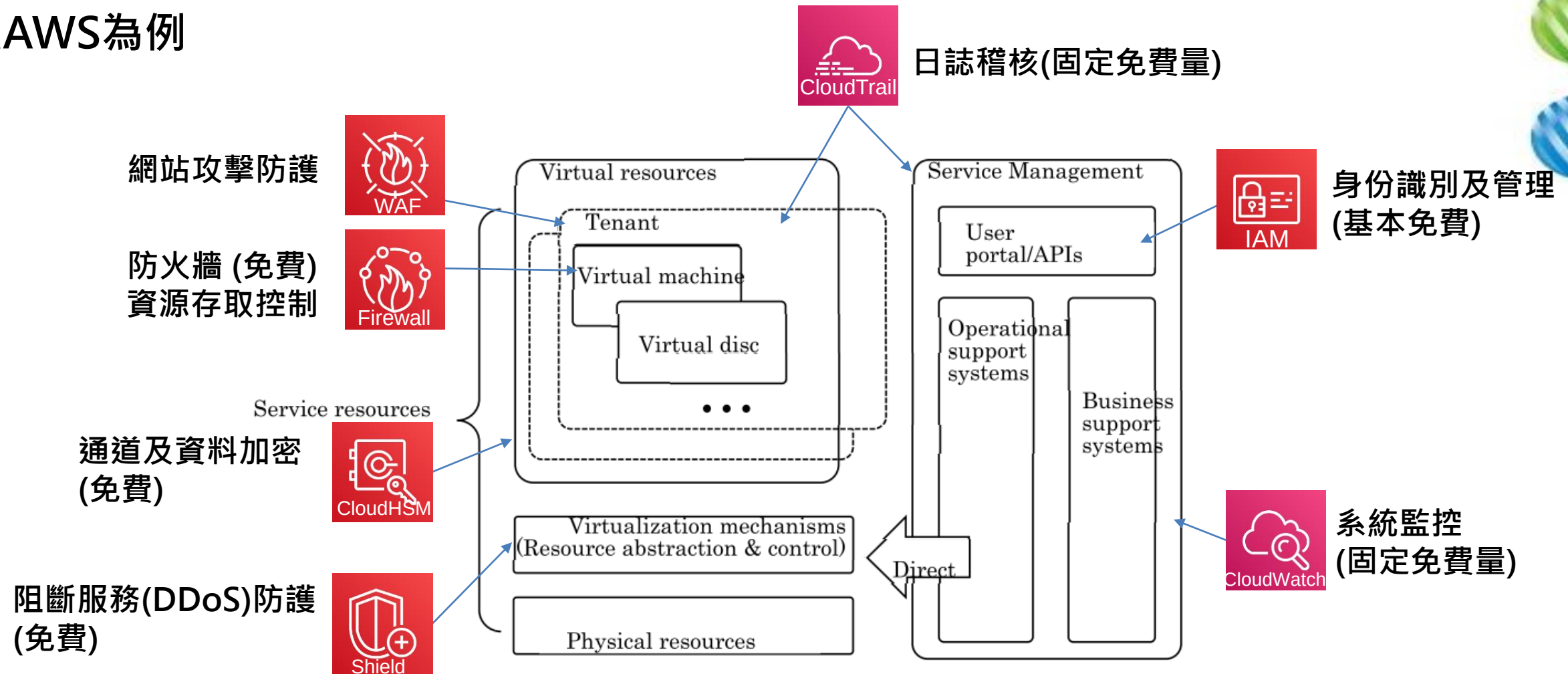


- 強制的安全管理政策
- 定期入侵檢測
- 多層次的DoS防護
- 硬碟加密及生命週期管理
- 多因子認證/非法登入防護
- 服務識別 / 加密通道 / 隔離
- 具身份的伺服器硬體
加密及簽章過的啟動流程

異地備援/HA架構

為什麼企業擁抱公雲-用戶可直接使用的安全功能

以AWS為例



NIST Cloud Architecture Model

中華電信 Chunghwa Telecom

為什麼企業擁抱公雲-用戶選擇的安全服務

以Azure為例

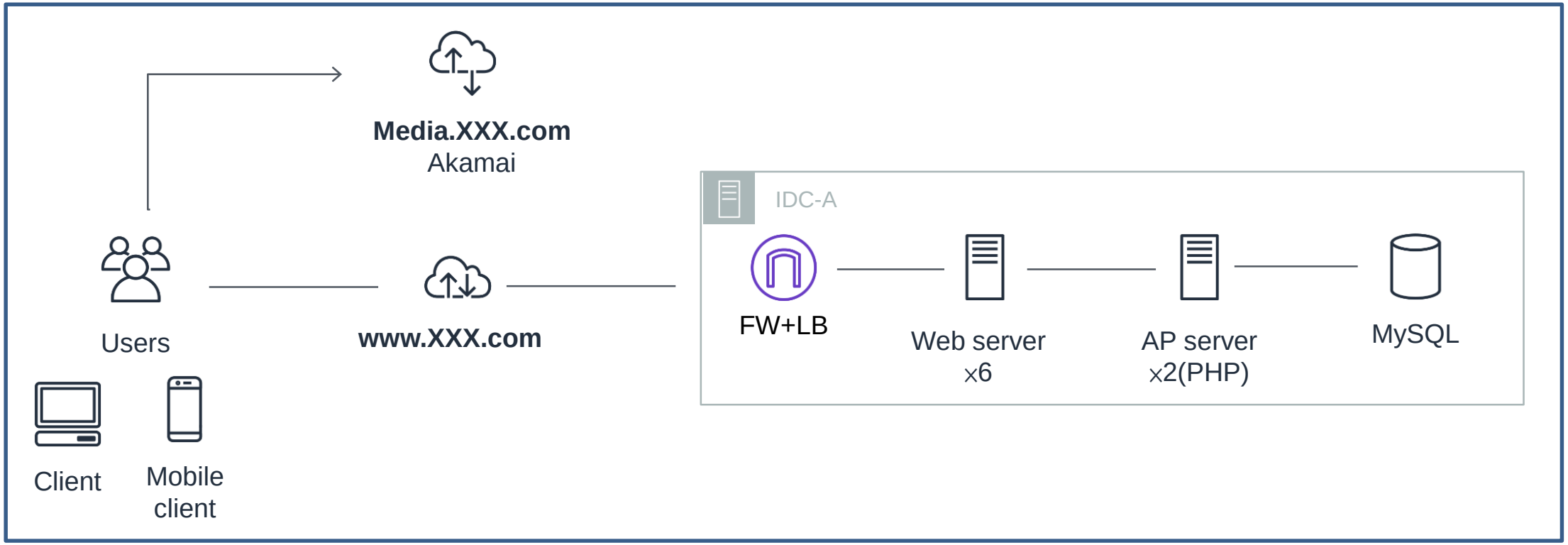
MSFT 信任中心	Azure 安全性合作夥伴	網路安全性諮詢
滲透測試	Azure 資訊安全中心	Azure 金鑰保存庫
磁碟加密	Azure 資訊保護	多重要素驗證 (MFA)

中華電信 Chunghwa Telecom

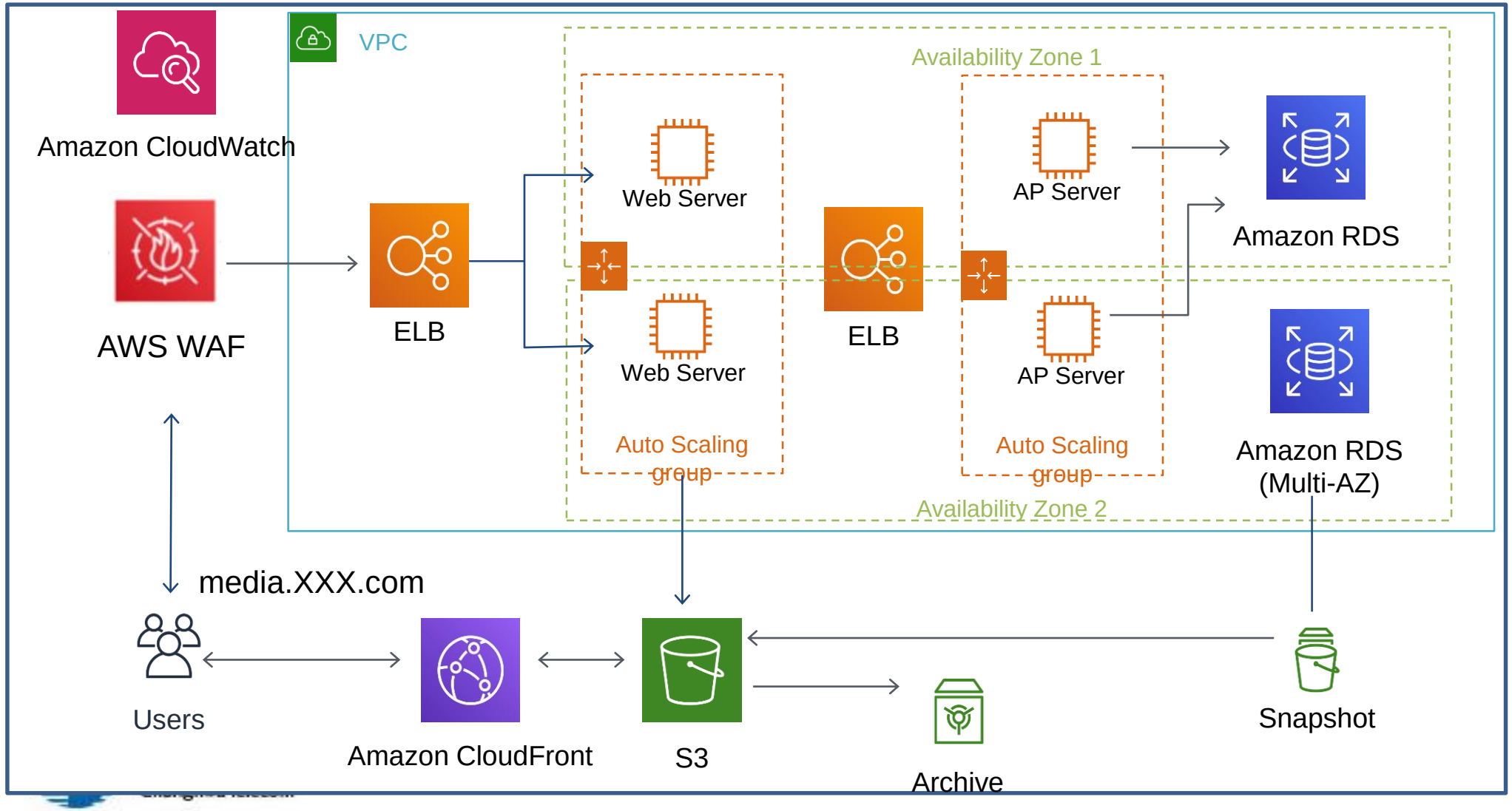
DMZ遷移：現行架構

瓶頸

- **面對未來需求成長，軟/硬體擴充一次性成本高且建置時程長**
- **DB維運複雜度高**
- **資安攻擊頻繁**



DMZ遷移：改採AWS後的架構設計



效益

- Cost down
- High Availability
- Scaling
- Secure

Cloud Customer Journey

Migrate | **Application modernization** | **SaaS**

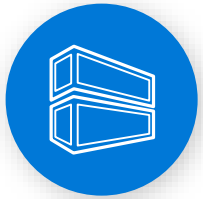
Rehost | Refactor | Rearchitect | Rebuild | Replace

On-Premises

Infrastructure platform

IaaS

Infrastructure platform
"lift & shift"



Containers

Managed container platform

PaaS/Serverless

Application platform

SaaS

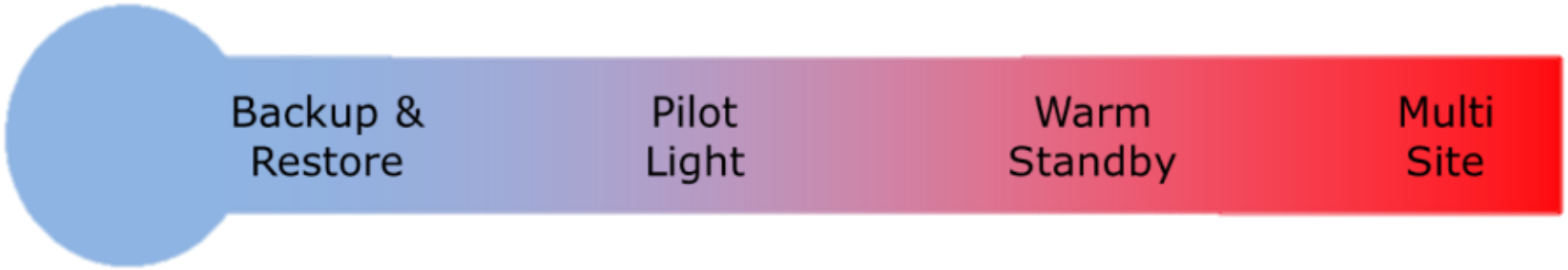
備援、面向客戶系統、DMZ、臨時專案、代管子公司系統

大數據處理、AI服務、IoT系統、資料交換

中華電信 Chunghwa Telecom

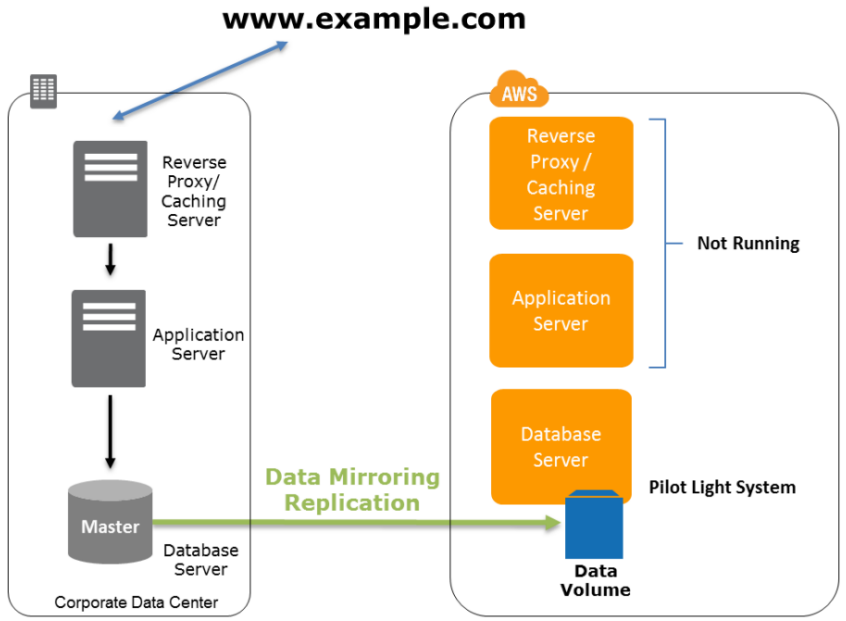
Example: Disaster Recovery Options

- How **quickly** a system can be available to users (RTO)
- How much the **amount of data** that can be lost (RPO)
- **Cost-effectively** operate each of DR strategies

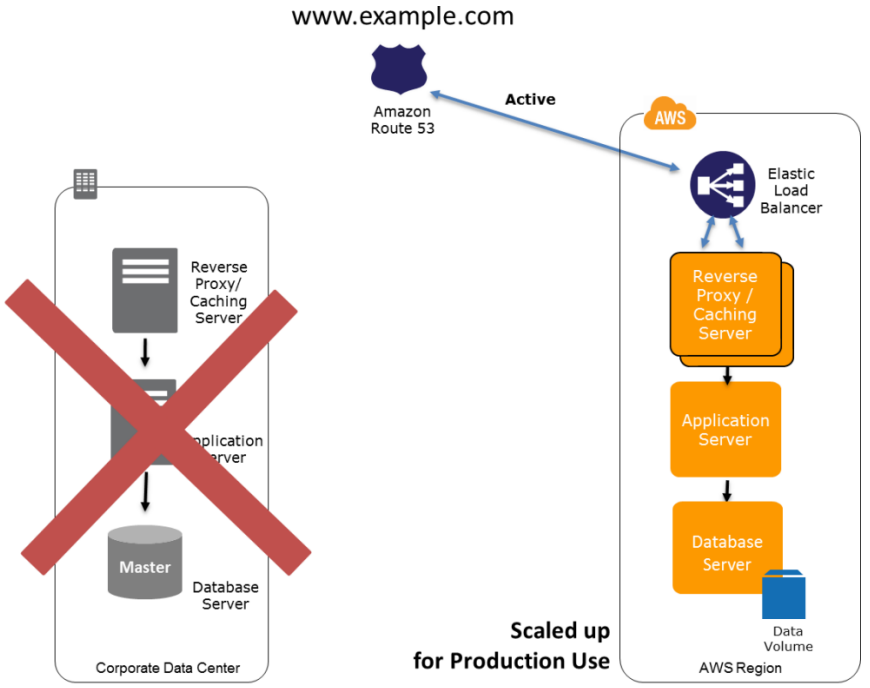


Pilot Light

Focus on database replication



1. Setup EC2 instances to replicate or mirror data
2. Create and maintain AMIs of key servers
3. Regularly test
4. Automating the provisioning



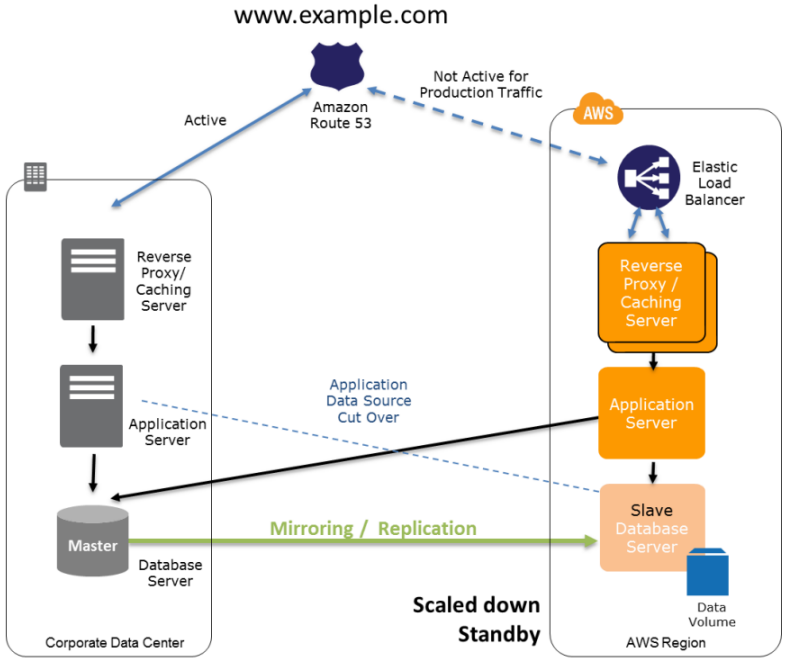
1. Start EC2 instances from custom AMIs.
2. Resize existing database/data store instances
3. Add additional database/data store instances (DR site resilience)
4. Change DNS to point at EC2 servers.
5. Install and configure any non-AMI based systems

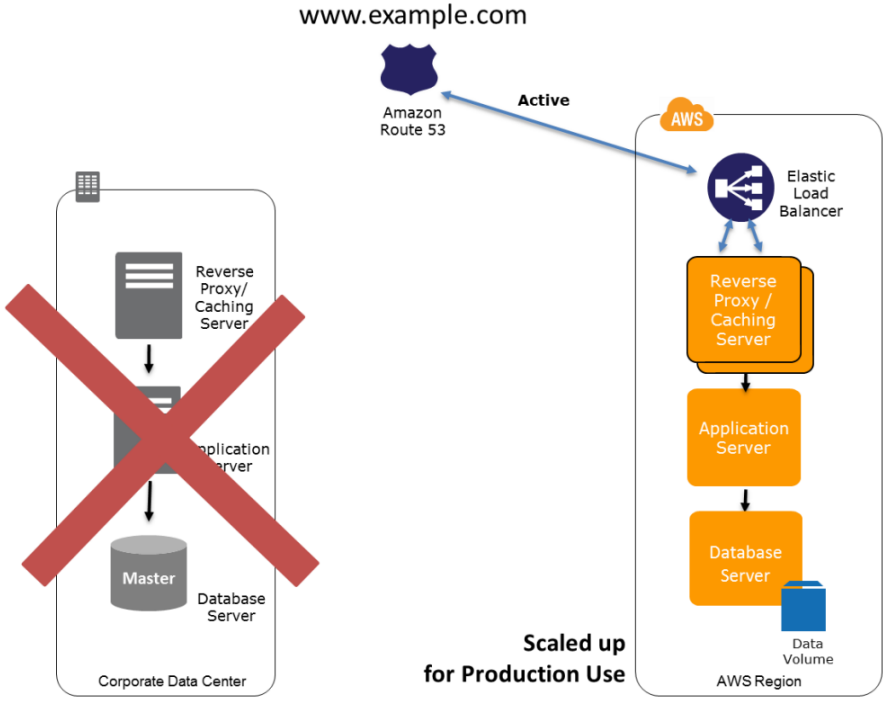
中華電信 Chunghwa Telecom

資料來源：Using Amazon Web Services for Disaster Recovery

Warm Standby

Fully duplicate systems (Active-Standby)





1. Set up EC2 instances to replicate or mirror data.
2. Create and maintain AMIs.
3. Run your application using a minimal footprint of EC2
4. Patch and update software and configuration files in line

1. Increase the size of EC2 fleets in service with the load balancer (horizontal scaling).
2. Either manually change the DNS records, or use Amazon Route 53 automated health checks
3. Add resilience or scale up your database.

資料來源：Using Amazon Web Services for Disaster Recovery

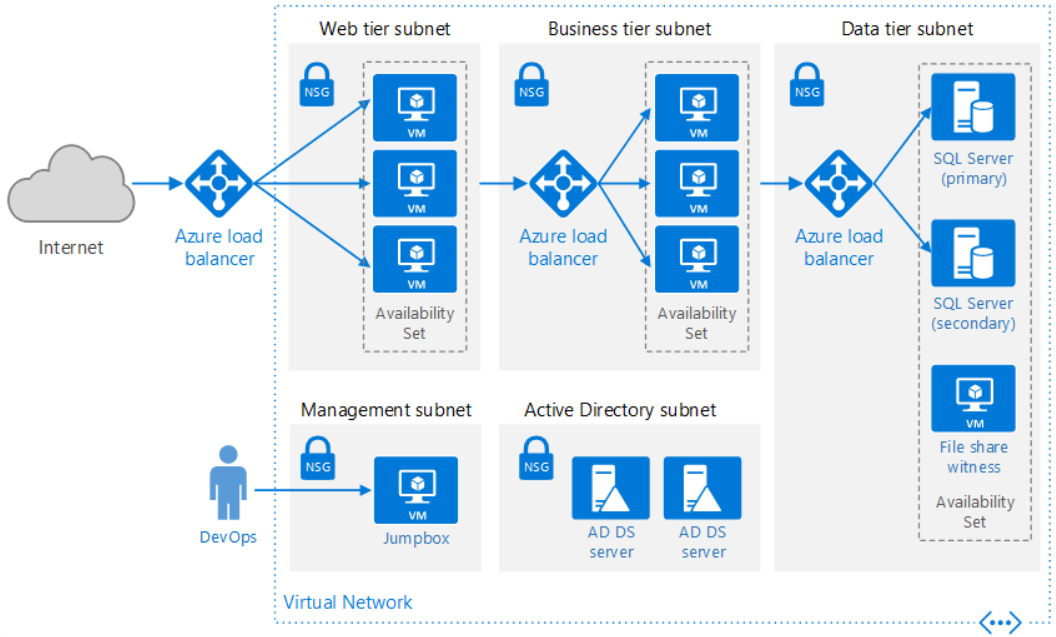
如何才能享受PaaS的優點

優點

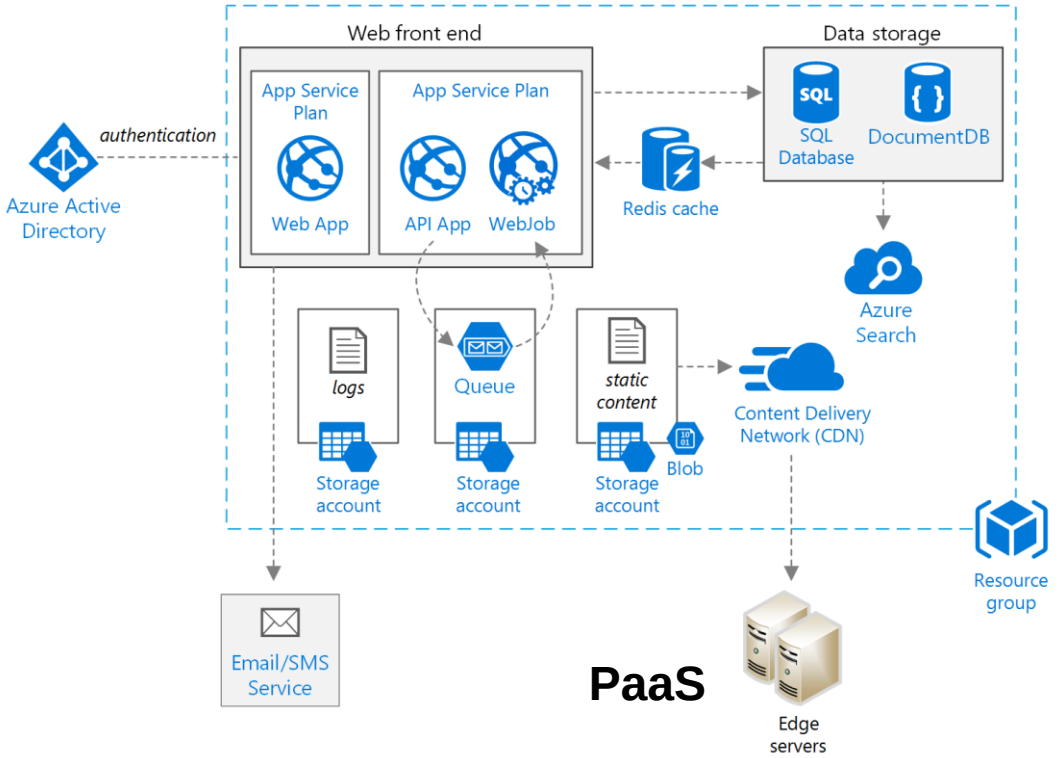
- 軟體自動更新
- 全代管的資料庫
- 作業系統自動更新(無作業系統)
- 快速擴展服務及備援

條件

- 自主開發能力
- Micro service設計
- DevOps/SRE管理機制
- 自動化工作流程



IaaS



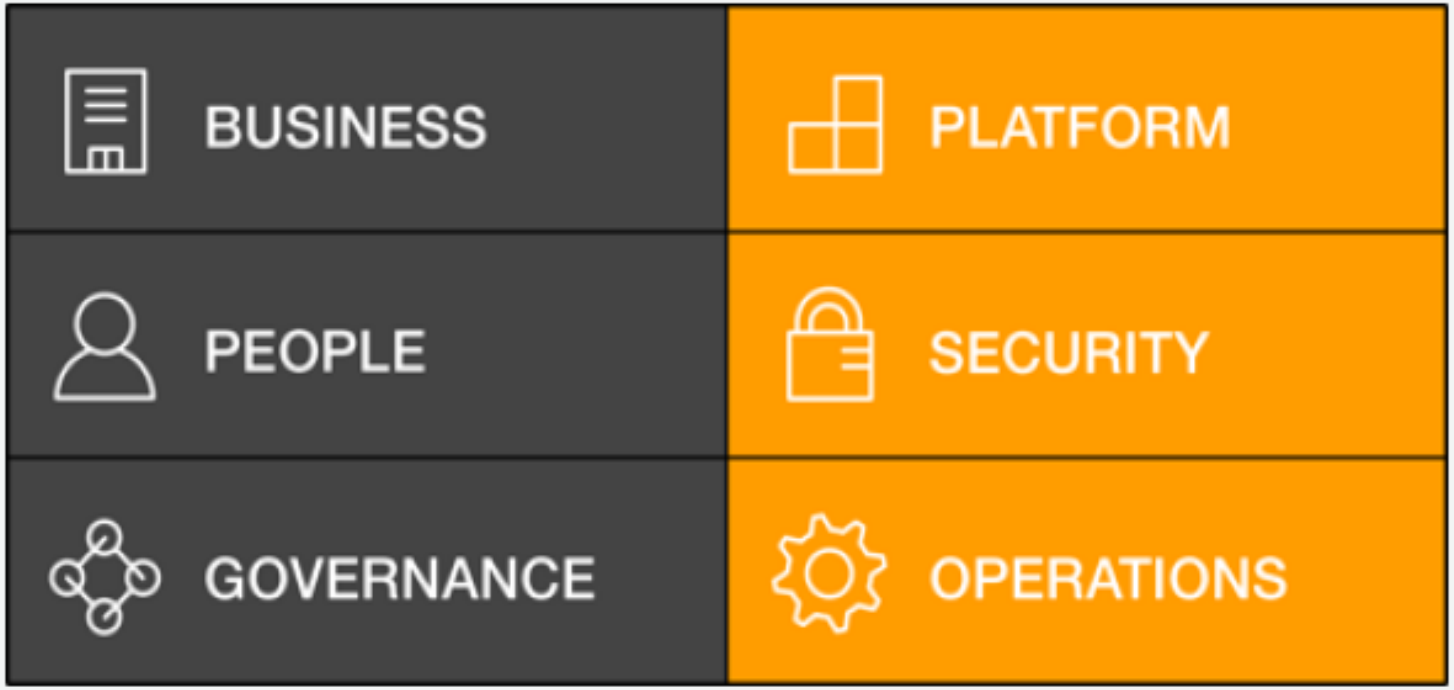
PaaS

遷移至雲端的6個注意

- 資源使用的彈性
- 多用戶使用情境
- 混合維運
- 軟體授權
- 無法預期的環境
- 符規

混合雲資安設計考量

採用Cloud的6個考量面向

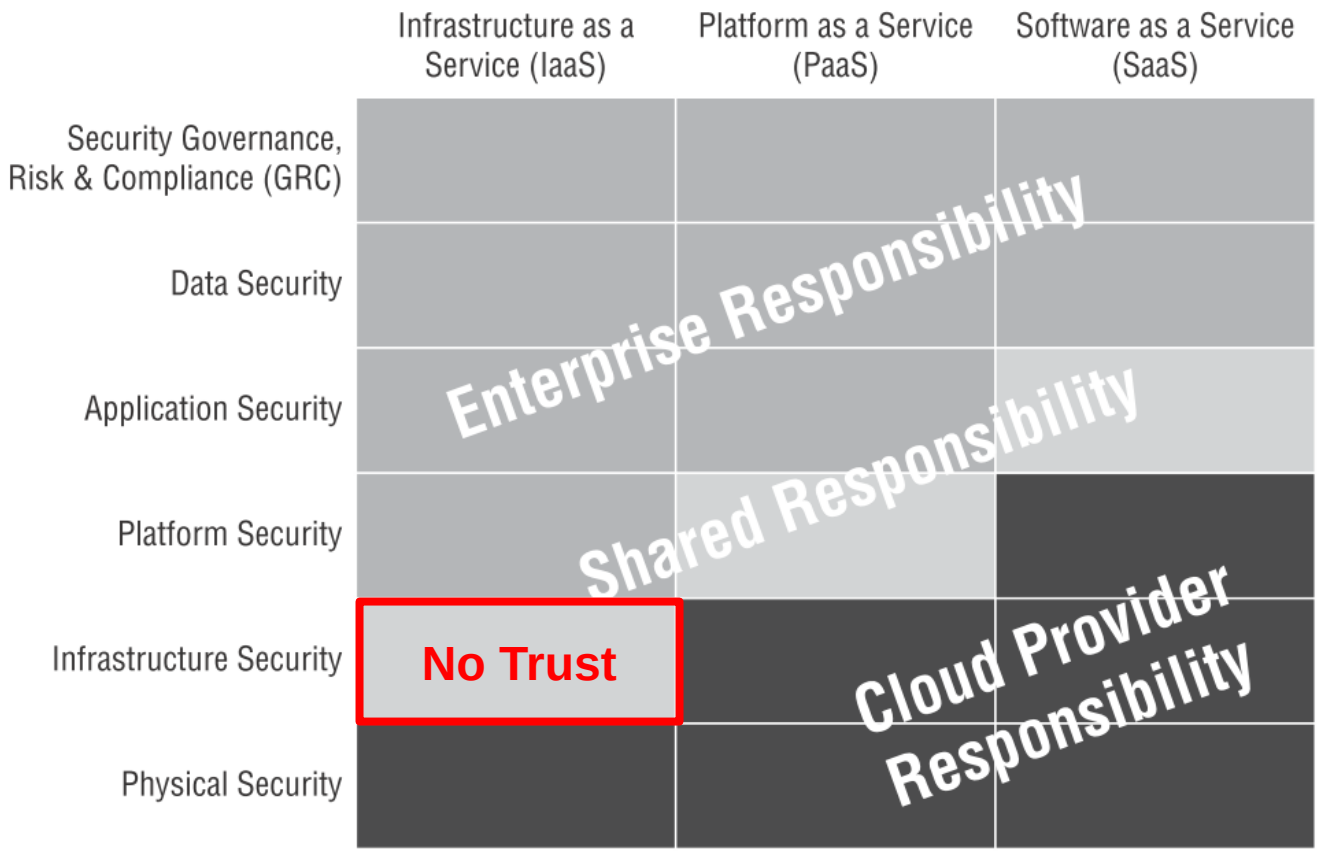


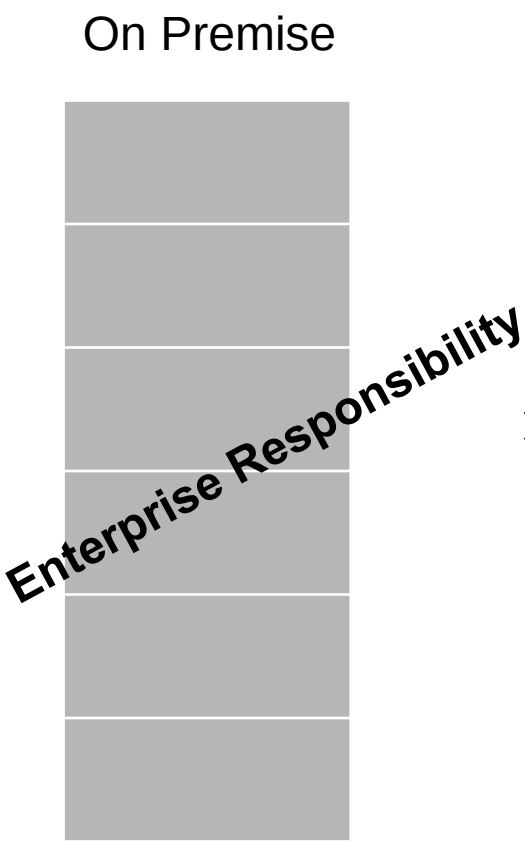
The AWS CAF leverages our experiences assisting organizations around the world, to help you complete your cloud journey.

It provides a framework for aligning technical and business stakeholders as well as updating the organization's processes and skills, to support successful cloud adoption.

資料來源：https://aws.amazon.com/tw/professional-services/CAF/

混合雲架構設計安全考量





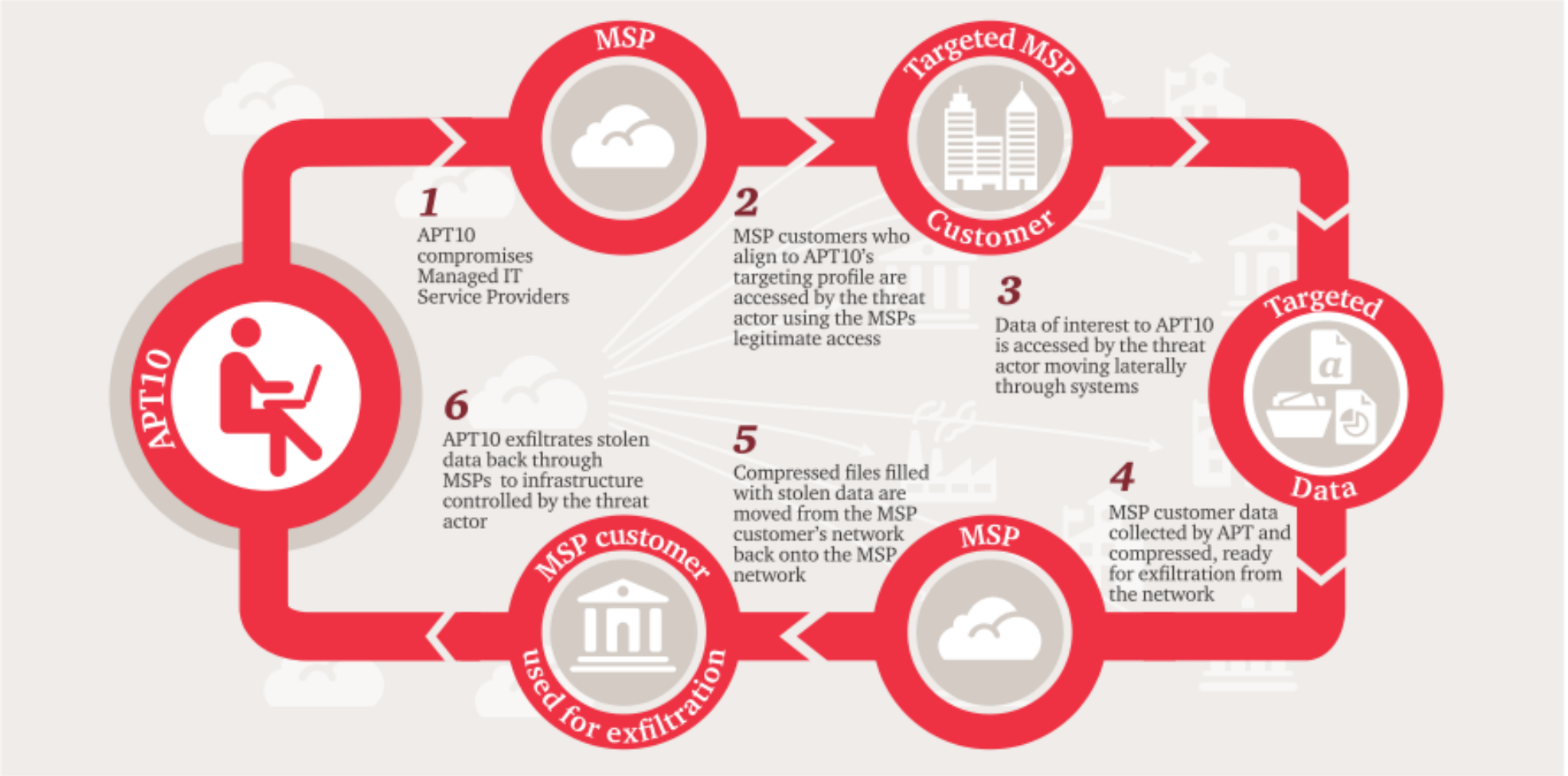
怎麼解決Share Responsibility

資料來源：Certified Cloud Security Professional Official Study Guide

中華電信 Chunghwa Telecom

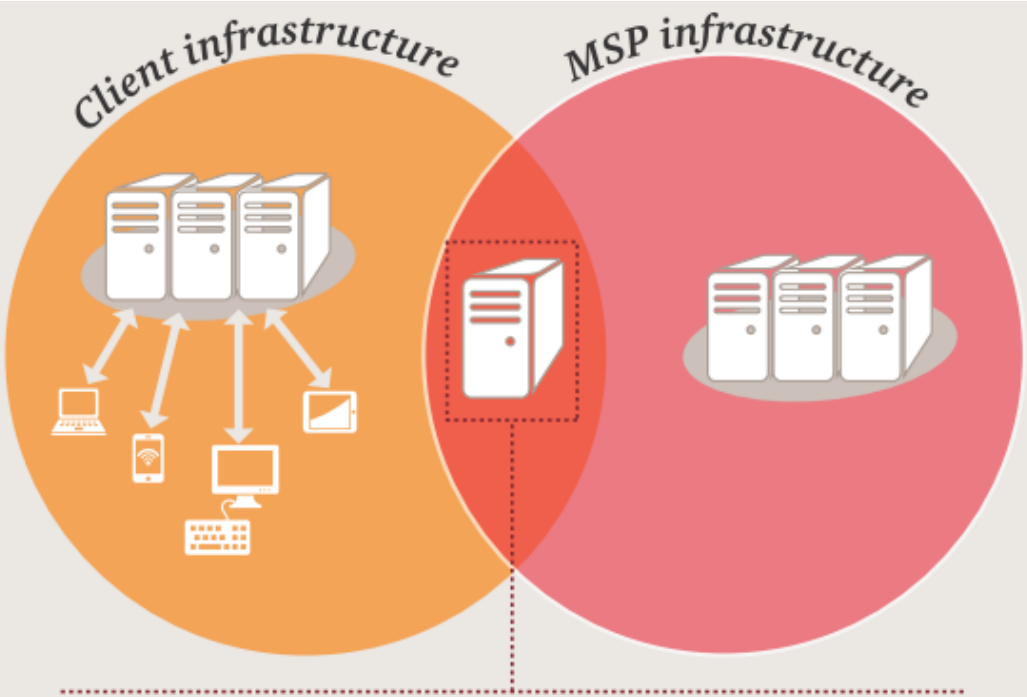
雲端攻擊案例

Operation Cloud Hopper



資料來源：http://www.pwc.co.uk/cyber

雲端攻擊案例問題分析



Systems sharing credentials across the client and the MSP are of particular interest to APT10, and are commonly used by the threat actor in order to gain access to new areas of the network

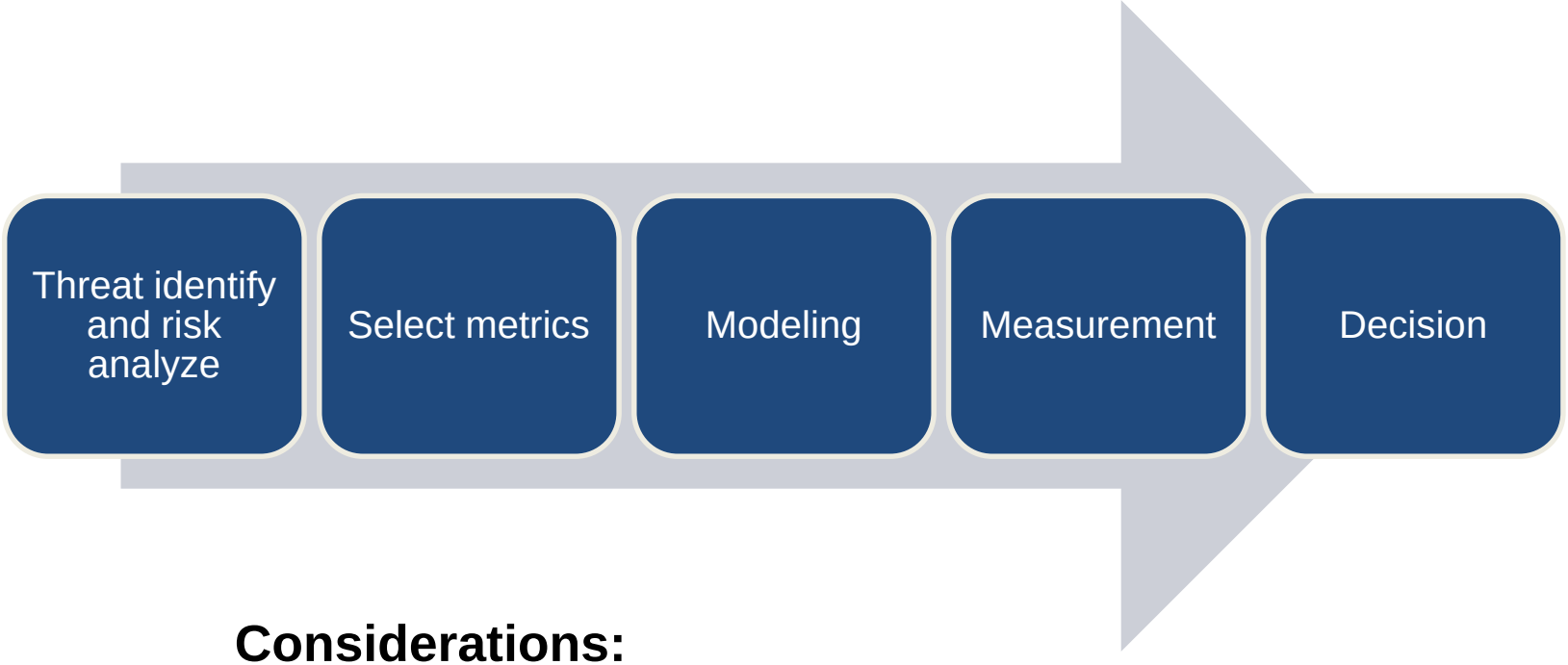
- Use of **legitimate MSP credentials** to management systems which bridge the MSP and multiple MSP customer networks (使用雲端供應商管理帳號)
- Use of **RDP** to interactively access systems in **both** the MSP management network and MSP customer networks (橫跨雲網管理網路與使用者網路)
- Use of t.vbs to execute command line tools (使用腳本語言)
- Use of PSCP and Robocopy to transfer data. (加密及快速的傳輸資料)

關鍵問題：

- 雲端隔離機制
- 管理者權限的使用

資料來源：http://www.pwc.co.uk/cyber

資安監測流程



Manage Threat (MSSP)

Hunting Threat (MDR)

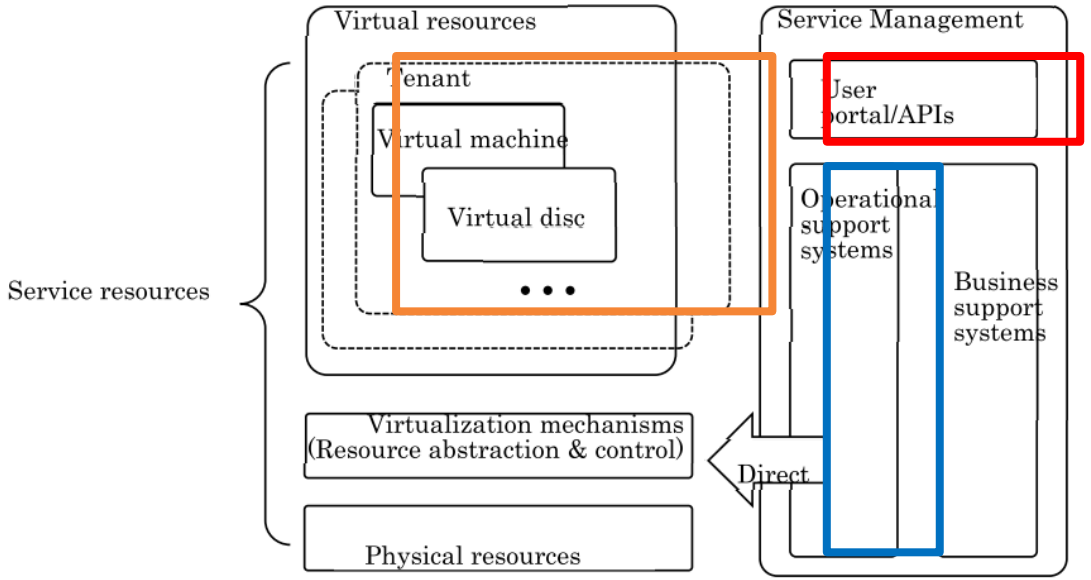
Considerations:

- **No Trust**
- **Secure channel for logging data**
- **Lower bandwidth consumption**
- **Central Monitoring**

集中監控應該放在雲端，還是放在內網？

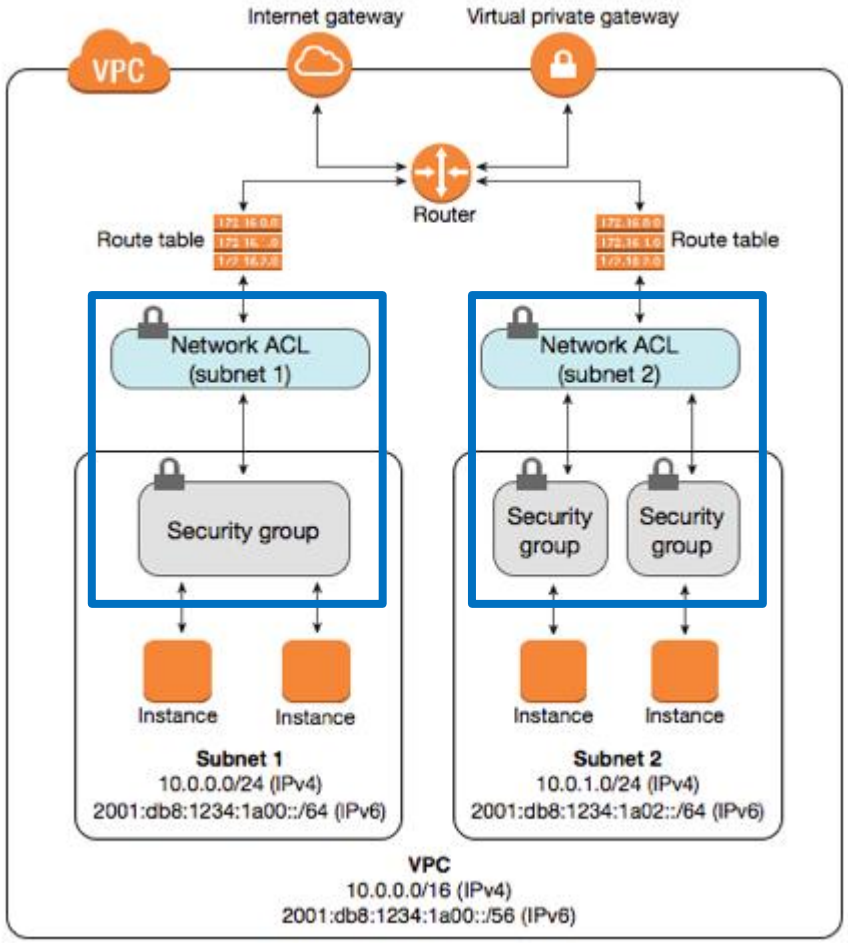
混合雲風險項目識別

Must assume their cloud provider is only taking care of the minimum requirement of security measures.



- Portal
- API
- Cloud shell

- IAM
- Group
- ACL
- Operation



Virtual private cloud example

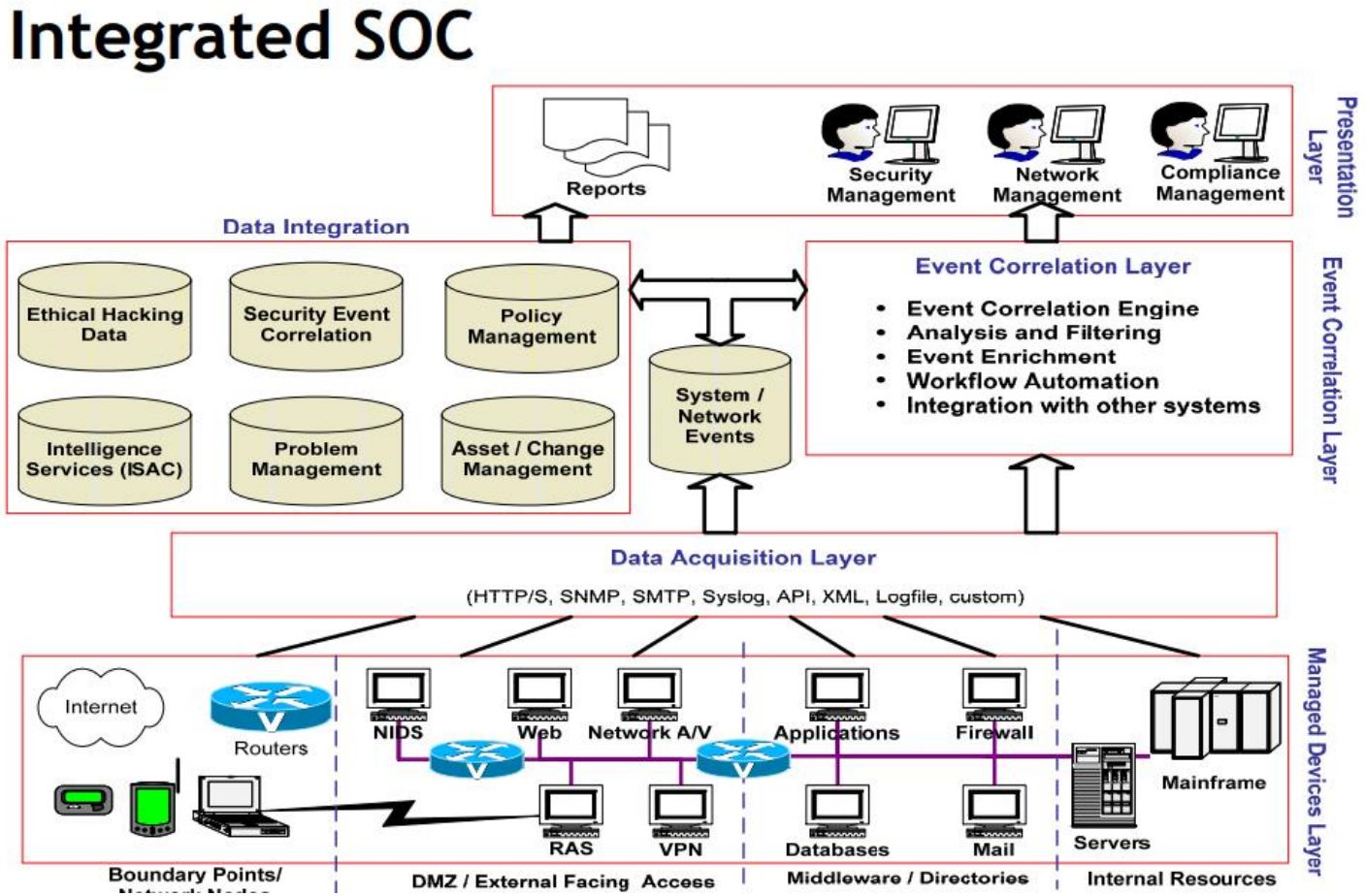
資料來源：AWS

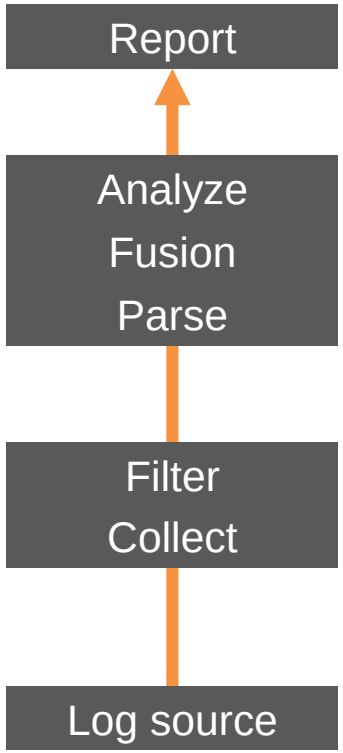
混合雲風險項目識別(參考ISO 27017)

技術相關構面	風險範例	Source of metrics
存取控制	非授權存取 非合法管道 特殊權限盜用 政策竄改	• Access control policy management log • Administrative capabilities usage log • Resources Access log • Privileged utility programs usage log (Portal/API)
加密機制	密鑰外洩 資料竊取	• Key management log • Cryptographic controls usage log
維運安全	弱點攻擊 非法授權	• Change management log • Capacity management log • System and service log • Vulnerabilities management log
網路安全	網路攻擊 流量監聽	• Network controls • Security of network services • Segregation in networks
事件應變	證據缺漏 復原失敗	• Information security event detected by the cloud service Provider • Collection of evidence • Backup log

Users or administrator?

企業內部SOC架構範例



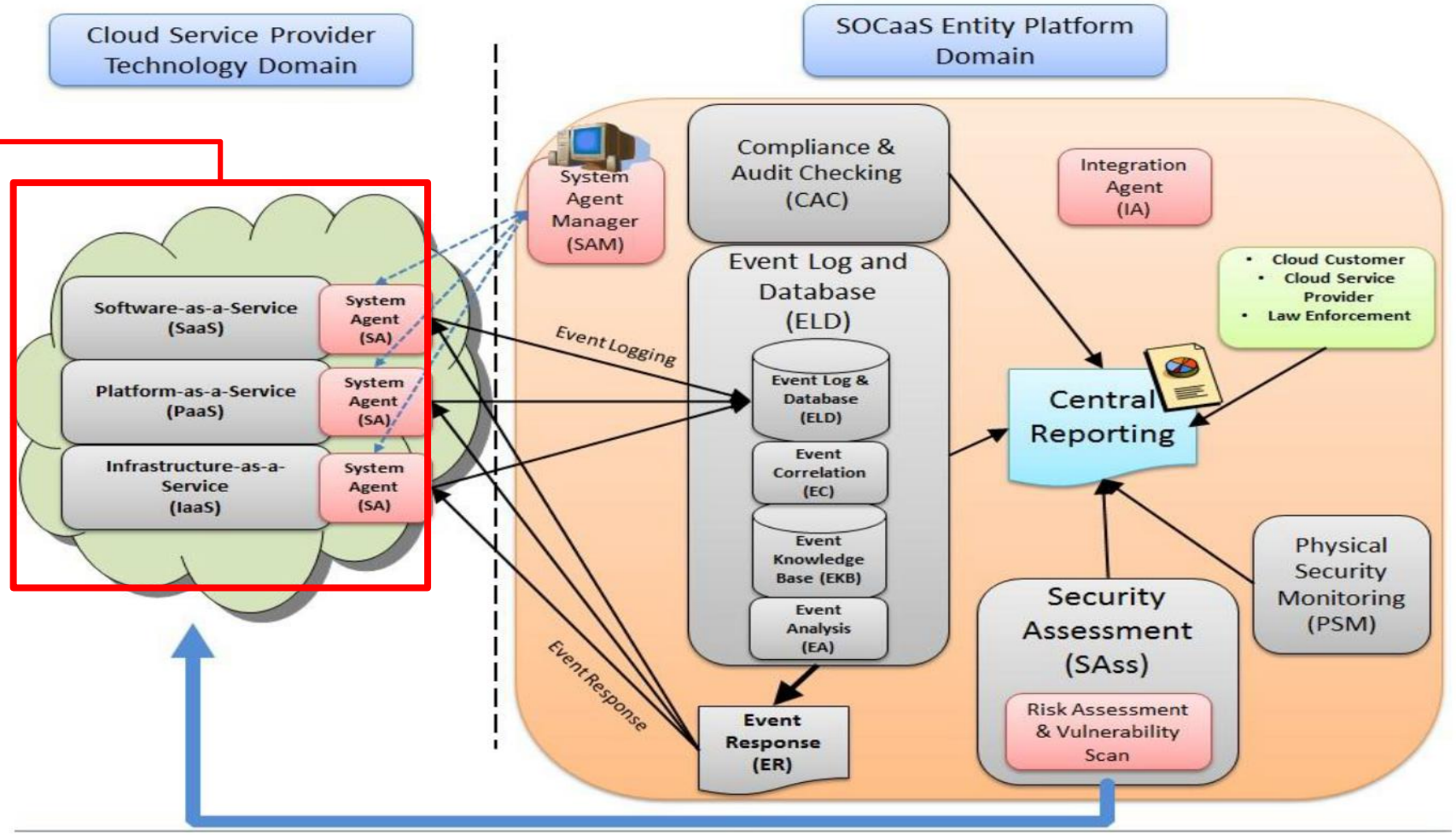


資料來源： https://www.slideshare.net/Benrothke/rothke-secure360-building-a-security-operations-center-soc

SOCaaS 範例

由Cloud Provider 支援Data Acquisition Layer

- Azure Monitoring
- AWS CloudWatch
- GCP Stackdriver



資料來源：SOCaaS: Security Operations Center as a Service for Cloud Computing Environments

SOCaaS Details

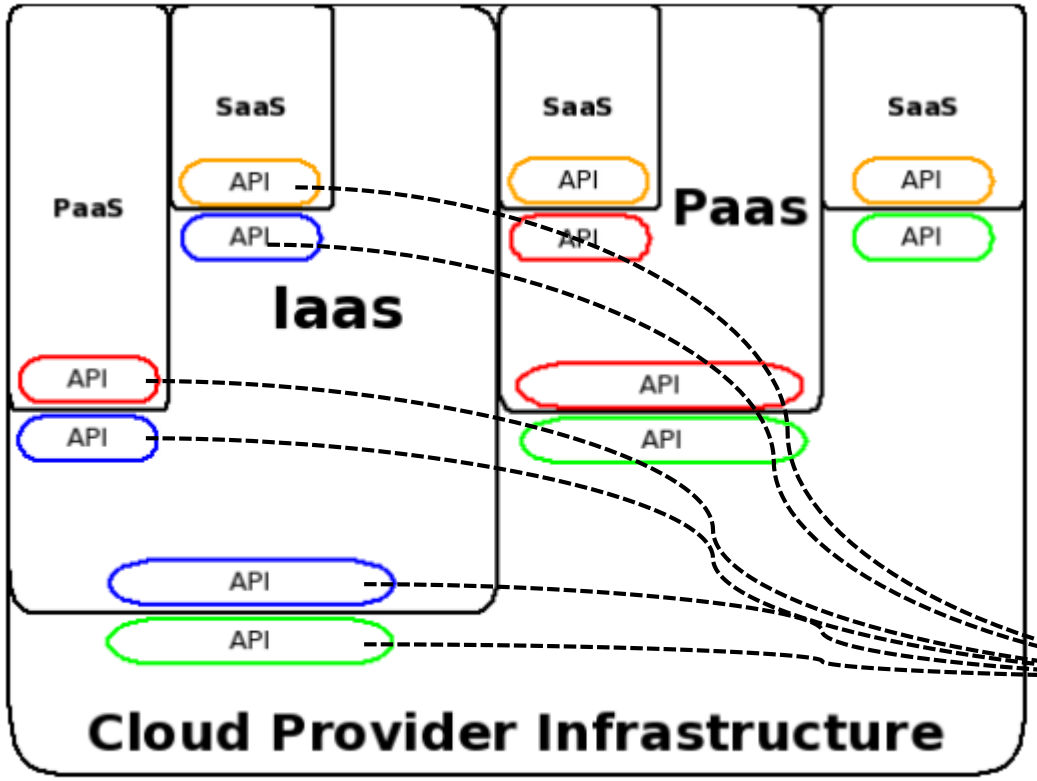
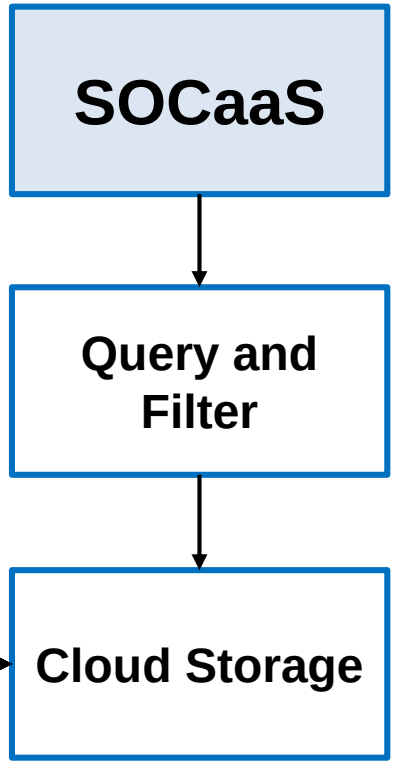


Fig. 1. Cross-Layer Security Monitoring



- Rules
- Models
- Statistic

依分析資料量、儲存空間計價

資料來源：Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments

混合雲監控架構設計

集中監控應該放在雲端，還是放在內網？

Self-managed SOC

優點
- 適合法規及政策遵循組織
- 具高隱私保護

缺點
- 管理複雜
- 不易找到或留住資安技術人才
- 建置及營運成本高
- 需要花費數月才能順利營運

放在內網

Co-managed SOC

優點
- 利用外部SOC平台管理及營運人力
- 借用外部資安技術人才
- 營運成本較低

缺點
- 仍需負最後資安管理責任
- 仍需投入人力與合作的SOC精進防護機制。
- 需要花費數月才能順利營運
- 需要管理合作的SOC

放在雲端

Managed SOC

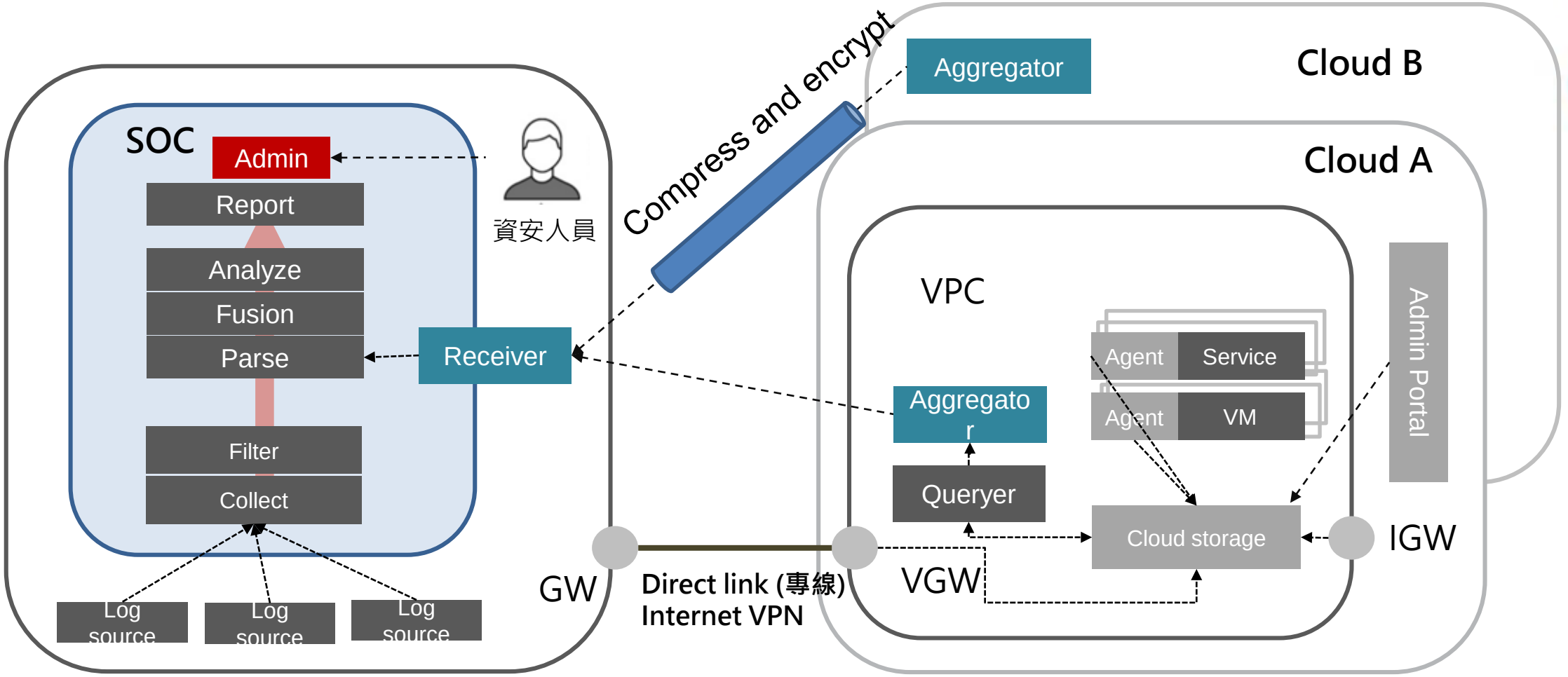
優點
- 由SOC業責建置及營運，可快數營運。
- 建置及營運成本低
- 允分使用外部資安技術人才

缺點
- 仍需協助復原工作。
- 較高的管理及稽核合作SOC成本

放在雲端

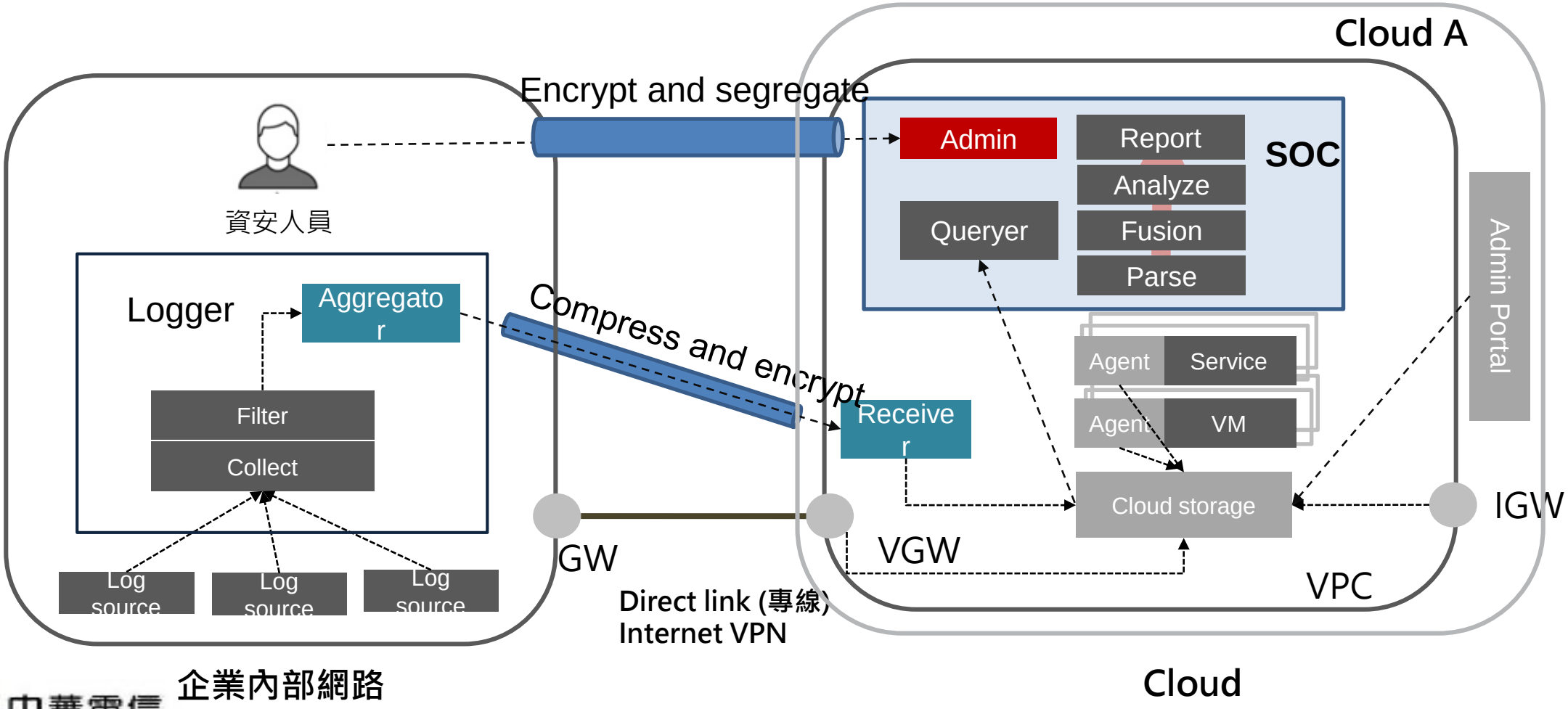
一種集中監控放在內網的架構

利用Aggregator解決傳輸安全及壓縮



一種集中監控放雲端的架構

利用Cloud Storage解決日誌保存及備援的問題



結語：遷移至雲端的準備工作

- 選擇適合的雲
- 人員養成及培訓 (做中學)
- 資安防護及監控設計
- 軟體管理流程變更(DevOps/SRE)