雲端安全管理

湧泉科技管理顧問有限公司
賴弘捷

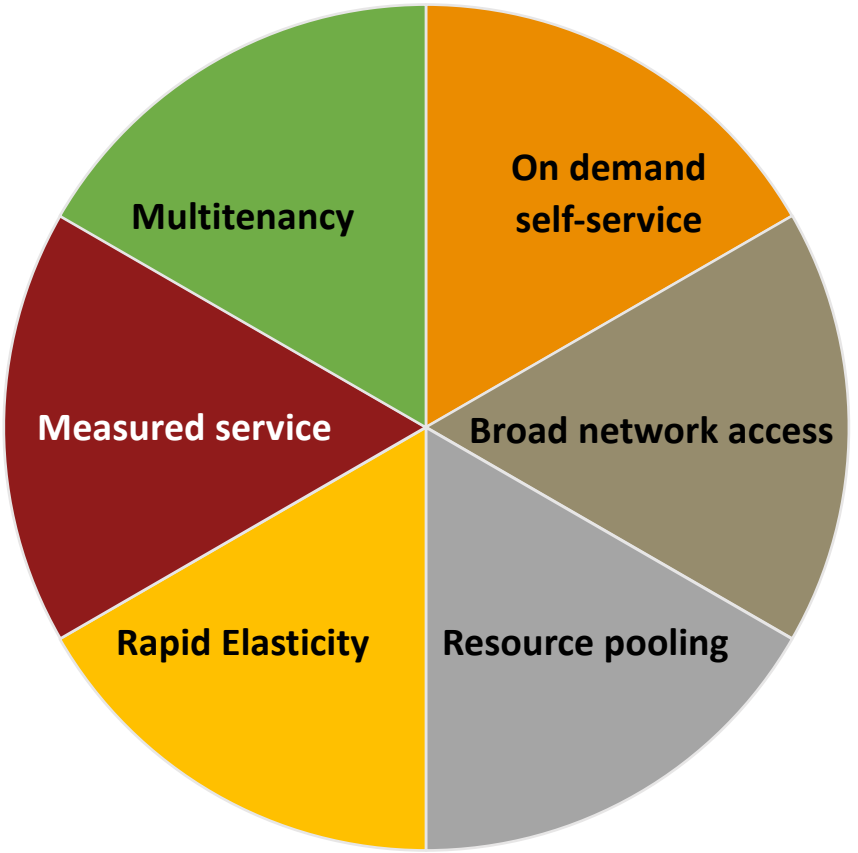
大綱

- 雲端-概念與定義
- 雲端-各種不同的角色
- 雲端-各種服務模式
- 雲端-各種部署模式
- 雲端相關之議題與安全概念
- 雲端-各種架構都適用之共通性安全議題
- IaaS/PaaS/SaaS之安全議題
- 雲端-安全標準與符合性要求

雲端-概念與定義

何謂雲端

- ✓On demand self-service
- ✓Broad network access
- ✓Resource pooling
- ✓Rapid Elasticity
- ✓Measured service
- ✓Multitenancy



各種角色-各司其職-Cloud Service Customer

- Cloud User
  使用Cloud 服務的使用者

- Cloud Service administrator
  測試/監控雲端服務,管理安全控制,提供管理報表

- Cloud Service Business Manager
  採購/簽署/監督雲端服務合約與費用,並在必要時要求提交稽核報告

- Cloud Service integrator
  負責將現有系統與服務整合入雲端

各種角色-各司其職-Cloud Service Provider

- Cloud Service operation manager
  準備,管理,監控雲端服務
  管理雲端資產及因應要求提供稽核資料
- Cloud Service development manager
  管理服務部署的步驟,定義環境與程序
- Cloud Service Manager
  提供,交付,管理雲端服務
- Cloud Service Business Manager
  審閱與管理雲端服務商務方案以及請款相關事宜
- Customer Service
  提供客戶服務並回應要求
- Inter-cloud provider
  提供內部雲端服務
- Cloud Service Security and Risk Manager
  管理雲端安全風險並且確保安控被確實執行
- Network Provider
  提供,管理,監控網路服務,確保網路可用性

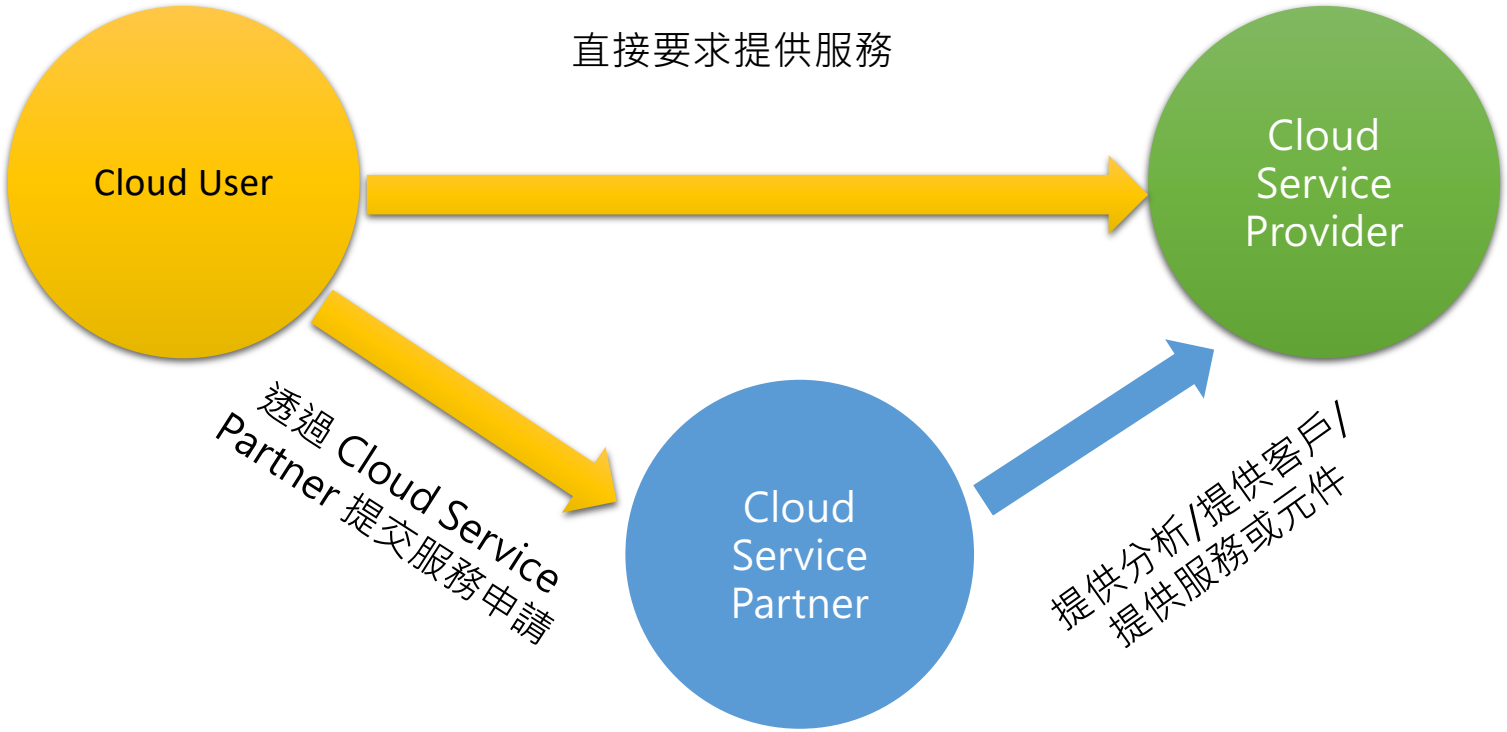
各種角色-各司其職- Cloud Service Partner

- Cloud Service Developer
  開發/測試/驗證雲端服務與元件

- Cloud Auditor
  執行稽核並產製報告

- Cloud Service Broker
  開發新客戶,分析市場潛力,研究安全議題以及制定合約

關聯關係


Cloud User
直接要求提供服務
Cloud Service Provider
透過 Cloud Service Partner 提交服務申請
Cloud Service Partner
提供分析/提供客戶/提供服務或元件

雲端-各種服務模式

各種雲端服務模式

你（妳）說得出這三種服務模式的主要功能/優點與差異嗎？

IaaS-Infrastructure as a Service

簡述

- 最基本且客戶控制權最大的服務
- 提供處理/儲存/網路及最基本的資源
- 不能夠管理網路基礎架構
- 僅能夠管理少部分的網路元件

主要功能與效益

- 擴展性
- 降低硬體持有成本
- 高可用性
- 實體安全-轉嫁Provider
- 不受限於地點的存取
- 可計價/調整的服務-高峰時才付費
- 提供“綠色機房”的方案

PaaS-Platform as a Service

定義

- 提供客戶部署自身開發或屬意的應用系統
- 由service provider提供系統運作之平台
- 客戶無須擔心平台之維運

主要功能與效益

- 自動調整所需(或不需要）之資源
- 對於作業系統與運作環境可有多種選擇
- 有彈性-與上述選項搭配
- 易於升級與更新-不需擔心downtime或升級問題
- 對於開發單位來說提供巨大的費用節省
- 有益於協作
- 版權控管-由Service provider統籌

SaaS-Software as a Service

定義

- 完整的應用系統已經為用戶準備好
- 應用系統所在的平台及應用系統之維運,升級與修補皆由Service Provider負責

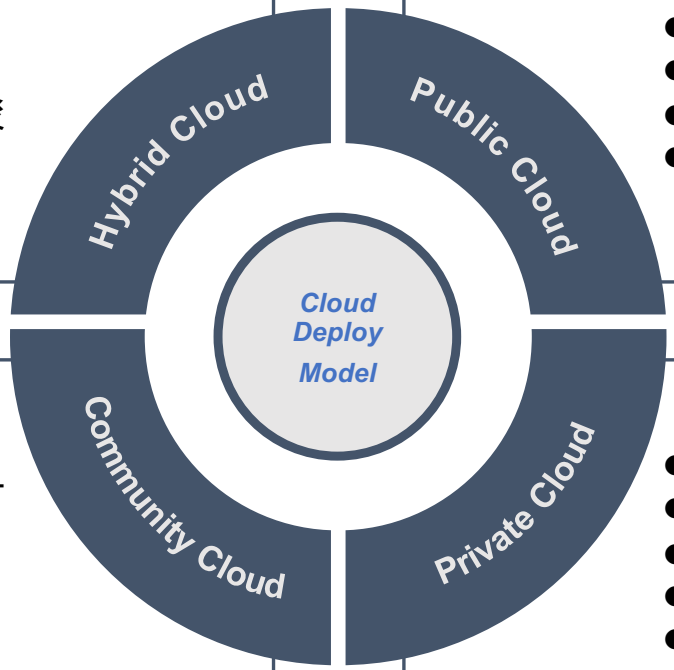
主要功能與效益

- 降低整體的費用
  - ✓降低授權費用
  - ✓降低支援的費用與時間
- 易於使用與管理
- 提供標準化-使用同樣版本的軟體

雲端-各種部署模式

各種部署模式

- 結合任意兩種Cloud部署模式
- 著重標準化與互相支援性
- 通常用在提供附載平衡以及災難復原使用



- 提供公眾使用
- 位於服務提供商之機房
- 對於使用者來說亦於設定且便宜
- 只需對於要使用的服務付費

- 由相同型態的組織或公司所一起建置
- 類似Private Cloud
- 可以建置在公司內部或外部

- 由單一公司或組織所擁有
- 為了該組織的商業目的所建置
- 由該公司獲授權的第三方維運
- 可以建置在公司內部或外部
- 提供內部“可計價式”的服務

各種部署模式-功能與效益比較

Public Cloud	Private Cloud	Community Cloud	Hybrid Cloud
• 易於設定 • 便宜 • 只需在需要使用時付費 • 擴展性-想加就加	• 保留所有控制權 ➢ 控制系統 ➢ 控制資料與軟體	• 效益與功能與Private Cloud一致 • 差別在於擁有控制權的是彼此類似的同一個群體（由兩個以上的公司或組織所組成）	• 依據成本效益與企業之風險,採用public / Private cloud之優點 ✓ 將重要關鍵系統保留在企業內部加以控制 ✓ 將需要快速有彈性的系統建置在public cloud ✓ 當災難發生時可以切換

雲端相關之安全議題與概念

雲端相關之議題

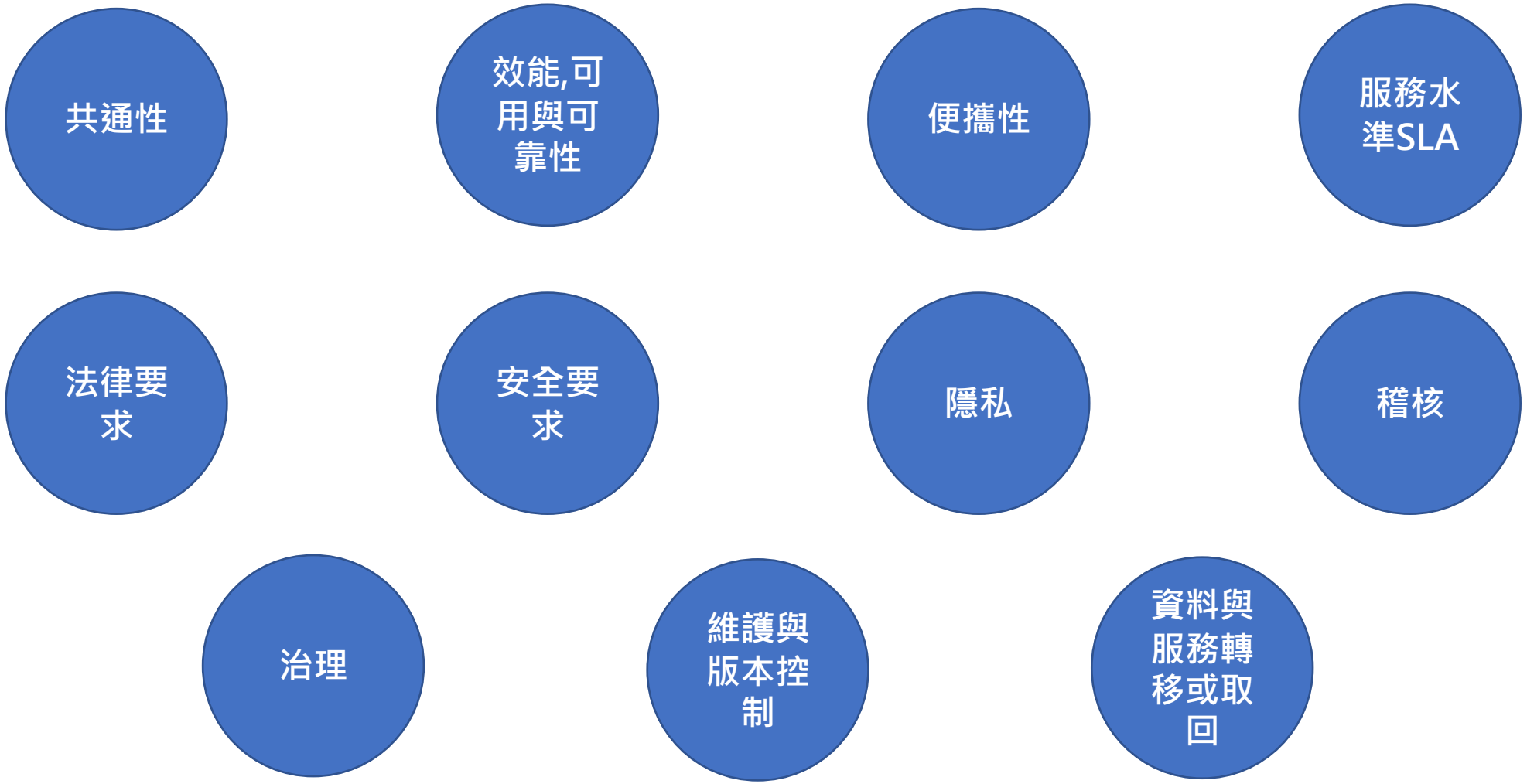
- 不論你使用哪種服務模式以及哪一種部署架構,下列議題都是共通性的！

在開始之前 ~ 我們先來談談責任與風險！

雲端之風險考量!

政策與組織風險	一般風險	虛擬化風險
• 服務商鎖定 • 掌控力...	• 單點失效與整合 • 服務商能力...	• Guest breakout • Snapshots and image • Sprawl
雲端特有之風險	**法律風險**	**非雲端特有之風險**
• 管理平台安全 • 資源耗盡 • 隔離控制 • 資料刪除...	• 個資/資料保護 • 法律管轄權 • 執法問題 • 版權問題	• 社交工程 • 天災 • 未受經授權存取 • 駭客攻擊(服務提供商)...

雲端相關之議題～有哪些？


共通性
效能,可用與可靠性
便攜性
服務水準SLA
法律要求
安全要求
隱私
稽核
治理
維護與版本控制
資料與服務轉移或取回

共通性

- 系統與資料結構越具有高度共通性(可跨平台,或採用公開標準）越不會被服務商所綁定
- 易於從Public cloud轉換到Private Cloud(反之亦然）
- 服務提供商若也採用這種方法,則：
  - 可能吸引企業用戶從private cloud轉換到服務提供商處
  - 價格變成重點

效能,可用性與可靠性

- 效能永遠在第一位
- 使用雲端服務,效能/可用性與可靠性是基本中的基本-如果有妥善規劃與維護的話

雲端與備份的真實故事！

便攜性

- 指的是系統是否可以很便捷的/無縫的在不同的雲端服務提供商間轉換

服務水準-SLA

- 何謂服務水準？
- 記載了有關於資源的提供,處理能力,客戶支援,可用時間與可用性以及安全控制措與稽核權利
- 可說是合約中最重要的部分
- 沒有寫的都不算

常見議題！

法律要求

例如:

- HIPAA/HITECH
- PCIDSS
- SOX

為什麼這些很重要？
什麼時候會被要求？
不管他或是沒遵守要求會怎樣？有沒有案例可循？

稽核權

- 稽核權-很重要
- 寫在合約裡面才算真的有
- 雖然很重要～但是cloud service provider可能還是不理你！（等等～我可是客戶耶）
- 就算讓你有稽核權好了～你有時間稽核？你知道要到哪稽核？你有能力稽核嗎？

安全要求

- 雖然“雲端”這個名詞已經出現很久了,但是“安全議題”仍然是許多人擔心的一個議題

- 身為雲端服務提供商,通常都：
  - 建立最基本的安全控制基線(baseline)-透過安全制度/認證的導入
  - 提供Report(SCO1-2-3)-後續會說明
  - 提供Tailored security services

- 身為cloud user：
  - 依照自身的風險考量與成本效益分析選擇是否將服務部署至雲端

隱私議題

- 特別注意歐盟與美國的隱私議題與爭議處理

身為一個資訊從業人員你該注意什麼？

治理

- 企業不能因為使用雲端服務而將IT安全治理的議題丟給服務提供商
- 通常夠Qualified的雲端服務提供商都會提供許多管理性報表,提供管理階層參考
- 但仍須注意“共通性”問題,意即在轉換服務提供商時,不同廠商所提供的報表如何mapping或轉換,以確保之前所搜集的數據在轉換後仍具有參考價值

維護與版本控制

- 採用IaaS以及PaaS時,系統或應用程式的更新與修補及維護需要service provider 與 Cloud user之間,相互協作以確保可用性

- 另外亦須建立版本控制機制,以確保所有用戶端都使用相同版本之應用程式

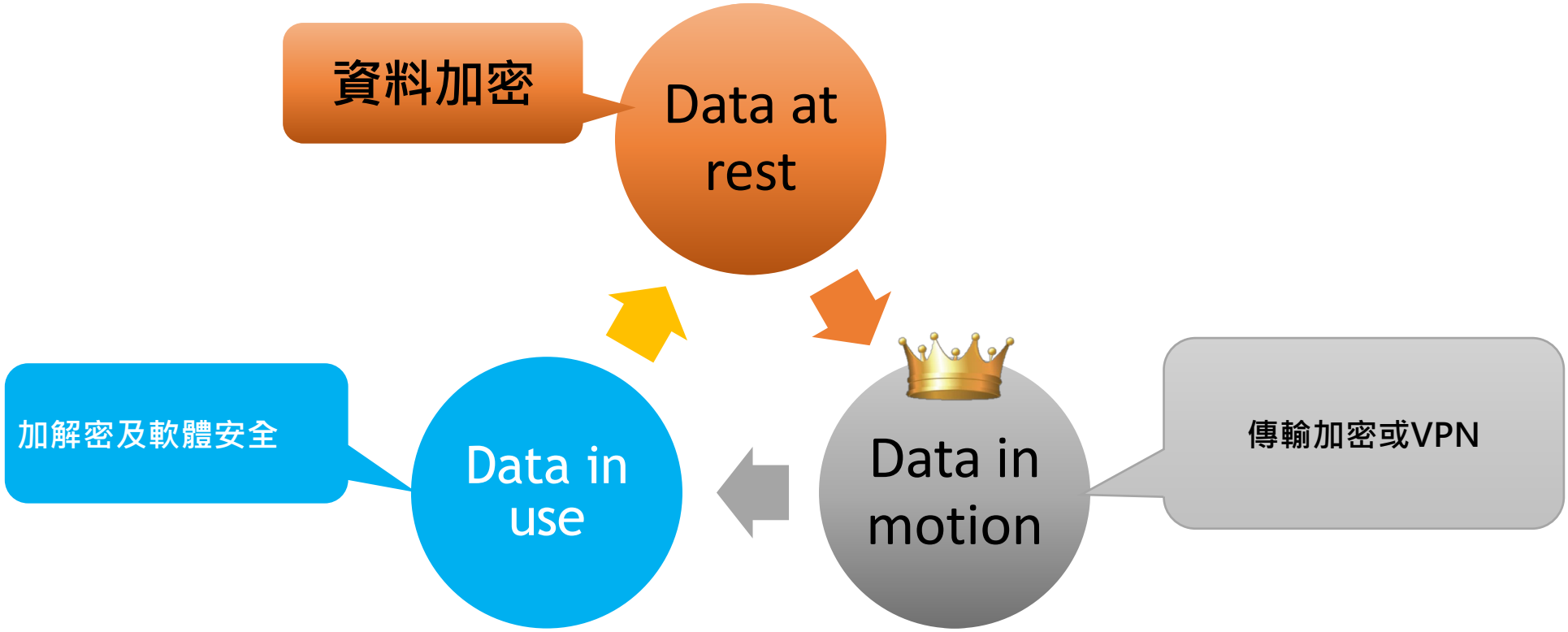
資料與服務轉移或取回

- 若你與雲端服務提供商即將結束合作,要求對方將你的資料歸還後刪除之...你會怎麼做？為什麼？

雲端相關之安全觀念

- 加密學
- 存取控制
- 資料與儲存媒體之刪除
- 網路安全
- 虛擬化安全
- 常見威脅

加密學與資料生命週期之關係與應用！

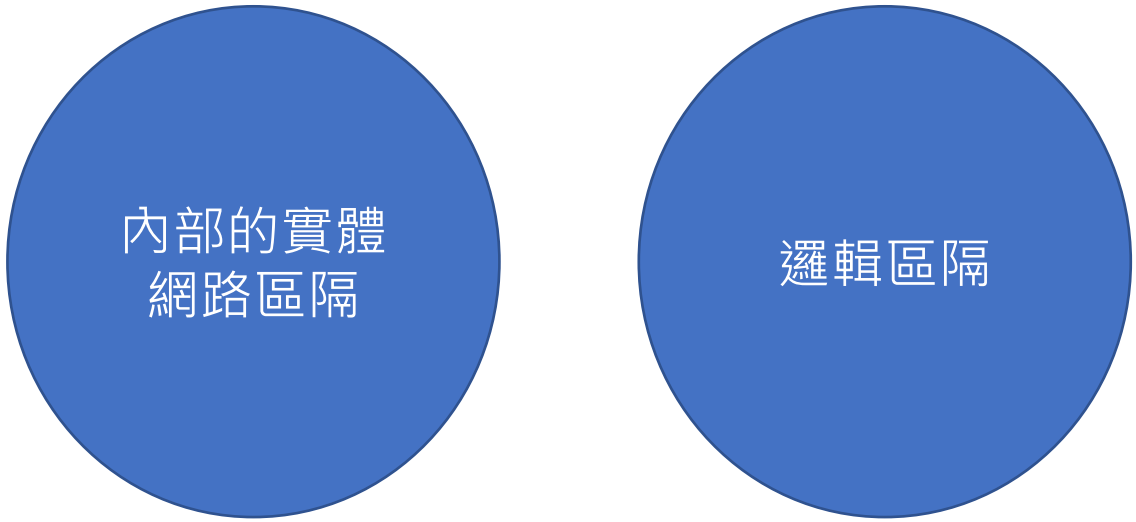


存取控制

- 識別
- 認證
- 授權
- 問責

網路安全

- 兩個主要的關注面向



虛擬化安全

- Hypervisor：用以建立，並管理、執行虛擬機的模組
- ＶM（Virtual Machine):透過 Hypervisor創造出來、模擬底層的軟體。
- Guest:運行在虛擬機上的作業系統或軟體程式

Hypervisor的重要性

- 一但被成功利用弱點-那麼在上面”居住“的虛擬機都將會暴露在被攻擊的風險之下

雲端常見威脅

- 資料外洩
- 權限控管不夠/不嚴謹
- 不安全的應用程式介面與帳號劫持
- 系統本身之弱點
- 惡意的內部人員
- ＡＰＴ公及
- 資料遺失
- 偷懶
- 雲端服務濫用與誤用
- ＤＯＳ攻擊
- 共用的問題

資料外洩

- 通常都是管理階層與資安專家最關注的議題
- 如何處置？
- 你防得了嗎？

權限控管不夠/不嚴謹與帳號劫持

- 雖然科技已經很進步了～但你最常用的仍然是帳號密碼！
- 儲存帳密或認證資訊的系統都是駭客優先攻擊的對象！
- 記得要和駭客一樣壞才行！
- 不管你採用哪一種雲端服務,這種威脅與攻擊對你都適用

- **誰最容易外洩自己的聯絡方式？**
- **哪些人不知不覺中洩漏了？**
- **哪些人洩漏了之後～若被成功利用,造成的危害最高？**
- **如何處置？**

不安全的應用程式介面

- 不管採用哪種雲端服務,各系統與服務間都需要中介介面來負責處理資料交換與服務請求
- 對於應用程式介面應該採用嚴格的安全控制或加密機制來確保其安全

系統弱點

- 不是放雲端就沒有弱點
- 一位資訊安全從業人員應建立：
  - 完善可行的修補程序(Patching Procedure)
  - 加強系統的監控
  - 定期掃描與測試
  - 採用縱深防禦之概念

惡意的內部人員

- 有權限的人害你最兇
- 權限越高害你越深
- 如何處置？你能處置？

資料遺失

- 何謂資料遺失？
- 資料遺失與資料洩漏有何區別？

偷懶！

- 以為什麼都丟雲端就安全了！
- 你要做的事情還很多呢！
- 什麼？我要做事？要做什麼事？

✓考量自身的商業模式與風險,決定服務模式
✓資料型態與重要性
✓法令法規
✓安全要求
✓廠商
✓合約條款與服務水準
✓如何轉移與抽身...

雲端服務濫用與誤用

- 此威脅特別是針對Service Provider!
- 此威脅適用於IaaS以及PaaS
- 因為太好用/太有彈性了~所以我想怎麼用就怎麼用！

DOS/DDOS-阻斷式或分散式阻斷服務攻擊

- 適用於Iaas/PaaS/SaaS
- 打趴Service Provider就打趴一堆人了

IaaS/PaaS/SaaS之安全議題

IaaS之安全議題

- Multitenancy-各家公司（部門）與不同系統共存,加密更顯重要
- Co-Location-許多虛擬機“住在“實體機上,一旦Hypervisor出狀況,這些image都有可能受攻擊
- Hypervisor Security-同上議題
- Network Security-雲端服務提供商通常不會允許你檢視網路封包與資安設備紀錄檔
- VM Security-雖說是虛擬機,但與實體機的安全議題是一樣的,但由於大家都“住在一起”...
- Virtual Switch Attack-所有會在網路第二層發生的攻擊在這裡都有可能發生,一但發生...
- DOS-阻斷服務攻擊

PaaS之安全議題

- System Isolation-
  不大可能允許客戶可以擁有系統層級的權限,要是可以,那麼就難以進行例如系統安全控制以及更新修補程式．．．等作業
- 使用者權限
  務必確保使用者之權限授予與撤銷是適切的

- 使用者存取
  - ✓知其所需與最小權限
  - ✓完善的認證與授權機制

✓惡意程式-永無止盡的惡夢！

SaaS之安全議題

- 網路應用程式安全
- 資料安全

雲端-安全標準與符合性要求

雲端-安全標準與符合性要求

- ISO27001:2013
- NIST-800-53
- PCIDSS
- SOC1,SOC2,SOC3
- Common Criteria
- FIPS 140-2
- More…