



# Azure Security

---

Alan Tsai



# 這節主要重點



- 整體安全性
  - Defense in depth
- 網路安全性
  - DDoS (distributed denial-of-service attack) 分散式阻斷服務攻擊
  - Network Security Groups (NSG) 以及 Firewalls (防火牆)
- 安全相關的服務
  - Security Center、Sentinel、Dedicated Hosts 以及 Key Vault



# 這節主要重點



- Identity Service (身份識別)
  - Authentication (驗證) 以及 Authorization (授權) 的差別
  - Azure Active Directory、Conditional Access、Multi-Factor Authentication (MFA) 以及 Single Sign On (SSO)
- Azure Governance Feature (管理功能)
  - Role Base Access Control (RBAC)
  - Resource Lock 以及 tag
  - Policy、Blueprint 以及 Cloud Adoption Framework (CAF)



# 這節主要重點



- Privacy
  - Microsoft Privacy Statement、Online Services Terms (OST) 以及 Data Protection Amendment (DPA)
- Compliance
  - Trust Center
  - Compliance Documentation
- Azure Sovereign Regions
  - Azure Government
  - Azure China

# 整體安全性





# Shared Security Responsibility



當系統被駭客入侵的時候  
請問是誰的責任？



# Shared Security Responsibility



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Shared
Identity & access management	Cloud Customer	Cloud Customer	Shared	Shared
Application level controls	Cloud Customer	Cloud Customer	Shared	Cloud Provider
Network controls	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Shared	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

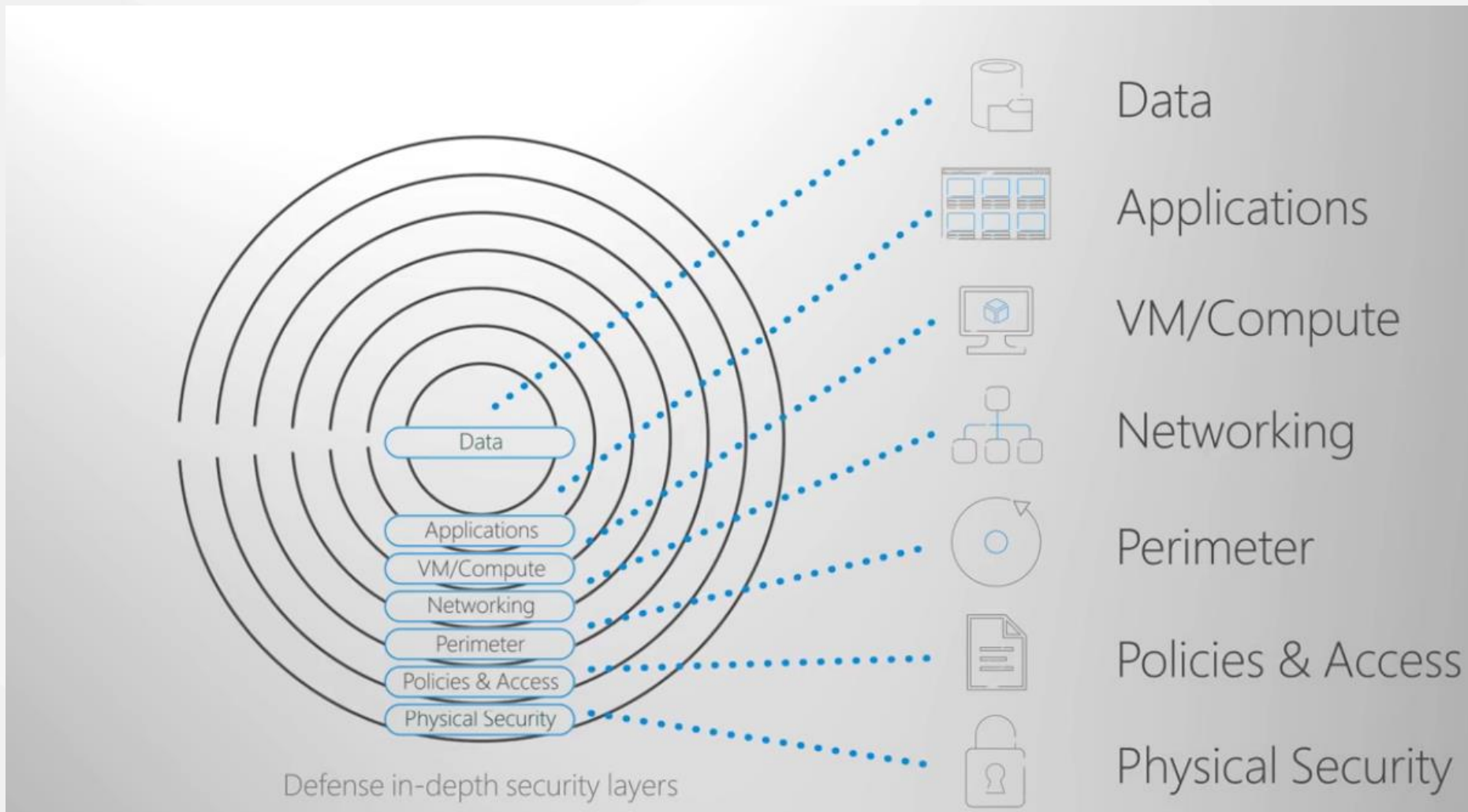
Cloud Customer Cloud Provider

[Shared Responsibility for Cloud Computing](#)

@Alan Tsai 的學習筆記



# Defense In Depth



## Defense in depth security in Azure

@Alan Tsai 的學習筆記

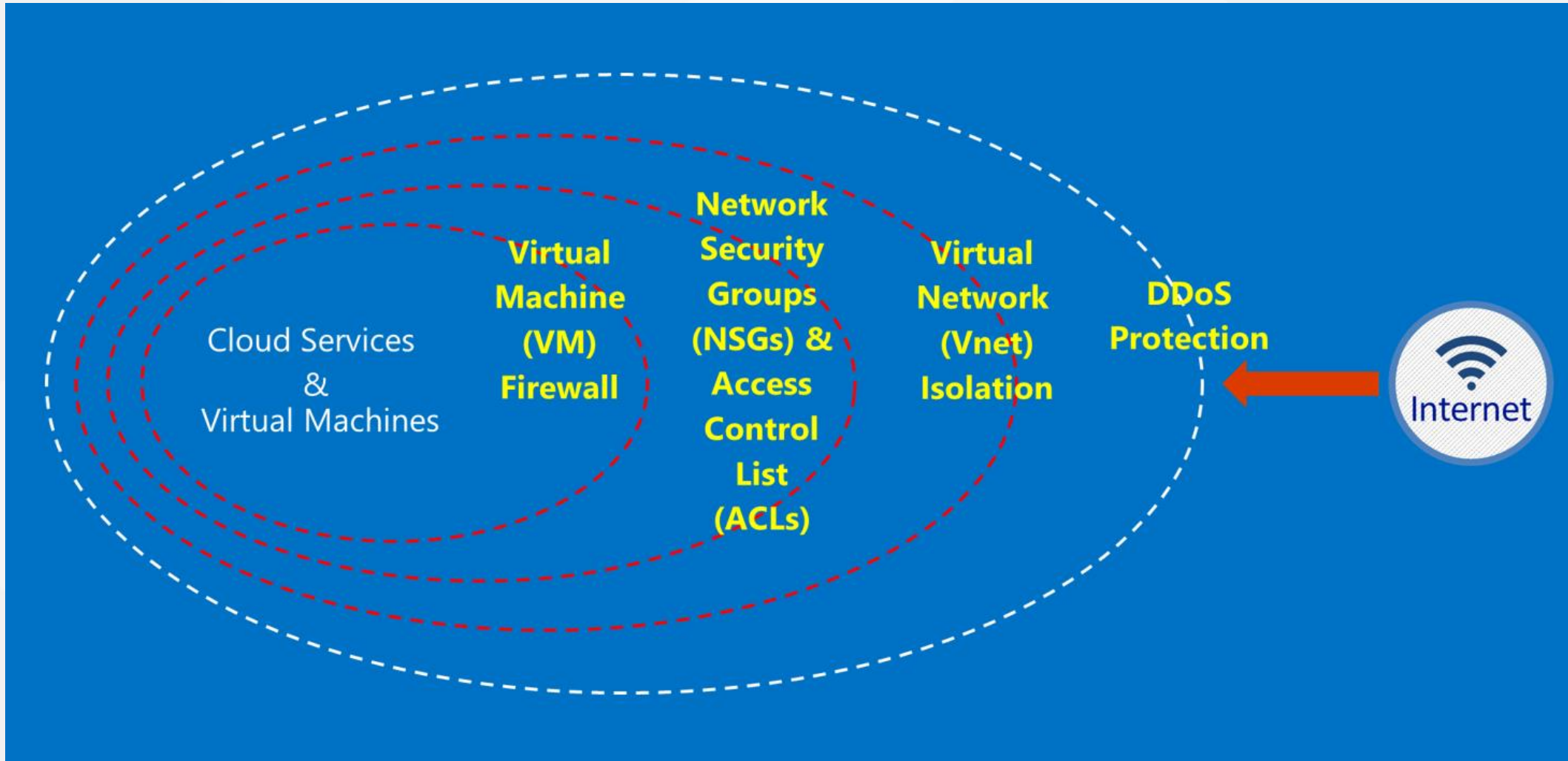


# 網路安全



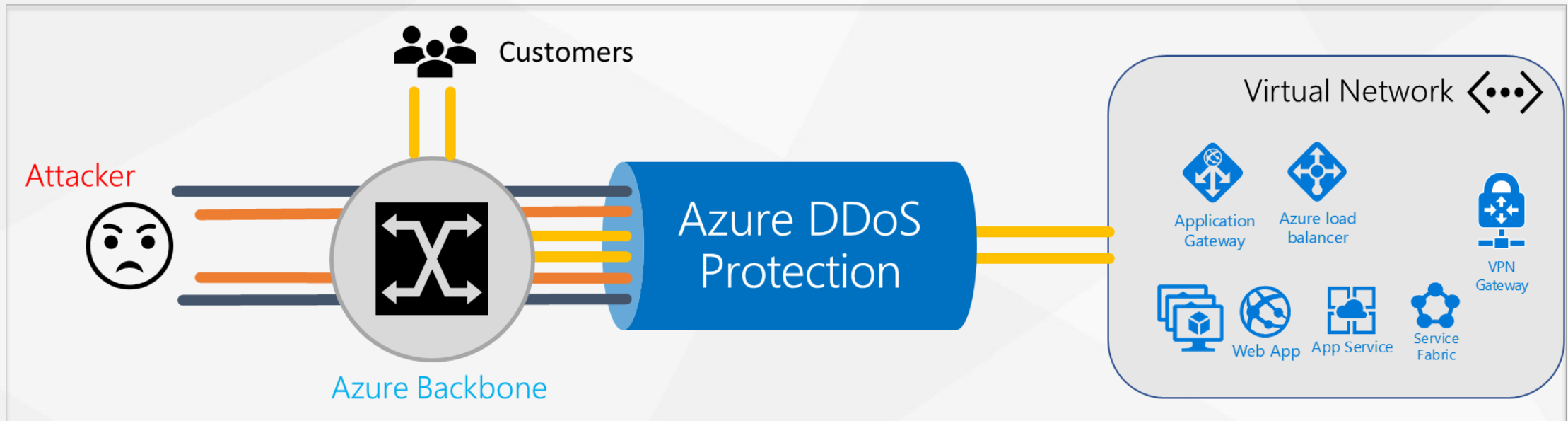


# 網路安全





# Azure DDoS Protection



## Azure DDoS Protection - Designing resilient solutions



# Network Security Groups (NSGs)



- 控制進來以及出去的流量
  - IP
  - Port
  - Protocol
- 規則依照 Priority 套用
  - 數字越**小**，優先度越**高**
  - 數字可以設定為：100 ~ 4096



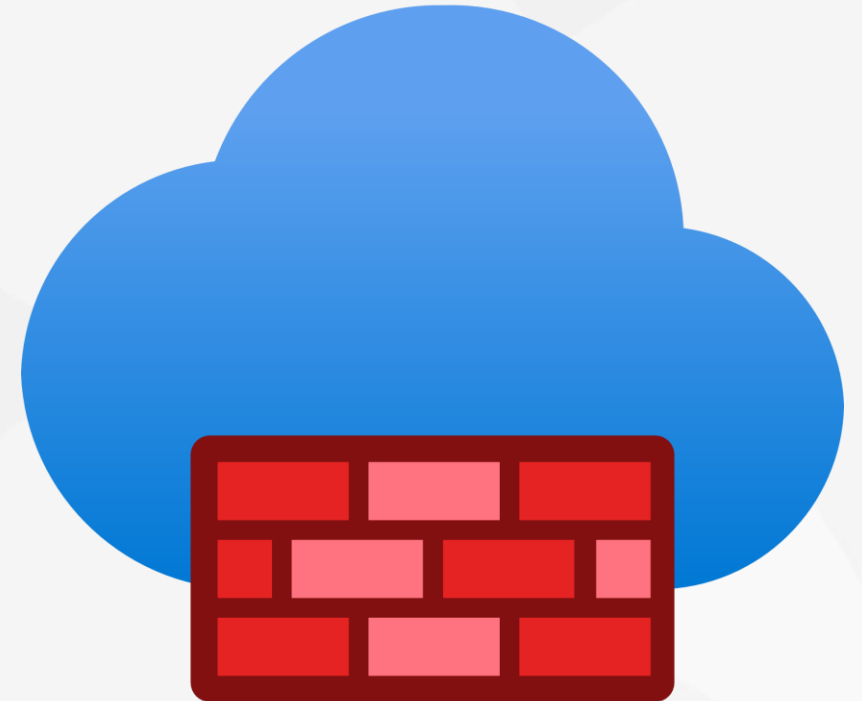
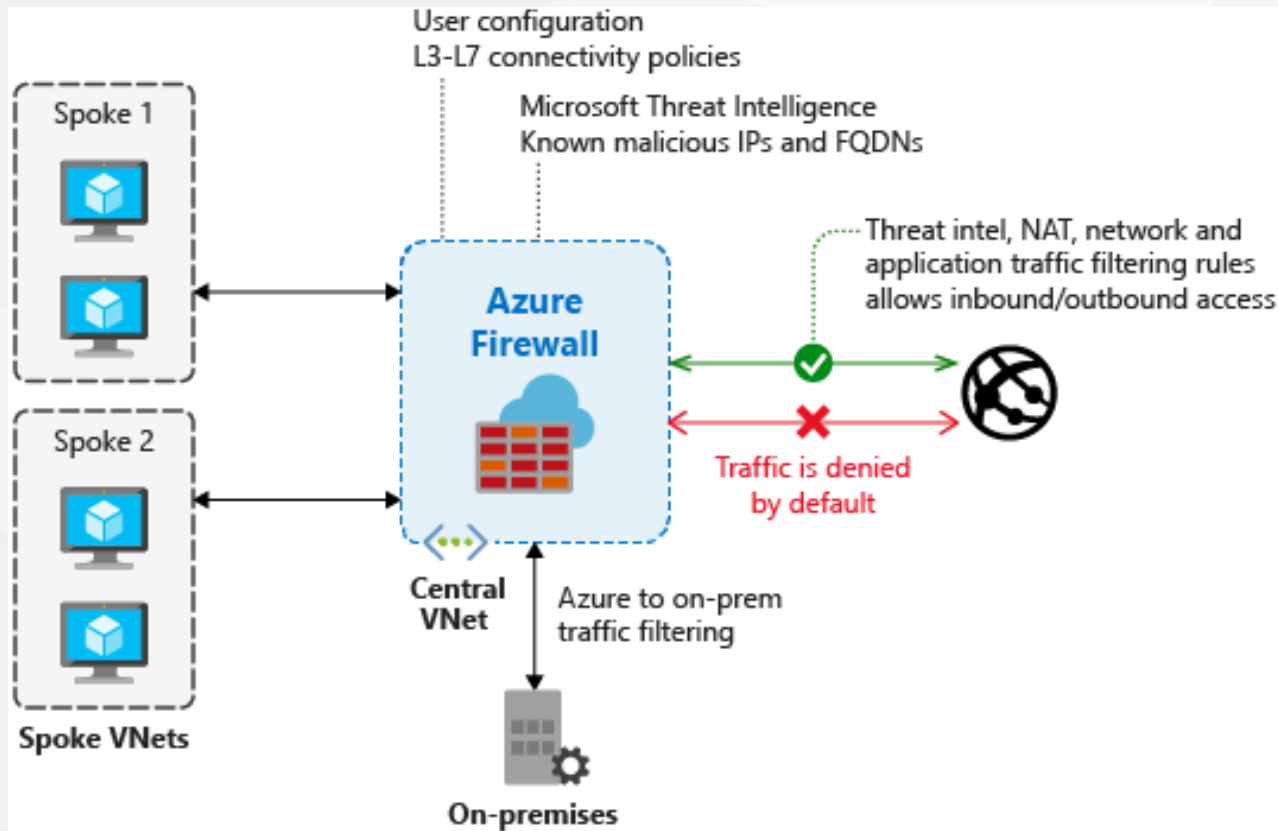
[Network security groups](#)



# Azure Firewall



- managed, cloud-based network security service that protects your Azure Virtual Network resources

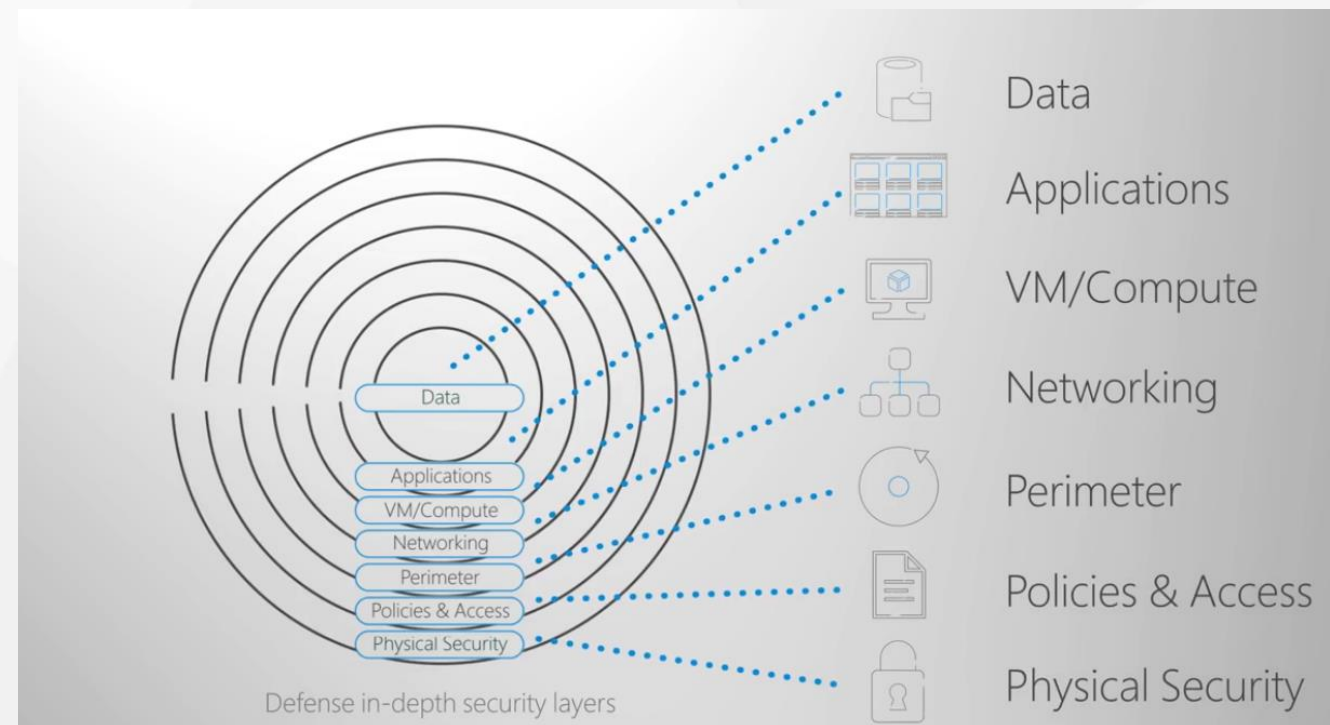




# Defense In Depth



- Perimeter
  - Azure DDoS Protection
  - Azure Firewall
- Network
  - NSG



[Defense in depth security in Azure](#)

@Alan Tsai 的學習筆記

# 安全性相關服務





# Security Center



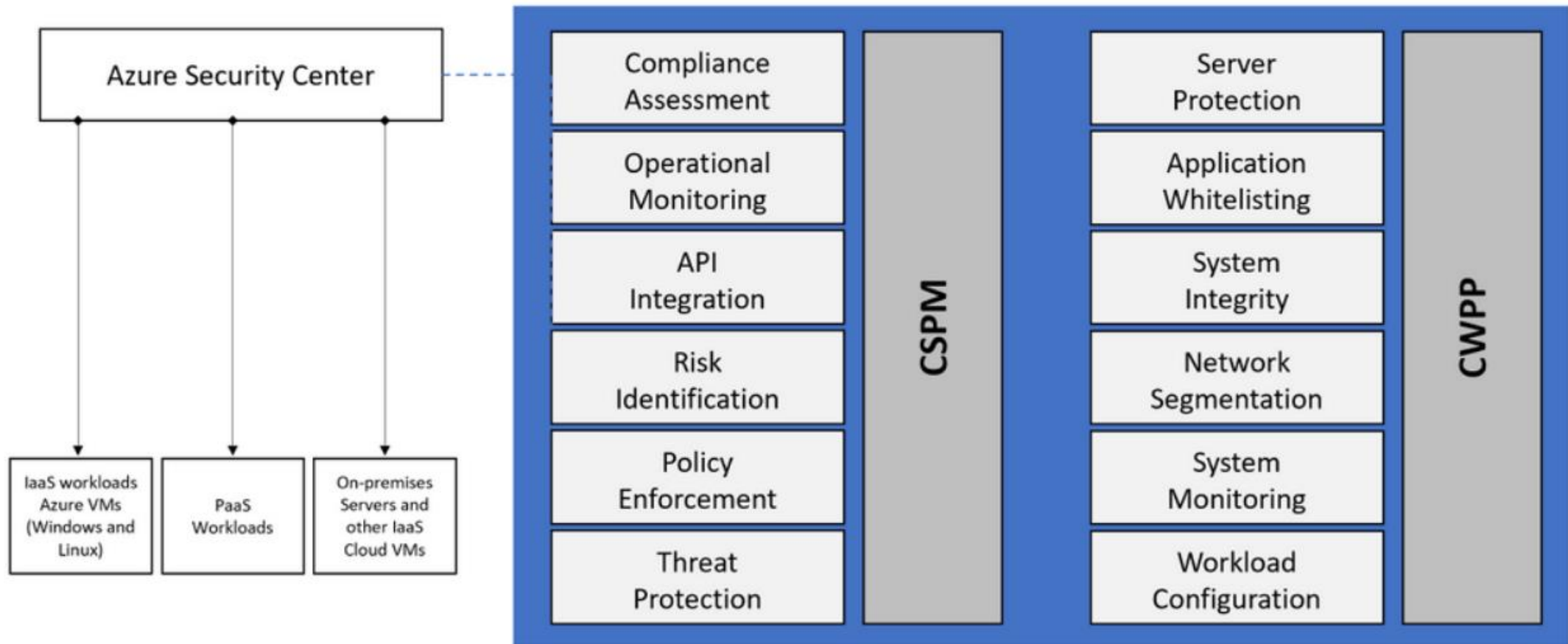
- 提供一些資訊安全建議
- Continuous assessments
- Policy Compliance
- Recommendation
- Threat Protection
- [Azure Security Center](#)







# Azure Security Center





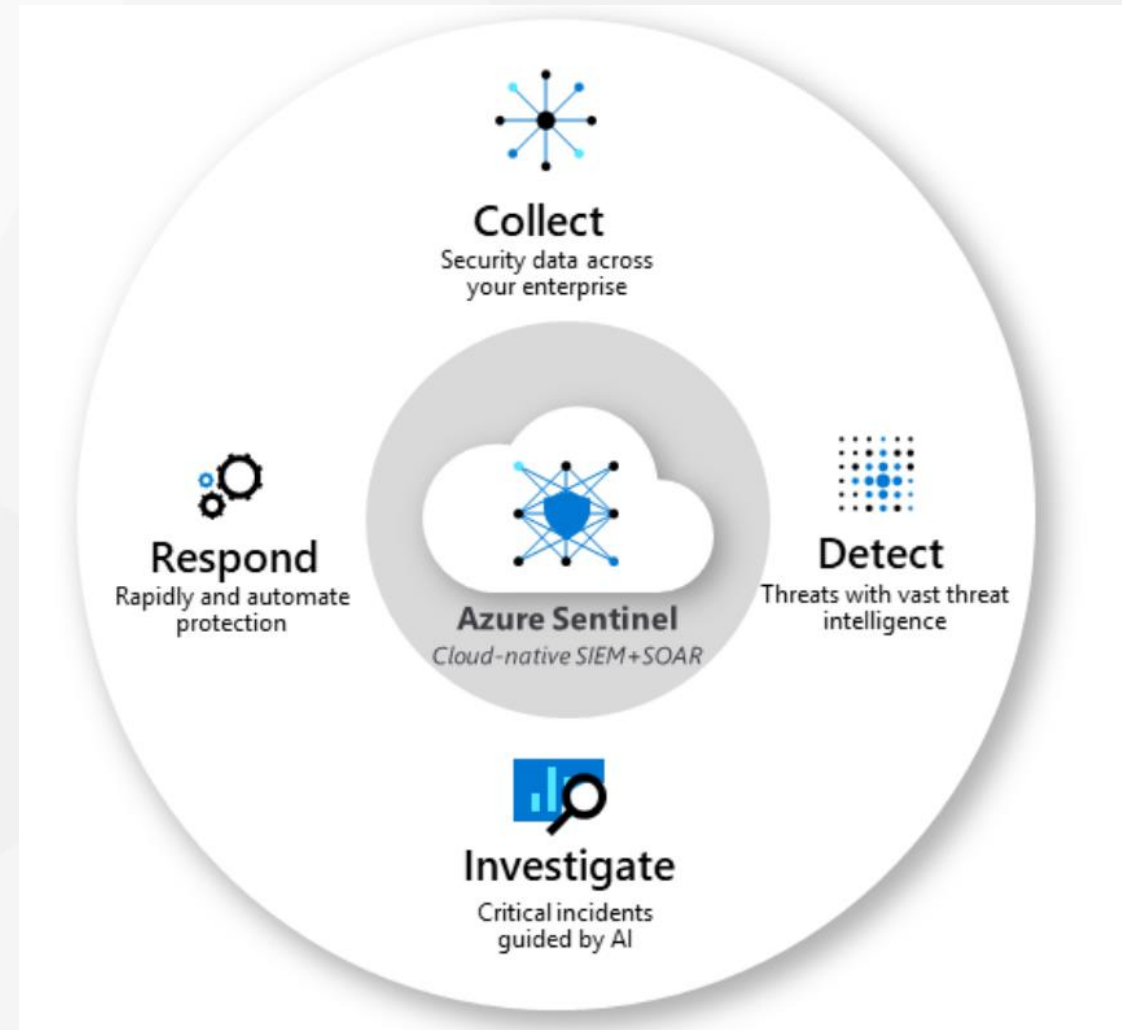
# Azure Sentinel



- Cloud Solution

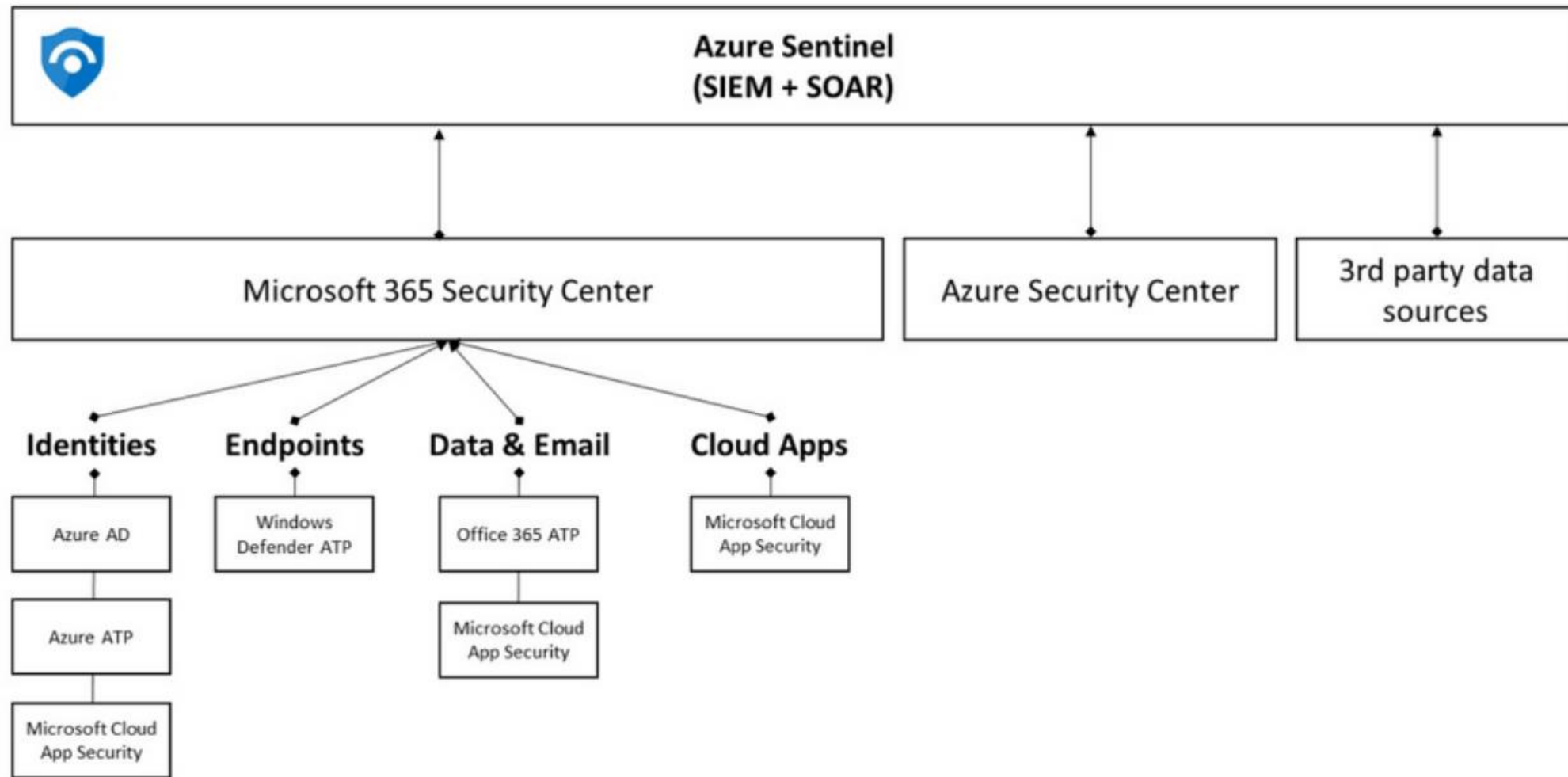
- security information event management (SIEM)
- security orchestration automated response (SOAR)

- 可以整合第三方的訊息





# Azure Sentinel

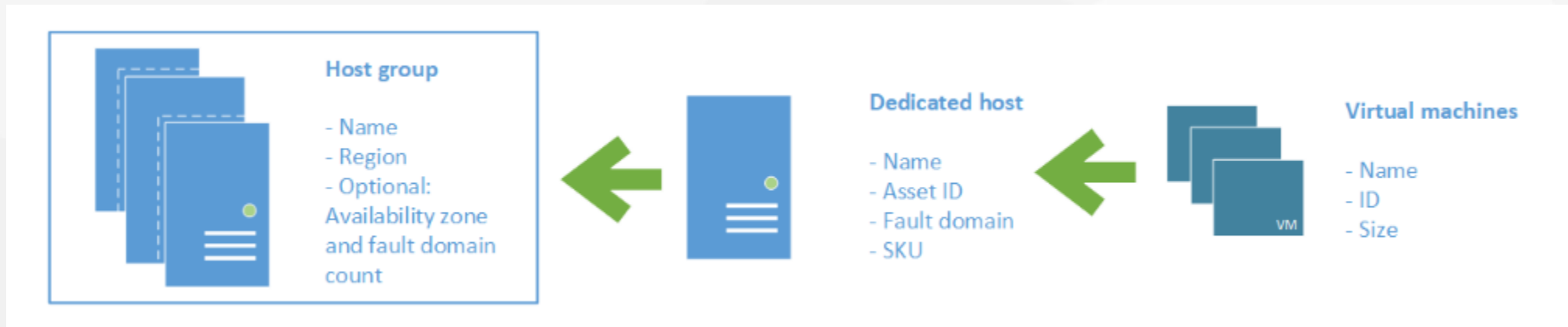




# Azure Dedicated Hosts



- 獨立的機器
- 用來跑 1 台或者多台 VM
- 可以自己控制更新時間





# Azure Key Vault



- 用來儲存應用程式需要的 3 中機敏訊息
- Key
- Secret
- Certificate
- 使用 FIPS 140-2 Level 2 以及 Level 3 驗證過的 Hardware security modules (HSMs)



# Identity Service





# 怎麼知道您是誰以及可以用什麼？




當您想要使用 Azure 的時候  
它怎麼知道您可以用什麼？



# 第一件事情



## Microsoft Azure

 Microsoft

### 登入

繼續至 Microsoft Azure

電子郵件、電話或 Skype

---

沒有帳戶嗎? [建立一個吧!](#)

無法存取您的帳戶嗎?

[使用安全性金鑰登入](#) (?)

下一步

 以 GitHub 登入



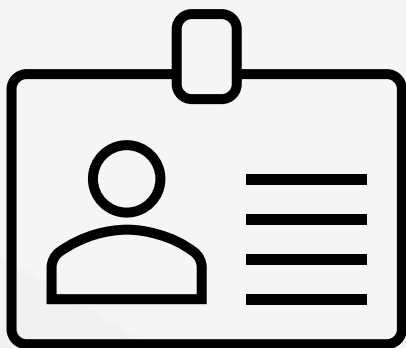


# Authentication vs Authorization



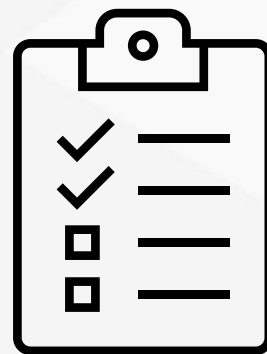
## Authentication (驗證)

- 是誰要用系統
  - 你告訴系統你是誰



## Authorization (授權)

- 這個人可以用什麼功能





# Azure Multi Factor Authentication (MFA)



- 最常見的 Authentication 方式就是透過帳號密碼
- 如果密碼被破解呢？
  - 使用好猜的密碼：ji32k7au4a83
- 如果可以增加別的因素進去就不容易
  - 發簡訊到電話號碼做第二次確認



# Azure Multi Factor Authentication (MFA)



- Something you know
  - 帳號密碼
- Something you possess
  - 手機
- Something you have
  - 指紋




# Single Sign On (SSO)



密碼太多不好記錄 – 用其他系統的帳號登入

Microsoft Azure

 Microsoft

**登入**  
繼續至 Microsoft Azure


電子郵件、電話或 Skype

沒有帳戶嗎? [建立一個吧!](#)

[無法存取您的帳戶嗎?](#)

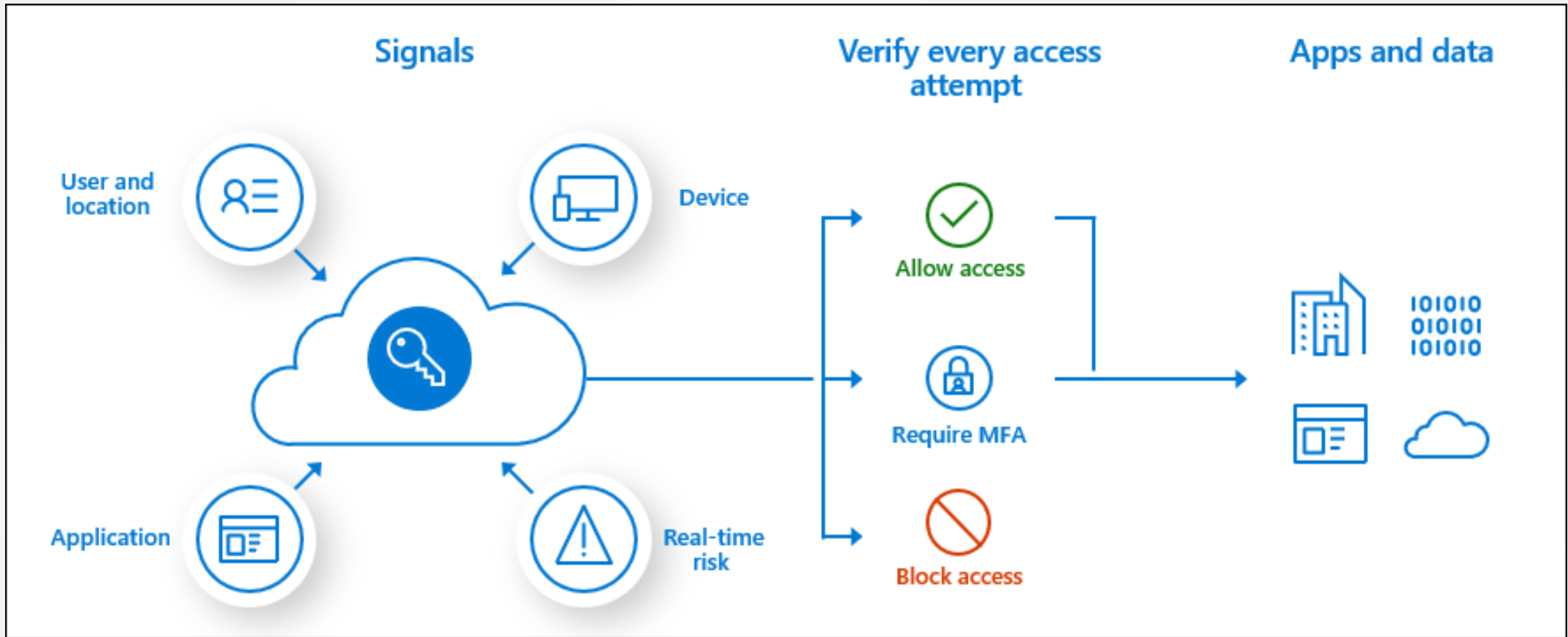
[使用安全性金鑰登入](#) ⓘ

下一步

 以 GitHub 登入



# Conditional Access



## What is Conditional Access?

# Role Base Access Control (RBAC)

- 3 個部分

- 什麼人

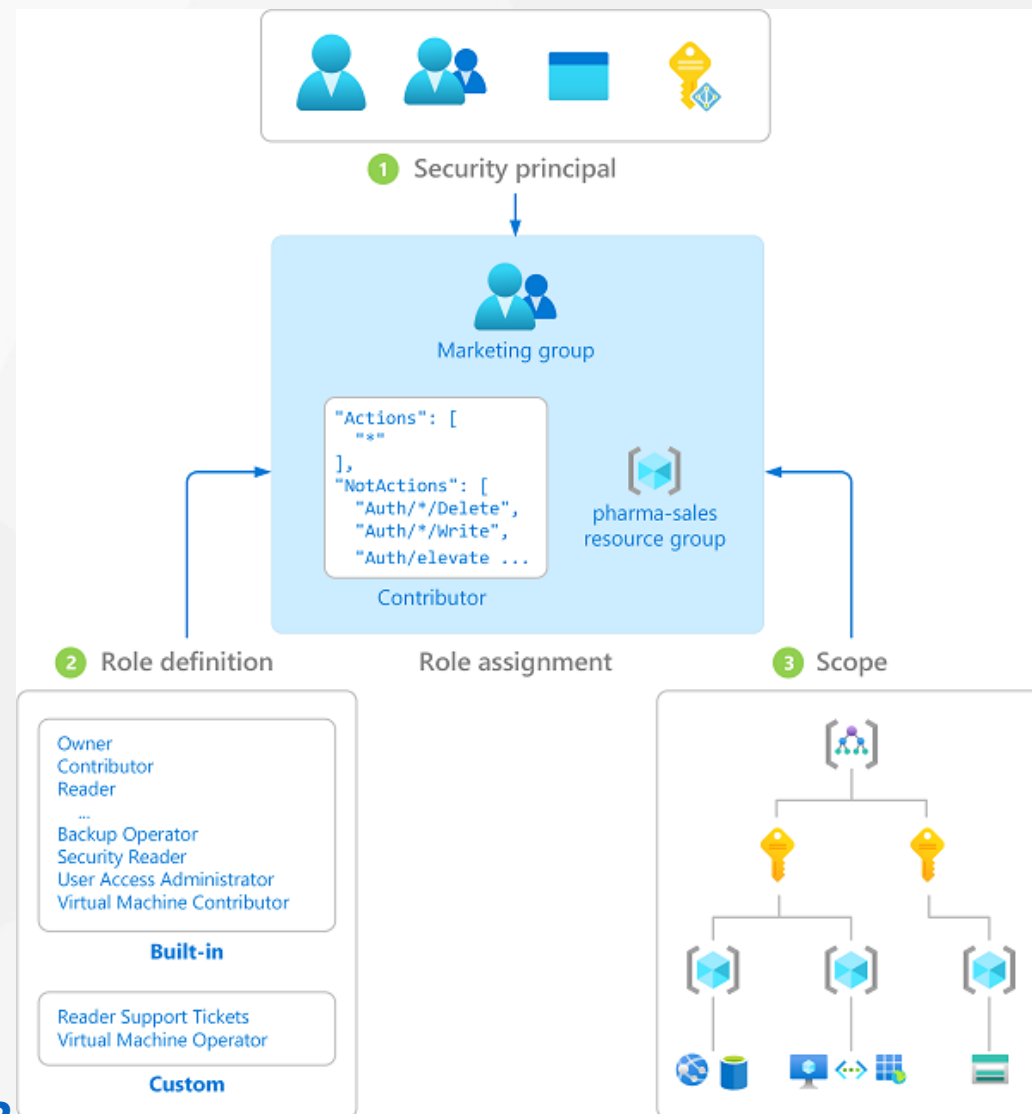
- 什麼範圍

- 什麼角色

- Owner
- Contributor
- Reader

## What is Azure role-based access control (Azure RBAC)?

@Alan Tsai 的學習筆記





# Azure Active Directory



- Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service
- Authentication
- Business to Business (B2B) , Business to Customer (B2C)
- Application 、 Device Management
- RBAC



# Governance Feature







# Resource Lock



- 避免被誤刪
- 可以控制在不同等級
  - Subscription
  - Resource Group
  - Resource

	Read	Update	Delete
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No



# Tag



- 可以用來區分不同資源用途
- 邏輯上面切割
- 在看費用可以進行過濾
- 可以依照不同情境：
  - environment
    - develop
    - production
  - Department
    - Marketing
    - Human Resource

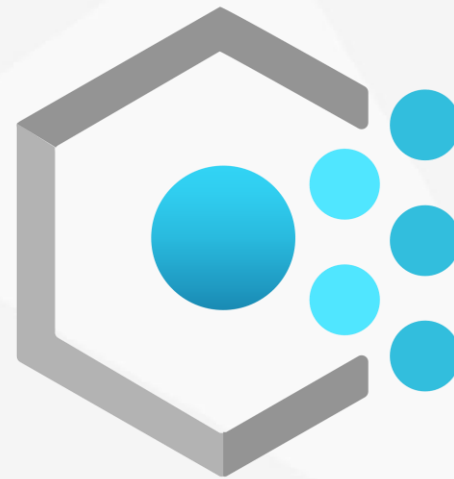




# Azure Policy



- 設定規範，避免不符合公司規定
- 例如
  - 只允許建立在東南亞
  - 只允許開某個大小的機器





# Azure Blueprint



- 和建築物的藍圖一樣概念
- 用來建立出環境
- 使用宣告式 (declarative) 定義
- 有些常見的 resource
  - Role Assignment
  - Policy Assignment
  - Azure Resource Manager Template (ARM Templates)
  - Resource Groups



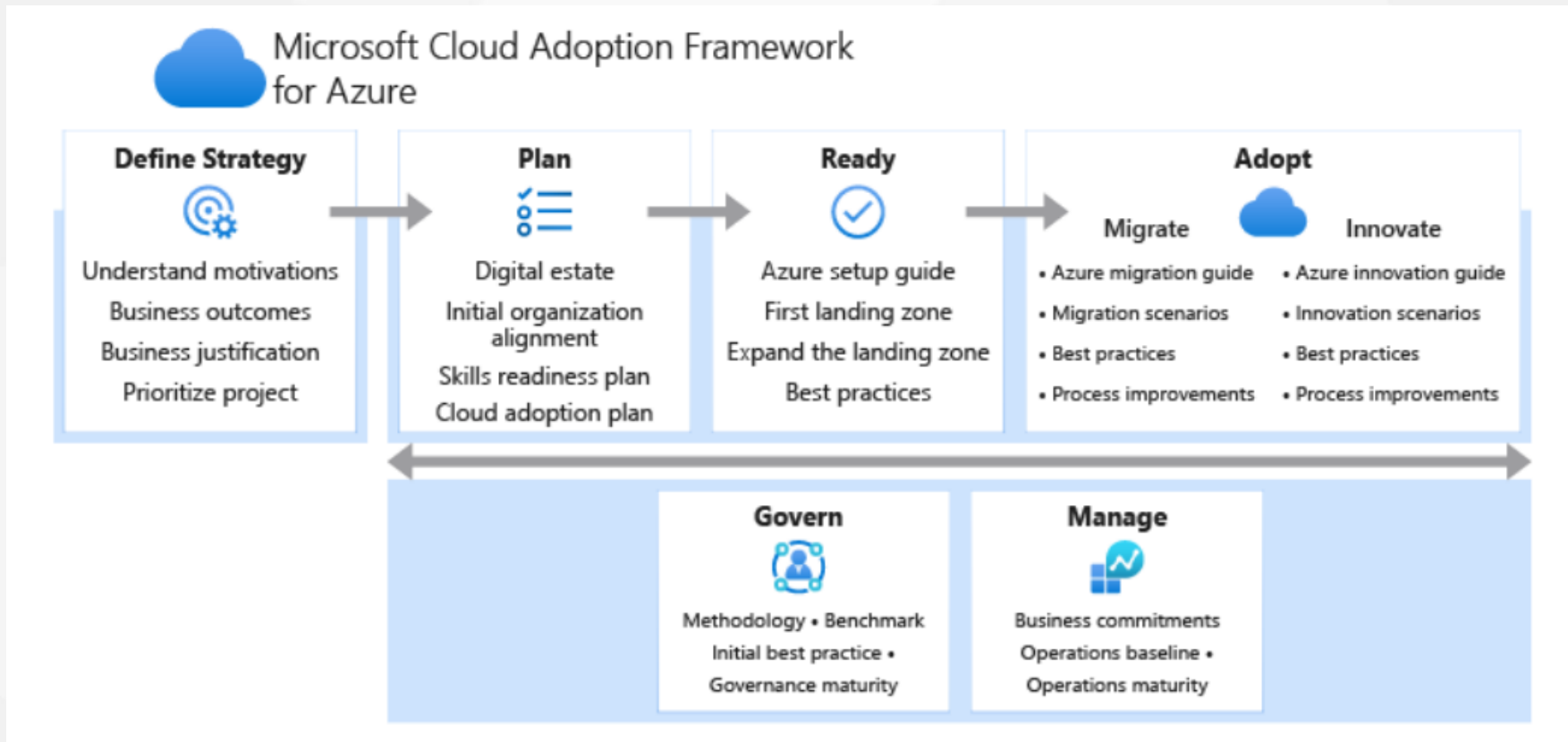
## [What is Azure Blueprints?](#)



# Cloud Adoption Framework for Azure



- 上雲的一些最佳實踐



[What is the Microsoft Cloud Adoption Framework for Azure?](#)

# Compliance 、 Privacy





# Security、Privacy and Compliance



- Security
  - Azure 建立的時候就有把資安作為重要的一環
  - 其中很多透過自動化以及 AI 方式處理已知和未知的攻擊
- Privacy
  - 明確告那些資料會保存並且進行處理
- Compliance
  - 符合國際以及當地國家/特定領域的合規要求



# Microsoft privacy statement



- 明確告知
  - 那些資料被搜集
  - 那些資料被使用
  - 這些使用資料用在那邊
- <https://privacy.microsoft.com/en-us/privacystatement>





# Online Services Terms and Data Protection Addendum



- Online Services Terms
  - <https://www.microsoft.com/en-us/licensing/product-licensing/products>
- Data Protection Addendum
  - <https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67>



# Trust Center



- 可以看到一些最新的訊息
  - 和 Security、Compliance 等有關的訊息
- <https://www.microsoft.com/en-us/trust-center>



# Compliance



2018 年

## Azure covers 85 compliance offerings

The deepest and most comprehensive compliance coverage in the industry

Global	<ul style="list-style-type: none"><li>ISO 27001:2013</li><li>ISO 27017:2015</li><li>ISO 27018:2014</li></ul>	<ul style="list-style-type: none"><li>ISO 22301:2012</li><li>ISO 9001:2015</li><li>ISO 20000-1:2011</li></ul>	<ul style="list-style-type: none"><li>SOC 1 Type 2</li><li>SOC 2 Type 2</li><li>SOC 3</li><li>CIS Benchmark</li></ul>	<ul style="list-style-type: none"><li>CSA STAR Certification</li><li>CSA STAR Attestation</li><li>CSA STAR Self-Assessment</li><li>WCAG 2.0 (ISO 40500:2012)</li></ul>
US Gov	<ul style="list-style-type: none"><li>FedRAMP High</li><li>FedRAMP Moderate</li><li>EAR</li><li>ITAR</li></ul>	<ul style="list-style-type: none"><li>DoD DISA SRG Level 5</li><li>DoD DISA SRG Level 4</li><li>DoD DISA SRG Level 2</li><li>DFARS</li></ul>	<ul style="list-style-type: none"><li>DoE 10 CFR Part 810</li><li>NIST SP 800-171</li><li>NIST CSF</li><li>Section 508 VPATs</li></ul>	<ul style="list-style-type: none"><li>FIPS 140-2</li><li>CJIS</li><li>IRS 1075</li></ul>
Industry	<ul style="list-style-type: none"><li>PCI DSS Level 1</li><li>GLBA (US)</li><li>FFIEC (US)</li><li>Shared Assessments (US)</li><li>SEC 17a-4 (US)</li><li>CFTC 1.31 (US)</li><li>FINRA 4511 (US)</li><li>SOX (US)</li></ul>	<ul style="list-style-type: none"><li>23 NYCRR 500 (US)</li><li>OSFI (Canada)</li><li>FCA + PRA (UK)</li><li>APRA (Australia)</li><li>FINMA (Switzerland)</li><li>FSA (Denmark)</li><li>RBI + IRDAI (India)</li><li>MAS + ABS (Singapore)</li></ul>	<ul style="list-style-type: none"><li>NBB + FSMA (Belgium)</li><li>AFM + DNB (Netherlands)</li><li>European Banking Authority (EBA)</li><li>FISC (Japan)</li><li>HIPAA BAA (US)</li><li>HITRUST Certification</li><li>GxP (FDA 21 CFR Part 11)</li><li>MARS-E (US)</li></ul>	<ul style="list-style-type: none"><li>NHS IG Toolkit (UK)</li><li>NEN 7510:2011 (Netherlands)</li><li>FERPA (US)</li><li>CDSA</li><li>MPAA (US)</li><li>FACT (UK)</li><li>DPP (UK)</li></ul>
Regional	<ul style="list-style-type: none"><li>Argentina PDPA</li><li>Australia IRAP Unclassified</li><li>Australia IRAP PROTECTED</li><li>Canada Privacy Laws</li><li>China GB 18030:2005</li><li>China DJCP (MLPS) Level 3</li></ul>	<ul style="list-style-type: none"><li>China TRUCS / CCCPPF</li><li>EU EN 301 549</li><li>EU ENISA IAF</li><li>EU Model Clauses</li><li>EU – US Privacy Shield</li><li>GDPR</li><li>Germany C5</li></ul>	<ul style="list-style-type: none"><li>Germany IT-Grundschutz workbook</li><li>India MeitY</li><li>Japan CS Mark Gold</li><li>Japan My Number Act</li><li>Netherlands BIR 2012</li><li>New Zealand Gov CIO Framework</li></ul>	<ul style="list-style-type: none"><li>Singapore MTCS Level 3</li><li>Spain ENS High</li><li>Spain DPA</li><li>UK Cyber Essentials Plus</li><li>UK G-Cloud</li><li>UK PASF</li></ul>

<https://twitter.com/anBenedetti/status/1049917137429716994/photo/1>

@Alan Tsai 的學習筆記



# Azure Sovereign Regions



- 和 Public Azure 隔離
- Azure Government
  - 針對美國政府
- Azure China
  - 世紀互聯運維

# 結語





# 結語



- 了解整個安全相關
  - 從外部到系統內部
  - 網路安全可以用什麼
- 了解 Identity Service
  - Authentication vs Authorization
  - RBAC
- Governance
  - Azure Policy



# 參考資料



- [Azure Fundamentals part 4: Describe general security and network security features](#)
- [Azure Fundamentals part 5: Describe identity, governance, privacy, and compliance features](#)



# 歡迎訂閱、按贊 + 分享



- Alan Tsai 的學習筆記
- <https://blog.alantsai.net>
- FB粉絲頁
- <http://fb.alantsai.net>
- Youtube
- <http://yt.alantsai.net>



[contact@alantsai.net](mailto:contact@alantsai.net)

@Alan Tsai 的學習筆記