實踐淨零碳排
邁向企業永續

流通服務業ESG治理刻不容緩
ESG沒做好將衝擊品牌形象、降低顧客黏著
更影響上市櫃版圖發展
企業必須快速建立**全方位永續機制，實踐淨零碳排**
因應營運風險、法規要求的衝擊

碳中和 打造淨零永續經濟

- 開創無碳未來的承諾
- 雙軸轉型實現永續商務
- 雲端服務助攻企業落實 ESG

Google Cloud
Anne Shih 史哲芳
anneshih@google.com

25

Google 已創立
滿 25 週年

17

Google 台灣辦公室
已成立超過 17 年

10

Google 資料中心與
Google Cloud 雲端區域
已在台營運 10 年

1st Google Data Center & Google Cloud Region in APAC in 2013

數位韌性

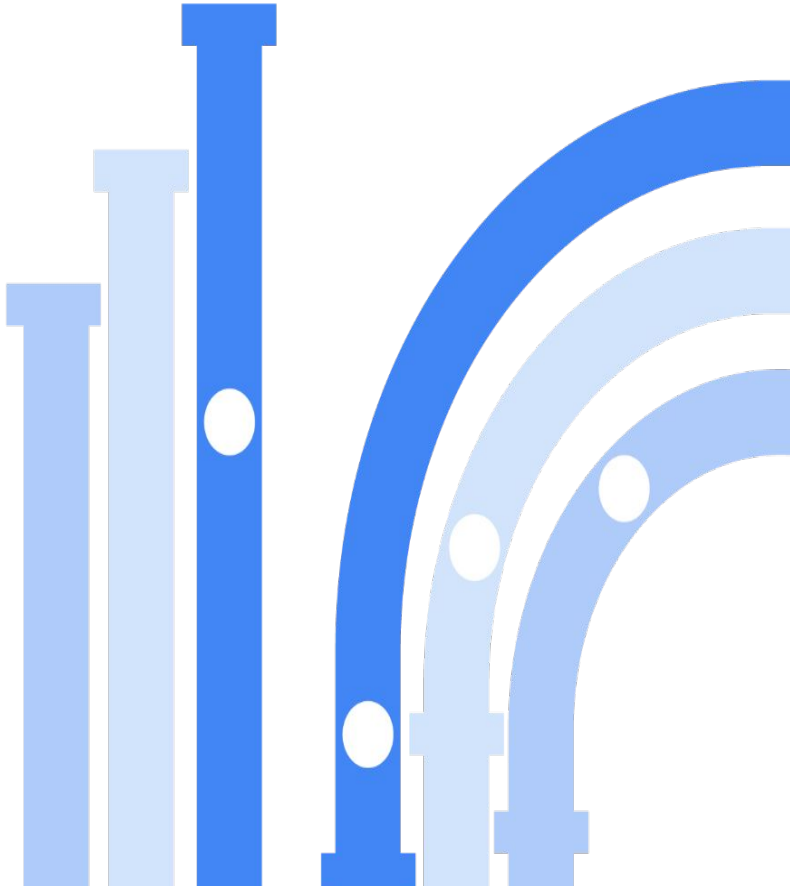
Digital Resilience

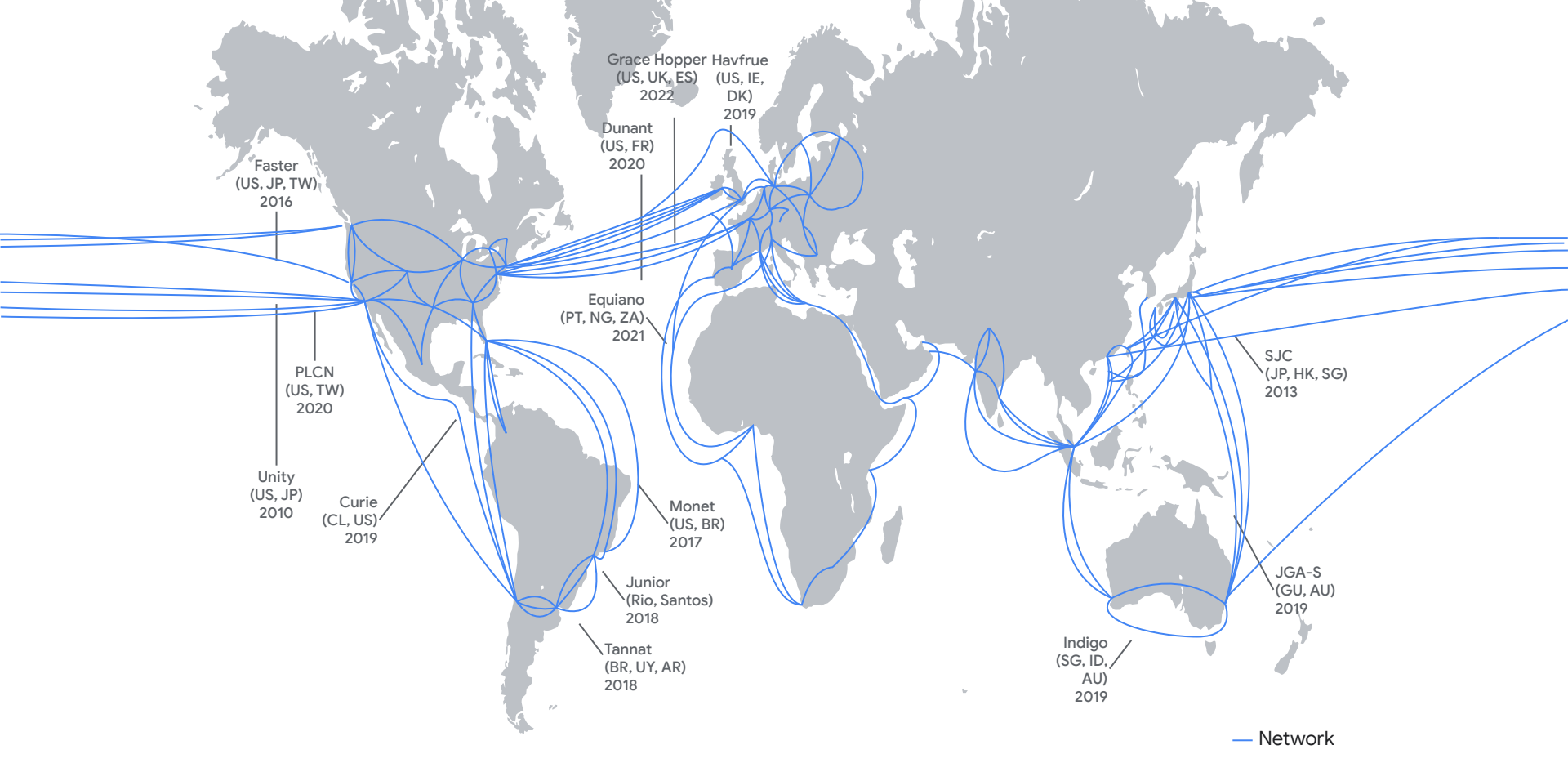
永續營運

Sustainable Operations

數位韌性

Digital Resilience



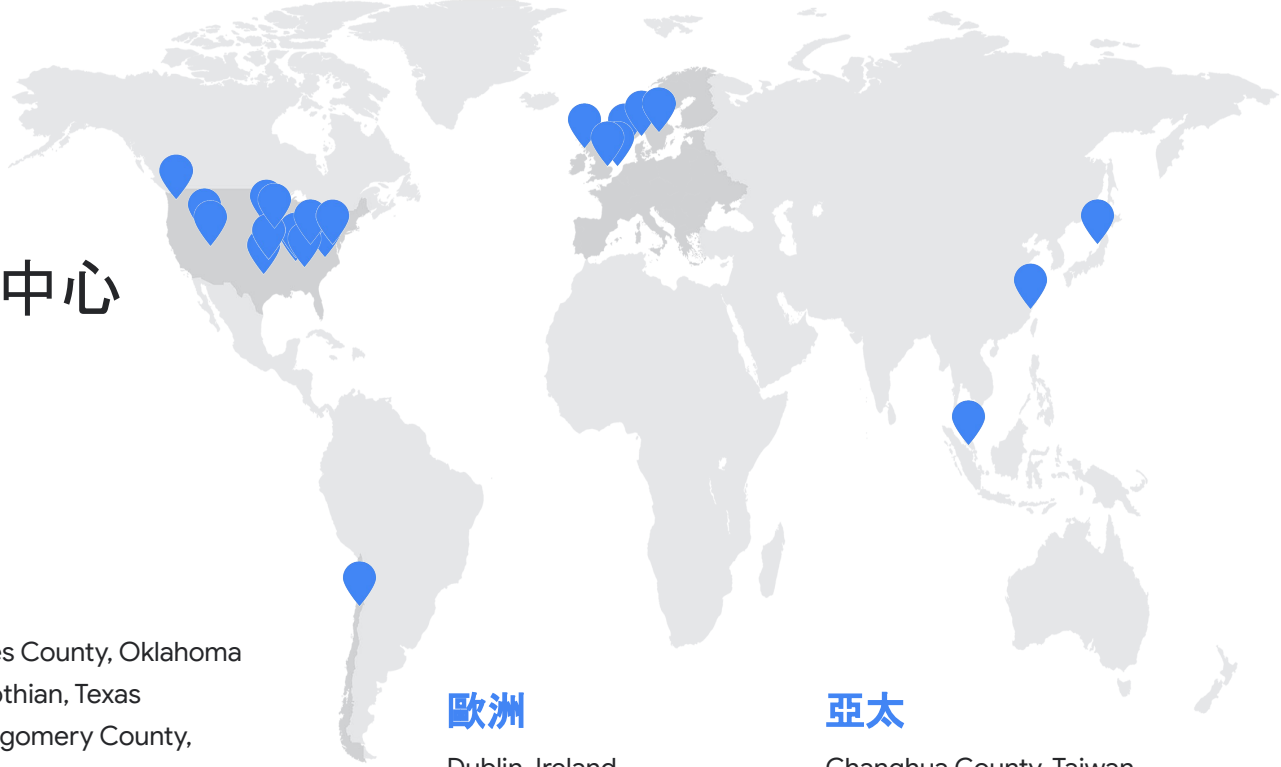


Google 海底電纜投資佈局

24 個城市

佈局全球的資料中心

4 大洲



美洲

Berkeley County, South Carolina
Council Bluffs, Iowa
The Dalles, Oregon
Douglas County, Georgia
Henderson, Nevada
Jackson County, Alabama
Lenoir, North Carolina
Loudoun County, Virginia
Mayes County, Oklahoma
Midlothian, Texas
Montgomery County, Tennessee
New Albany, Ohio
Papillion, Nebraska
Storey County, Nevada
Quilicura, Chile

歐洲

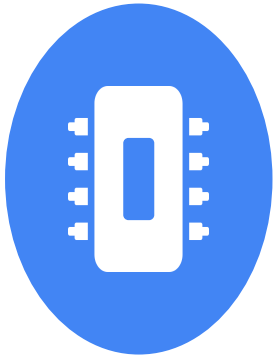
Dublin, Ireland
Eemshaven, Netherlands
Middenmeer, Netherlands
Fredericia, Denmark
Hamina, Finland
St Ghislain, Belgium

亞太

Changhua County, Taiwan
Singapore
Inzai, Japan

數位韌性

從裡到外層層維護，守護資訊安全



特製專用晶片
Purpose-built chips

特製專用伺服器
Purpose-built servers

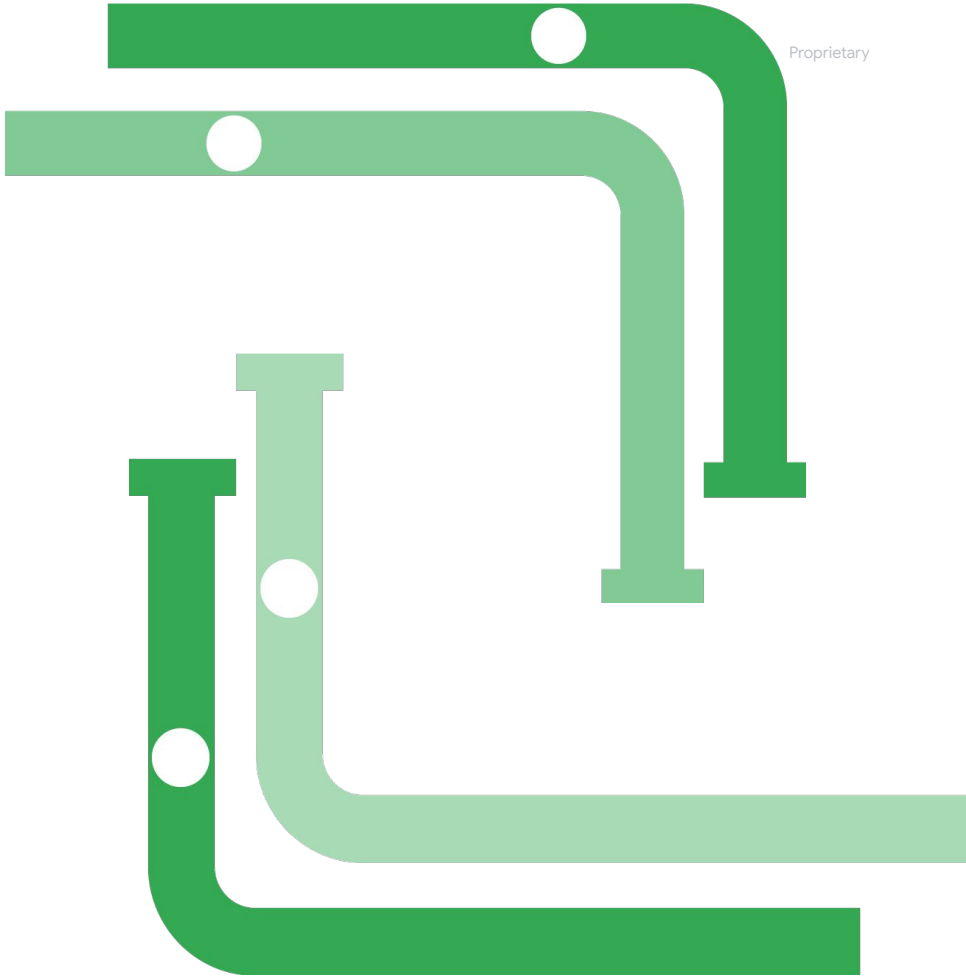
特製專用儲存空間
Purpose-built storage

特製專用網路
Purpose-built network

特製專用資料中心
Purpose-built data centers

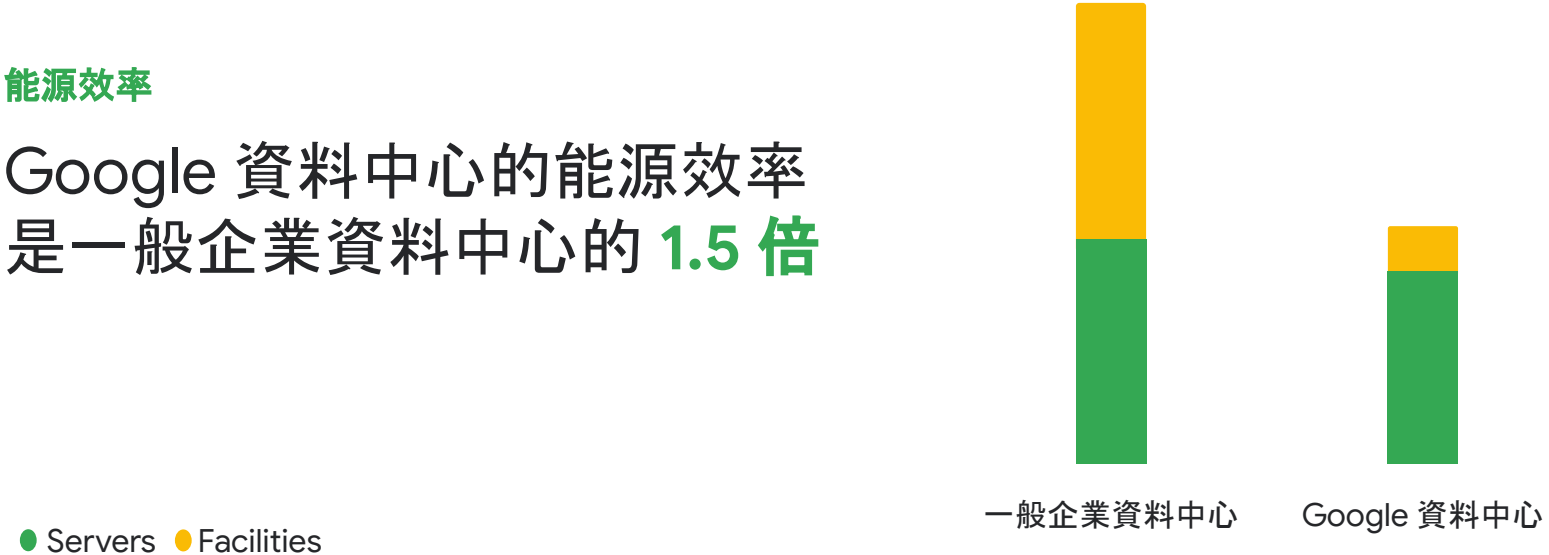
永續營運

Sustainable Operations



能源效率

Google 資料中心的能源效率是一般企業資料中心的 1.5 倍



3X

Google 資料中心五年前的用電量，可在現今產生高出**三倍**的運算力

Source: Google Environmental Report

碳智慧運算平台

透過轉移彈性的運算工作與電網的綠色時間一致，來減少資料中心的碳足跡

跨域運算

超越時間

降低碳排放

台灣彰濱資料中心: Google在亞洲規模最大的資料中心

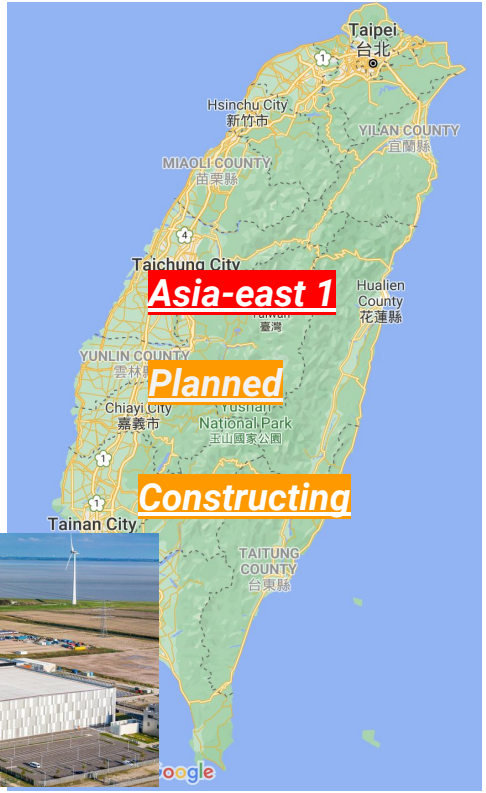
第一座 Google 在亞洲 Data Center 位於台灣彰濱 (彰化縣線西鄉彰濱西二路85號)，面積**45,000**坪

台南 **30,000**坪及**雲林** **60,000**坪資料中心規劃建置中

三大公有雲在全亞洲**費用最低**之雲端資料中心

彰濱資料中心在台灣島內，可確保**最低的網路延遲**、及更完善的資料安全

100% 使用再生能源，PUE為**1.1**



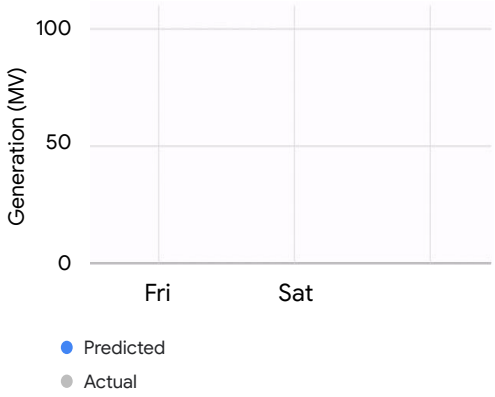
Google 台灣資料中心節能、省水、不破壞當地產業生態

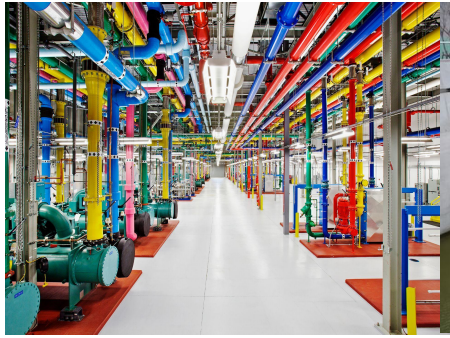
DeepMind 系統透過神經網路能提前 36 小時預測風力電量，將風力發電的價值提升 20%

採用夜間降溫、熱能儲存，比一般資料中心節能5成

儲存雨水再利用，作為冷卻水用途

全球首樁在亞洲的再生能源採購，漁電共生與當地漁業共榮





每一次 **搜尋**...

每一次 **路徑規劃**...

每發送一封 **E-mail**...

每一次 **視訊會議**...

每一份 **儲存的資料**...

0 碳足跡

永續地球

共好社會

協助合作夥伴 提供藍圖：Carbon Footprint

進行測量、產出報告，以及減少雲端運算產生的碳排放

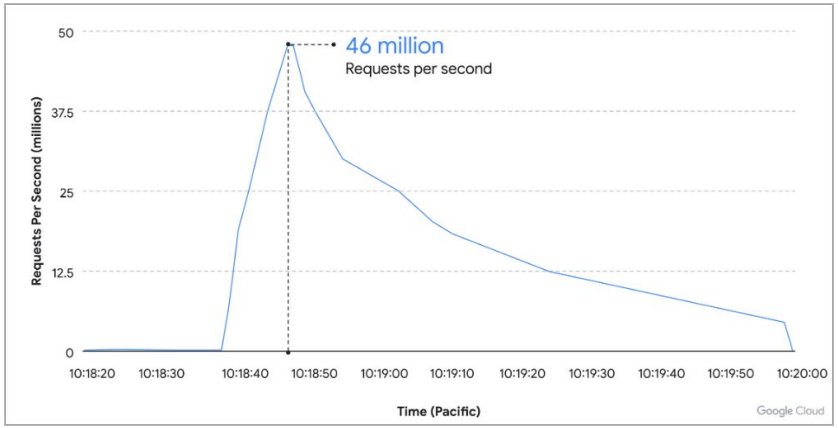
- 提供總碳排放量數據 - 但淨碳排放量永遠是零
- 第三方專家認證的計算方法
- 被溫室氣體盤查議定書所接受
- 可匯出資料整合至組織整體的碳排放計算中
- 所有 GCP 的用戶可免費使用
- 提供減少碳排放的建議作法

Introducing

GCP 雲端安全實務分享 (防護、監控、合規)

Google Cloud

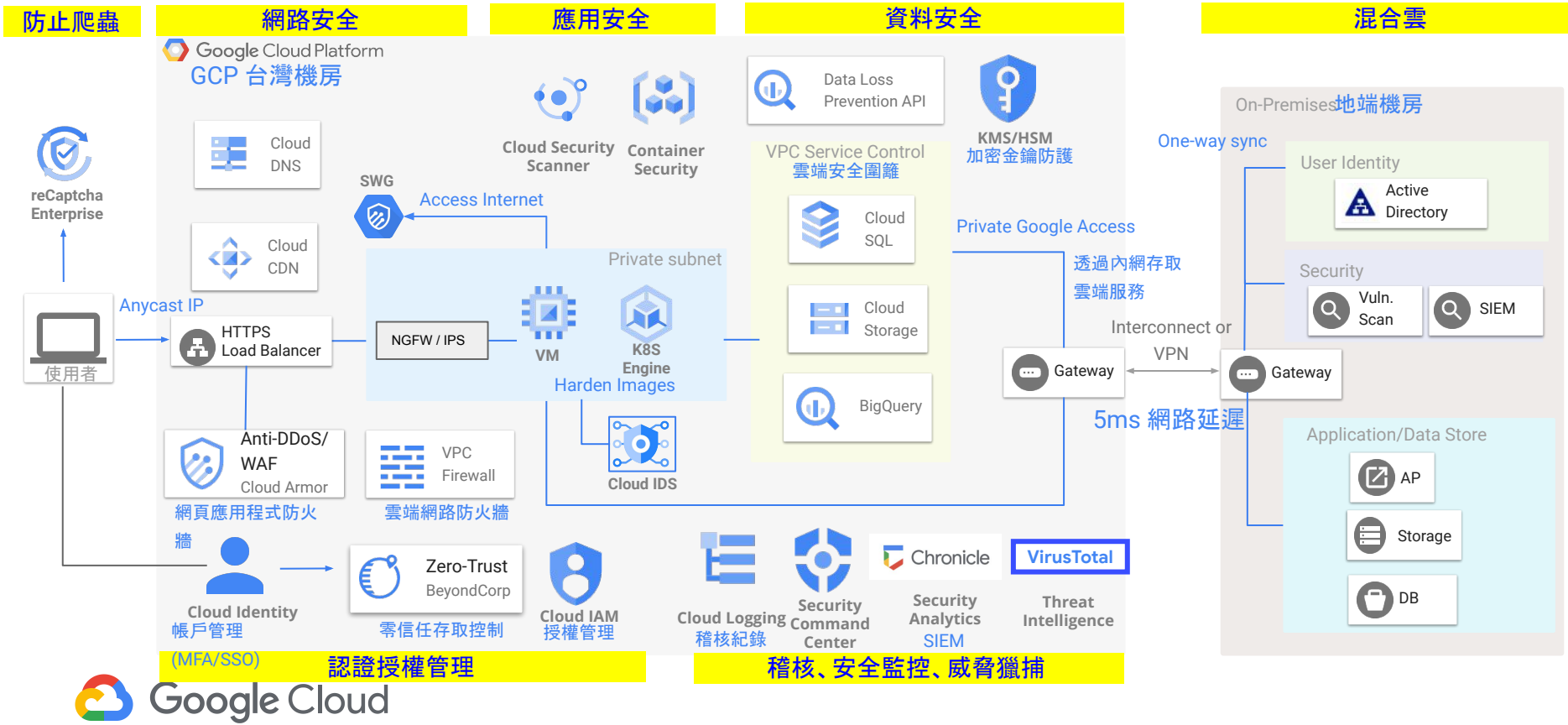
每秒4600萬次連線請求! Google阻止目前最大規模DDoS 攻擊



- 相對於常見L3/L4 DDoS攻擊、駭客使用L7 應用層DDoS 連線攻擊
- DDoS 攻擊來自132個國家、5,256個IP (22% IP 來自Tor Network)
- 駭客入侵網路上具有漏洞的網路設備做為跳板，發送大量連線請求並隱匿攻擊來源
- 客戶使用自動產生相關防護規則 (**Adaptive Protection**)以及**Rate-limiting** 有效抵禦DDoS 攻擊

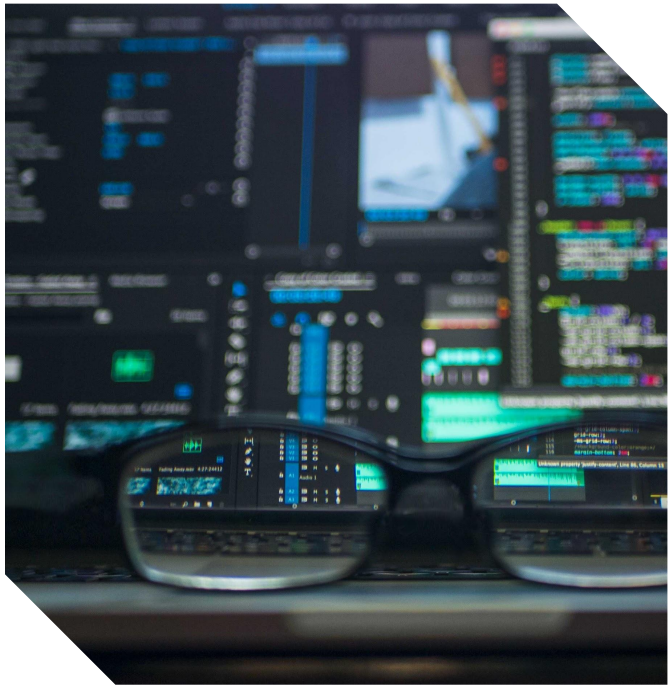
https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

Google Cloud 安全架構



Google Cloud 雲端基礎設施安全

- 跨裝置、內部網路和系統的可疑活動監控和資訊收集
- 漏洞掃描、滲透測試和稽核、安全研究、獎勵計劃
- 防毒引擎可協助識別惡意軟體，裝置管理代理程式監控惡意軟體、應用程式修補程式和管理配置
- 事件管理和回應團隊全年 365 天、每天 24 小時對潛在資料和安全事件進行分類、調查和回應。如果發生已確認的資料事件，Google 將立即通知您，並立即採取合理措施來最大程度地減少損害並保護您的資料。



GCP 對資料安全及個資隱私保護的承諾

Our **commitment to transparency** means that you – and only you – have explicit control over your data and how it is used.

- 我們只在客戶授權同意下存取客戶資料
- 我們不會將客戶的資料銷售給第三方
- 我們不會使用客戶資料用來進行廣告行銷業務
- 存取客戶資料提供完整稽核紀錄
- 資料傳輸及儲存預設進行加密
- 我們不會使用客戶資料來進行AI 模型訓練
- 當有客戶資料外洩事件發生，我們會儘速通知客戶
- 資料安全及隱私保護符合國際標準

Sources: Google Cloud Platform Data Processing and Security Terms (Customers) | Google Workspace Data Processing Amendment | Google Cloud Privacy Notice

Google Cloud's 通過國際資安標準及第三方獨立單位稽核

Our products regularly undergo **independent third-party audits** with over 2 million control instances audited annually.
Google maintains certifications, attestations of compliance, or audit reports against standards and regulations around the world.

Global

ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27110
ISO/IEC 27701
ISO/IEC 9001
SOC 1
SOC 2
SOC 3
PCI DSS
PCI 3DS
CSA STAR
CyberGRX
KY3P
SIG

Americas

USA
Sarbanes- Oxley
SEC Rule 17a-4(f)
CFTC Rule 1.31(c)-(d)
FINRA Rule 4511(c)
FFIEC
FDIC
OCC
Federal Reserve Guidance
CCPA
COPPA

Canada
PIPEDA
OSFI Guideline B-10

Brazil
LGPD

Argentina
PDPA

Mexico
CNBV LIC
CNBV LMV

Europe, Middle East & Africa

Europe
GDPR
EU Model Contract Clauses
EU CoC
SWIPO
EBA Guidelines
EIOPA Guidelines
ESMA Guidelines

Germany
BaFin
MaRisk

Austria
BWG
VAG

Switzerland
FINMA
ISAE 3000 Type 2

Netherlands
DNB

Spain
Banco de España - Circular 2/2016

UK
FCA FG16/5
FCA SYSC 8
PRA SS2/21

France
ACPR

Italy
Banca D'Italia - Circular 285

Portugal
Banco de Portugal

Luxembourg
CSSF

Poland
KNF

Sweden
SFSA

South Africa
POPI

Asia Pacific

Australia
APP
APRA CPS 231
APRA CPS 234

India
RBI

Malaysia
BNM

Indonesia
SEOJK 21
POJK 38

Taiwan
FSC Banking Outsourcing
FSC Insurance Outsourcing
PDPA

Philippines
BSP

Japan
FISC
My Number Act
APPI

Korea
FSC

Singapore
MTCS Tier 3
OSPAR
MAS Guidelines
ABS Guide
PDPA

Hong Kong
HKIA Outsourcing GL14
HKMA Outsourcing SA-2
PDPO

Additional compliance offerings and further information is available at
cloud.google.com/security/compliance

GCP 通過第三方獨立稽核、國際認證並提供參考文件

	Global
資安防護	ISO/IEC 27001
雲端安全防護	ISO/IEC 27017
雲端個資保護	ISO/IEC 27018
個資保護	ISO/IEC 27701
歐盟資料保護規範	GDPR
機房管理	SOC 2
支付卡產業資料安全	PCI DSS
雲端安全驗證	CSA STAR
	下載稽核、認證報告

台灣法規相關文件

1. 金融機構作業委託他人處理 內部作業制度及程序辦法
   - 說明網頁
   - Google Cloud 合規需求對應
   - Google Workspace 合規需求對應
2. 保險業作業委託他人處理應注意事項
   - 說明網頁
   - Google Cloud 合規需求對應
   - Google Workspace 合規需求對應
3. 個人資料保護法
   - 說明網頁
   - Google Cloud 合規需求對應

GCP 雲端安全實務分享 (防護、監控、合規)

Google Cloud

Security Command Center

管理您的雲端安全狀況

Near real-time visibility into Google Cloud resources and policies

資產管理
(資產清單、變更清單)

Security monitoring for misconfigurations and web app vulnerabilities

安全配置
(網路、權限、弱點掃描、Log)

Threat detection for malicious activity and unauthorized behavior

威脅監測
(網路、權限、容器、金鑰)

Compliance violations based on industry standards and benchmarks

合規/最佳實踐
(ISO, PCI, NIST, CIS, OWASP)

https://cloud.google.com/security-command-center

安全配置管理

Security Health Analytics

持續評估 GCP 基礎架構的設定錯誤和漏洞

存取權限、加密設定

Storage

- Publicly exposed buckets
- Storage resources missing CMEK
- Use of legacy bucket ACLs

防火牆規則、網路安全實踐

Networking

- Overly permissive firewall rules
- Use of default and/or legacy networks
- Subnetworks that do not use private access to Google APIs

稽核軌跡、監控規則

Logging/ Monitoring

- Monitoring disabled
- Storage buckets with logging disabled
- Stackdriver monitoring for Kubernetes clusters not enabled
- VPC Flow logs disabled

帳戶安全、權限設定

Identity

- Overprovisioned admin accounts
- Permission grants outside your org
- Insufficient separation of duties

虛擬機安全設定

VM Instances

- IP forwarding enabled
- Broad service account or API access enabled
- SSL & SSH misconfigurations

容器安全

GKE Clusters

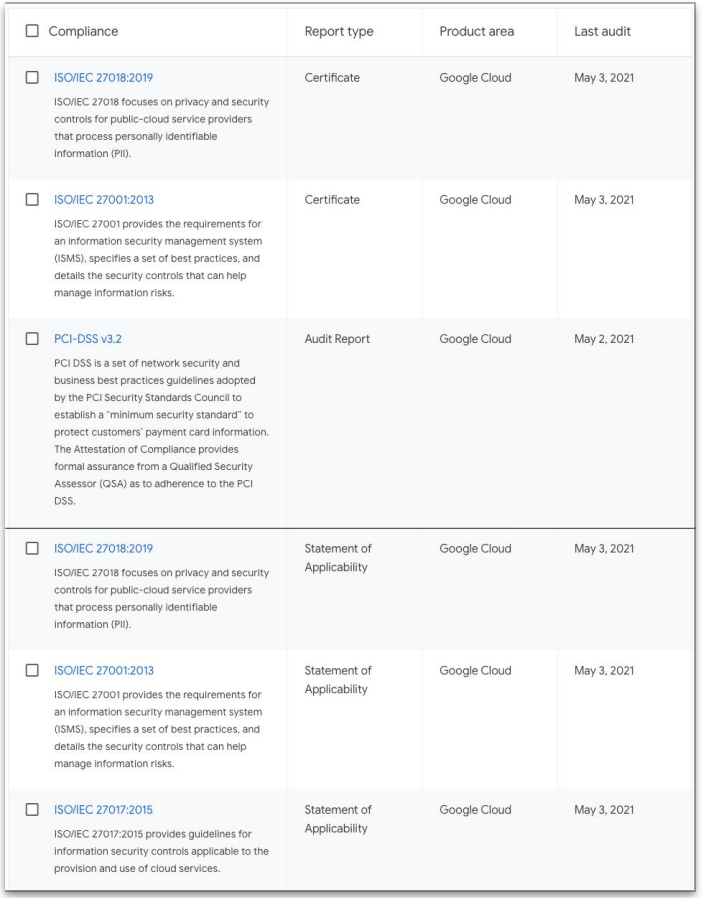
- Private cluster disabled
- Network policy disabled
- Master authorized network disabled
- IP alias disabled
- Legacy authorization enabled

GCP 雲端安全實務分享 (防護、監控、合規)

Google Cloud

您可以在GCP網站直接取得最新稽核及驗證報告

- Customer can access up-to-date GCP compliance and audit report (ISO, PCI-DSS, SOC2, CSA, etc.)
- https://cloud.google.com/security/compliance/compliance-reports-manager



Compliance	Report type	Product area	Last audit
ISO/IEC 27018:2019 ISO/IEC 27018 focuses on privacy and security controls for public-cloud service providers that process personally identifiable information (PII).	Certificate	Google Cloud	May 3, 2021
ISO/IEC 27001:2013 ISO/IEC 27001 provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks.	Certificate	Google Cloud	May 3, 2021
PCI-DSS v3.2 PCI DSS is a set of network security and business best practices guidelines adopted by the PCI Security Standards Council to establish a "minimum security standard" to protect customers' payment card information. The Attestation of Compliance provides formal assurance from a Qualified Security Assessor (QSA) as to adherence to the PCI DSS.	Audit Report	Google Cloud	May 2, 2021
ISO/IEC 27018:2019 ISO/IEC 27018 focuses on privacy and security controls for public-cloud service providers that process personally identifiable information (PII).	Statement of Applicability	Google Cloud	May 3, 2021
ISO/IEC 27001:2013 ISO/IEC 27001 provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks.	Statement of Applicability	Google Cloud	May 3, 2021
ISO/IEC 27017:2015 ISO/IEC 27017:2015 provides guidelines for information security controls applicable to the provision and use of cloud services.	Statement of Applicability	Google Cloud	May 3, 2021

Certificate - ISO 27001

條列出通過驗證的服務及所在機房

Google LLC

Scope for certificate 2012-001b

Google Cloud Platform (continued):

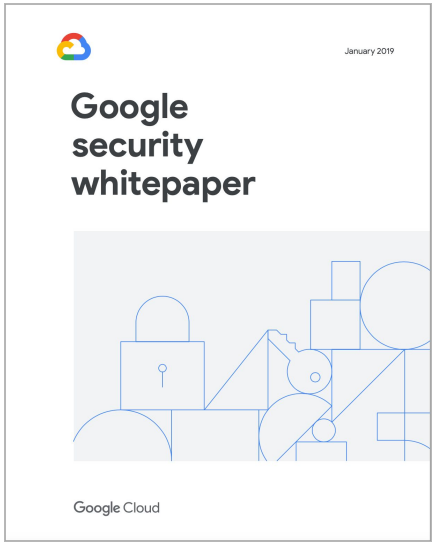
- Container Registry
- Data Catalog
- Database Migration Service
- Dataflow
- Datalab
- Dataproc
- Datastore
- DataStream
- Dialogflow
- Document AI
- Firebase Authentication
- Firebase Test Lab
- Firestore
- Game Servers
- GCP Marketplace
- Google Cloud Armor
- Google Cloud Identity-Aware Proxy
- Google Kubernetes Engine
- Hub
- Identity & Access Management (IAM)
- Identity Platform
- Insights
- IoT Core
- Key Access Justification (Access Sovereignty)
- Lux
- Managed Service for Microsoft Active Directory (AD)
- Memorystore
- Network Intelligence Center
- Network Service Tiers
- Persistent Disk
- Pub/Sub
- reCAPTCHA Enterprise
- Resource Manager API
- Risk Manager
- Secret Manager
- Security Command Center
- Service Directory
- Service Infrastructure
- Speech-to-Text
- Storage Transfer Service
- Talent Solution
- Text-to-Speech
- Traffic Director
- Transfer Appliance
- Video Intelligence API
- Virtual Private Cloud
- VPC Service Controls

The following locations are in scope:

Data Centers:

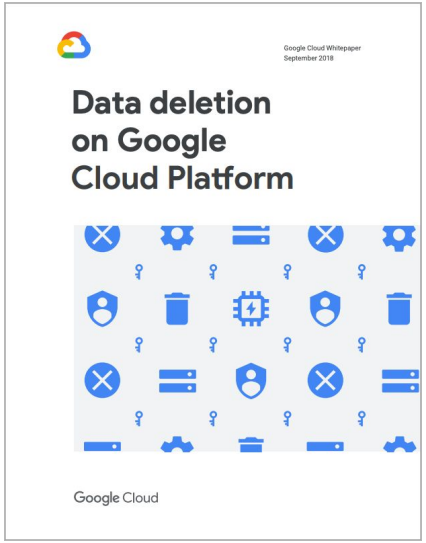
- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America
- Atlanta (1) (GA), United States of America
- Atlanta (2) (GA), United States of America
- Changhua, Taiwan
- Clarksville (TN), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Delhi, India
- Dublin, Ireland
- Eemshaven, Groningen, The Netherlands
- Frankfurt (1), Hesse, Germany

提供完整資訊並協助客戶進行報部及查核準備

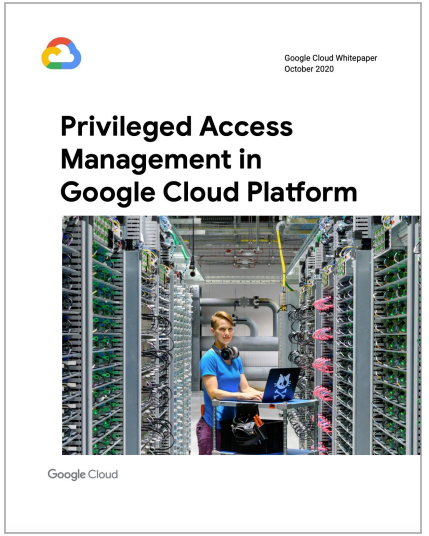


點擊下載

點擊下載



點擊下載



點擊下載

協助客戶 提供ESG藍圖：Carbon Footprint

進行測量、產出報告，以及減少雲端運算產生的碳排放

- **提供總碳排放量數據 - 但淨碳排放量永遠是零**
- **第三方專家認證的計算方法**
- **被溫室氣體盤查議定書所接受**
- **可匯出資料整合至組織整體的碳排放計算中**
- **所有 GCP 的用戶可免費使用**
- **提供減少碳排放的建議作法**

https://cloud.google.com/carbon-footprint?hl=zh-tw

碳排報告 sample


2023/10/11 中午12:06
帳單帳戶 [redacted] 的總覽 – 碳足跡 – Google Cloud 控制台
帳單帳戶 [redacted] 因使用列入計算的 Google Cloud 服務而產生的溫室氣體總排放量。
這些排放量資料尚未經過第三方驗證或確認，由於供應鏈和相關碳排放量非常複雜，上述估計值會隨著我們方法和資料來源的改善而改變。瞭解這項資料的估算方式
年度碳足跡
從 2023年3月到 2023年8月
按位置計算的總量： 1.8 tCO₂e
範圍 1： 0.002 tCO₂e
範圍 2 按位置計算的碳足跡： 0.90 tCO₂e
範圍 3： 0.92 tCO₂e
月份碳足跡
2023年8月
按位置計算的總量： 0.40 tCO₂e
↑ 1.9% 與 2023年7月相比的退步幅度
範圍細目代表了 Google 可列入報表的碳排放類別，提供這些資訊的用意在於提高明確性和透明度。
按位置計算的每月碳足跡估計值
2023年4月
2023年5月
2023年6月
2023年7月
2023年8月
2023年8月各項專案按位置計算的碳足跡估計值
圖表檢視
hhgalaxy-183504
data-337210 0.12
cosmos-325501 0.041
adsystem-319705 0.014
publicfiles-325708 0.012
hhg-ai 0.012
aisystem-331603 0.003
hhgalaxy-orderdata <0.001
kaodata <0.001
finance-54357012 <0.001
專案
碳足跡 · tCO₂e
2023年8月各項產品按位置計算的碳足跡估計值
圖表檢視
Compute Engine 0
BigQuery 0.11
Vertex AI 0.002
Cloud Monitoring 0.002
Cloud Storage 0.001
Networking <0.001
Cloud Logging <0.001
Cloud Key Management Service (KMS) <0.001
Notebooks <0.001
Cloud Run <0.001
產品
碳足跡 · tCO₂e
2023年8月各個區域按位置計算的碳足跡估計值
圖表檢視
asia-east1
asia-east2 0.018
us-central1 0.013
全球或多區域 0.003
us-central2 <0.001
us-east1 <0.001
europe-west1 <0.001
us-west1 <0.001
asia-northeast1 <0.001
asia-southeast1 <0.001
地區
碳足跡 · tCO₂e

您可以使用和Google 相同的資安工具保護您在GCP 及地端的IT系統

NIST 網路安全框架 (Cyber Security Framework, CSF)

Identify

資產管理

Cloud Asset Inventory

安全配置及威脅監控

Security Command Center

提供威脅情資

VirusTotal Enterprise

支援地端/其他雲服務

Protect

零信任存取控制

chrome BeyondCorp Enterprise

支援地端/其他雲服務

Google Workspace + 帳戶保護

Security Command Center

防止機器人/爬蟲

reCAPTCHA

支援地端/其他雲服務

Anti-DDoS

Cloud Armor

支援地端/其他雲服務

Detect

SIEM

Chronicle

支援地端/其他雲服務

Security Command Center

網路安全監控

Cloud IDS

Cloud DLP

支援地端/其他雲服務

Respond

SOAR 自動化回應

Siemplify

支援地端/其他雲服務

資安事故調查及應變

MANDIANT

支援地端/其他雲服務

Recover

資料備份和災難復原

Actifio Go

支援地端/其他雲服務

資安事故調查及應變

MANDIANT

支援地端/其他雲服務

為何考慮ERP上雲？

Google Cloud

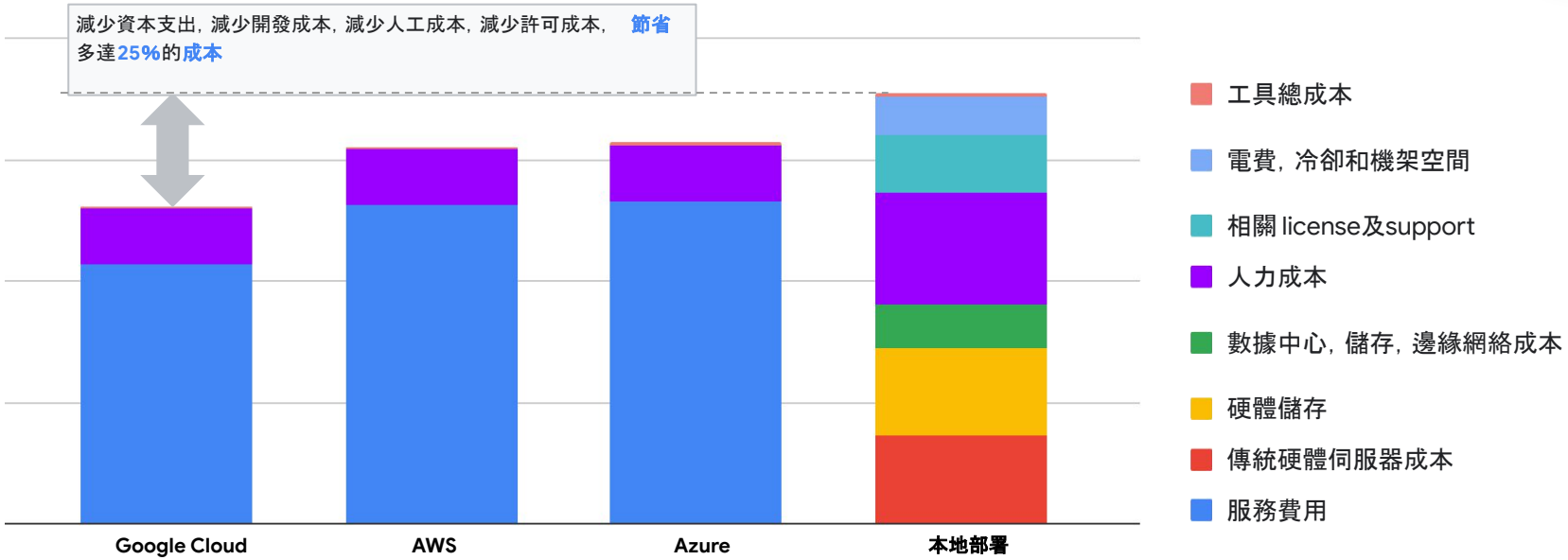
企業常見問題....

- 人力不足，資訊部門每天要處理好多需求，身兼多職...
- 主機維護不易，擔心停機、停電問題....
- 硬體成本高，新機採購還有系統搬遷 & 軟體授權費...
- 碰到攻擊就一個頭兩個大...
- 老闆擔心地緣政治、災難風險，資料丟失...
- 稽核文件需求好多，該如何符合條件？(ESG、資安...)

Why Cloud

1. 減少建置機房成本
2. 可依實際營運彈性調整主機與資料庫等級
3. 國際級設備，降低天災人禍資料損毀風險
4. 無須專人維護主機與擴充汰換硬體設備
5. 彈性的自動化備份機制
6. 全球多處據點，可擴充異地備援
7. 可應用AI或數據分析服務

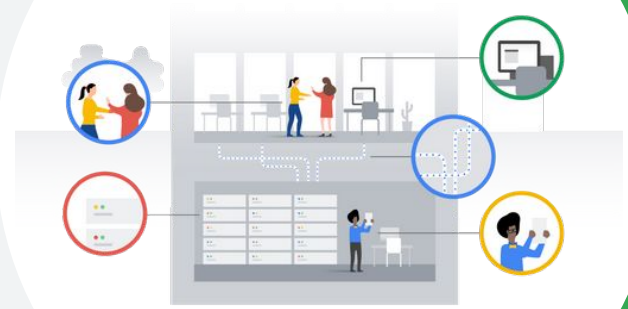
將地端機器遷移到Google Cloud，TCO可降低25%以上



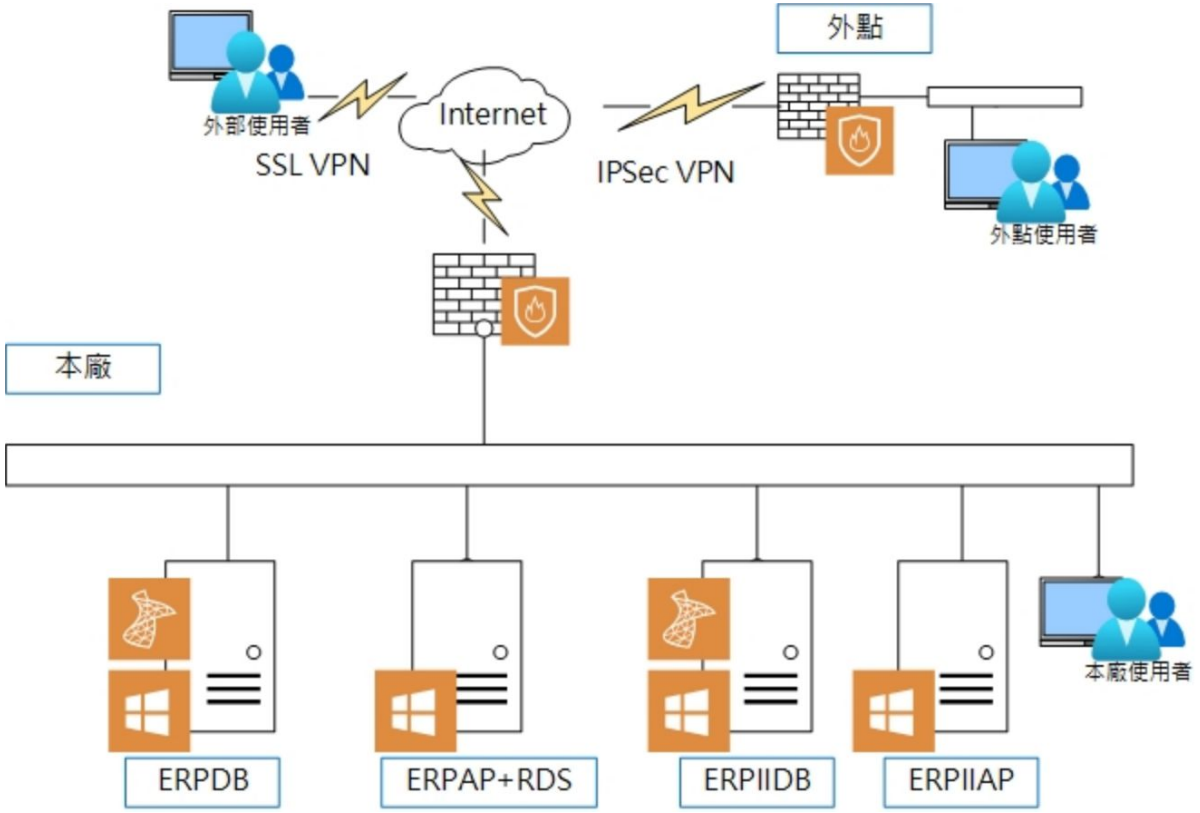
* 計算標準：200 虛擬機，8 主機，2 全職員工 (用於操作本地部署的設備)

Source: Kinsta

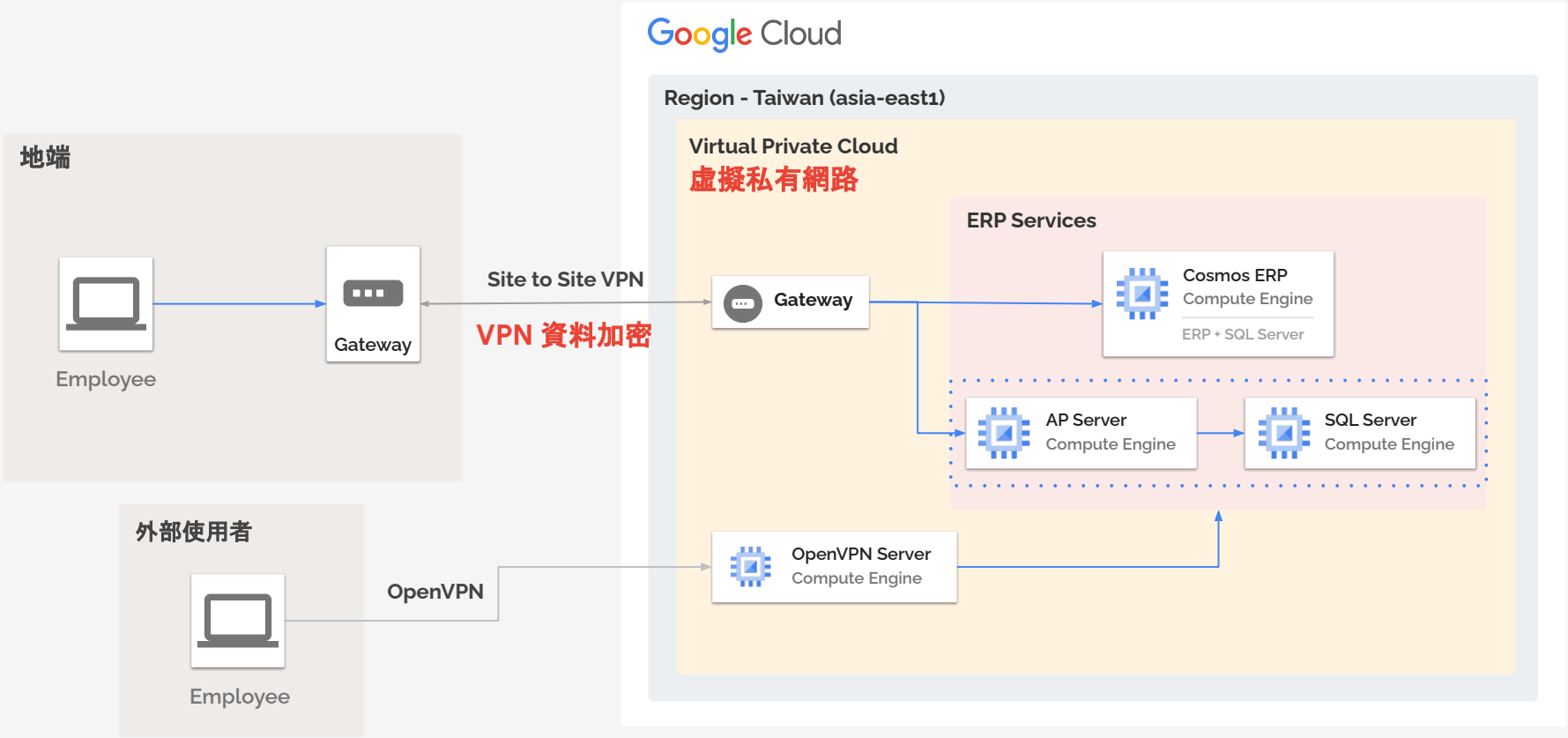
鼎新 ERP上雲說明



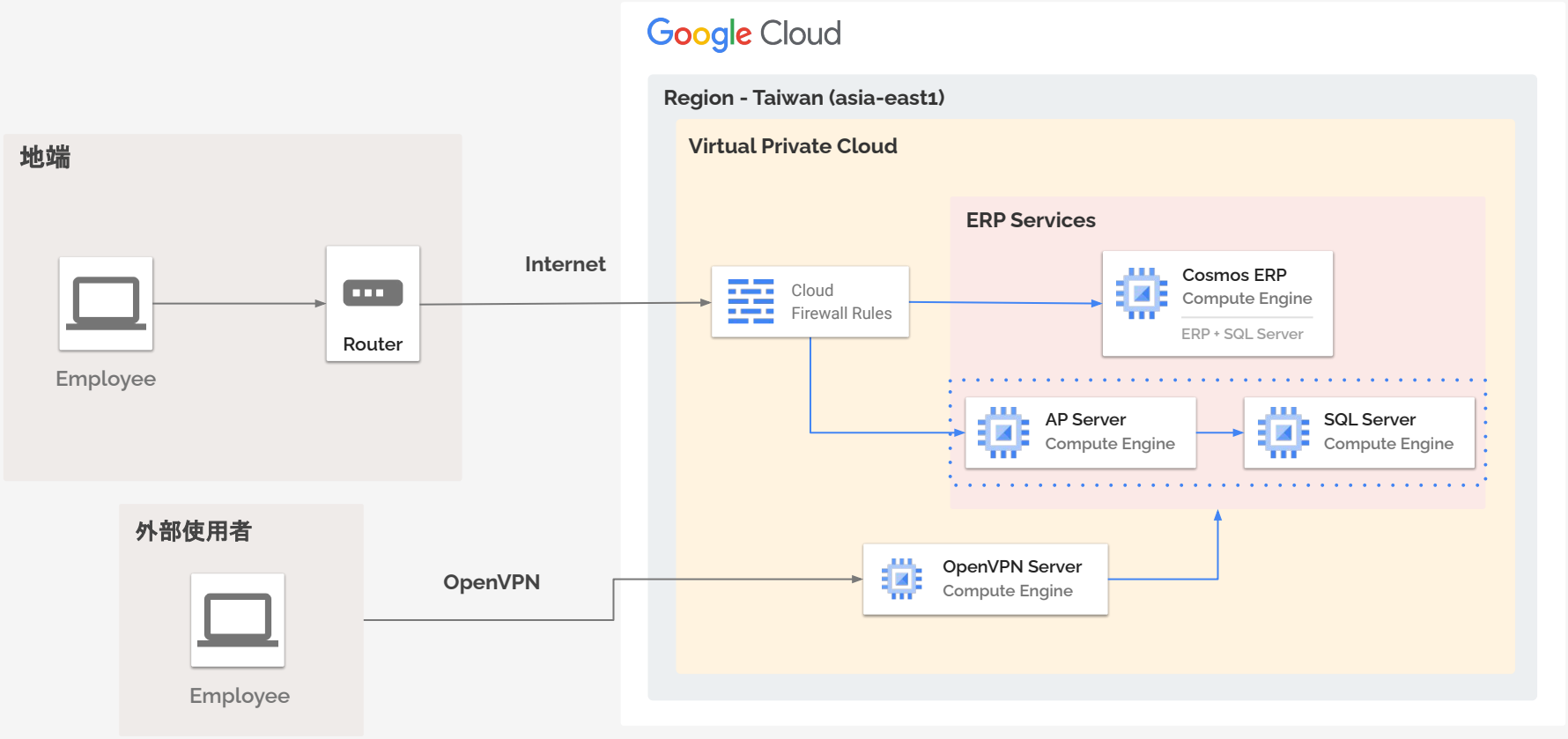
鼎新 ERP 地端架構


外點
外部使用者
SSL VPN
Internet
IPSec VPN
外點使用者
本廠
本廠使用者
ERPDB
ERPAP+RDS
ERPIIDB
ERPIIAP

鼎新 ERP on Google Cloud 雲端架構

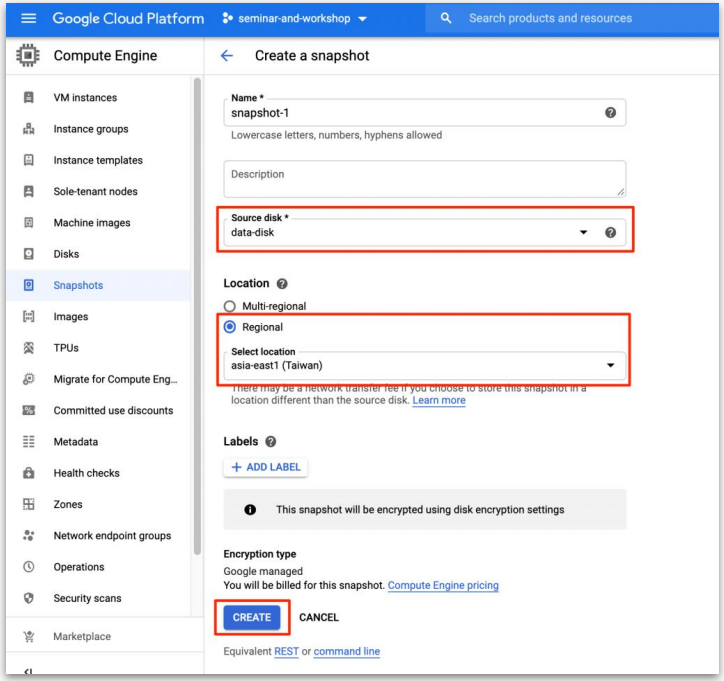


鼎新 ERP on Google Cloud 雲端架構

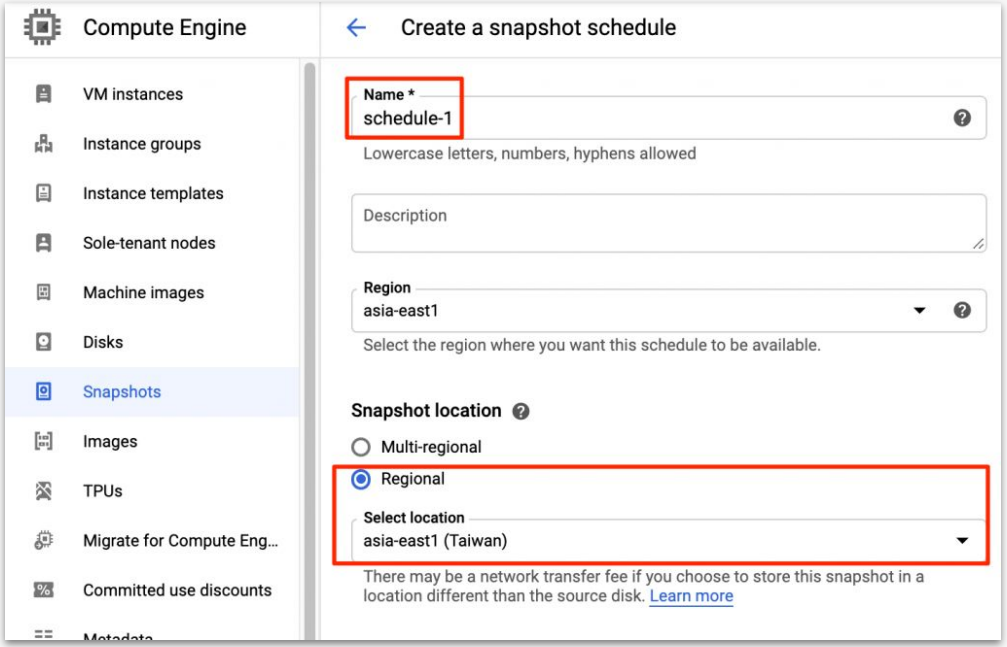


雲端備份方式：快照備份＆排程

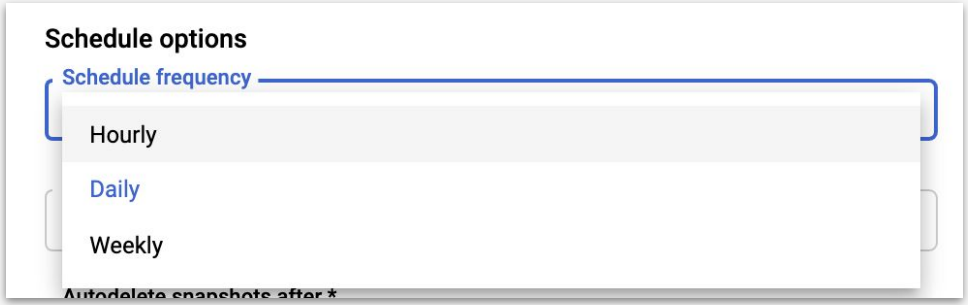
⬇️1.建立快照



⬇️2.建立排程

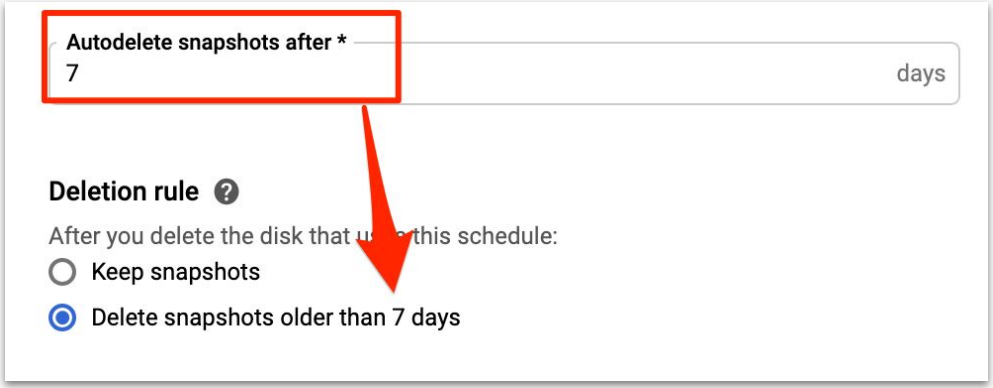


雲端備份方式:快照備份＆排程

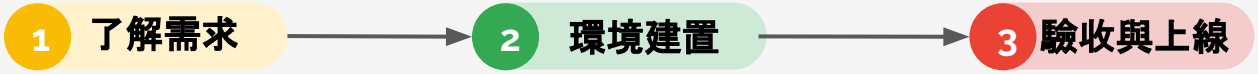


⬆️設定備份頻率

⬇️可自動刪除節省儲存空間



POC - 鼎新 ERP on GCP



- 了解使用情境
- 規劃架構圖
- 依據架構圖提供報價

- 雲端環境建置
- ERP服務安裝
- 使用者開始測試並回報使用情況

- 驗收(一～兩週)
- 確認上線時間
- 測試後最終架構確認(備份規則、連線方式、機器規格、其他...)
- 系統上線

Thank you!