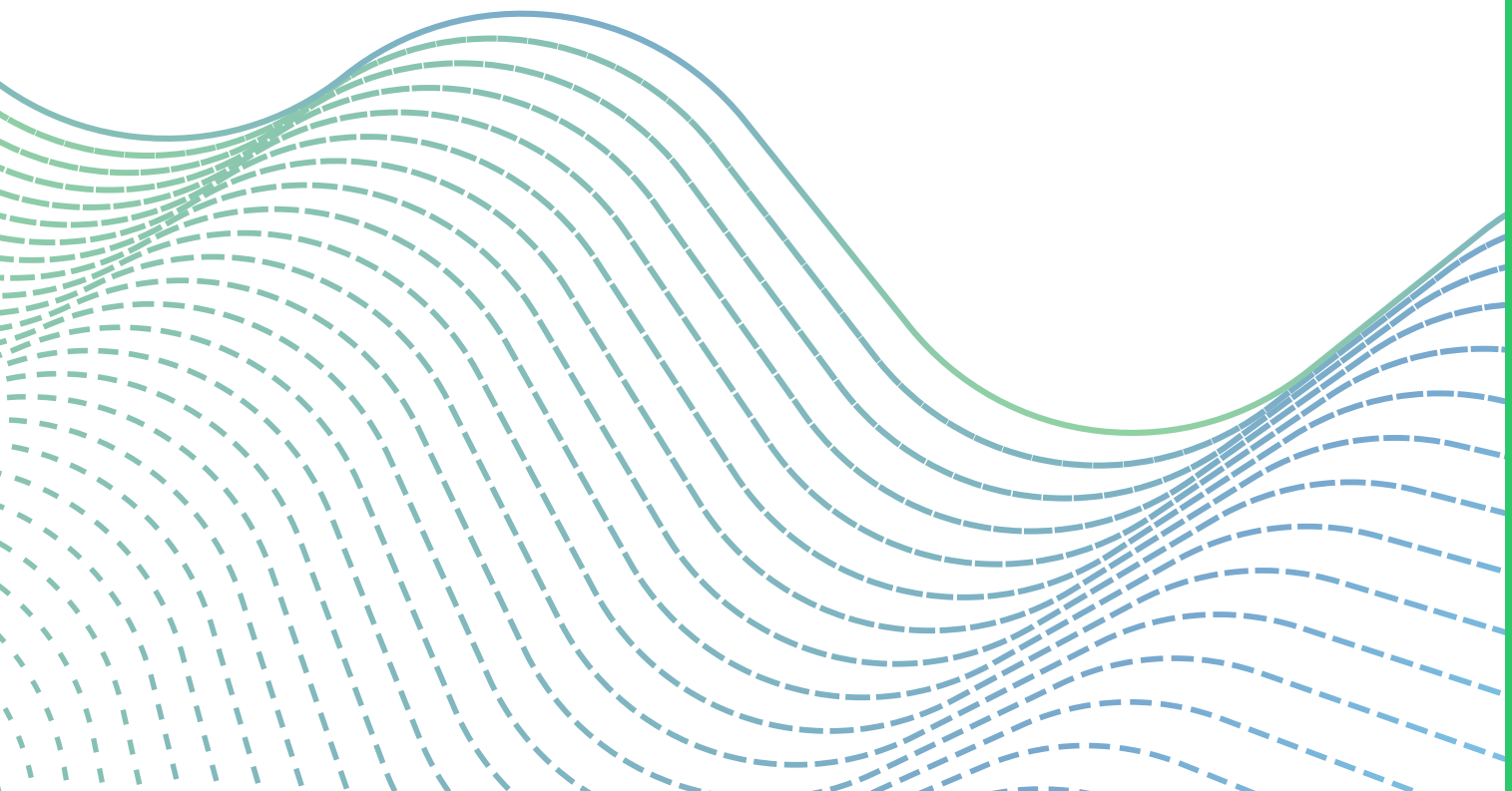
iKala Cloud

資安淺談

提升企業防護力
破解雲端安全迷思

GCP 資安白皮書

目錄



Google Cloud 安全嗎？

網路安全是 Google 最重視的事情之一，並持續以維護客戶的隱私權為先。Google 透過以下原則，做到維護隱私權[1] 這件事。

1. 對於您的資料，您有完全的控制權。
2. Google 不會將您的資料用於 Google Ads。
3. 關於資料的搜集及應用，Google 會遵守透明原則，並依循相關標準（如：GDPR）。
4. Google 不會出售客戶資料。
5. 在所有產品的規劃/設計上，安全及隱私權總是會放在第一順位。

Google 安全原則

Security of the Cloud

為您所選擇使用的服務作最小權限設定。

Security in the Cloud

為 Google Cloud 中的工作負載提供全面的分層防禦。

- Security Command Center
- Cloud Armor CAMP (WAF/ML based protection)
- Certificate Authority Service (Private CA/PKI)

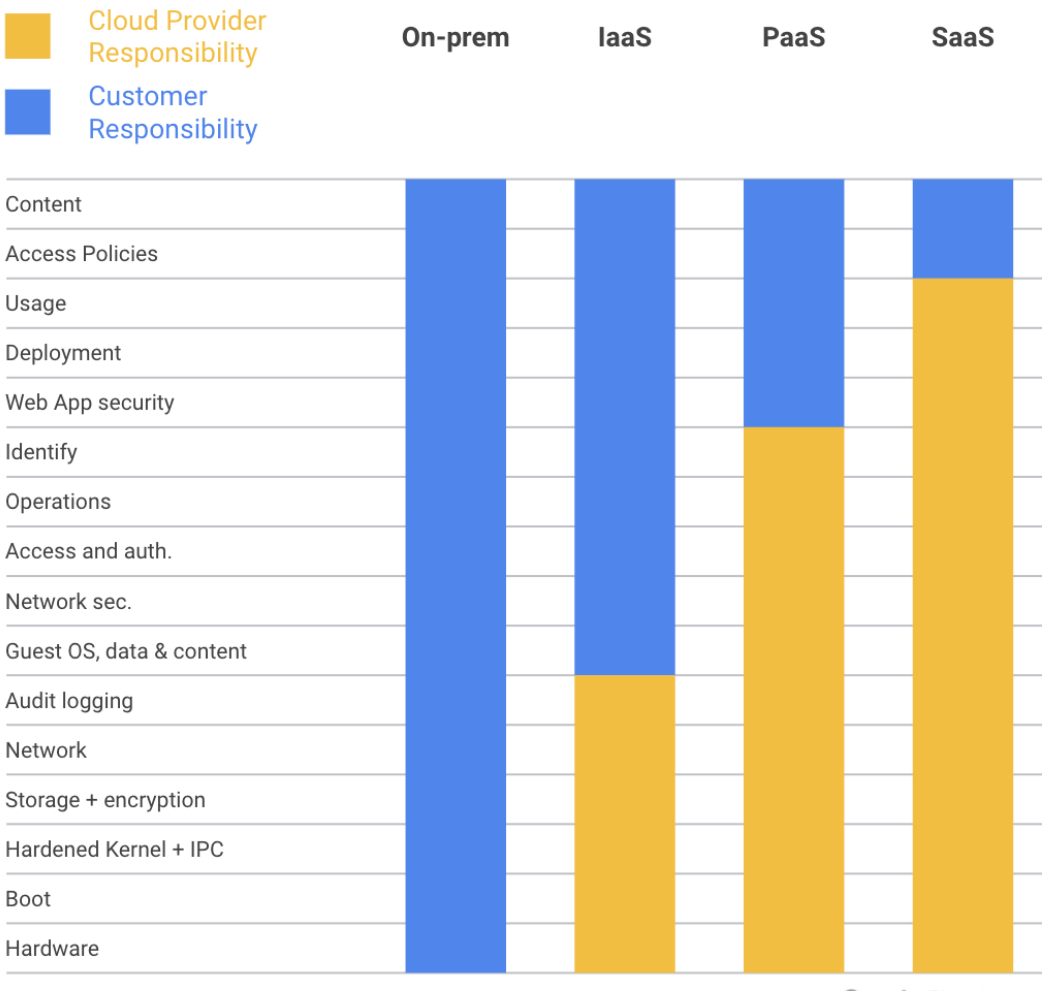
Security anywhere

在任何環境中都可以應用的安全實踐。

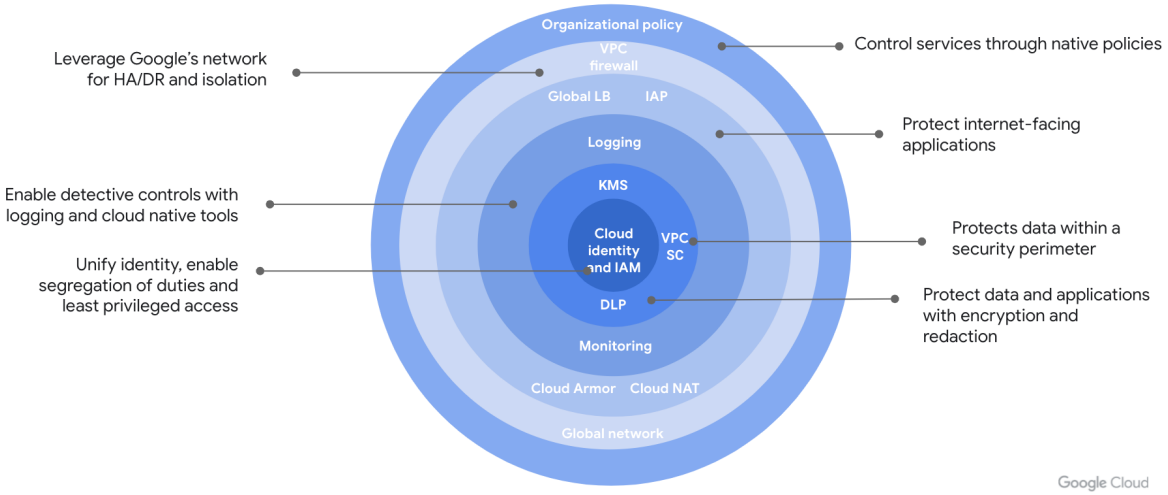
- Chronicle (XDR/SIEM)
- reCAPTCHA Enterprise (Anti-bot)
- BeyondCorp Enterprise (Zero Trust)

責任共同承擔

在公有雲的世界，責任共同承擔是一個重要觀念。透過 Security of the Cloud (雲本身的安全) 及 Security in the Cloud（雲裡面的安全） 的準則來做到安全的責任區分。Google 將保障雲本身相關安全，如資料中心硬體的安全、確保基礎設施穩定運行。而企業與使用者則是負責雲裡面的安全管理，如資料的存儲及權限的控管。簡單來說，就是您管理您的資料及資料安全；Google 則是協助保障您所使用的產品的 infra 或網路的安全。簡單舉例來說，您開了一台虛擬機，裡面架設了一個 Web Server，那您的責任就是管理您的虛擬機以及虛擬機裡面的資料，還有誰可以登入這台虛擬機 (firewall)；而 Google 的責任就是維持該台虛擬機硬體設備以及作業系統層的安全，自動更新安全補丁並將寫入硬碟的資料加密等等。當然，每個服務都會有不同責任歸屬，詳細資訊可以參考下圖。



Google Cloud 安全解決方案



Google Security 的服務藍圖，是由上方的同心圓結構做對應的分層式防護。

由圖中可知，Google 以身份權限控管 IAM（Identity & Access Management）為資安基礎核心，　向外擴充了更多如系統監控、網路層防護等對應服務供使用者做更細緻的層級設定，並於最外圈的 Organizational policy (組織政策) 統合管理整個組織內可被存取的政策。

以下會針對各個不同的安全性狀況提供不同的解決方案，協助企業快速的提升雲端環境保護力。

Cloud Armor

在 Google Cloud 的網路防禦服務中，最值得關注的就是 Cloud Armor。 Cloud Armor 是 Google Cloud 所提供的應用程序防火牆 (WAF, Web Application Firewall) ，搭配 HTTP(S) Load Balancer 使用，提供 Layer 7 的攻擊防禦。

針對 Layer 3~4 的網路攻擊，Google Cloud 的 Proxy based Load Balancer[2] 已內建提供 anti-DDOS 的防護[3]，例如：SYN 洪水攻擊 (TCP SYN floods) 、DNS 放大攻擊 (Amplification attacks) 等，這些都不用額外再做設定。

Cloud Armor 可以利用設定安全性政策 (security policies) 來設定規則，以撰寫公式的方式來設定封包接收或丟棄的判斷規則。例如：只接收來自台灣的流量，其他擋掉；或是 header 的內容沒有 user-id 這個參數就直接擋到等等...更多的使用範例可以參考[5]。

除此之外，Cloud Armor 也提供了預先定義的規則[4]，可以迅速地針對 OWASP 十大資安攻擊做最快速、有效的阻擋。這種預先定義的規則，使用方式也非常簡單，只需要在安全性政策的地方加入一條類似下的規則，即可設定完成。

```
evaluatePreconfiguredExpr('xss-stable', ['owasp-crs-v020901-id981136-xss',
'owasp-crs-v020901-id981138-xss'])
```

當然，之前鬧得沸沸揚揚的 log4j 事件，也是可以透過預先定義的規則直接來做到防擋。在 2021 年，更提供了以下三個重要更新，讓 Cloud Armor 的防護性又更上一層樓：

1. 頻率限制 (rate limiting) 的功能

以頻率為基礎的規則可協助保護應用程式，避免大量要求影響執行個體，並封鎖正當使用者的存取權。

2. 針對機器人的應用程式防護 (Cloud Armor bot management) (beta)

此功能良好的整合了 reCAPTCHA Enterprise ，讓網站開發者可以針對 reCAPTCHA 提供的風險指數來決定是否要讓封包進到後端網頁。

3. 自動調整式防護機制 (Adaptive Protection)

可運用在本機訓練的機器學習系統，自動偵測及減輕大量針對應用程式發動的第 7 層的 DDoS攻擊。還可以根據偵測出來的結果提供安全性政策建議來做對應的防護，大大地減少人工審查時間。

Security Command Center

Security Command Center (以下簡稱 SCC) 是Google Cloud 的安全性和風險管理平台。使用者可透過 SCC 集中控管的儀表板，一眼掌握目前 Google Cloud 中服務的使用狀況，是否有異常設定 (例如權限開啟過大) 或是不符合相關法規的情況。

SCC 會針對 Google Cloud 中組織內的所有專案去做對應的掃瞄，即時地抓出不合理或惡意的行為。

SCC 用以下四個面向的儀表板來做對應的檢查：

內部威脅 – 針對異常權限開啟過大的設定做適當的提醒，例如：service account 的權限過大，不符合最小權限原則；或是 VM 開啟的防火牆規過度寬鬆等，皆是在偵測的範圍內。並針對這類的不當配置提供建議的做法。

資產管理及可視性 – 即時地監控組織內所有專案的服務使用狀況。

稽核/合規 (Compliance) – 目前針對 CIS 1.0, 1.1, 1.2, PCI–DSS, ISO, NIST 等等的合規性，皆會產生對應的報表。

外部威脅監控 – 主要提供 ETD (Event Thread Detection) 及 KTD (Container Thread Detection) 兩種監控方式：

- ETD (Event Thread Detection)：協助監控組織內有關惡意軟體 Malware / 加密貨幣挖礦 Cryptomining / SSH 暴力攻擊 Brute force SSH / 連出的 DoS Outgoing DoS / 異常的身分與存取權管理授予行為 IAM anomalous grant / 資料竊取 Data exfiltration 等的檢查

- KTD (Container Thread Detection)：協助偵測 container 內是否異常執行二進位檔/載入媒體庫/shell script 等檢查

另外，針對上述的內/外部威脅監測所觀察到的 log 資訊，SCC 亦提供安全性狀態分析 (Security Health Analytics) 針對異常的 log 或是使用行爲做進一步的監測。

若您的組織內有對應的專案牽涉到 web 應用程式的服務，也可以啟用 web security scanner 去做自動定期/手動不定時的掃描，掃描偵測應用程式是否有符合對應 OWASP 的弱點或風險。

最值得一提的是，只要有使用 Google Cloud 服務就可以直接免費使用 SCC 標準版，且可支援上述大部分的功能。當然，進階版還有額外提供更為詳盡的外部威脅監控資訊，並提供額外的定期自動掃描等較為方便的功能。

BeyondCorp Enterprise

Zero–Trust 這個觀念在這一兩年由於疫情的關係，流行起來。Zero–Trust 中文翻譯為零信任，意思是在任何情況下，若進來的 request 沒有經過驗證，就視為不被信任的 request。

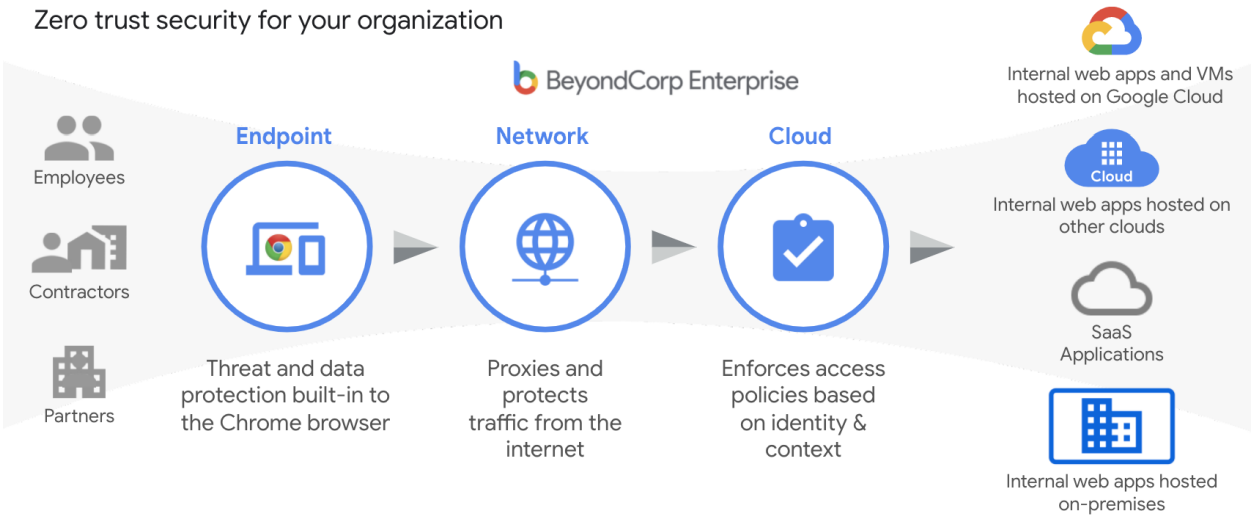
Zero–Trust 為何流行？ 因為疫情期間，大家都在家工作/遠距工作，家裡的網路環境總是會比公司/企業裡面的環境相對的不安全，也因此這個觀念就漸漸地能被大眾接受了。

在 Google 內部，其實很多年來就一直是奉行著 Zero–Trust 的觀念，進而將這個觀念延伸成了 BeyondCorp 這個產品。

BeyondCorp Enterprise (以下簡稱 BCE) 協助企業/組織做到端點對端點的控管，給予資料內容安全的保護，從您在家裡上網的那刻起，就可以透過對應的帳號/權限控管機制做到層層的防護。

BCE 可以將存取權控管設定從網路邊界移轉至個別使用者，讓世界各地的人們都能安全地工作，而不必使用傳統的 VPN。
BCE 提供單一登入、存取權控管政策、存取權 Proxy，以及以使用者與裝置為基礎的驗證與授權。原則如下：

- 服務存取權不得由您連線的網路決定
- 根據使用者及其裝置的相關要素授予服務存取權
- 不論存取任何服務，您都必須經過驗證、授權及加密程序



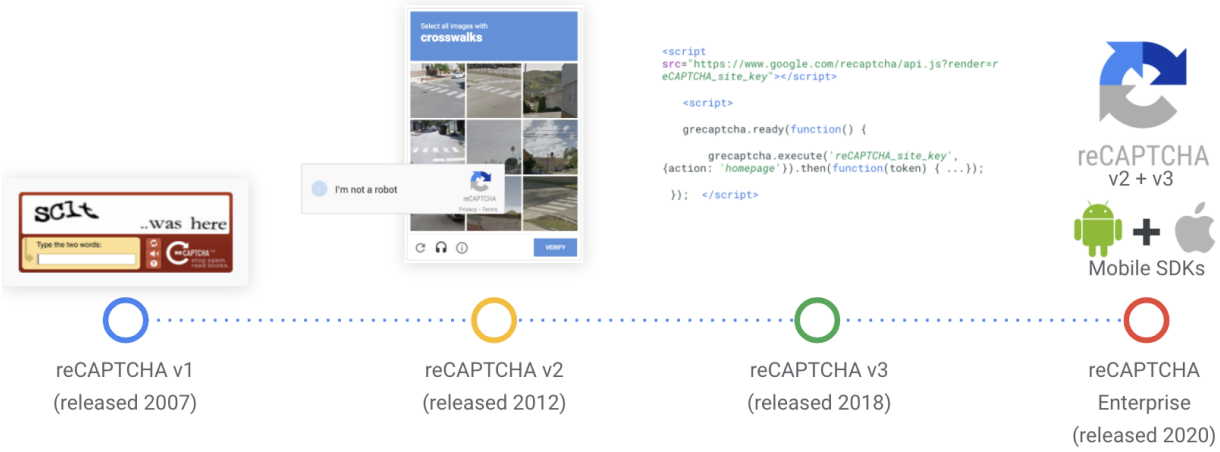
以上圖說明，您家裡的網路連上網際網路的當下，chrome 瀏覽器就會針對您上傳或下載的資料做對應的檢查，若同時啟用 DLP (Data Loss Prevention) API 做到機敏性資料判定，讓使用者無法偷偷上傳/下載機敏性資料。

接著在網路層中，為了降低 DDoS 攻擊風險，Google 在全世界超過200個國家的端點網路 (Edge locations) 皆有做對應的安全防護。

最後在順利通過上述兩步驟證之餘，Google 仍然會根據 Google Workspace (or Cloud Identity or Cloud IAM) 的設定，確認使用者該有的權限才能允許 request 通過。甚至可以設定到指定的電腦/手機等設備，才能有權限做登入請求，給予管理者相當多元且嚴謹的設定。

reCAPTCHA Enterprise

reCAPTCHA 這個服務在軟體業已經熱門超過十年，從 2007 的 v1 演進到 2018 的 v3 ，直到 2020 年更推出了 Enterprise 的版本。



Enterprise 除了原有免費版（v1/v2/v3）的就有的防止機器人及廣告的掃擾外，另外還提供了下述幾大好處：

- 協助偵測詐騙行為，例如：憑證填充攻擊(credential stuffing) 、帳戶侵權行為(account takeover) (ATO)
- 風險分數 (Risk Data)：根據使用者的對應瀏覽行為，會回傳對應的風險分數，讓網站開發者根據風險分數進行對應的動作，例如：風險分數過高，則需要再請使用者進行二階段驗證 (2 factor authentication, 2FA)，甚至直接封鎖該使用者的瀏覽行為。
- 針對行動裝置 (iOS / Android) 提供對應的 mobile api 讓使用者的體驗可以更上一層樓。

另外，就算您的服務/應用程式目前不在 Google 也還是可以使用，十分推薦。

參考資料

[1] https://cloud.google.com/privacy

[2] https://cloud.google.com/load-balancing/docs/choosing-load-balancer#ddos

[3] https://cloud.google.com/load-balancing/docs/https#open_ports
Even without a Google Cloud Armor configuration, Google infrastructure and GFEs provide defense-in-depth for DDoS attacks and SYN floods.

[4] https://cloud.google.com/armor/docs/rule-tuning#preconfigured_rules

[5] https://cloud.google.com/armor/docs/configure-security-policies#sample-expressions
https://cloud.google.com/armor/docs/rules-language-reference

iKala Cloud

地址：110台北市信義區東興路41號10樓　電話：+886 2 8768 1110
網站：https://ikala.cloud/　Email：cloud@ikala.tv

欲了解更多資安解決方案或雲端規劃需求，歡迎聯繫 iKala Cloud