Google Cloud資訊安全解決方案

享有 Google 級分散式阻斷服務 (DDoS) 防護機制與網路應用程式防火牆 (WAF)

偵測並減緩針對 Cloud Load Balancing 工作負載的攻擊

Adaptive Protection 機器學習型機制，協助偵測及封鎖第 7 層分散式阻斷服務攻擊

防範 OWASP 機構所彙整的十大資安風險，保護地端部署或雲端環境中的工作負載

透過與 reCAPTCHA Enterprise 原生整合的機器人管理功能，防止邊緣詐欺

產品特色

企業級分散式阻斷服務防護
我們在保護 Google 搜尋、Gmail 和 YouTube 等重要網路資產上累積的豐富經驗，如今也運用於 Cloud Armor。Cloud Armor 提供的內建防護機制可有效防禦 L3 和 L4 分散式阻斷服務攻擊。

防範 OWASP 十大資安風險
Cloud Armor 提供預先定義的規則，有助於阻擋跨網站指令碼攻擊 (XSS) 和 SQL 插入 (SQLi) 攻擊等威脅。

Managed Protection
有了 Cloud Armor Managed Protection Plus 方案，即可使用分散式阻斷服務防護機制和網路應用程式防火牆服務、精選規則集及其他服務，而每月付費的方式也可讓您提前掌握支出。

自動調整式防護機制
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 層分散式阻斷服務攻擊。

支援混合式雲端和多雲端部署作業
不論應用程式部署於 Google Cloud、混合雲或多雲端架構中，Cloud Armor 皆可協助防禦分散式阻斷服務或網路攻擊，並且強制執行第 7 層安全性政策。

預先設定的網路應用程式防火牆規則
這些是符合業界標準的現成規則，可降低常見網頁應用程式安全漏洞的風險，且有助於防範 OWASP 機構彙整的十大資安風險。詳情請參閱我們的網路應用程式防火牆規則指南。

機器人管理
自動保護應用程式，防範機器人攻擊，並且透過 reCAPTCHA Enterprise 的原生整合，協助防堵內嵌和邊緣詐欺。
頻率限制
以頻率為基礎的規則可協助您保護應用程式，避免受到會導致執行個體超載及迫使正當使用者無法存取資源的大量要求。

功能規格/基本需求

此服務需透過 Chrome, Edge, and Safari browser, or installed SDK (CLI) 等瀏覽器登入，可運用瀏覽器登入服務，所有雲端服務的新增、修改、刪除、部署皆可透過瀏覽器達成。
所需硬體基本環境:
CPU: Intel系列 &AMD系列
記憶體：2 GB以上
硬 碟：256GB以上
所需軟體基本環境:
基本桌面環境即可。
