Google Cloud

Google Cloud Armor

提供完善的應用程式和網站保護機制，防範阻斷服務和網路攻擊。

- 享有 Google 級的分散式阻斷服務防護機制與網路應用程式防火牆
- 偵測並減緩針對 Cloud Load Balancing 工作負載的攻擊
- 自動調整式防護機制 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 機構彙整的十大資安風險，保護內部部署系統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

主要功能與特色

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。瞭解詳情。

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、混合式雲端或多雲端架構中，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
依據業界標準設定的現成規則，可縮減常見的網頁應用程式安全漏洞，並防範 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
針對機器人提供自動化應用程式防護功能，並且透過 reCAPTCHA Enterprise 的原生整合，協助防堵內嵌和邊緣詐欺。瞭解詳情。

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

所有功能與特色

使用預先定義的 WAF 規則來防範 OWASP 十大資安風險	依據業界標準設定的現成規則，可縮減常見的網頁應用程式安全漏洞，並防範 OWASP 機構彙整的十大資安風險。
豐富的規則語言，便於部署網頁應用程式防火牆	您可以使用 L3 至 L7 參數和地理位置資訊的任意組合建立自訂規則，透過彈性的規則語言保護您的部署項目。
資訊可見度與監控能力	透過 Cloud Monitoring 資訊主頁，輕鬆監控所有與安全性政策有關的指標。您也可以透過 Security Command Center 資訊主頁，直接查看來自 Cloud Armor 的可疑應用程式流量模式。
記錄	您可以透過 Cloud Logging，瞭解 Cloud Armor 對於各要求的決策，以及當中涉及的政策與規則。
預覽模式	在預覽模式中部署 Cloud Armor 規則，可以讓您先行掌握規則效率及對實際工作環境流量的影響，再開始強制執行政策。
透過規則建立政策架構	您可以利用規則階層設定一或多項安全性政策，再將不同精細程度的政策套用至一或多個工作負載。
以 IP 和地理位置為基礎的存取權控管	根據 IPv4 和 IPv6 位址或 CIDR 篩選傳入的流量。依據傳入流量的地理位置，決定應強制執行怎樣的存取權控管機制。
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、混合式雲端或多雲端架構中，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。
已命名 IP 清單	根據系統收錄的已命名 IP 清單，透過 Cloud Armor 安全性政策允許或拒絕流量。