

AWS WAF

保護您的 Web 應用程式免受常見 Web 入侵程式的危害

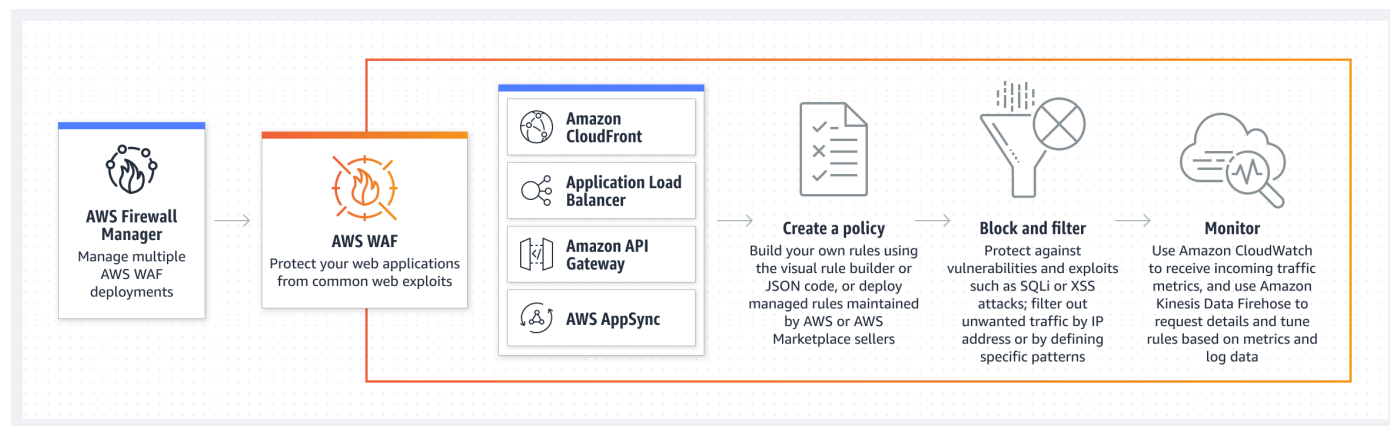
使用受管規則節省時間，讓您有更多時間建置應用程式。

更加輕鬆地監控、封鎖常見和普遍的機器人攻擊或限制其速率。

透過精細控制發出指標的方式，提升 Web 流量可見性。

運作方式

AWS WAF 協助您保護應用程式免受可能影響可用性、安全性危害、或耗用過多資源的常見 Web 入侵程式和機器人程式的侵擾。



為何選擇 AWS WAF ?

借助 AWS WAF，您可以建立安全規則來控制機器人流量，並阻止常見的攻擊模式，如 SQL 密碼攻擊或跨網站指令碼 (XSS)。

使用案例

篩選 Web 流量

建立規則以根據各種條件篩選 Web 請求，例如 IP 地址、HTTP 標頭和內文，或自訂 URI。

防止帳戶接管詐騙

監控應用程式的登入頁面，偵測以盜用憑證對使用者帳戶進行的未經授權存取。

使用 API 管理 AWS WAF

自動建立和維護規則，並將這些規則併入開發和設計程序中。