引領業界的雲端網頁應用程式防護服務

網頁應用程式開發變得比過去更為複雜、迅速與脆弱。Radware 的雲端網頁應用程式防火牆（簡稱 CWAF）服務藉著使用機器學習技術，提供業界最佳的網頁應用程式安全性，以針對 OWASP 十大威脅及其他漏洞實施全方位的防護 。Radware 的雲端 WAF 服務提供動態的安全策略機制，藉由自動誤報修正、內建的分散式阻斷服務（簡稱 DDoS）防護、整合式機器人緩解與許多其他特色，幫助企業防止資料外洩的風險。

完整保護

Radware 根據主動安全模式提供業界最佳的網頁應用程式防護，以全面覆蓋防止 OWASP 十大威脅與更多攻擊

提升能見度

Radware 提供一套精密分析，能讓安全管理人員迅速深入瞭解其應用程式發生的情況

多重面向的安全性

Radware 的機器人管理員直接整合到雲端 WAF 服務中，提供針對應用程式漏洞、機器人與API 威脅的整合防護。

減少管理經常性費用

雲端 WAF 服務是配置專家的全面託管安全服務，能為顧客減輕重擔

Radware 如何讓您保持敏捷與安全

自動流量學習

Radware 使用先進的機器學習演算法，能分析流量、學習構成正當行為的規則及自動封鎖惡意活動

應用程式勘測

Radware 會自動勘測受保護的應用程式、在每次增加或修改新功能時變更偵測程式碼，以及辨識潛在的漏洞

適應性策略

Radware 會持續適應安全策略以優化對應用程式威脅組合的範圍，進而擴大安全性覆蓋與減少誤報

Radware 的雲端 WAF 服務完全符合 PCI 規定

Radware 的雲端 WAF 服務是全球唯一的可擴展雲端 WAF 服務，能全面實施 PCI DSS 要求6.6 推薦的所有 10 個安全性機制，包括強制執行主動安全模式與實施資料外洩防護（簡稱 DLP）控制。雲端 WAF 同樣獲得 PCI DSS 認證，並且是以 NSS 實驗室與 ICSA 實驗室認證技術為基礎，這意味著顧客能使用Radware雲端 WAF 服務，以達到最全面的合規性。

全球存在，近源防護

Radware 的雲端 WAF 服務是以分散式 WAF 節點（簡稱 POP）的全球網路為基礎，確保您總是獲得來自最接近原始伺服器之節點的保護。雲端 WAF POP 都位在主要的流量中心，並連接至第一層 ISP，確保低延遲及對網頁應用程式效能的最小影響。

Radware 雲端 WAF 服務的服務特色

防止 OWASP 十大威脅的完整防護

- 使用進階行為分析的主動安全模式機制來偵測惡意威脅
- 內建 DDoS 防護，可阻止網路及應用程式層級的 DDoS 攻擊
- 使用先進的數位指紋追蹤，根據獨特的裝置特徵來辨識惡意機器人
- 資料外洩防護機制能自動遮蔽敏感的使用者資料，如個人識別資訊（簡稱 PII）

增加持續交付的敏捷性

- 由 Radware 專門緊急應變團隊（簡稱 ERT）提供的全面託管安全服務，這是業界人數最多、經驗最豐富的安全團隊之一
- 專門的技術客戶經理（簡稱 TAM）是所有問題的聯絡人，包括配置、整合、更新與攻擊緩解等
- 持續適應策略能自動勘測應用程式、偵測應用程式的改變，以及動態部署最佳安全策略
- 使用高效機器學習演算法自動修正誤報，辨識合理的應用程式行為

部署彈性

- 直接與 Radware 的機器人管理服務整合，提供針對最新第三代與第四代惡意機器人的防護
- 支援高容量的 SSL 流量，即使在尖峰時間也能確保來自最近 POP 的完整 SSL 可用性
- 進階的負載平衡能力，包括本地及廣域式負載平衡（簡稱 GSLB），以及站點故障切換、高可用性與健康狀態監控
- 超越競爭品牌，無可比擬的大規模合規與認證能力，包括產業特定認證，如 PCI 與 HIPAA，以及雲端安全性標準，如 ISO 27001、ISO 27017、ISO 27018、ISO 27032 等

輕鬆管理與控制

- 豐富的集中式主控台能顯示威脅及管理配置
- 細微警示能力，確保您能在狀況發生時率先知道
- 強大的分析引擎能將大量的安全性事件合併成少量、可管理的使用者活動，讓資安人員得以迅速深入瞭解其應用程式流量
- 集中通報，提供 WAF、DDoS、機器人管理與 API 防護