

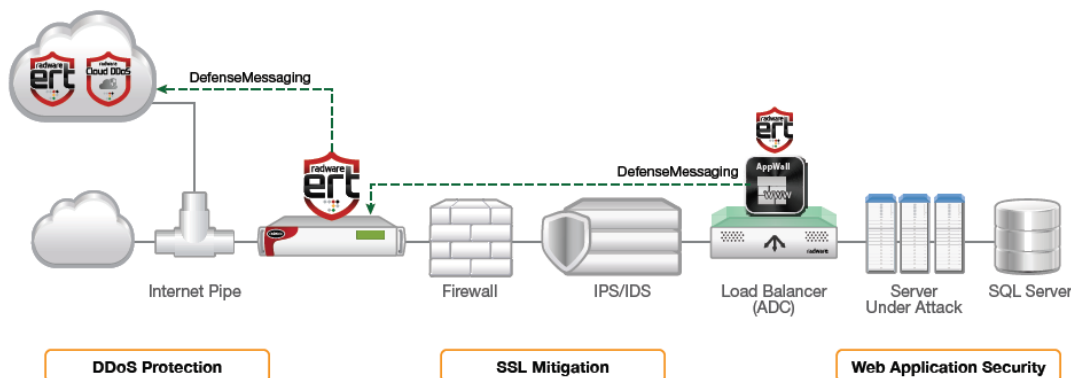
整合檢測和緩解工具的單一廠商安全解決方案

目前企業的標準防護技術包括DDoS防護、IPS、異常及行為分析、SSL防護和WAF，這些功能往往由多個單點解決方案提供。但這些系統幾乎不能整合，並且需要由IT經理和安全專家等組成的專用資源來進行維護和同步。Radware攻擊緩解解決方案(AMS)結合了必要的技術，讓企業可以依靠內部系統防禦網路攻擊，並按需求擴展雲端清洗中心。這是一個整合了內部檢測和緩解措施以及雲端大流量攻擊清洗的混合攻擊緩解服務。該解決方案可以幫助企業緩解檢測到的攻擊，並提供整合了檢測和緩解工具的單一廠商安全解決方案。其提供了最大的攻擊覆蓋範圍、精確的檢測和最短防護時間。

解決方案技術概覽

該解決方案的核心是受專利保護的行為基礎分析演算法的檢測、即時特徵碼生成以及自動策略生成，可以處置攻擊生命週期過程的自動化，並針對最複雜的動態攻擊提供高度的防護措施，同時將對合法流量的影響降至最低。

- 位於資料中心邊緣的即時DDoS檢測器和緩解器，可以防禦應用攻擊和網路攻擊。該緩解器可以作為針對任何自動檢測到的事件的緩解措施的中心點。
- 位於應用程式旁的Web應用防火牆，可以檢測商務和應用攻擊。
- 專利SSL攻擊緩解措施，可以提供最低延遲，最有效的SSL攻擊防護，以及對基於SSL的DDoS攻擊的最全面覆蓋。
- 雲端DDoS防護服務用以供應洪水量超過資料中心的網路或應用容量時的需要。
- 由實戰經驗豐富的安全專家組成的緊急回應團隊(ERT)。
- 全自動化的紀錄攻擊週期和同步資訊，可以提高檢測和緩解的回應和準確性。



覆蓋多向攻擊的進階IoT僵屍網路防護措施

該解決方案提供了多向量攻擊檢測和緩解，可以處理網路層攻擊、伺服器架構的攻擊、惡意軟體傳播和入侵活動。解決方案還可以防禦大流量和非大流量攻擊、SYN洪水攻擊、低速慢速攻擊、HTTP洪水攻擊、SSL架構的攻擊、暴力攻擊等。由於該解決方案可以分析流量，因此可以為已部署的企業定制流量基礎防線。

該解決方案提供了業界最先進的自動化防護措施，可以防禦近來如Mirai等針對IoT架構攻擊而快速發展的威脅。該解決方案以獨特的方式克服在現今IoT架構下僵屍網路的複雜性和規模。Radware DDoS防護措施包括業界首個可以以最具成本效益的方式防護已知和未知DNS洪水攻擊的行為基礎分析演算法，如防護DNS水酷刑襲擊等。

Radware內部防護措施由5個模組組成；這些模組是專為資料中心和營運商部署而設計的，而且經過了優化，可以實現更好的線上業務和資料中心防護。

DoS 防護——防護所有類型的網路 DDoS 攻擊，包括：

- UDP 洪水攻擊
- TCP 洪水攻擊
- IGMP 洪水攻擊
- SYN 洪水攻擊
- ICMP 洪水攻擊
- Out-of-state 洪水攻擊

NBA (網路行為分析)——網路行為分析模組可以防止應用資源濫用和零分鐘惡意軟體傳播。可以防護的攻擊包括：

- HTTP 頁面洪水攻擊
- SIP 洪水攻擊
- 網路和埠掃描
- DNS 洪水攻擊
- 暴力破解攻擊
- 惡意軟體傳播

IPS

- 程式漏洞和漏洞利用
- 網路基礎架構漏洞
- 匿名網站
- 惡意軟體，如蠕蟲、電腦程式
- IPv6 攻擊
- 協定異常
- OS 漏洞和漏洞利用
- 木馬、間諜軟體

SSL 攻擊緩解——提供針對 SSL 架構的 DDoS 攻擊的防護措施。

- 獨特的 HTTPS 攻擊緩解機制
- 保障用戶數據隱私
- 可運行在對稱及非對稱架構

WAF——防止所有類型的 Web 伺服器攻擊，如：

- 跨站腳本(XSS)
- Web 應用漏洞
- Cookie 中毒、會話
- SQL 注入
- 跨站請求偽造(CSRF)
- 劫持、暴力破解

高準確度的檢測和緩解措施

Radware攻擊緩解解決方案採用了專利的行為基礎分析的檢測和即時特徵碼生成演算法。這些演算法建立了正常情況下網路、應用和使用者行為的基礎防線，並且可以利用這些基礎防線發現異常流量並準確檢測攻擊。當檢測到以前未知的新零日攻擊時，該解決方案就會即時建立一個採用了攻擊特徵的特徵碼，並立即在18秒內開始攔截攻擊。通過實施受專利保護的行為分析技術，攻擊緩解解決方案可以在很短的時間內檢測到已知和未知攻擊，並實現最低的誤報率。

關於Radware

Radware®(NASDAQ: RDWR)是為虛擬、雲端和軟體資料中心提供[應用交付](#)和[網路安全](#)解決方案全球領導者。Radware屢獲殊榮的解決方案組合可為關鍵業務應用提供服務品質保證，同時最大化IT使用效率。Radware的解決方案協助全球10,000多家企業和營運商快速應對市場挑戰，維持業務不中斷，並在生產力最大化的同時有效降低成本。更多訊息，請洽www.radware.com。