防護基礎架構和應用程式
免於遭受 DDoS 攻擊和持續演變的威脅

分散式阻斷服務 (DDoS) 攻擊日益頻繁且嚴重。在暗網很容易就能付費使用強大的 IoT 殭屍網路，使得發動大規模攻擊更為輕鬆且便宜。專業的駭客一直企圖以新的手法中斷網路流量並干擾使用者體驗，因而導致營收損失、品牌受害，以及客戶大量流失。

DefensePro 是 Radware 獲獎的即時邊界攻擊緩解裝置，可確保組織免於遭受新興網路多途徑攻擊、強大的 DDoS 活動、IoT 殭屍網路、應用程式弱點攻擊、惡意軟體和其他類型的網路攻擊所造成的危害。經實證的 DefensePro 行為式技術，是為防範現今複雜的攻擊工具和網路罪犯而設計。

自動零時差攻擊防範

行為式偵測和緩解可以防範不明的零時差攻擊，合法使用者體驗完全不受影響

無金鑰 SSL/TLS 洪水攻擊緩解

SSL/TLS 型 DDoS 攻擊的高容量無金鑰防護，完全不會造成客戶通訊延遲，並且可以保護使用者隱私

先進的攻擊防護

偵測和緩解現今最新手法的攻擊，包括突發攻擊、網域名稱系統 (DNS) 放大攻擊、IoT 殭屍網路泛洪、第 3-7 層和其他 DDoS 要害攻擊

專利保護的即時攻擊特徵碼

自動特徵碼建立和先進的挑戰向上呈報，得以實現最高的緩解準確度，因此可以自動緩解不明攻擊，並大幅減少攻擊對合法流量造成的影響

Radware 如何確保您的網路元件安全無虞

專用 DDoS 緩解硬體

DefencePro 藉由專用硬體模組緩解攻擊，完全不影響合法流量和使用者體驗，即使是大型攻擊也能夠予以緩解。

分析和報告

對於阻斷服務 (DoS) 和網頁應用程式攻擊，Radware 的管理平台會提供警示、報告、鑑識和見解，藉以獲得歷史資料和即時資料。

防範訊息

解決方案中的各個元件之間皆能同步掌握攻擊資訊並設定基準，藉以改善偵測、緩解回應及準確度。

最大攻擊涵蓋範圍

- 全面第 3-7 層防護可防範濫用網路頻寬、伺服器和應用程式資源的已知和零時差 DoS/DDoS 攻擊。
- 雙向能見度有助於防範需要檢查入埠和出埠流量，才能識別之最複雜的攻擊。
- 突發攻擊防護透過特徵碼建立和即時實施，提供行為式即時偵測和緩解，並以最快速的補救措施防範現今最嚴重的威脅之一。
- 先進的 DNS 攻擊涵蓋範圍；運用一流的行為式演算法、以最符合成本效益的方式防範已知和不明的 DNS 洪水攻擊，包括 DNS 水刑攻擊。
- 專利保護的無狀態和無金鑰 SSL/TLS 攻擊緩解解決方案可以減少延遲，而且不需要進行封包解密即可防範所有類型的加密攻擊，展現出高防護能力。

多樣化部署選項滿足您的需求

- 支援透通模式或路徑外 (SmartTap) 實作或淨化中心部署。
- 與 Radware 的混合雲端 DDoS 防護服務整合，構成單一供應商的混合解決方案，發揮零時差緩解成效。
- 透過多租戶和多策略支援，服務供應商能夠為託管應用程式和網路租戶提供領先市場的 DDoS 緩解服務。
- 虛擬設備能夠為軟體定義型資料中心 (SDDC) 緩解 DDoS。
- 防護裝置的範圍可提供 6Gbps 到 400Gbps 的緩解能力。

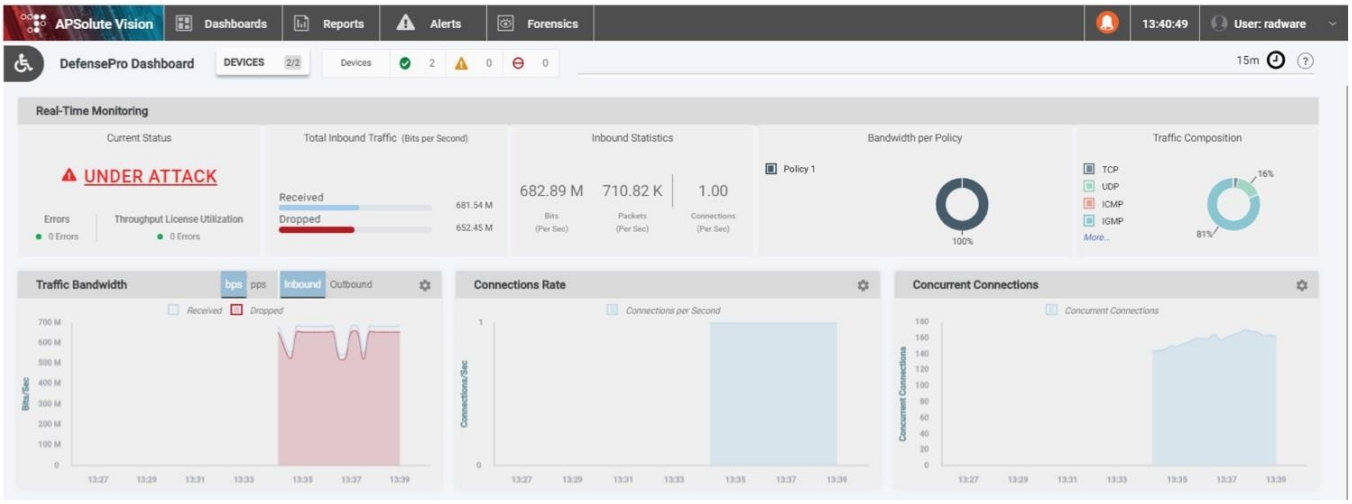

圖 1：集中式儀表板可即時顯示威脅，並具備向下切入功能，可提高對於特定攻擊資料和特徵的可見度

持續的威脅情報和安全專家支援

安全更新訂閱 - Radware 的安全研究團隊會持續為已知攻擊類型提供攻擊特徵碼。

緊急回應團隊 (ERT) 主動攻擊者摘要 - 自動更新，阻絕主動涉入 DDoS 攻擊的攻擊來源。

位置型緩解 (GeoIP) - 依據 IP 子網路的地理位置對應，過濾國家和地區的網路流量。

ERT 服務和裝置管理 - 直接由安全專家全年無休支援和協助防範持續的攻擊，並對於內部部署的裝置進行管理和設定。