Adaptive Protection From The Most Advanced DDoS Threats

Distributed denial-of-service (DDoS) attacks are increasing in frequency and ferocity. Powerful IoT-botnets for hire over the dark web make launching largescale attacks accessible, effortless and cheap. Professional hackers are continuously seeking new ways to disrupt the flow of network traffic and undermine the user experience, resulting in loss of revenue, tarnishing of the brand and increased customer churn rates.

DefensePro, Radware's industry leading, real-time perimeter attack mitigation device, secures organizations against emerging network multi-vector and DDoS attack campaigns, IoT botnets, application vulnerability exploitation, malware and other types of cyberattacks. DefensePro's proven behavioral-based technology is designed to prevail over modern sophisticated attack tools and cybercriminals.

Key Features:



Automated Zero-Day Attack Defense
Behavioral-based detection and mitigation to defend against unknown zero-day attacks without impacting legitimate user experience



Keyless SSL/TLS Flood Mitigation
High-capacity keyless protection from SSL/TLS-based DDoS attacks without adding latency to customer communications and while preserving user privacy



Advanced Attack Protection
Detection and mitigation of today's most advanced attacks, including Burst attacks, Domain Name System (DNS) amplification attacks, IoT botnet floods, Layer 3–7 and other crippling DDoS attacks



Patent Protected Real-Time Attack Signature
Automatic signature creation and advanced challenge escalations to achieve the highest mitigation accuracy that can automatically mitigate unknown attacks and minimize the impact on legitimate traffic

State-of-the-Art Protection

- **Industry-recognized protection** from DDoS threats leveraging machine learning-based algorithms for automated protection with no need for human intervention
- **Behavioral-based algorithms** to ensure legitimate user experience under attack and a minimum rate of false positives
- **Protection from the most advanced threats**: Burst attacks, encrypted attacks, carpet bombing attacks, IoT botnets and many more
- **Encrypted flood protection without decrypting all TLS traffic**, but rather effectively identifying an anomaly to selectively pick the session for inspection

Frictionless Security Experience

- **Rich user experience & visibility** with advanced security operation dashboards that provide unified visibility into attack lifecycle and mitigation analysis for both inline and out-of-path deployments
- **Networks analytics** with comprehensive visibility of traffic statistics during peacetime and attack
- **Simplified management and configuration** with unified visibility and control for both out-of-path and inline DDoS protection solutions, optimized troubleshooting and enriched search and filter capabilities
- **Multiple deployment options** to fit your needs offering a range of protection devices offers mitigation capacity from 6Gbps to 800Gbps, virtual appliance and integrated hybrid solution with Radware's Cloud DDoS Protection Service

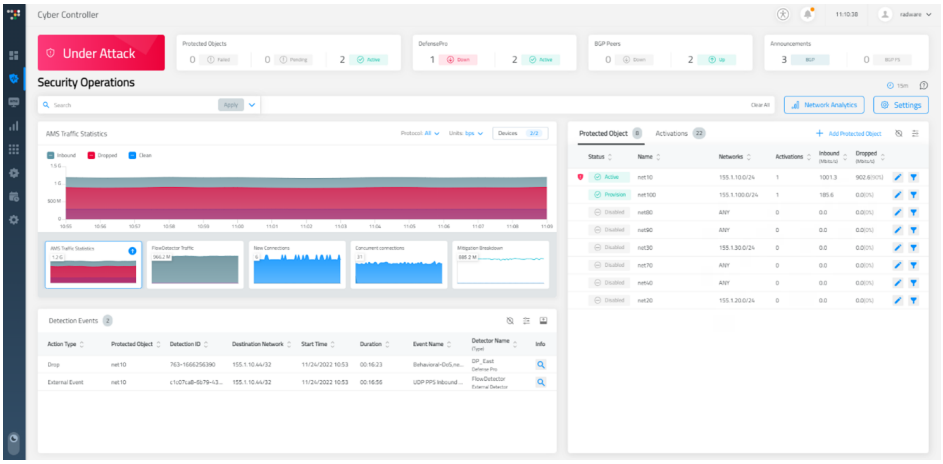


Figure 1

A centralized Cyber Controller dashboard to display threats in real time with the ability to drill down for increased visibility into specific attack data and characteristics

©2022 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.