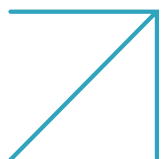


DefensePro X- Network Intrusion Prevention System

Adaptive Protection Against Advanced Intrusion-Based Threats



Intrusion-based attacks are increasing in frequency and ferocity. Powerful IoT botnets for hire over the dark-web make launching large-scale 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 X, Radware's industry-leading, real-time perimeter attack and intrusion prevention device, secures organizations against emerging network multivector intrusion-based attack campaigns, IoT botnets, application vulnerability exploitation, malware, and other types of cyberattacks. DefensePro X'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



Comprehensive Layer 7 Protection

Protects against L7 attacks using hardware-based SSL decryption engine, providing precise blocking and enhanced performance.



Advanced Attack Protection

Detection and mitigation of sophisticated cyber threats, including burst attacks, DNS amplification attacks, IoT botnet attacks, and scan-based attacks, with capabilities such as geo-blocking and real-time threat blocking.



Patented Real-Time Attack Signature Creation

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

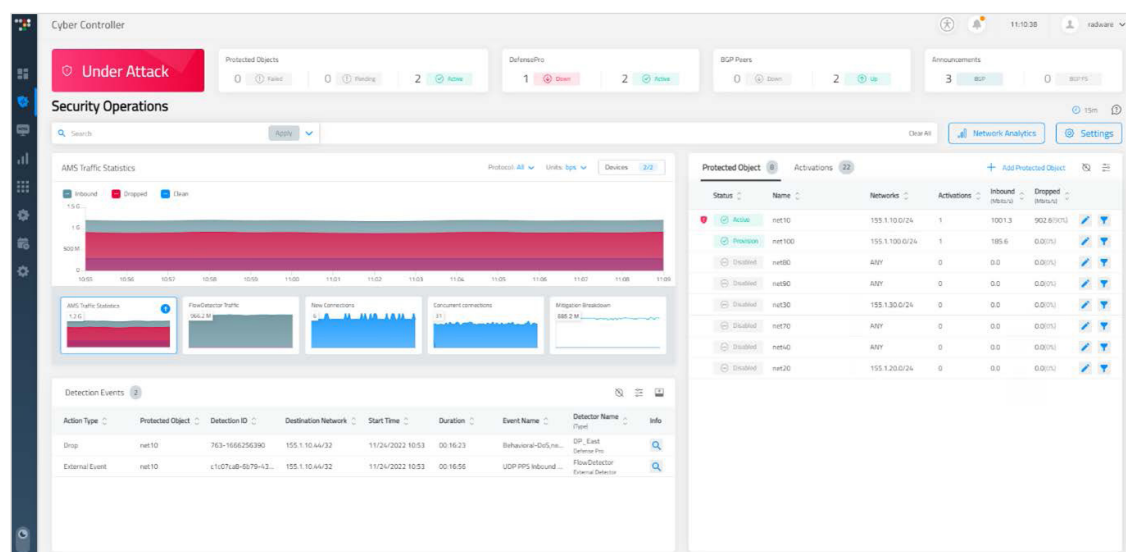
- **Industry-recognized IPS protection** powered by machine learning-based algorithms that automatically detect and block sophisticated threats, reducing the need for manual intervention.
- **Behavioral-based algorithms** to ensure legitimate user experience under attack and a minimum rate of false positives
- **Protection from the most advanced threats including** burst attacks, encrypted attacks, carpet bombing attacks, IoT botnets, application vulnerability exploitation, malware, and many more
- **Encrypted 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
- **Networks analytics** with comprehensive visibility of traffic statistics during peacetime and attack
- **Simplified management and configuration** with unified visibility and control, for optimized troubleshooting and enriched search and filter capabilities
- **Multiple deployment options** to fit your needs, offering a range of protection devices including virtual appliance and hardware solutions.

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



To learn how Radware DefensePro X can protect your network against evolving intrusion-based threats, [contact us](#) today.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2026 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.

