

DefensePro, Radware's award-winning real-time perimeter attack mitigation device, secures organizations against emerging network multivector attacks, powerful DDoS 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.

## 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

Automated 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.



## HOW RADWARE KEEPS YOUR NETWORK ELEMENTS SECURE

### DEDICATED DDOS MITIGATION HARDWARE



A dedicated hardware module that allows DefensePro to mitigate attacks without impacting legit traffic and the user experience, even large attacks.

### ANALYTICS AND REPORTS



Radware's management platform provides alerts, reports, forensics and insight into denial-of-service (DoS) and web application attacks both for historical data and in real time.

### DEFENSE MESSAGING



Synchronizes attack information and baselines across the various elements of the solution to improve detection and mitigation response and accuracy.



## DEDICATED DDOS MITIGATION HARDWARE

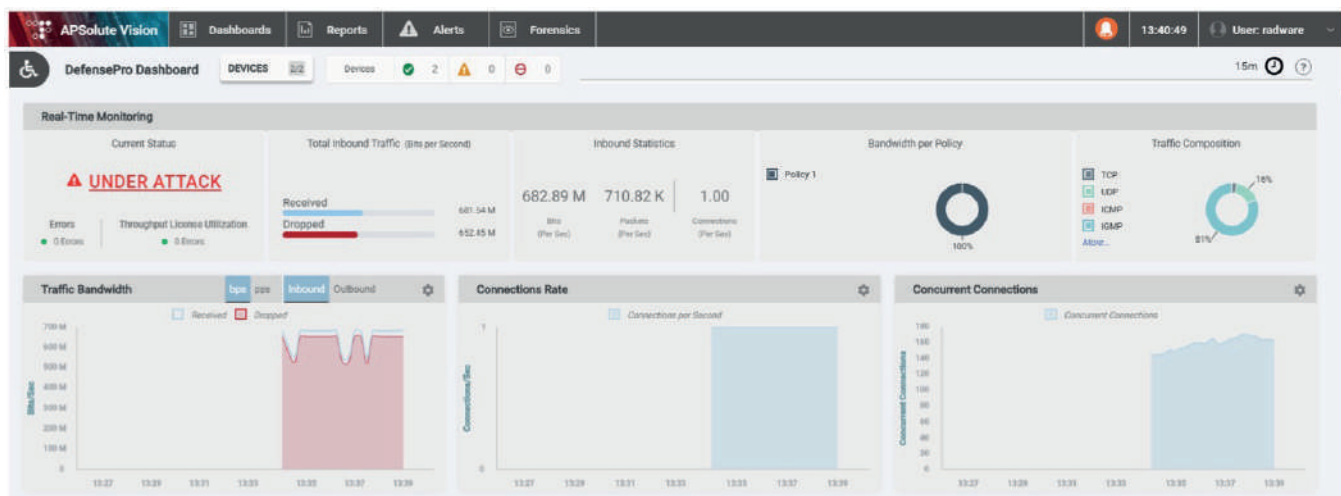
A dedicated hardware module that allows DefensePro to mitigate attacks without impacting legit traffic and the user experience, even large attacks.

### Widest Attack Coverage

- Complete Layer 3–7 protection against known and zero-day DoS/DDoS attacks that misuse network bandwidth, server and application resources.
- Bidirectional visibility to defend against even the most complicated attacks that require looking at both ingress and egress traffic.
- Burst attack protection provides immediate behavioral-based detection and mitigation from one of today's top threats with signature creation and instant enforcement for the fastest remediation.
- Advanced DNS attack coverage that leverages fist-in-class behavioral-based algorithms to protect from known and unknown DNS Flood attacks, including DNS Water Torture attacks, in the most cost-effective way.
- A patent-protected stateless and keyless SSL/TLS attack mitigation solution that protects from all types of encrypted attacks with reduced latency and no packet decryption for high protection capacity.

### Multiple Deployment Options to Fit Your Needs

- Supports both in-line or out-of-path (SmartTap) implementations or a scrubbing center deployment.
- Integrates with Radware's Hybrid Cloud DDoS Protection Service to offer a single vendor hybrid solution that provides zero time to mitigate.
- Enables service providers to offer market-leading DDoS mitigation services to hosted applications and network tenants with multitenant and multipolicy support.
- Virtual appliance enables DDoS mitigation for software-defined data centers (SDDC).
- Range of protection devices offers mitigation capacity from 6Gbps to 400Gbps.



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