The Industry's Most Advanced DDoS Protection

Distributed denial-of-service (DDoS) attacks are becoming more frequent, powerful and sophisticated. With the growth in online availability of attack tools, the pool of possible attacks is now larger than ever. Radware's Cloud DDoS Protection Service defends organizations against today's most advanced DDoS attacks, using advanced behavioral-based detection for both network-layer (L3/4) and application-layer (L7) attacks, automatic real-time signature creation to protect against zero-day attacks, unique SSL DDoS protection, and flexible cloud-based and hybrid deployment options that suit every customer.

State of The Art DDoS Protection

Comprehensive DDoS protection from all possible threats using behavioral-based detection, automatic signature creation and unique SSL attack mitigation.

Industry Leading SLA

Committed to detect, alert, divert and mitigate due to advanced automation and predefined workflows. Broad set of additional services and metrics for visibility and control.

Frictionless Deployment Modes

On-demand, always-on and hybrid deployment models to uniquely suit customer needs, network topology or threat profile.

Experts by Your Side

An Emergency Response Team; DDoS protection expert serves as a focal point for best practices, strategy and alerts throughout any attack.

Quadrant Knowledge Solutions SPARK MATRIX: DDoS Mitigation, 2022 LEADER

Quadrant Knowledge Solutions SPARK MATRIX: DDoS Mitigation, 2021 LEADER

FORRESTER® WAVE LEADER 2020 DDoS Mitigation Solutions

IDC Analyze the Future

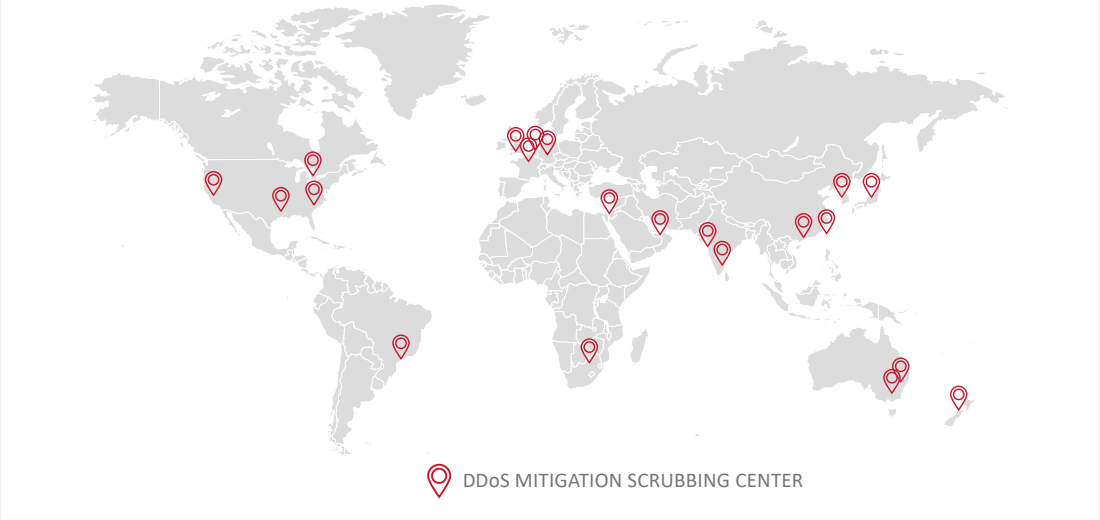
Choosing the Right Solution for You

On-Demand	Always-On	Hybrid
↗ No added latency in peacetime; traffic diversion only upon attack detection	↗ Always available, real-time cloud based DDoS protection	↗ Combines on-premise devices backed by cloud-based scrubbing capacity
↗ Allows lowest cost, cloud-only simple deployment	↗ Provides immediate protection but with minimal added latency	↗ Real-time protection and minimal latency in peacetime
↗ Best suited for latency-sensitive applications and organizations that are infrequently attacked	↗ Best suited for cloud-hosted applications and organizations constantly under DDoS attacks	↗ Recommended security best practice; best suited for data center protection

Global Coverage, Massive Capacity

Radware's Cloud DDoS Protection Service is backed by a worldwide network of 21 scrubbing centers, with 15 Tbps of mitigation capacity (and growing). Radware's scrubbing centers are globally connected in full mesh mode, using Anycast-based routing. This ensures that DDoS attacks are mitigated closest to their point of origin and provides truly global DDoS mitigation capable of absorbing even the largest volumetric attacks.

DDoS Mitigation Scrubbing Center



Easy Management & Control

Full Visibility
A single location for relevant information and data. From elaborate traffic details and important peacetime information to advanced analytics that contribute to the management of the network

Enhanced User Experience
With a highly intuitive GUI, navigation across screens and interfaces is just a few clicks. A dark mode experience as well as regular mode is available to meet the user's preference.

Attack Centric
Network health status is updated in real-time while under attack and a clear indication is displayed. An attack asset display provides important attack information. This enables users to respond promptly.

Detailed Reporting
Valuable reports and analysis are provided whether in peace time or under attack. Information is easily viewed by a single widget. This data can be exported for additional analysis.

White Glove Support

- Expert managed service through Radware's Emergency Response Team (ERT).
- Pre-attack alerts from Radware's library of cyberthreat advisories, gathered by continuously mining data across the web, darknet and post-attack forensic analysis and recommendations.
- Dedicated Technical Account Manager (TAM) who serves as a focal point for all issues, including configuration, integration, upgrades and attack mitigation.
- Backed by the industry's most granular service-level agreement (SLA), with detailed commitments for time to mitigate, detect, alert and divert, thus enabling consistency of mitigation and overall service availability.

RW 1204 | 03.19.2024