Emergency Onboarding DDoS Protection When Under Attack

Dealing with and mitigating DDoS attacks when under attack can be challenging. Radware offers a one-time Emergency Attack Mitigation Service for new customers to help mitigate on-going DDoS attacks, neutralize security risks and safeguard operations before irreparable damage occurs.

This fixed-fee service is offered to organizations that have not purchased Radware's security solutions but are experiencing a DDoS attack on their network. The service provides organizations that are actively under attack, the most efficient service and support to help resolve the situation.

What The Service Includes

- Emergency onboarding to Radware's Cloud DDoS Protection Service in Always-On mode to allow mitigation of ongoing attacks
- One-time protection against unlimited number of DDoS attacks and attack sizes for a period of up to seven days (subject to terms of the service)
- Service will be provided for up to eight protected networks for each customer's data center and up to a total of 4Gbps of legitimate traffic
- Service will be provided as an emergency service and under attack, on a best-effort basis
- Service fees are $30,000 per each company's data center and will credited from future purchase of Radware's Cloud DDoS Protection service annual contract if purchased within a period of 30 days from the start date of the service.
- Available for new Radware customers or existing customers that have not implemented Radware's DDoS solutions.

How Does the Service Work?

Step 1: Service Registration

Once the company reaches out to Radware, they receive an on-boarding invitation to register protected assets in Radware's Cloud Security Services portal with the assistance of Radware's Emergency Response Team (ERT).

Step 2: Traffic diversion set-up

For BGP-based traffic diversion, the company signs an LOA for BGP diversion, which gets submitted by Radware for the upstream provider's approval. For DNS-based traffic diversion, the company changes its DNS record to direct traffic to a Radware scrubbing center.

Step 3: Tunnel configuration for clean traffic return

A GRE tunnel is configured for clean traffic return in the scrubbing center and on the company side.

Step 4: Traffic diversion

Traffic is diverted to Radware's nearest scrubbing center out of its global scrubbing network.

Radware's ERT Emergency Response Team

The ERT team is a group of security experts that provide 24x7 security services for customers-facing DoS attacks or malware outbreaks that require immediate assistance. Radware's ERT is staffed by experts with extensive knowledge and experience handling network threats, detection mitigation and in-depth understanding of Radware's products. In addition, the ERT learns from each customer engagement and simulates the same scenario internally for further analysis and proactive implementation of defense techniques for other customers that may face a similar security threat.

Global Coverage, Massive Capacity

Radware's Cloud DDoS Protection Service is backed by a worldwide network of 25 scrubbing centers, with 30 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

The Industry's Most Advanced DDoS Protection

Comprehnsive DDoS Protection

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

Industry-Leading SLAs

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.

Multiple Deployment Options

On-demand, always-on or hybrid deployment models to suit any customer need, 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.