Defend Your Network and Applications with Radware's End-to-End DDoS Protection Solutions

Distributed denial-of-service (DDoS) attacks are a growing threat to businesses and organizations becoming more frequent, powerful and sophisticated over time. And with the growth in online availability of attack tools, the pool of possible attacks is now larger than ever. As a result, businesses must be proactive in implementing comprehensive DDoS protection solutions to mitigate the effects of these attacks and ensure that their network and application resources remain available to legitimate users.

Radware's DDoS protection solutions defend organizations against today's most advanced DDoS attacks, using advanced behavioral-based detection for both network-layer (L3/4) and application-layer (L7) attacks. They also provide automatic real-time signature creation to protect against zero-day attacks, unique SSL DDoS protection, and flexible appliance, cloud-based and hybrid deployment options that suit every customer.

Radware's DDoS protection solutions defend organizations against today's most advanced DDoS attacks, using advanced behavioral-based detection for both network-layer (L3/4) and application-layer (L7) attacks

The Challenges of the Modern DDoS Threat Environment

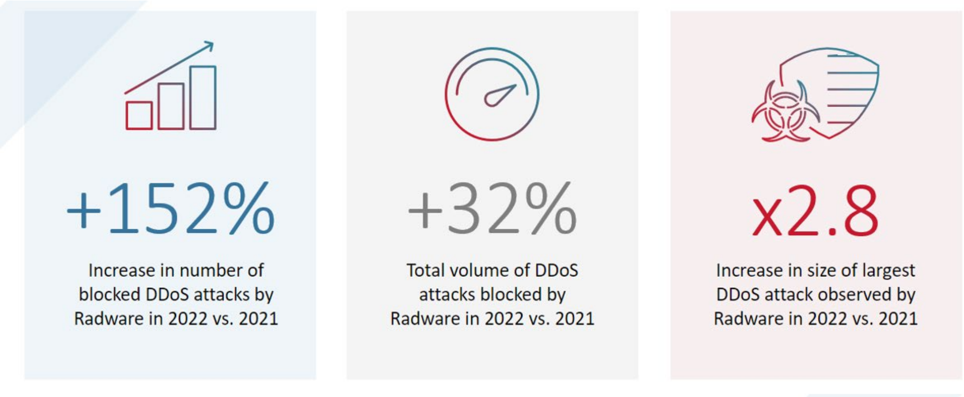
The world is now experiencing an unprecedented rise in DDoS attack activity. A conversion of multiple factors, centering around the Russian invasion of Ukraine, has brought together an explosion in DDoS attack size, frequency and sophistication. The result is a more dangerous and complex threat landscape than ever before.

Here are some of the key factors impacting DDoS attack activity today:

- **Emergence of State Actors**
  The attack landscape has witnessed a significant change with the involvement of state-sponsored groups, particularly notable since Russia's invasion of Ukraine. These groups, including independent state-supported organizations like Killnet, Passion, Zarya and NoName057(16), operate in coordination with the Russian military, constantly forming, re-forming, merging and splintering. This development has elevated the scale and sophistication of DDoS attacks.
- **Increase in Size and Complexity**
  DDoS attacks have grown both in size and complexity, primarily due to the rise in state-sponsored hacking groups. These groups have developed new attack tools that enable larger and more intricate attacks. Attackers now employ multiple attack vectors within a single assault, utilizing short bursts by one vector before swiftly switching to another. This increased complexity challenges traditional DDoS mitigation tools.
- **Shift to the Application Layer**
  There has been a significant shift of DDoS attacks to the application layer, a trend that has been ongoing for years but has recently reached new heights. Botnets, such as the Mirai botnet in 2017, pioneered the use of application-layer HTTP/S attacks. However, newer botnets developed in the aftermath of the conflict in Ukraine have significantly enhanced these capabilities. They utilize advanced web DDoS attack tools like Blood, MHDDoS and Saphyra, employing multiple attack vectors and mitigation bypass techniques, making them particularly challenging to mitigate with traditional tools.
- **Staff and Skills Shortages Continue to Affect Organizations**
  The shortage of cybersecurity staff and skills continues to impact organizations, with the global cybersecurity workforce gap reaching 3.4 million people in 2022. This shortage is worsening and affecting organizations' ability to combat cyberattacks. Reasons for the shortage include the inability to find qualified talent, high employee turnover, limited budgets and the inability to offer competitive wages. To address this challenge, organizations can adopt three key measures: consolidation of security tools to reduce complexity, automation of processes to alleviate the workload on staff and leveraging fully managed security services to outsource certain functions to expert providers. These measures help organizations maintain effective cybersecurity programs and enhance protection while alleviating the burden on internal staff.

Figure 1

DDoS Attack Trends (Source: Radware Global Threat Analysis Report 2022)



The Radware DDoS Protection Solution

To overcome these sophisticated threats, Radware offers DDoS protection across any infrastructure implementation.

Our DDoS protection secures your data center and private and public cloud, using a single-vendor solution that is agnostic to the environment and designed to protect your networks and applications. This solution provides maximum coverage, accurate detection and the shortest time to protection from the most advanced attacks. It gives organizations the control and visibility they need over their networks, services and applications.

Solution Highlights

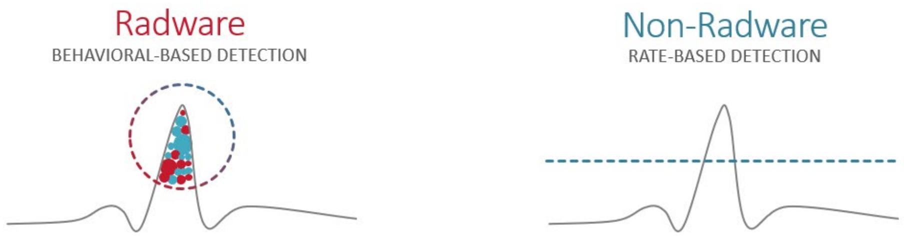
Highlights of Radware’s DDoS protection solution include:

- **State-of-the-art protection from the most advanced threats –** Industry-recognized DDoS protection is automated and does not require human intervention.
- **Highest-accuracy detection and mitigation to avoid blocking legitimate traffic –** Top-rated behavioral-based detection only blocks malicious traffic and automatic real-time signature generation protects from unknown threats and zero-day attacks.
- **Comprehensive Web DDoS protection –** Protects against application-layer web DDoS Tsunami attacks, using behavioral-based protections against HTTP/S floods, low-and-slow attacks, encrypted attacks and more.
- **Frictionless integration –** Radware's DDoS protection solutions offer flexible deployment options, with cloud, hardware and hybrid solutions to match any customer use case, environment or architecture, and provide consistent protection with centralized management for all customer assets.
- **Fully managed services –** Managed-application and 24x7 network-security services, provided by security experts and covering a broad range of attack types.
- **Full visibility and simple management** – Robust peacetime and under-attack analytics, a rich user experience, unified management and control across for all deployments.

Radware's solution provides maximum coverage, accurate detection and the shortest time to protect from the most advanced attacks, giving organizations the control and visibility they need over their networks, services and applications.

Key Features of Radware's DDoS Protection Solutions

- **Behavioral-based Detection**
  Unlike competing solutions, which detect DDoS attacks using volumetric detection or signatures of known attack patterns, Radware uses behavioral-based detection using advanced, patented machine-learning algorithms to protect against known and unknown threats. Radware uses machine-learning algorithms to automatically distinguish between legitimate user traffic and attack traffic. This allows for more accurate detection with lower rates of false positives.



- **Real-time Signature Creation**
  Real-time signature creation algorithms provide zero-day protection against network and application-layer DDoS attacks such as: Burst attacks, Dynamic-IP, DNS attacks and others. Radware's technology generates an optimal signature to block unknown attacks with a minimal false-positive rate, even when no prior knowledge of the specific vulnerability exists.
- **Advanced Web DDoS Protection**
  Mitigation of L7 attacks uses the similar behavioral and machine-learning mechanisms as L3/4 DDoS attacks. Radware's L7 DDoS protection is provided as part of our Cloud Radware DDoS Protection Service and does not depend on an external WAF.
- **Managed Services and Attack-Time Protection**
  Radware's Cloud DDoS Protection Service is provided as a fully managed service and is supported by Radware's Emergency Response Team (ERT). Radware's ERT provides customers with a single point-of-contact for both their routine and emergency needs, ensuring better security and lower overhead than doing it by themselves.
- **Industry Leadership**
  Radware is consistently acknowledged as a leader in DDoS protection, according to multiple industry reports by top analyst firms such as Gartner, Forrester, IDC and others. This means that you can trust Radware with the protection of your network and applications.

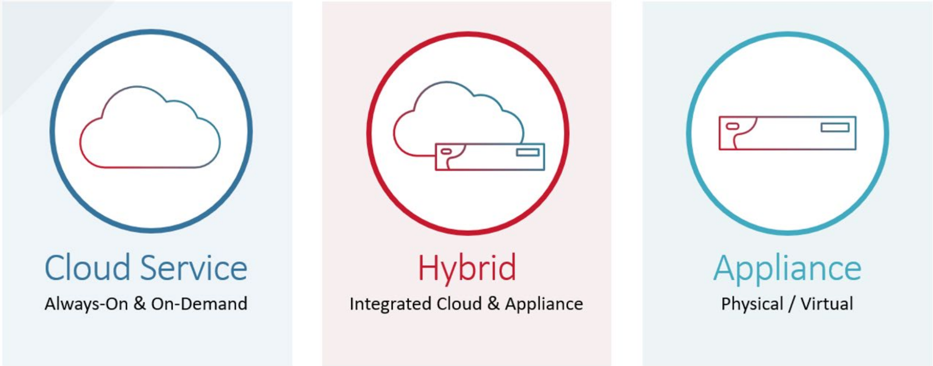
"Radware knows DDoS attacks better than anyone"

- THE FORRESTER WAVETM DDoS Mitigation Solutions, Q1 2021

- **Easy-to-use Centralized Management Portal**
  An easy management portal that provides robust peacetime and under-attack analytics, a rich user experience, unified management and control across all deployments.
- **The Most Extensive SLA Commitments in Industry**
  Backed by the industry's most comprehensive SLA with detailed commitments for Time-to-Mitigate, Time-to-Detect, Time-to-Alert, Time-to-Divert, consistency of mitigation and overall service availability.
- **Multi-terabit Dedicated Mitigation Capacity**
  Radware's solution can handle high-volume attacks, absorb and scrub the malicious traffic, and ensure that legitimate traffic reaches its intended destination without interruption. This capability is crucial for organizations that require robust protection against large-scale DDoS attacks, such as service providers, e-commerce platforms, financial institutions and other high-profile targets.

Flexible Deployment Models

Radware DDoS protection solutions can be deployed in **multiple deployment models.**



Each deployment type is based on Radware's technology with identical DDoS protections for each. The decision on which deployment model to choose depends on customer needs and considerations.

Cloud Service

Radware's DDoS Protection Service can be deployed as a cloud service for globally-scalable, multi-layered protection against any attack vector. It provides the following:

- **Infrastructure DDoS Protection**
  Protects the organization's networks and infrastructure against network-layer (L3/4) volumetric floods such as SYN floods, TCP handshake violations, RFC violations, TCP RST attacks, ACK floods, UDP floods and more. In addition, it protects DNS infrastructure against DNS DDoS attacks such as DNS query floods, DNS amplification attacks, DNS randomized subdomain ('water torture') attacks and more.

  Radware's infrastructure DDoS protection uses advanced behavioral detection and real-time signatures to block advanced attack techniques such as burst attacks, carpet bombing attacks, dynamic IP attacks, multi-vector attacks and others.

- **Web DDoS Protection**
  Protects against both volumetric and non-volumetric application-layer (L7) DDoS attacks such as HTTP/S floods, SSL negotiation attacks, SSL floods, low-and-slow attacks and more.

  Radware's Web DDoS Protection add-on uses advanced L7 behavioral-based detection and mitigation to block sophisticated Web DDoS Tsunami attacks that use advanced evasion techniques such as attack vectors randomizations, dynamic argument parameters, IP spoofing, forged X-Forwarded-For IP, cookie harvesting and more.

Radware's cloud service supports both BGP and DNS traffic diversion and can be deployed in multiple deployment models, such as:

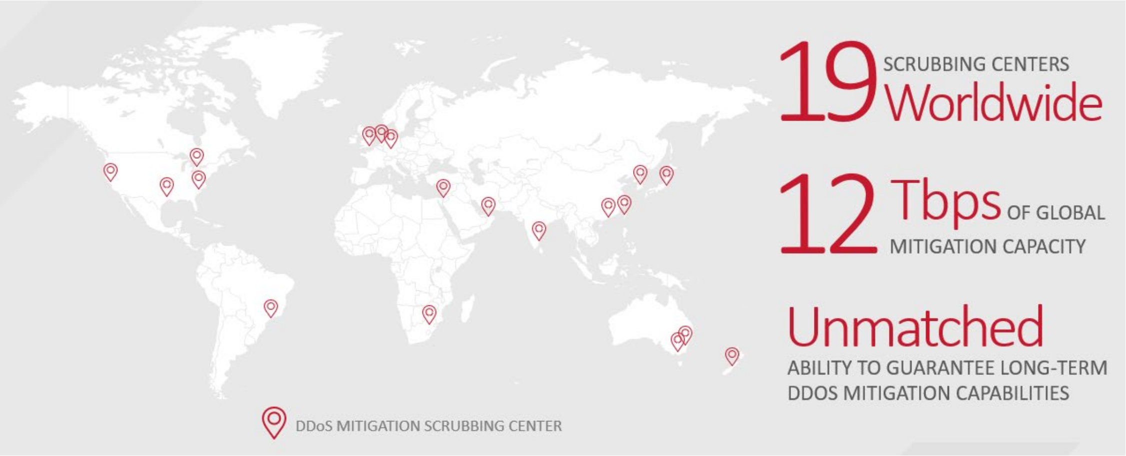
- **On-Demand Cloud Service**
  Activated only when a volumetric DDoS attack threatens to saturate the organization's internet pipe. Recommended for organizations that are not frequently attacked and for assets which are not mission-critical.
- **Always-on Cloud Service**
  Provides always-on protection where traffic is constantly routed through Radware's cloud security scrubbing centers with no on-premises device required for detection and mitigation. All traffic will be analyzed and scrubbed by Radware with no traffic diversions required. Recommended for applications that are frequently attacked—and for assets that are mission-critical and cannot afford any downtime.

Radware's Cloud DDoS Protection Service is backed by a worldwide network of 19 scrubbing centers, with 12 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.

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. It provides truly global DDoS mitigation capable of absorbing even the largest volumetric attacks.

Figure 2

Radware's Global Cloud DDoS Scrubbing Network


19 SCRUBBING CENTERS Worldwide
12 Tbps OF GLOBAL MITIGATION CAPACITY
Unmatched
ABILITY TO GUARANTEE LONG-TERM DDOS MITIGATION CAPABILITIES
DDoS MITIGATION SCRUBBING CENTER

Add-ons to cloud services

- **Cloud Firewall as a Service (FWaaS)**
  Radware's Cloud Firewall as a Service provides a cloud-based network firewall solution that helps offload dirty traffic before it reaches the organization's network, thereby improving network efficiency and providing consistent protection for the entire network. With no appliance to manage and IP blocking at scale, the service helps organizations manage their traffic in a more efficient and less human-intensive manner.
- **Single IP Protection**
  Radware offers single IP protection, for the protection of individual assets which require to be protected for more than just the web traffic (I.e., not just ports 80/443), as the individual IP addresses are also not owned by the customer or are a part of a customer-owned ASN.

  With single IP protection, Radware allocates an IP address from its own pools, which is connected to the customer via GRE tunnel. All traffic to the customer IP addresses first reaches Radware's network, where it is inspected for attack traffic, and only the clean traffic is delivered to the customer. This solution is best used for individual non-DNS assets such as routers, firewalls, VPNs and so on.

On-Premises DDoS Mitigation Appliance

For on-premises protection against DDoS that takes place directly in the customer's data center, Radware offers DefensePro X – a real-time, behavioral-based attack mitigation device that offers scalable protection against network and application DDoS attacks.

Radware offers a line of DDoS mitigation appliances with multiple hardware and virtual configurations, depending on the customer's needs and throughput. The platform provides automated DDoS protection against high-volume, fast-moving, encrypted and zero days threats. It brings automated protection for Radware customers against burst, DNS, TLS attacks and many other types of threats. The platforms leverage new and unique capabilities including updated platforms with 25 Gig and 400 Gig interfaces, modular platforms, internal optical bypass, high port density, and SSL acceleration hardware.

Main Benefits of DefensePro X are:

- **Industry-leading performance** to keep up with increasing customer demands and traffic throughputs.
- **Dedicated hardware** for DDoS mitigation combined with robust processors for high performance protection metrics, including mitigation and legit throughput, RSA CPS (connections-per-second) and total PPS (packets-per-second), to secure the business continuity under attack.
- **Industry-recognized, advanced and automated protection** from the most advanced network and application-layer threats. Built-in advanced protections to mitigate encrypted attacks, DNS attacks and application-layer (L7) DDoS attacks in real time.
- **Enriched user experience and visibility with robust analytics**—during peacetime and under attack — provide insights into network behavior and assist in identifying anomalies as they occur.

Hybrid DDoS Protection

Radware Hybrid DDoS protection combines the benefits of on-premises and cloud-based protection to provide advanced and effective DDoS attack mitigation. This enables businesses to detect and mitigate both network and application-layer DDoS attacks, regardless of their size or complexity.

This hybrid solution offers a comprehensive and effective solution for businesses seeking to protect themselves against the growing threat of DDoS attacks—tier 1 enterprises that must protect their business and cannot afford downtime at all.

The Benefits of Radware's Hybrid DDoS Protection Include:

- **Granularity of Appliances and Capacity of Cloud:** Offers multiple protection layers against any type of DDoS attack, combining the advanced capabilities of Radware's hardware appliances with the multi-terabit capacity of Radware's cloud scrubbing network.
- **Comprehensive Protection Against Any Attack Vector:** Protects against both volumetric and non-volumetric attacks, including some types of attacks which require bi-directional visibility into internet traffic, such as scanning, brute force attacks, outbound pipe saturation attacks and some types of application-layer attacks.
- **Granular Encrypted DDoS Protection:** Customers can manage their SSL/TLS certificates either in-house or on the cloud and enjoy full control over where and how encrypted traffic is inspected. This is particularly important for customers in highly regulated industries such as financial services, healthcare and government.
- **Service and SLA:** Supported by Radware's Emergency Response Team (ERT), one of the industry's most experienced teams in the field of DDoS protection and backed by the industry's most extensive SLA.

Summary

As distributed denial-of-service (DDoS) attacks continue to increase in frequency, power and sophistication, organizations face significant challenges in safeguarding their network and application resources. The growing pool of attack tools available online has expanded the range of possible attacks, necessitating proactive measures to implement comprehensive DDoS protection solutions.

Radware's DDoS protection solutions effectively defend organizations against advanced DDoS attacks by leveraging advanced behavioral-based detection, automatic real-time signature creation, unique SSL DDoS protection and flexible deployment options.

By implementing Radware's DDoS protection solutions, businesses can effectively defend against today's most advanced DDoS attacks, mitigate risks and maintain the availability and reliability of their network and application resources. With a comprehensive set of features and deployment options, Radware empowers organizations to proactively protect their digital assets, maintain a secure online presence and stay ahead of evolving threats in the complex DDoS landscape.

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.