



Advanced DDoS Protection for Public Clouds with Radware DefensePro

WHITE PAPER



The escalating pace of digital transformation and the critical need to increase business agility are two of the main factors driving organizations to the cloud. By 2022, global analyst firm Gartner predicts worldwide public cloud services revenue will reach a massive \$354.6 billion.

Despite this rapid adoption of the cloud, the security and availability of applications remain key concerns facing customers moving to the cloud. For instance, distributed denial of service (DDoS) attacks, a common threat companies may encounter, will attempt to exhaust an application's resources, rendering it unavailable to legitimate users and potentially damaging hard-earned user trust.

Radware delivers advanced and programmable L4-L7 DDoS protection solutions that ensure application availability and performance in public clouds.

Radware's DDoS protection consists of DefensePro Virtual Appliances, Vision, and a unique set of cloud-native tools for cloud automation, auto-scaling and high availability (HA) services, enabling customers the ability to:

- ▶ Protect the availability of applications through unmatched attack mitigation, visibility, forensics, and precise control.
- ▶ Prevent DDoS threats from moving laterally between workloads.
- ▶ Eliminate security-induced application development bottlenecks through automation and centralized

DDoS Risks In Public Cloud

In public clouds, DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet or from within the cloud environment.

There are two main attack categories:

- ▶ **Volumetric, Brute-Force Attacks** – These attacks consist of traffic floods (e.g. User Datagram Protocol (UDP)/ Transmission Control Protocol (TCP) attacks) that exhaust resources by creating high bits per second (bps) or packets per second (pps) volumes and overwhelm the cloud network infrastructure. Their impact on public clouds' network infrastructure is reduced due to the shared responsibility model. Public Cloud vendors guarantee the security and availability of the cloud, including all network resources and links. Nevertheless, DDoS attacks overwhelm compute resources, resulting in auto-scaling which poses a moving-target infinite billing risk and in other cases might impact application's availability when auto-scaling is neither supported (e.g. "lift-and-shift" applications) nor required (e.g. monolithic applications such as gaming rooms).
- ▶ **L4-L7 Smart Attacks** – These attacks impact cloud resources as well as customer's applications. Resource exhaustion attacks (e.g. TCP floods) exploit vulnerabilities in L4 protocol stack to render a target inaccessible. They impact end-user applications and public cloud resources and services, such as load balancing services that cannot scale infinitely. In the most likely scenario, public clouds absorb these attacks by auto-scaling, but still incur significant billing charges as a result of the resulted outbound traffic. There are cases where customers chose not to use native load balancing services for security or functionality reasons and deploy their own load balancing solutions (e.g. Radware's Alteon VA), leaving them responsible to protect their own availability. Application attacks like HTTP floods take out services by exploiting weaknesses in the application that disrupt its ability to normally serve legitimate traffic. HTTP/S attacks such as cache busting bypass content delivery network (CDN) services to overwhelm application services with randomized URL queries, resulting in overconsumption of central processing unit (CPU) resources.

➔ Public Cloud DDoS Protections or Radware's DDoS Protection

There are various reasons organizations are migrating their enterprise applications to the cloud, including business agility and a desire to reduce their data center footprints. In many cases, large organizations follow hybrid cloud models – leveraging cloud bursting to handle resource peaks in IT demand or migrating some of their applications to the cloud, but still maintaining some applications in their data centers. Security best practices dictate that organization's cloud security posture should mimic their data center approach.

Public cloud vendors provide organizations with basic DDoS protection that is automatically enabled as part of the cloud platform. It provides the same defenses utilized by other cloud services, including always-on traffic monitoring and real-time mitigation of common network-level attacks. It guarantees availability of the cloud platform and regions, but it is not tuned to specific customer applications.

Most public cloud vendors offer an add-on paid service that is built on top of standard protection, offering additional detection and mitigation capabilities tailored to customer's applications, better visibility and analytics, access to DDoS emergency teams, and limited cost protection.

Radware's DDoS protection solution is an alternative to native public cloud offerings. Built on Radware's DDoS technology and equipped with automation and centralized management, customers can embed best-in-class DDoS protection into cloud application workflows, allowing security to keep pace with development, while providing the following benefits:

- ▶ **Most Comprehensive DDoS Protection Coverage** – Radware's DDoS technology protects against all DDoS attack vectors and all applications, while patented machine-learning algorithms allow enforcement of positive and negative security models to reduce false-positive.
- ▶ **Unique Protection Against Sophisticated DDoS Attacks** – Radware's DDoS technology protects against all DDoS attack vectors and all applications, while patented machine-learning algorithms allow enforcement of positive and negative security models to reduce false-positive.
- ▶ **Customized and Precise DDOS Protection Tailored to Application's Needs** – Granular DDoS protection according to specific application use case and behavior, and multiple security policies for fine-tuned protection of different application tenants.
- ▶ **Full Control and Integration with On-Premises Security Policies** – Seamlessly leverages already available security policies on-premises to protect services in public clouds.
- ▶ **Application Protection Against Known and Unknown Attacks** – Machine learning algorithms detect zero-day DDoS attacks in real-time and apply mitigation signatures in seconds. Radware's Threat Intelligence feeds provide an additional layer of protection against known attacks and known attackers by leveraging a worldwide network of honeypots to detect active attackers and preemptively deploy mitigation rules on DefensePro VA.

➔ Protection Against Smart Attacks

Resource-exhaustion and application attacks are the most advanced attack vectors threatening applications in public clouds. These stealthy attacks leverage legitimate sessions to target applications and compute resources. Gaming applications are known to be very sensitive to low-volume attack floods and can be taken off completely without creating large floods. Web applications can easily be targeted after session establishment with CPU-intensive, carefully crafted requests. Low and slow attacks, such as half-opened sessions or concurrent session overwhelming, may trigger auto-scaling or disrupt the service.

Encrypted HTTP/S floods pose a challenge for all DDoS mitigation techniques. On one hand, traffic decryption is needed for visibility into L7 attack patterns, but on the other hand organizations prefer not to expose encryption keys with cloud vendors or DDoS protection services in order to protect their application's data. Radware is the only DDoS protection vendor who provides keyless encrypted flood protection technology as part of its DDoS solution. With DefensePro VA, customers can protect against in-session encrypted web flood requests without sacrificing data privacy and customer information.

In recent years, a new attack pattern has emerged. Bursts attacks, also known as hit-and-run DDoS, use repeated short bursts of high-volume attacks at random intervals. Each short burst can last only few seconds, while a burst attack campaign can span hours and even days. It is difficult to protect against such attacks since the attack vector might change between burst hits. Common practice calls for rate-limiting, as signature-based protection cannot be accurately created in seconds, resulting in a high level of false positives. DefensePro VA provides unique machine learning protection against zero-day burst attacks while minimizing false positives.

Granular DDoS protection per service, per source(src.)/destination (dst.) port, and per user allows limiting the level of pps, bps, and number of connections and is sometimes needed to defend against DDoS attacks on monolithic applications that don't need to scale, especially for UDP-based services.

➔ North-South and East-West Protection

The most known DDoS attack pattern relates to internet induced (north-south) attacks, but less attention is given to within-the-environment (east-west) attacks. Attack patterns within the cloud environment may bypass protection. In addition, DDoS bots can easily compromise and control in-VPC workloads, allowing attackers to inject such attacks.

DefensePro VA allows multiple deployment models where DefensePro appliances can be inserted at various points to achieve both north-south and east-west protection. It can reside within the VPC inspecting all incoming traffic from the internet gateway or between VPCs or availability zones for east-west protection.

➔ Automation and Programmability

Organizations often use multiple public and private cloud platforms and want to embed DefensePro VA into their application development processes. They can deploy and configure DefensePro VA using 3rd party Infrastructure-as-Code native or third-party toolsets, such as AWS CloudFormation and Terraform. The combination of these tools and DefensePro VA automation features allow the deploying and configuration of heterogeneous environments at pace with great agility.

DefensePro VAs can bootstrap with complete licenses and configurations that can be deployed in an automated, scalable manner.

➔ High Availability

A typical deployment of DefensePro is based on inline inspection of traffic directed towards application workloads. Consequently, the availability of DefensePro is critical.

Bypass High Availability

Radware supplies bypass functionality for the case of DefensePro failure. This functionality is provided by means of an AWS Lambda function that monitors the health of one or more DefensePro instances, and upon failure or high CPU utilization, fails open – which guarantees that customers' applications are always available.

Cloud-Native High Availability

High availability can also be achieved by utilizing cloud-native load balancing services for autoscaling and resiliency. In this scenario, a native load-balancing service is used to distribute traffic across a fleet of DefensePro instances. If DefensePro VA fails, the load balancer reroutes traffic through another DefensePro instance automatically.

➔ Central Management and Analytics

Vision provides centralized DDoS security management for DefensePro VA appliances across multiple cloud deployments alongside customers' physical appliances, ensuring consistent and cohesive policy. Rich, centralized reporting and comprehensive analytics capabilities provide full visibility into DDoS attacks and peacetime traffic, allowing end-users to fully understand what's happening in their networks with actionable insights and actions per security policy, while also drilling down to specific attack details and forensics. Vision can be deployed on-premises or in the cloud.

➔ Use Cases

Gaming Services Protection

Gaming services are very sensitive to high-rate bps and pps volumes. DDoS attacks are popular with gaming services where gamers try to knockout their rivals by launching DDoS attacks against their gaming rooms. Latency is also a major concern with online gaming, and DDoS attacks can easily chock CPU and network resources resulting in unacceptable game delays.

DefensePro VA is equipped with unique protections for gaming services. Machine-learning algorithms detect and block all UDP volumetric floods, while precise granular protections of gaming rooms provide per gaming room, per user, and per session protection.

DefensePro can be deployed in front of a gaming lobby room for protection or in front of gaming room instances.

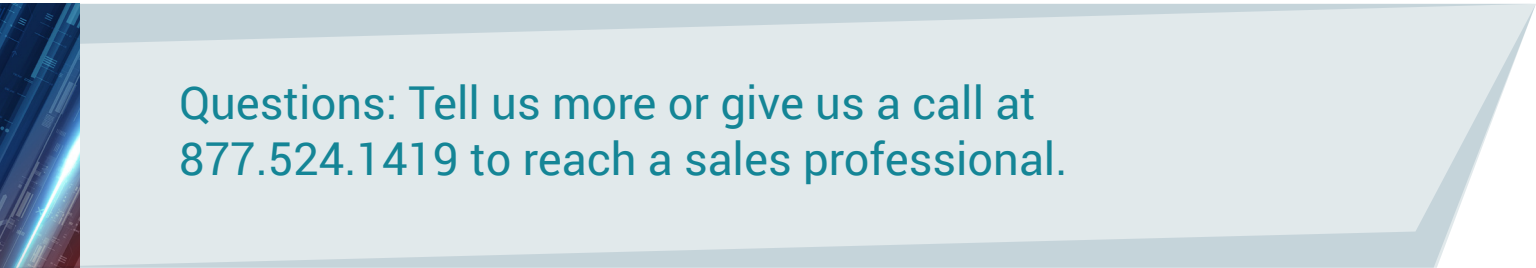
Web Services Protection

AWS provides security best practices for protecting web applications from DDoS attacks by enhancing support for keyless encrypted DDoS attacks as well as granular in-session protections.

DefensePro can be deployed in front of a web application to detect and mitigate various attacks.

Summary

Radware's DefensePro VA for public clouds provides advanced DDoS protection beyond native DDoS services. It guarantees application availability, protecting gaming and web services with machine learning algorithms for detection and mitigation. It also supports automation and native integration, providing high availability and auto-scaling in case of surges in traffic due to attacks. Radware's APSolute Vision takes this protection even further, providing advanced monitoring, analytics, and forensics, offering a single pane of glass for hybrid cloud deployments.



Questions: Tell us more or give us a call at
877.524.1419 to reach a sales professional.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of [cybersecurity](#) and [application delivery](#) solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: [Radware Blog](#), [LinkedIn](#), [Facebook](#), [Twitter](#), [SlideShare](#), [YouTube](#), [Radware Connect](#) app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

© 2021 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this ebook 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.