Knowledge Brief

Quadrant Knowledge Solutions

Radware is a Leader in SPARK Matrix: DDoS Mitigation Q3, 2023

Quadrant
Knowledge Solutions

SPARK MATRIX:
DDoS Mitigation,
2023

LEADER

An Excerpt from Quadrant Knowledge Solutions
"SPARK Matrix^{TM}: DDoS Mitigation, Q3 2023"

Radware is a Leader in SPARK Matrix: DDoS Mitigation, Q3 2023

Technological developments such as the rise in the number of unsecured devices that can be used as attack vectors, as well as the availability of attack tools through models like RaaS and MaaS, are fueling a rise in various types of DDoS attacks, including network-based attacks, protocol-based attacks, and application-level attacks. Such attacks can cause significant damage to the reputation, revenue, and customer satisfaction of the targeted organization. Therefore, organizations need to implement DDoS mitigation solutions that can detect and mitigate such attacks in real-time to prevent user organizations from being affected by such attacks.

The new age DDoS mitigation solutions utilize newer technologies like machine learning and artificial intelligence to enable more precise and adaptive detection and mitigation of DDoS attacks. These solutions learn from both normal and atypical traffic patterns and use cutting-edge algorithms and models to dynamically adjust their mitigation plans in response to the context and features of an attack. With the implementation of these new-generation AI & ML related technologies, the DDoS mitigation solution is anticipated to offer a more thorough and proactive defense against present and potential DDoS threats.

Vendors offer DDoS mitigation solutions through two types of deployment models: on-prem and cloud-based. The on-prem solution inspects incoming and outgoing traffic and blocks suspicious traffic. The cloud-based solution diverts the web traffic to its own servers and then filters the traffic and forwards the clean traffic.

Quadrant Knowledge Solutions' 'SPARK MatrixTM: DDoS Mitigation, 2023' research includes a detailed analysis of the global market regarding short-term and long-term growth opportunities, emerging technology trends, market trends, and future market outlook. This research provides strategic information - for technology vendors to better understand the existing market, support their growth strategies, and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

The research includes detailed competition analysis and vendor evaluation with the proprietary SPARK MatrixTM analysis. The SPARK MatrixTM includes ranking and positioning of leading DDoS Mitigation vendors with a global impact. The SPARK MatrixTM includes an analysis of vendors, including Akamai, Allot, A10 Networks, Cloudflare, Fortinet, Fastly, F5, Huawei, Imperva, Lumen, Link11, NSFOCUS, NETSCOUT, Nexusguard, Radware, Verizon, and Vercara.

Market Dynamics and Trends

The following are the key market drivers as per Quadrant Knowledge Solutions' DDoS Mitigation strategic research:

- **Growing adoption of cloud services and IoT devices:** The Organizations migrating their data to the cloud are exposing themselves to more DDoS risk. DDoS attackers can directly attack the cloud service or use it as a source of attack. Similarly, IoT devices, such as smart cameras, sensors, and routers, can be converted to botnets to launch DDoS attacks. Hence, with the adoption of cloud services and IoT devices, there is a need for organizations to adopt robust and reliable DDoS mitigation solutions.

- **Rising regulatory compliance requirements:** There are industries that handle sensitive or personal data, such as healthcare providers, financial institutions, e-commerce platforms, and gaming platforms. Such organizations need to comply with various regulations and standards that mandate data security. Implementation of DDoS mitigation solutions can ensure compliance with regulations and standards,and prevent data loss.

- **Emergence of sophisticated DDoS attack vectors:** DDoS attacks are becoming increasingly sophisticated. The bad actors are using more advanced techniques, such as amplification, reflection, and encryption, to bypass traditional defenses and evade detection. For instance, cybercriminals are increasingly leveraging automated software bots to carry out click fraud along with launching DDoS attacks. The mutating botnets can result in even more complex and massive DDoS attacks. Hence, DDoS mitigation vendors are using anti-fraud technologies like bot management to identify and mitigate advanced ad fraud.

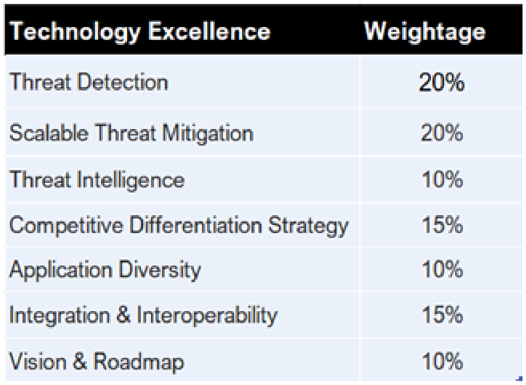
- **Application Layer attacks:** Application layer attacks or L7 attacks aim to exhaust the application's resources or logic, causing performance degradation or functionality loss. These attacks target specific applications or services on the target's server, such as web servers, databases, or APIs. Vendors are using Web Application Firewall, integrated bot management capabilities, and advanced API capabilities along with their DDoS mitigation solution to block the attacks without stopping legitimate traffic.

- **Rise of cloud-based DDoS mitigation services:** Cloud-based DDoS mitigation services offer scalability, flexibility, and cost-effectiveness to enterprises who need to protect themselves from sophisticated, large-scale DDoS attacks. These services employ the cloud provider's network design and security expertise to filter and divert hazardous traffic away from the target. Vendors are providing cloud-based DDoS mitigation services that can be combined with on-premises or hybrid solutions to provide a comprehensive defense layer.

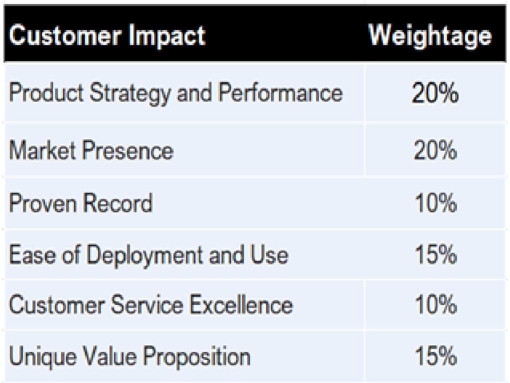
- **Adoption of AI and ML for DDoS detection and response:** Using AI and ML capabilities ensure the accuracy and efficiency of DDoS mitigation solutions, as they reduce false positives and minimize human intervention. The DDoS mitigation solution providers make use of AI and ML technology to analyze traffic patterns, identify anomalies, and respond to traffic in real time. With the continuous evolution and increasing sophistication of DDoS attacks, vendors are rapidly adopting AI, ML, and anti-fraud techniques for a robust solution that can detect and mitigate the most complex DDoS attacks. Vendors are using ML and AI to automate the process and assist in the deployment of appropriate solutions and mitigation filters rapidly to scale up the mitigation process.

SPARK Matrix Analysis of the DDoS Mitigation, 2023

Quadrant Knowledge Solutions conducted an in-depth analysis of the major DDoS Mitigation vendors by evaluating their product portfolio, market presence, and customer value proposition. The DDoS Mitigation Market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK MatrixTM. SPARK MatrixTM analysis provides a snapshot of key market participants and a visual representation of market participants. It provides strategic insights on how each vendor ranks related to their competitors based on their respective technology excellence and customer impact parameters. The evaluation is based on primary research, including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall DDoS Mitigation Market.



Technology Excellence	Weightage
Threat Detection	20%
Scalable Threat Mitigation	20%
Threat Intelligence	10%
Competitive Differentiation Strategy	15%
Application Diversity	10%
Integration & Interoperability	15%
Vision & Roadmap	10%



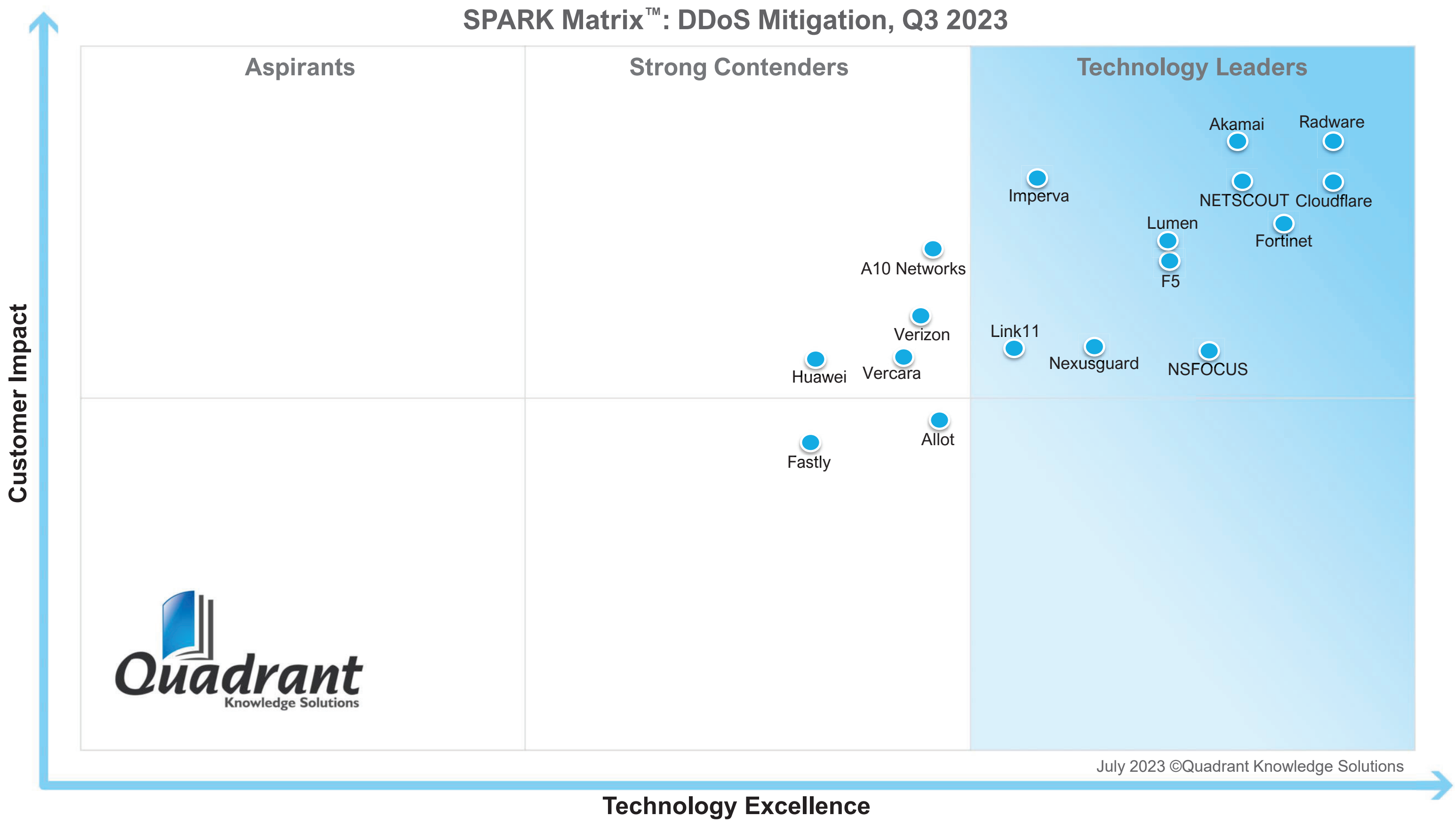
Customer Impact	Weightage
Product Strategy and Performance	20%
Market Presence	20%
Proven Record	10%
Ease of Deployment and Use	15%
Customer Service Excellence	10%
Unique Value Proposition	15%

According to the SPARK MatrixTM analysis of the global DDoS Mitigation Market, "Radware is a leading cybersecurity solution provider offering robust functional capability through its products "Radware DefensePro Solution and Cloud DDoS Mitigation" to detect and mitigate threats in real-time." Radware, owing to the robust functional capability of its product "DDoS Mitigation Product Suite," compelling customer references, comprehensive roadmap and vision, cloud-native platform, and high scalability, has been positioned among the technology leaders in the 2023 SPARK MatrixTM of the DDoS Mitigation market.

Figure: 2023 SPARK Matrix™

(Strategic Performance Assessment and Ranking)

DDoS Mitigation Market



July 2023 ©Quadrant Knowledge Solutions

Radware Capabilities in the Global DDoS Mitigation Market

URL: https://www.radware.com/

Founded in 1997 and headquartered in Tel Aviv, Israel. Radware is a provider of application delivery and cyber security solutions for virtual, cloud, and software-defined data centers. Radware provides DDoS mitigation capabilities through its DefensePro solution and Cloud DDoS mitigation services.

Radware's DDoS mitigation solution offers protection against advanced as well as automated zero-day attacks. The solution also provides behavioral-based threat detection, encrypted attack mitigation, as well as centralized visibility and management of the organization's threat landscape. Radware also offers flexible deployment options for its DDoS solution, including on-prem, cloud, and hybrid.

Analyst Perspective

The following is the analysis of Radware's capabilities in the DDoS Mitigation market:

- Radware's DefensePro solution protects organizations against new network multi-vector attacks, ransom DDoS campaigns, IoT botnets, phantom floods, and other types of cyberattacks. The solution guards networks against IoT-based, Burst, DNS, and TLS/SSL threats. Radware's Cloud DDoS Protection Services offer enterprise-grade DDoS protection in the cloud and enable detection and the shortest time to protection against dynamic and continuously changing DDoS threats.

- Radware offers strong capabilities through its smart encrypted attack mitigation, which protects against SSL/TLS attacks with a full suite of solutions to answer every business need without compromising user privacy or adding latency. Radware also provides fully managed security services with attack time protection through an Emergency Response Team (ERT). The ERT team is a team of experts that manages organizational devices and keeps them aligned with the business processes.

- Radware also offers advanced web DDoS protection against HTTP/S-based Tsunami DDoS attacks. Radware uses advanced learning capabilities designed to quickly detect and surgically block web DDoS attacks while minimizing false positives and keeping legitimate traffic unblocked.

- Radware offers comprehensive DDoS protection through its DDoS Cloud mitigation service. Radware provides SLA with six individual performance KPIs for detection, diversion, alerting, mitigation time, consistency of mitigation, and service availability. The DDoS cloud mitigation service uses behavior-based detection to detect and mitigate L3, L4, and L7 attacks, protect from zero-day attacks, along with providing SSL DDoS protection. It offers on-demand, always-on, and hybrid deployment models as per the user's requirements. Radware provides a network of 19 scrubbing centers with 12 Tbps of mitigation capacity.

- Radware differentiates itself from other vendors by providing behavior-based detection, which enables organizations to detect attacks in real time, along with reducing false positives. The Radware DDoS solution also provides automated zero-day DDoS attack protection by using patent-protected real-time signature creation technology. It can automatically protect against zero-day attacks by generating an optimal signature to block unknown attacks with a minimal false-positive rate. Radware uses a quantile DoS algorithm that enables service providers to identify and mitigate hidden phantom attacks and traffic anomalies.

- Another differentiator is the Cloud Network Analytics service that provides users with peacetime network traffic information. The solution allows administrators to eliminate errors when planning network deployments and stay ahead of DDoS threats via early detection of network abuse and intrusion in peacetime.

- Radware also provides a cyber controller that provides frictionless security, increased visibility, and an improved user experience via multiple security operation dashboards that also offer a unified view into the attack lifecycle and mitigation analysis for both inline and out-of-path DDoS deployments. The cyber controller provides network analytics with comprehensive visibility into traffic statistics during peacetime and attack, as well as simplified management and configuration with unified visibility and control.

- From a geographical presence perspective, Radware has a significant presence in North America, followed by EMEA and JAPAC. From an industry perspective, the company holds a strong position in the BFSI, E-commerce, retail, and govt and public sector industries, followed by healthcare, gaming, transportation and media, and entertainment industries.

- From a use case perspective, Radware provides DDoS protection through a hybrid, on-demand cloud service, which allows organizations to deploy the on-prem attack mitigation device DefensePro in their data center. DefensePro detects and mitigates all types of DDoS attacks in real-time, and the volumetric DDoS attacks are mitigated in the cloud. Other use cases offered include always-on cloud service, on-demand cloud service, hybrid with always-on cloud service, and on-premise devices.

- From a technology roadmap perspective, the company focuses on enhancing the detection and mitigation of encrypted attacks that help in protecting organizations from the latest web DDoS attacks, complete L7 visibility, behavioral SSL/TLS protection, and protection from QUIC/HTTPS floods. Also, Radware aims to enhance DNS protection for DNS water torture, DNS tunneling, and DNS over HTTPS. The company also plans to introduce data-driven AI-based anomaly detection. The company plans to expand its scrubbing center network to new locations in Latin America and the United States.