Knowledge Brief

Quadrant Knowledge Solutions

Radware is the Leader in SPARK Matrix: DDoS Mitigation Q2, 2024

An Excerpt from Quadrant Knowledge Solutions
"SPARK Matrix™: DDoS Mitigation, Q2 2024"

Radware is the Leader in SPARK Matrix: DDoS Mitigation, Q2 2024

Protection against DDoS attacks is critical, as such attacks pose a grave threat to the operational integrity of targeted organizations' websites, online services, as well as their reputation. However, these attacks are also harder to detect and, therefore, need to be mitigated quickly before they do any harm. Otherwise, the repercussions extend beyond immediate downtime, encompassing severe damage to the targeted organization's reputation, revenue streams, and customer satisfaction. The advances in technology now allow bad actors to compromise a large number of machines and use them to launch large-scale DDoS attacks.

These factors underline the need to deploy robust DDoS mitigation solutions capable of real-time detection and swift mitigation to fortify themselves against such malicious onslaughts. Over time, these mitigation solutions have evolved in tandem with the expanding attack surface, incorporating cutting-edge technologies such as machine learning and artificial intelligence (AI). These solutions leverage AI and ML algorithms to provide enhanced precision and adaptability in identifying and thwarting DDoS attacks. By assimilating insights from both regular and anomalous traffic patterns, the solutions dynamically adjust mitigation strategies to counter the evolving tactics of attackers, providing a proactive defense mechanism against present and potential DDoS threats.

In addition, Vendors in the DDoS mitigation market offer a range of solutions that encompass both on-premises and cloud-based deployments to cater to the varying user needs. On-premises solutions function by scrutinizing incoming and outgoing traffic to discern and block suspicious activity in real-time. While cloud-based solutions redirect incoming traffic away from the targeted website or service and funnel it through their own servers for filtration. This process enables the identification and removal of malicious traffic, ensuring that only clean, legitimate traffic reaches the intended destination.

In essence, the evolving landscape of DDoS attacks underscores the critical importance of proactive defense mechanisms for organizations. The integration of advanced technologies like AI and ML into DDoS mitigation solutions heralds a new era of sophistication and efficacy in combatting malicious cyber threats, offering organizations a robust shield against the ever-changing tactics of cyber adversaries.

Quadrant Knowledge Solutions' 'SPARK Matrix™: DDoS Mitigation, 2024' 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 Matrix™ analysis. The SPARK Matrix™ includes ranking and positioning of leading DDoS Mitigation vendors with a global impact. The SPARK Matrix™ includes an analysis of vendors, including Akamai, Allot, Alibaba Cloud, A10 Networks, Cloudflare, Corero Network Security, Fortinet, Fastly, F5, Google Cloud, Huawei, Imperva, Lumen, Microsoft, Link11, NSFOCUS, NETSCOUT, Nexusguard, Radware, Vercara, and Verizon.

Market Dynamics and Trends

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

- **Evolution of DDoS Attack Techniques:** DDoS attackers continuously refine their methodologies by incorporating advanced tactics such as IoT botnets, AI-driven attacks, and multi-vector assaults to circumvent traditional defense mechanisms and maximize disruption. The emergence of such sophisticated attack vectors presents a pressing challenge for organizations seeking to safeguard their digital infrastructure. Attackers exploit techniques like amplification, reflection, and encryption to amplify the impact of their assaults while minimizing the risk of detection. Moreover, the integration of automated software bots for click fraud alongside DDoS attacks adds a layer of complexity, further complicating mitigation efforts. In response to these evolving threats, DDoS mitigation vendors are compelled to innovate continuously, developing advanced technologies and strategies to counteract sophisticated attack vectors effectively. For instance, the implementation of anti-fraud technologies like bot management enables vendors to detect and mitigate advanced ad fraud schemes, thereby enhancing the resilience of DDoS defense mechanisms. The necessity for continuous innovation in DDoS mitigation strategies and technologies underscores the critical role of research and development within the industry. As attackers adapt and evolve, proactive investment in cutting-edge solutions becomes imperative to stay ahead of the curve and mitigate the escalating risks posed by sophisticated DDoS attacks. Consequently, the evolution of DDoS attack techniques serves as a compelling market driver, driving demand for innovative mitigation solutions and fostering dynamic growth within the DDoS mitigation market.

- **Increased DDoS Risk Due to Cloud and IoT Adoption:** As organizations embrace cloud computing to store and manage their data and deploy IoT devices to enhance operational efficiency, they inadvertently expand their attack surface, exposing themselves to heightened DDoS risks. Attackers can directly target cloud infrastructure or leverage compromised IoT devices connected to the cloud to launch large-scale assaults. Similarly, the proliferation of unsecured IoT devices introduces a multitude of attack vectors for attackers, as these devices can be hijacked and orchestrated into botnets for DDoS attacks. The increasing reliance on cloud services and IoT devices underscores the critical need for organizations to invest in robust and reliable

DDoS mitigation solutions. Proactive measures such as deploying dedicated DDoS protection mechanisms have become imperative to safeguard against potential disruptions and downtime caused by malicious attacks. As a result, the demand for comprehensive DDoS mitigation solutions is expected to surge in response to the growing adoption of cloud services and IoT devices. Organizations seek solutions that offer advanced threat detection capabilities, real-time monitoring, and rapid response mechanisms to effectively mitigate the evolving DDoS threats posed by cloud-based attacks and IoT botnets.

- **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.

- **5G Network Vulnerabilities:** The widespread deployment of 5G networks introduces new vulnerabilities and attack vectors that threat actors can exploit to launch DDoS attacks. As organizations adopt 5G technology to support their operations, securing these networks against DDoS threats becomes paramount.

- **Evolution and adoption of cloud-based DDoS mitigation services:** In the face of escalating DDoS threats, the market is witnessing a paradigm shift towards cloud-based DDoS mitigation services. These services are becoming increasingly vital for enterprises as they offer scalability, flexibility, and cost-effectiveness, which are essential in protecting against sophisticated, large-scale DDoS attacks. Leveraging the cloud provider's expansive network and security acumen, these services proficiently filter and divert hazardous traffic, ensuring business continuity. Moreover, the integration of cloud-based services with existing on-premises or hybrid solutions is creating a multilayered defense strategy, enhancing the overall resilience against DDoS disruptions. However, the ongoing migration to the cloud also introduces new vulnerabilities, underscoring the need for robust DDoS protection mechanisms to address the expanding attack surfaces and safeguard critical cloud-based infrastructure and services from potential disruptions. This driver highlights the dual nature of cloud-based DDoS mitigation services as both a solution and a challenge, reflecting the complex dynamics of the DDoS mitigation market in 2024.

- **Increasing Regulatory Compliance Requirements:** Regulatory frameworks and compliance mandates, such as GDPR (General Data Protection Regulation) and industry-specific regulations, exert significant influence on organizations' approaches to DDoS mitigation and risk management. Industries that handle sensitive or personal data, including healthcare providers, financial institutions, e-commerce platforms, and gaming platforms, are subject to stringent regulations and standards aimed at safeguarding data security and privacy. Compliance with these regulations necessitates the implementation of adequate DDoS mitigation measures to mitigate the risk of data breaches, loss, or unauthorized access. By investing in DDoS mitigation solutions, organizations can ensure compliance with regulatory requirements by fortifying their cybersecurity posture and safeguarding critical data assets from DDoS attacks. These solutions play a crucial role in preventing service disruptions, maintaining operational continuity, and safeguarding the integrity and confidentiality of sensitive information. Furthermore, the evolving regulatory landscape and the enforcement of stricter compliance mandates drive the demand for advanced DDoS mitigation technologies and services that offer robust protection against evolving cyber threats. Organizations seek comprehensive DDoS mitigation solutions that not only mitigate the risk of DDoS attacks but also facilitate compliance with regulatory requirements through proactive threat detection, real-time monitoring, and adaptive response capabilities. As regulatory compliance requirements continue to rise, organizations are compelled to prioritize investments in DDoS mitigation solutions as part of their broader risk management and compliance strategies. This heightened focus on regulatory compliance serves as a significant market driver, fueling the demand for innovative DDoS mitigation solutions and driving growth within the DDoS protection market.

- **Cyber Insurance Impact:** The growing prevalence of cyber insurance policies affects how organizations perceive and address DDoS risks. Insurers may incentivize or mandate the adoption of specific DDoS mitigation strategies and technologies as part of risk mitigation efforts, shaping market dynamics and investment priorities.

- **Geopolitical Tensions and Cyber Warfare:** Escalating geopolitical tensions and the proliferation of cyber warfare activities contribute to the complexity and severity of DDoS threats. Nation-state actors and politically motivated groups leverage DDoS attacks as a tool for sabotage, or coercion, underscoring the need for robust defense mechanisms at national and organizational levels.

- **Advancements in AI and ML-Powered DDoS Mitigation Solutions:** The integration of AI and ML capabilities into DDoS mitigation solutions enables organizations to enhance their cybersecurity posture by proactively identifying and mitigating DDoS attacks in real-time with greater accuracy and efficiency. The adoption of AI and ML for DDoS detection and response addresses several key challenges faced by organizations in combating DDoS threats. These technologies facilitate the analysis of network traffic patterns, enabling the identification of anomalies and malicious activities indicative of DDoS attacks. By leveraging AI and ML algorithms, DDoS mitigation solutions can distinguish between legitimate traffic and malicious traffic with greater precision, reducing false positives and minimizing the need for human intervention. Moreover, AI and ML-driven DDoS mitigation solutions enable rapid response to evolving threats by automating the detection and mitigation process. These solutions can dynamically adjust mitigation filters and deploy appropriate countermeasures in real-time to mitigate the impact of DDoS attacks effectively. As DDoS attacks continue to evolve in complexity and sophistication, the integration of AI and ML technologies equips organizations with the agility and scalability needed to combat emerging threats. Furthermore, DDoS mitigation solution providers are rapidly incorporating AI, ML, and anti-fraud techniques into their offerings to deliver robust and comprehensive protection against DDoS attacks. By harnessing the power of AI and ML, vendors can develop adaptive and intelligent solutions capable of detecting and mitigating even the most complex DDoS attacks with minimal latency and maximum efficacy. The increasing adoption of AI and ML-powered DDoS mitigation solutions reflects the growing recognition among organizations of the importance of leveraging advanced technologies to safeguard against evolving cyber threats. As a result, the demand for AI and ML-driven DDoS mitigation solutions is expected to continue rising, driving market growth and fostering innovation within the DDoS protection industry.

- **Supply Chain Risks:** The interconnected nature of supply chains amplifies the impact of DDoS attacks, as disruptions to key suppliers or service providers can cascade across multiple organizations. Businesses, recognizing the interconnectedness of their ecosystems, are prioritizing supply chain resilience and invest in collaborative DDoS defense strategies to mitigate collective risks.

- **Emergence of Quantum Computing Threats:** While still in its nascent stages, the potential advent of quantum computing poses significant challenges to traditional encryption methods and cybersecurity protocols. In anticipation of future quantum-enabled threats, organizations explore quantum-resistant encryption techniques and invest in next-generation DDoS mitigation solutions capable of defending against quantum-powered attacks.

SPARK Matrix Analysis of the DDoS Mitigation, 2024

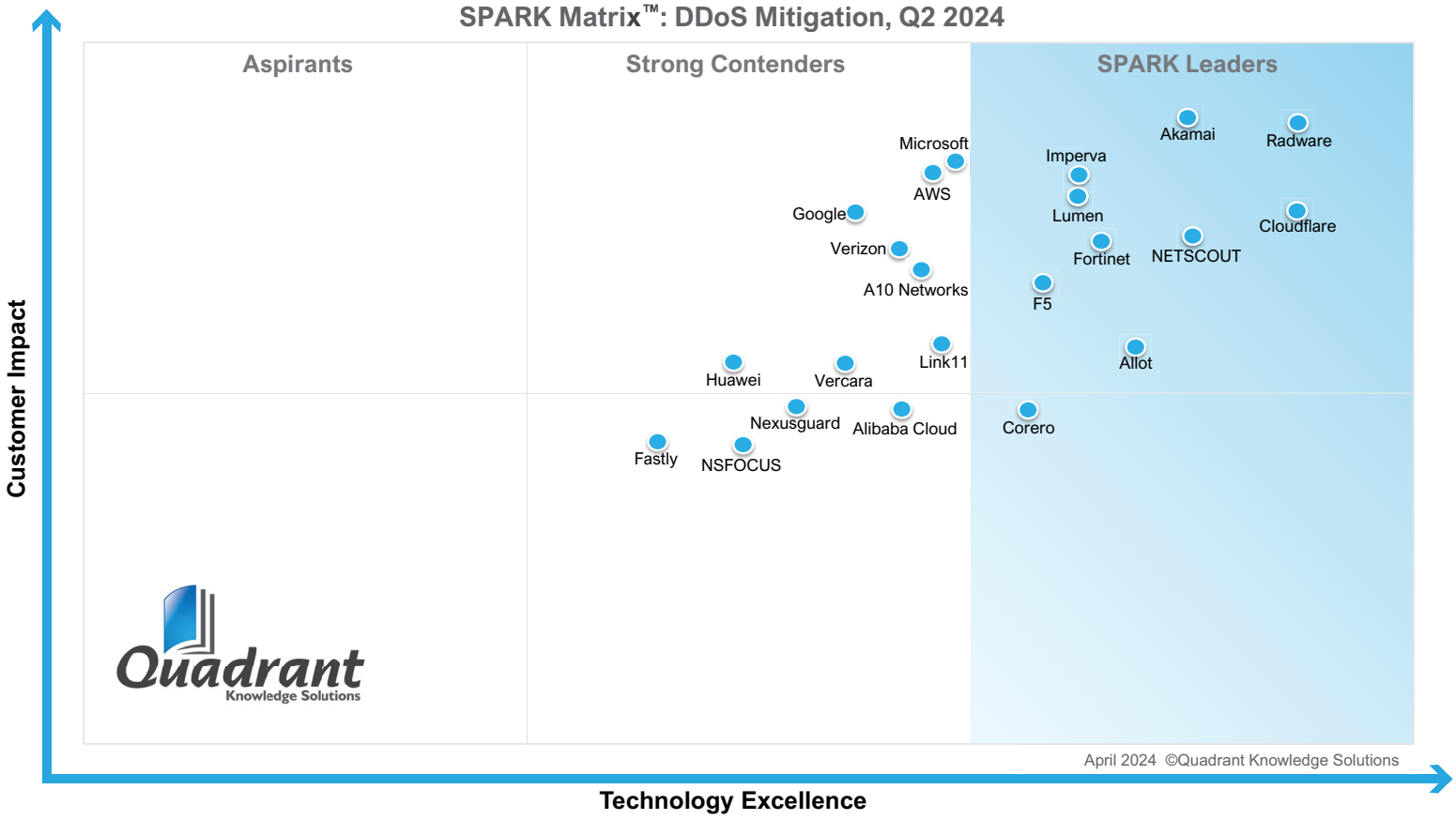
Quadrant Knowledge Solutions' conducted an in-depth analysis of the major DDoS Mitigation vendors by evaluating their product portfolio, market presence, and customer value proposition. DDoS Mitigation Market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. SPARK Matrix 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.

According to the SPARK Matrix analysis of the global DDoS Mitigation Market, "Radware a leading cybersecurity solution provider offers robust functional capability through its 'Radware DefensePro Solution and Cloud DDoS Mitigation to detect and mitigate threats in real-time.' Radware, with robust functional capability of its product DDoS Mitigation Product Suite, compelling customer references, comprehensive roadmap and vision, cloud-native platform, and high scalability, Radware has been positioned among the technology leaders in the 2023 SPARK Matrix of the 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 & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Figure: 2024 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
DDoS Mitigation Market



Radware

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

Company Introduction:

Founded in 1997 and headquartered in Tel Aviv, Israel. Radware provides application delivery and cyber security solutions for virtual, cloud, and software-defined data centers. Radware provides DDoS mitigation capabilities through its Cloud DDoS Protection Service and DefensePro hardware appliances.

Product Introduction:

Radware's cloud-based and hardware DDoS mitigation solutions offers protection against various types of threats, including advanced, encrypted, and automated zero-day attacks, provides behavioral-based threat detection, and centralized visibility and management. Radware offers flexible deployment options for DDoS protection solutions, including on-premises, cloud, and hybrid.

Technology Perspective:

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

- Radware's Cloud DDoS and DefensePro solutions protect organizations against threats such as new network multi-vector attacks, ransom DDoS campaigns, IoT botnets, and phantom floods. The service uses behavior-based detection to detect and mitigate L3, L4, and L7 attacks, protect users from zero-day attacks, and provides protection against encrypted DDoS attacks.

- Radware also offers protection from IoT-based, Burst, DNS, and TLS/SSL threats. The company's cloud DDoS Protection Service offer enterprise-grade DDoS protection in the cloud and enable detection and the accelerated mitigation measures against dynamic and continuously changing DDoS threats.

- Radware offers flexible cloud-based deployment options with 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 offers zero decryption protection against encrypted attacks, 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 a fully managed security service with attack time protection by Radware's Emergency Response Team (ERT). Radware's ERT is a team of experts that manages both hardware devices and cloud deployments and keeps them aligned with the business processes.

- Radware also provides a web (L7) DDoS protection solution that uses advanced learning capabilities designed to quickly detect and surgically block disruptive L7 DDoS attacks while minimizing false positives and keeping legitimate traffic flowing.

- Radware provides the industry's most comprehensive DDoS protection SLA with six individual performance KPIs for detection, diversion, alerting, mitigation time, consistency of mitigation, and service availability.

- The key differentiator for Radware DDoS offering is providing behavior-based detection, which enables organizations to detect attacks in real-time along with reducing false positives. The Radware DefensePro Cloud DDoS solution also uses patent-protected real-time signature creation technology to provide automated zero-day DDoS attack protection. The solution 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 for a unified view into the attack lifecycle and mitigation analysis for both inline and out-of-path DDoS deployments. The controller provides network analytics along with comprehensive visibility into traffic statistics during peacetime and attack, simplified management and configuration, and unified visibility and control.

Market Perspective:

- Regarding geographical perspective, Radware has a significant presence in North America, followed by EMEA and JAPAC. From an industry vertical 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 hybrid with on-demand cloud service, which allows the organizations to deploy the on-premises 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-premises devices.