Knowledge Brief

QuadrantKnowledgeSolutions

Radware is Leader in SPARK Matrix: DDoS Mitigation, 2021

Quadrant
Knowledge Solutions

2021
SPARK MATRIX
LEADER

DDoS Mitigation Market

An Excerpt from Quadrant Knowledge Solutions
“SPARK Matrix: DDoS Mitigation, 2021”

Radware is Leader in SPARK Matrix: DDoS Mitigation, 2021

DDoS attacks involve flooding of bogus internet traffic on the target company's network, coming from a large number of computer workstations, often called bots. The primary goal of these attacks is to block access or reduce performance for the company's users. These workstations form a widely distributed attack network called 'botnet'. DDoS attacks are often carried out to interrupt business operations and disturb communications to harm the company's reputation and brand image.

Such attacks result in network downtime and can cause significant damage to organizations in terms of lost opportunities, information theft, and damage to their brand value. For industries that primarily rely on their online presence for businesses, such as eCommerce, online payment, online gaming, and others, DDoS attacks can result in huge losses. DDoS Mitigation is a technique to secure the company's network or server against DDoS attacks. DDoS mitigation requires an effective approach to distinguish human activity from fake bots and captured web programs. DDoS attacks are mainly classified into three attacks that includes volumetric attacks, protocol attacks, and application layer (layer7) attack.

DDoS protection is often achieved by deploying purpose-built DDoS protection appliances or cloud-based protection services. DDoS Mitigation appliances are the first line of defense and are popular amongst large enterprises and services providers for protection against sophisticated DDoS attacks. DDoS appliances are the on-premises solution and are useful for instant threat protection against threats. These appliances can provide over 40 Gbps of attacks, and by combining different appliances, it can handle multiples of hundreds of attacks volume capacity. DDoS mitigation service providers use multiple high-capacity scrubbing centers and can handle multiple TBPS of attack volume capacity. Most of the large organizations are looking at deploying hybrid solutions by investing in both on-premises appliances as well as cloud-based DDoS mitigation services.

This research service includes a detailed analysis of the global DDoS Mitigation solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides a comprehensive competition analysis and ranking of the leading DDoS Mitigation vendors in the form of the SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

SPARK Matrix includes ranking and positioning of DDoS Mitigation vendors with a global impact. The SPARK Matrix includes analysis of vendors, including Akamai, Cloudflare, Fortinet, Fastly, F5, Huawei, Imperva, Lumen, Link11, Neustar, NSFOCUS, NETSCOUT, Nexusguard, Radware, and Verizon.

Market Dynamics and Trends

The following are the key research findings of Quadrant Knowledge Solutions DDoS Mitigation research:

- Large-scale volumetric attacks that overwhelm the targeted network are getting bigger and increasingly complex. These large-scale mega-attacks capable of exhausting the bandwidth capacity of even large enterprise companies will continue to evolve. Multi-vector attacks are showing a continuous rise as they are complex in nature and have very high chances of success. Also, ransom attacks are becoming more targeted and sophisticated to cause considerable damage to target organizations. The threat landscape is expected to expand further with the transition to 5G networks and IoT.

- The market drivers for the growth of the DDoS Mitigation market include continued investments in digital transformation projects leading to increased adoption of cloud and hybrid infrastructures, increased use of mobile, personal devices and IoT devices, remote working and growing complexities of global regulatory environment.

- Driven by the growing market opportunity, DDoS mitigation vendors are looking at offering robust DDoS mitigation platforms to secure organizations’ networks, servers, websites, and applications from all types of DDoS attacks. These solutions offer features such as greater attack coverage, holistic mitigation capabilities, high mitigation capacity, and threat intelligence.

- DDoS attacks are always evolving and getting more complicated as attackers grow more tech-savvy. Multi-vector attacks and DDoS botnet attacks are amongst the most popular types of evolving attacks. 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 is capable of detecting and mitigating the most complex DDoS attacks. Vendors are using machine learning and AI to automate the process and assist in the deployment of appropriate solutions and mitigation filters rapidly to scale up the mitigation process.

- 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 frauds. Several DDoS mitigation vendors are offering Bot Management tools to prevent ad frauds along with preventing content scraping, content spam, inventory hoarding, credit card stuffing, and such others.

- Due to the ongoing pandemic, most organizations and enterprises have accelerated their digital transformation journey and migrated to the cloud. Enterprises' digital migration, as well as increased usage of mobile and IoT devices, and remote working, has extended the attack surface and created new vulnerabilities. DDoS ransom attacks and multi-vector attacks have become even bigger and more complex during this time, targeting multiple organizations across multiple locations. A majority of the DDoS mitigation vendors have claimed that there has been a substantial surge in DDoS attacks employing more and more attack vectors compared to the pre-covid era. Vendors providing DDoS mitigation services are continuously making efforts to combat these complex attacks through advanced solutions while constantly improving their capabilities based on the attack types. Vendors are adopting new strategies like automated attack detection and orchestrated mitigation using multiple methods, behavioral-based detection, real-time signature creation, encrypted attack protection, and others.

Figure: DDoS Attacks, Market Developments and Mitigation Strategies

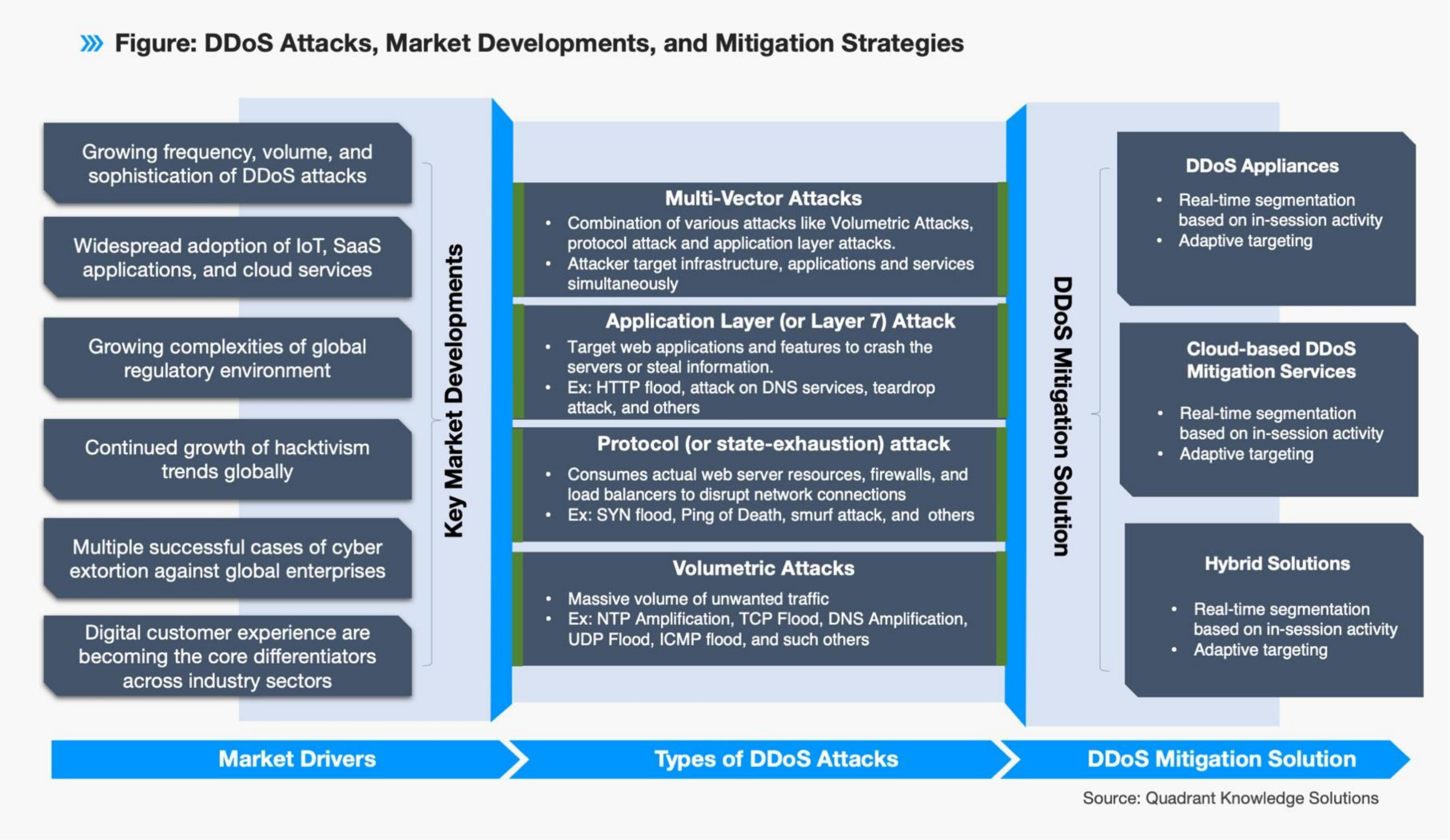


Figure: DDoS Attacks, Market Developments, and Mitigation Strategies

Market Drivers

Key Market Developments

- Growing frequency, volume, and sophistication of DDoS attacks
- Widespread adoption of IoT, SaaS applications, and cloud services
- Growing complexities of global regulatory environment
- Continued growth of hacktivism trends globally
- Multiple successful cases of cyber extortion against global enterprises
- Digital customer experience are becoming the core differentiators across industry sectors

Types of DDoS Attacks

Multi-Vector Attacks

- Combination of various attacks like Volumetric Attacks, protocol attack and application layer attacks.
- Attacker target infrastructure, applications and services simultaneously

Application Layer (or Layer 7) Attack

- Target web applications and features to crash the servers or steal information.
- Ex: HTTP flood, attack on DNS services, teardrop attack, and others

Protocol (or state-exhaustion) attack

- Consumes actual web server resources, firewalls, and load balancers to disrupt network connections
- Ex: SYN flood, Ping of Death, smurf attack, and others

Volumetric Attacks

- Massive volume of unwanted traffic
- Ex: NTP Amplification, TCP Flood, DNS Amplification, UDP Flood, ICMP flood, and such others

DDoS Mitigation Solution

DDoS Mitigation Solution

DDoS Appliances

- Real-time segmentation based on in-session activity
- Adaptive targeting

Cloud-based DDoS Mitigation Services

- Real-time segmentation based on in-session activity
- Adaptive targeting

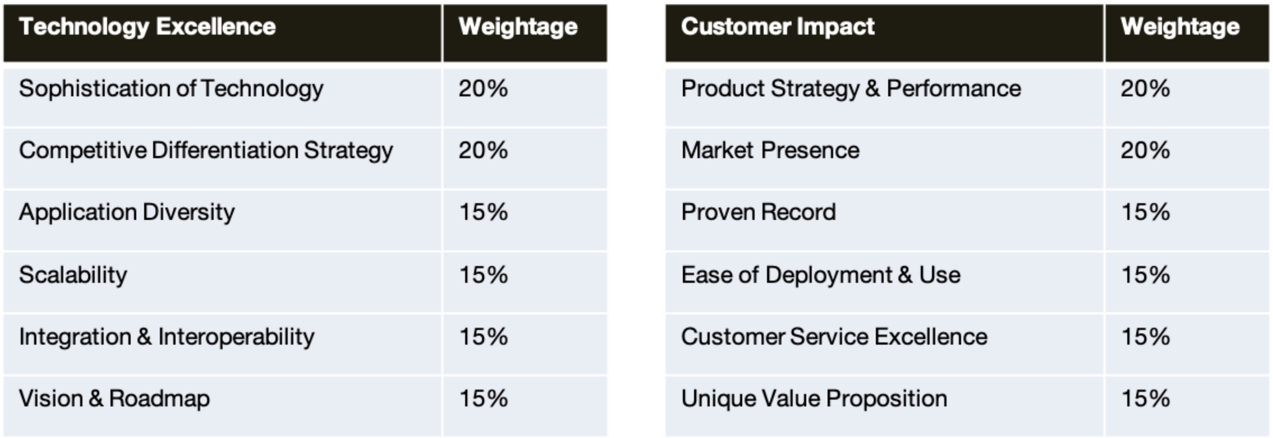
Hybrid Solutions

- Real-time segmentation based on in-session activity
- Adaptive targeting

Source: Quadrant Knowledge Solutions

SPARK Matrix Analysis of the DDoS Mitigation Market

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^{TM}. 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 the primary research including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall DDoS Mitigation market.



Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%

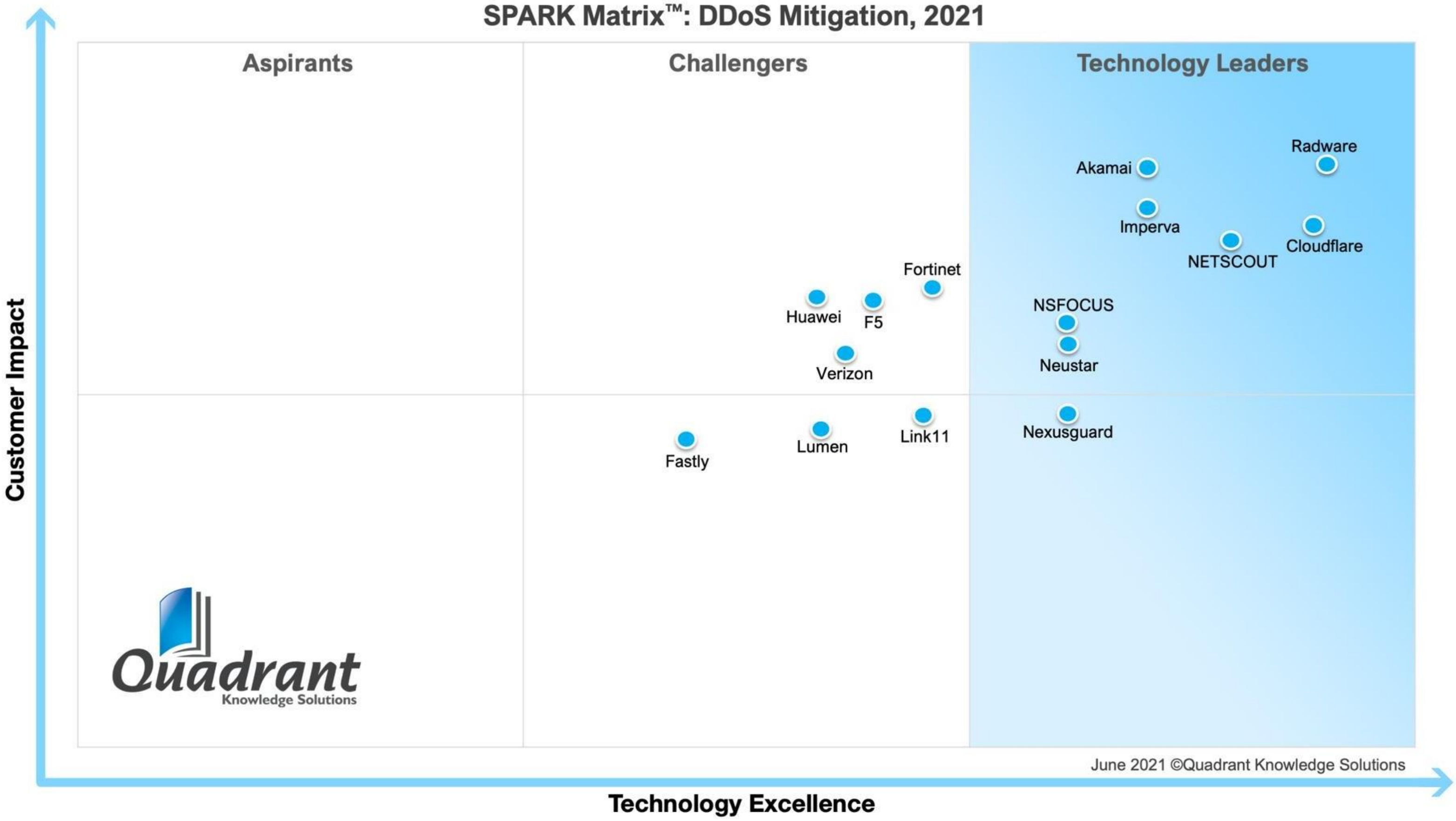
Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

According to the SPARK Matrix analysis of the global DDoS Mitigation market, “Radware with a robust functional capability of its product- ‘Radware DefensePro Solution and Cloud DDoS Protection (Mitigation) Service.’, has secured strong ratings across the performance parameters of technology excellence and customer impact, and has been positioned amongst the technology leaders in the 2021 SPARK Matrix of the DDoS Mitigation market.”

Figure: 2021 SPARK Matrix

(Strategic Performance Assessment and Ranking)

DDoS Mitigation Market



Radware Capabilities in the Global DDoS Mitigation Market

Founded in 1997 and headquartered in Tel Aviv, Israel, Radware is a global provider of cybersecurity and application delivery solutions for virtual, cloud, and software-defined data centers. The company provides automated DDoS security and protection from threats such as IoT-based attacks like Mirai, Pulse, Burst, DNS, TLS/SSL attacks, and connected with Permanent Denial of Service (PDoS) and Ransom Denial-of-Service (RDoS) techniques through its Radware DefensePro and Cloud DDoS Protection Service.

Radware DefensePro leverages behavioral-based detection algorithms to effectively identify attacks in a short time with minimal false positives. Radware DefensePro utilizes patent-protected real-time signature creation technology to automatically and immediately block and protect from zero-day and unknown arracks. Radware is able to identify, classify, and produce an accurate signature to block unknown attacks without false positives in just 18 seconds. In addition, Radware DefensePro includes dedicated hardware network to prevent high-volume DoS and DDoS flood attacks without impacting legitimate traffic.

Radware offers multiple deployment options for DDoS mitigation and application protection including cloud-based, on-premises and hybrid solutions.

Radware offers a patent-protected SSL DDoS attack mitigation solution, DefenseSSL, that helps secure all encrypted attacks with a low-latency solution. Radware leverages unique behavioral-based algorithms to provide for a full suite of accurate protections against HTTPS flood attacks, including a keyless SSL protection option that doesn’t require any decryption. Additionally, Radware DefensePro supports asymmetric deployment environments, including scrubbing centers, service providers, and multi-homed deployment, which are important in cloud-based deployments. Radware DefensePro provides up to 400Gbps of mitigation capacity and 330M PPS to secure large- scale organizations from cyber-attacks. Additionally, support an increasing number of customers with high complexity and capacity.

Radware also offers unique protections for carriers & service provides through its innovative quantiles-based DDoS protection algorithms that are designed to protect large scale and mobile edge networks from phantom floods and anomalies that sneak below the radar.

Radware Emergency Response Team (ERT) provides on-premises system management consisting of security experts to set up, maintain, and configure devices to maintain compliance with business processes and policies. Radware provides maximum mitigation efficiency in a short time deploying DefensePro DDoS protection and DDoS prevention devices in a scrubbing center.

Radware Cloud DDoS Protection Service automatically protects systems from DDoS attacks on the network and application layers, volumetric and non-volumetric attacks, and SSL-based DDoS attacks in real-time. Leveraging Radware DefensePro technology, Radware Cloud DDoS Protection Service utilizes DDoS prevention and real-time signature creation technologies, behavioral-based detection, smart SSL attack mitigation, and a robust global cloud security network to provide real-time protection against complex DDoS and web security attacks. Radware Cloud DDoS Protection Service allows a wide range of network sizes from a single IP address to a/24 block and beyond and provides an industry-leading SLA commitment to its customers. Additionally, Radware Cloud DDoS Protection Service provides flexible diversion techniques that can be tailored to operate seamlessly with the organization's network infrastructure. Radware Cloud DDoS Protection Service is a core part of Radware’s Cloud Security Services that also include WAF, Bot and API protection, and is available in multiple deployment options, including always-on, on-demand, or fully managed hybrid DDoS protection services.

Analyst Perspective

Following is the analysis of the Radware capabilities in the DDoS Mitigation market:

- Radware offers on-premises and cloud-based DDoS mitigation solutions that help organizations secure themselves from known and zero-day DoS/DDoS attacks by identifying and mitigating attacks in real-time. Radware includes DDoS protection, behavioral analysis, and IPS/SSL protection in a single platform. Additionally, Radware provides DDoS protection for any infrastructure, including on-premises data centers, private or public clouds, integrated WAF, bot and API protection for all environments, multi-faceted protection for public cloud environment, and advanced multi-cloud ADC.

- Radware offers DefensePro VA to secure public clouds. It helps secure networks utilizing Amazon Web Services and Microsoft Azure from sophisticated Layer 3 and 7-Layer floods attacks, encrypted attacks, in-session, and east-west attacks. Additionally, it provides automated zero-day attack defense with behavioral-based detection and mitigation, keyless SSL/TLS flood mitigation, advanced attack protection, and accurate network flood mitigation.

- Radware's hybrid attack mitigation solution integrates real-time WAF, SSL protection, and DDoS protection on-premises with an on-demand cloud service.
- Some of the key features of Radware's DDoS Mitigation solution include accurate attack detection with rate-based and rate-invariant traffic parameters, widest attack coverage, including advanced burst attack protection, zero-day attack protection, industry-leading SLA with individual performance KPIs, and patent-protected SSL attack mitigation solution that includes keyless HTTPS flood protection.

- Geographically, Radware has a strong presence in the US and Europe, followed by the Asia Pacific. From the industry vertical perspective, the company has a presence across a wide variety of industry verticals, including banking & financial services, IT & telecom, retail & e-commerce, healthcare & life sciences, education, travel & hospitality, gaming, and media & entertainment. From a use case perspective, Radware supports DDoS attack prevention and mitigation across all environments (physical data centers, private and public cloud) and all form factors (appliance & cloud services) and includes out of path deployment mode, machine-learning and automation capabilities, and fully managed hybrid deployment model and coverage. Radware also offers robust application security solutions (WAF, Bot and API protection), cloud native protection and Radware Alteon for application delivery and Layer 4–7 load balancing.

- The primary challenges of Radware include the growing competition from emerging vendors with innovative technology offerings, in addition to continued competition from established vendors. The emerging DDoS vendors have successfully gained significant market traction and are strengthening their market penetration, especially amongst small to mid-market organizations. These vendors are amongst the primary targets for ongoing mergers and acquisitions trends. The company needs to intensify its focus on creating custom dashboards and increasing interactions with SOC staff. It also needs to offer more pricing options for small and mid-size vendors. However, with its sophisticated technology platform, multiple security operations centers (SOCs) and scrubbing centers in three geographies, comprehensive functional capabilities, and strong customer value proposition, Radware is well-positioned to expand its market share in the global DDoS Mitigation market.

- As part of its technology roadmap, Radware is investing in improving protections against IoT botnets, DNS, and burst attacks. As attacks move to the application layer, Radware is constantly investing in and enhancing its Layer 7 protection and SSL DDoS attack protection. Additionally, Radware is focusing on new environments, including hybrid cloud, public cloud, and 5G solutions. The company plans to add automatic service discovery and usability features to automate network rollout.

and application security services for DevOps and SecOps application developers. The company also plans to add new features to mitigate new threats such as east-west attacks (machine to machine), API surface, advanced Bots, sophisticated application attacks, and emerging protocols such as Google QUIC.