Knowledge Brief

Quadrant Knowledge Solutions

Radware is a Leader in SPARK Matrix: Bot Management, 2021

Quadrant
Knowledge Solutions

2021
SPARK MATRIX
LEADER

Bot Management

An Excerpt from Quadrant Knowledge Solutions
“SPARK Matrix: Bot Management, 2021”

Radware is a Leader in SPARK Matrix: Bot Management, 2021

Due to significant rise in the sophistication of automated attacks using bad bots, organizations are increasingly relying on bot management tools to stop automated attacks on websites, mobile applications and APIs. A bot management solution leverages bot intelligence and machine learning algorithms to prevent cyber-attacks carried out using bad bots, such as credential stuffing, account takeover, theft of corporate and personal information, application fraud, ad fraud, API abuse, and card fraud, among others.

A bot management solution protects against automated attacks by malicious actors to ensure a seamless experience for the authentic user when browsing websites and mobile applications. The solution performs real-time analysis of the intent behind all incoming traffic to protect the organization's website, mobile apps, and APIs from bad bots. Bot management tools are often expected to offer functional capabilities to detect and prevent automated attacks, but the breadth and depth of the functionalities may differ between various vendors and their offerings due to the nature of ever-evolving sophistication of bad bots and their ability to closely mimic human behavior.

An increase in competition and the emergence of a variety of vendors with different technological strengths has led bot management solution vendors to improve their product and market strategy and enhance their overall technology value proposition to gain a competitive edge in the bot management solution market. The primary differentiators to evaluate bot management tools include the sophistication of attack detection and mitigation techniques to ascertain and block advanced bad bots mimicking human behavior, real-time reporting and analytics, robust threat research and intelligence to capture emerging bot trends, detection accuracy and scalability, integration and interoperability, and technology vision and roadmap.

Quadrant Knowledge Solutions research, SPARK Matrix™: Bot Management, 2021, 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 a detailed analysis of the global bot management solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. 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.

This research includes detailed competition analysis and vendor evaluation with the proprietary SPARK Matrix™ analysis. SPARK Matrix™ includes ranking and positioning of leading bot management vendors with a global impact including Akamai Technologies, Alibaba Cloud, AppsFlyer, Cloudflare, DataDome, F5, HUMAN, Imperva, Netacea, PerimeterX, Radware, and Reblaze.

Market Dynamics and Trends

The following are the key research findings of Quadrant Knowledge Solutions bot management research:

- Bot management solutions are evolving and becoming more robust, especially when the vendors are expanding into multiple domains by introducing new capabilities to detect and prevent automated attacks across different channels such as web applications, mobile applications, and APIs.

- With the massive proliferation of unsecured BYOD, WYOD, and IoT devices across the enterprise resulting in an increase in threat and data loss, there is an increasing focus on detecting, classifying, and managing malicious bot activities across connected devices.

- Most of the bot management vendors are investing in improving attack detection, response, and reporting capabilities to detect and block bot attacks, provide research on new attack methodologies and display granular attack data out-of-the-box, smarter mitigation techniques and API security.

- Driven by the growing market opportunity, vendors are focusing on offering robust bot management platforms to secure websites Mobile apps and APIs from OWASP-listed automated attacks. With continuously evolving bot attacks, vendors are leveraging AI, ML, and other technologies to identify suspicious behavior and stop attacks in real-time, automate API discovery, reporting, detect threats, detect low and slow attacks, and provide an accurate and self-tuning assessment of bot traffic.

- COVID-19 induced disruptions in business scenarios, accelerated the growth in remote working, and increased the need to access internal resources from the outside. However, this has also led to an increase in the reach and opportunities for cybercriminals to use these disruptive factors to increase their attacks. Such high risks are driving significant investments in bot management solutions to keep attackers at bay. Hence, organizations across industries are increasingly focusing on fortifying their digital portals against fraud and abuse.

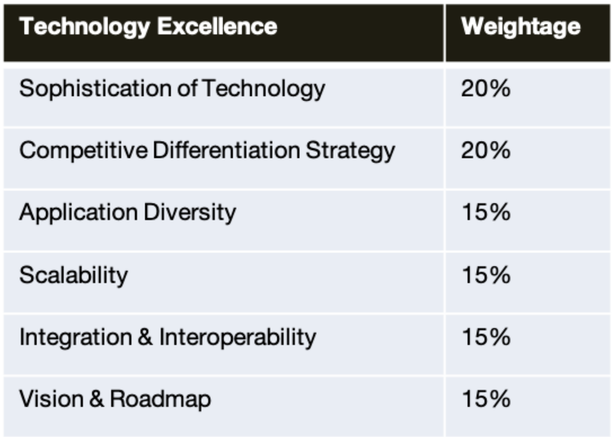
- The emergence of data privacy regulations such as GDPR, CCPA, and others are forcing businesses to adopt advanced security and compliance solutions to improve their defense strategies and comply with stringent regulatory requirements.

- Organizations are looking for vendors offering continuous, real-time security to prevent bad actors from launching automated attacks, that can harm their customers, revenue and brand. Additionally, the vendors are providing robust features, supporting diverse use cases, and have a presence in different verticals, including banking & financial services, retail, IT & Telecom, gaming, public sector, marketing and others.

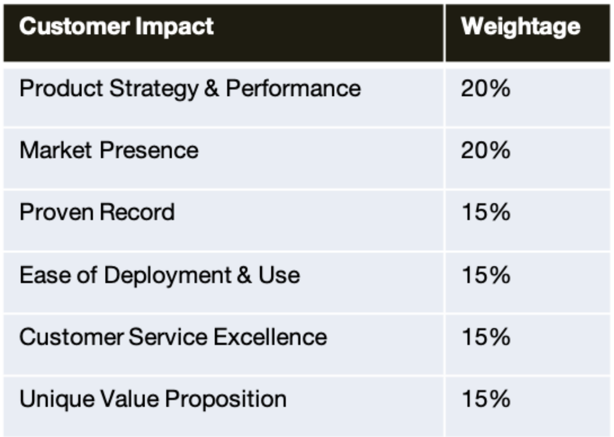
SPARK Matrix Analysis of the Bot Management Market

Quadrant Knowledge Solutions conducted an in-depth analysis of the major bot management vendors by evaluating their product portfolio, market presence, and customer value proposition. The Bot Management market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. It also provides strategic insights on how each vendor's rank is related to their competitors based on their respective technological 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 bot management market.

According to the SPARK Matrix™ analysis of the global bot management market, "Radware with a functional capability of its product 'Bot Manager', 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 bot management market."

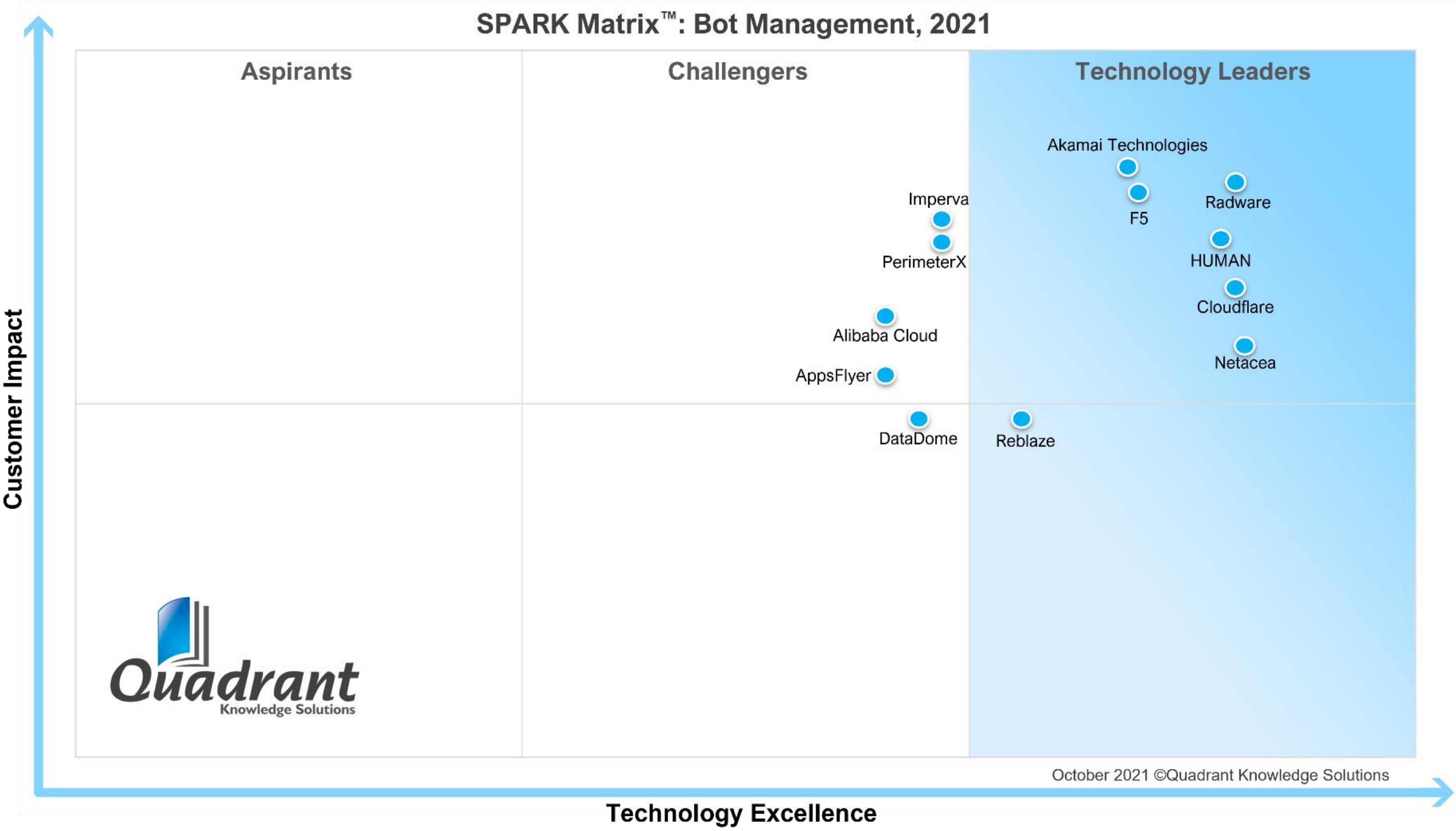


Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%



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%

Figure: 2021 SPARK Matrix
(Strategic Performance Assessment and Ranking)
Bot Management Market



Radware Capabilities in the Global Bot Management Market

Founded in 1997 and headquartered in Tel Aviv, Radware is a leading provider of cyber security and application delivery solutions for virtual, cloud, and software-defined data centers. Radware offers the industry's most advanced application protection suite with a web application firewall, application protection and DDoS mitigation. Through its Bot Manager solution, Radware provides real-time protection against OWASP-listed automated attacks across different channels such as web, mobile and APIs. The solution helps organizations detect, classify, and manage malicious bot activities through its comprehensive capabilities, including intent analysis, ML and AI, a variety of mitigation options, granular analytics and reporting, collective bot intelligence, browser and device fingerprinting.

Radware Bot Manager solution is equipped with proprietary IDBA, semi-supervised machine learning models, along with collecting over 250 parameters to identify malicious bots in real-time traffic with the highest accuracy. While some competitors collect only client-side or server-side data, Radware Bot Manager engine collects both to get a unified customer profile and provide the best customer experience. To determine illegitimate traffic from good bots and humans, both server-data (API data) and client-level data (telemetry data) is required. Collecting and working with both types of data gives accuracy in detection and response. The solution provides several mitigation options that allow users to act according to the bot types and signatures as per organizational needs. The platform also enables publishers to show content only to humans and block non-human invalid traffic. Radware Bot Manager's granular reporting and analytics classifies different types of bots and helps efficiently manage non-human traffic, clearly understand web traffic, and provide visibility of bot intent to the user. The Bot Manager can seamlessly integrate with leading marketing analytics platforms to give look-to-click ratio and clean data. Radware's collective bot intelligence uses bot data from its global customers base to identify and flag bad bots and share new information with the other websites on new bot attack patterns.   In addition, the solution leverages cutting-edge technologies such as Kubernetes container orchestration and Kafka to maintain high scalability during peak network traffic.

Radware Bot Manager is integrated with Radware's application protection solution to offer integrated WAF, Bot, API and DDoS protection to protect organizations from a variety of threats such as web application attacks, DDoS, bot attacks, and advanced malware. Radware provides several types of integration with SDKs, JavaScript tags, web server plugins, edge computing platforms, third-party plugins load balancer, virtual appliances, and DNS redirection. Additionally, Radware provides a virtual appliance for entire web applications or selected sections, allowing users to optimally deploy Bot Manager in their existing infrastructure.

Radware Bot Manager provides a superior architecture to enable scalability in handling massive amounts of traffic while providing negligible latency in responding to requests, its proprietary IDBA bot detection technology analyzes the intent of sophisticated bots that can mimic human-like behavior to evade detection, and provides powerful bot mitigation capabilities with minimal false positives and real-time visibility over all types of site traffic, including legitimate bots, search engine crawlers, bad bots, and human traffic. Radware Bot Manager offers various mitigation options, including CAPTCHA, feed fake data, progressively challenging JavaScript, throttle, drop request, session termination, redirect loop, tarpit, log only, and custom response. Radware supports the overall network and application security with cloud-based, on-premises, and hybrid deployment options to secure applications running in Public Cloud, Private Cloud, and Hybrid Cloud environments.

Radware Bot Manager goes a step further than other competitors in their API protection from malicious parties trying to steal Personally Identifiable Information (PII), payment card details or disrupt business-critical services. Radware Bot Manager for APIs uses a multi-layered detection method for deep analysis of machine-to-machine communication, leveraging contextual and historical information in unison with its deterministic engine to assess the legitimacy of every API call, along with an immediate response engine, behavioral analysis and machine learning modules to detect and block bad API calls that can lead to potential attacks.

Analyst Perspective

The analysis of Radware's capabilities in the global Bot Management market.

- Radware Bot Manager offers robust security from automated threats to web applications, mobile devices, and APIs. The solution provides precise bot management across all platforms by integrating behavioral modeling for granular intent analysis, collective bot intelligence, and fingerprinting of browsers, apps, and machines. Additionally, the solution protects the user from a wide array of threats such as account takeover, gift card fraud, application DoS, price scraping, content scraping, digital ad fraud, skewed analytics, form spam, and others.

- Some of the key differentiators of Radware Bot Manager includes broad application security coverage with integrations with Radware Cloud WAF and Radware Alteon ADC, patented intent-based behavioral analysis, API protection, comprehensive reporting and analytics to provide detailed information about bots, fully managed end to end service, negligible false positives, extensive deployment options, and customizable IAM roles creation.

- From a geographical presence perspective, Radware has a strong presence in North America and Europe, followed by APAC. The company is expanding in markets like South America, India, the Middle East, and Australia with its strong partner ecosystem. From an industry vertical perspective, the company has a strong presence in retail & eCommerce, travel & hospitality, media & entertainment, IT & Telecom, banking & financial services, government & public sector, as well as manufacturing. From a use case perspective, Radware supports application and DDoS protection, public cloud protection and application delivery, with Radware Bot Manager providing specialized bot mitigation against ATO attacks, carding, scraping, ad fraud, fake account creation, denial of service attacks, and other types of bot attacks.

- Radware's primary challenges include the growing competition from emerging vendors with innovative technology offerings, continued competition from fairly established bot management solution vendors, in addition to competitive development such as partnerships, collaboration, and more. However, with its sophisticated technology platform, comprehensive functional capabilities, and strong customer value proposition, Radware is well-positioned to expand its share in the global Bot Management market.