Knowledge Brief

Quadrant Knowledge Solutions

Radware is a Leader in SPARK Matrix: Bot Management, 2023

An Excerpt from Quadrant Knowledge Solutions
"SPARK Matrix™: Bot Management, 2023"

Radware is a Leader in SPARK MatrixTM: Bot Management, 2023

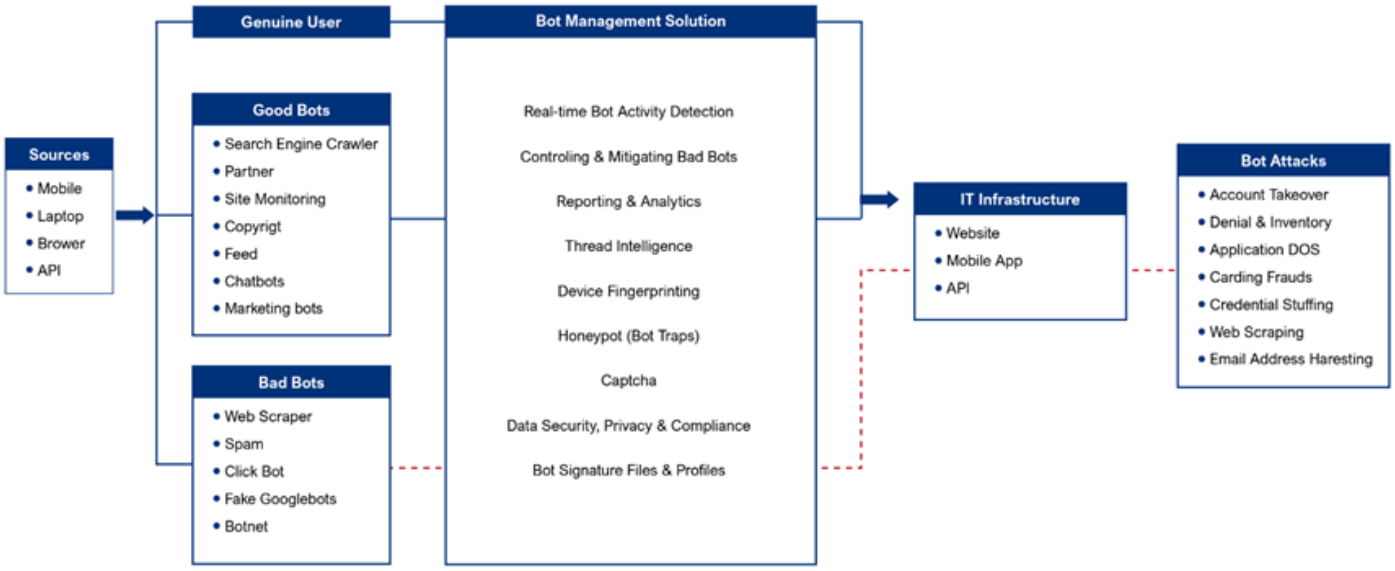
A bot Management solution is software that allows an organization's security teams to block malicious internet bot traffic and allows only good bots to access web properties. The solution works by differentiating between desirable and undesirable bot activity by leveraging bot detection techniques, such as user behavioral analysis, as well as device fingerprinting, and automatically preventing undesirable bots from accessing the user's critical IT assets,

Organizations are adopting cloud-based infrastructure to increase the customer base and provide a holistic customer experience inside the corporate network landscape. Due to the increased digital transformation, shift to cloud infrastructure, remote working culture, and increasingly sophisticated technologies like AI have led evolved automated attacks have evolved, and attackers are now using bad bots to breach security and access the organizational IT system. Organizations are facing the challenge of differentiating between bad bots, good bots, and genuine users and mitigating the bad bots, as cyber attackers are using advanced technology like machine learning (ML) to mimic human behavior to intrude into the organizational IT systems and access the discrete network zones.

Due to the increased traffic of bad bots, organizations are facing issues like account takeover (ATO), data breaches, credential spills, denial of service, fraud, and such other threats. To mitigate bad bot attacks and provide access to good bots and genuine users to websites, mobile applications, and APIs, to strengthen their security infrastructure, organizations have started using bot management solutions. The solution providers are also offering advanced functional capabilities like real-time bot activity detection and user identification by leveraging bot signatures to detect and mitigate automated attacks. However, the breadth and depth of the capabilities differ owing to the nature of the ever-evolving sophistication of bad bots and their ability to mimic human behavior.

Quadrant Knowledge Solutions' SPARK MatrixTM: Bot Management, 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. SPARK MatrixTM includes ranking and positioning of leading Bot Management Vendors with a global impact. The SPARK MatrixTM includes an analysis of vendors, including Akamai Technologies, AppsFlyer, Arkose Labs, Cloudflare, Cequence Security, DataDome, F5 Networks, HUMAN, hCaptcha, Imperva, Kasada, Netacea, Radware, and Reblaze.



Market Dynamics and Trends

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

- Bot Management solution providers are proactively protecting web applications from sophisticated bot threats like account creation, token cracking, and many others by leveraging Intent-based deep behavioral analysis, embedded machine-learning algorithms, and device and browser fingerprinting.

- A robust Bot Management solution safeguards organizational IT ecosystems from OWASP-listed cyber vulnerabilities such as Injection, broken authentication, sensitive data exposure, external entities (XXE), broken access control, security misconfigurations, cross-site scripting (XSS, Insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring) to prevent IT network vulnerability holistically.

- The demand for Bot Management solutions has increased owing to the need for mitigation of data poisoning attacks in organizational systems by blocking outdated browsers or user agents, blocking known bad hosts and proxies, shielding access points vulnerable to bots, evaluating traffic sources, and investigating spikes in usage in website or application.

- Bot Management solution providers are planning to assist organizations in ensuring adherence to ever-changing industry and regulatory compliance specifications such as PCI DSS, HIPAA, and many others. A dedicated Bot Management solution provides stringent data protection processes to organizations by continuously ensuring data compliance, maintaining their brand reputation, and preventing them from potential fines and penalties.

- Bot management solutions are evolving, becoming more robust, and gaining traction with forward-thinking solution providers, especially when bot management vendors are expanding into multiple sectors by introducing new capabilities to detect and prevent automated bot 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 like credential stuffing, web scraping, email address harvesting, etc.

- The other market drivers for the growth of the bot management market include continued investments in digital transformation projects leading to increased adoption of cloud and hybrid infrastructures, increased use of mobile and personal devices, remote working, investments in various bot management techniques like data mining and others, the launch of CAPTCHA products and growing complexities of the global regulatory environment.

- Most of the bot management vendors are investing in improving their products' attack detection, response, and reporting capabilities to detect and block simple and sophisticated bot attacks, provide research on new attack methodologies, and display attack data out of the box. Additionally, vendors are investing in dashboard explainer, signal-producing bot management, in-dashboard feedback loop, no captcha, and API security products.

- Organizations are looking for vendors offering continuous, real-time security to prevent bad bots from launching automated bot attacks, including credential stuffing, account takeover, application fraud, ad fraud, API abuse, card fraud, and such others. Additionally, the vendors provide robust features, support diverse use cases, and have a presence in different verticals, including banking & financial services, retail, IT & Telecom, and such others.

SPARK MatrixTM Analysis of the Bot Management Market, 2023

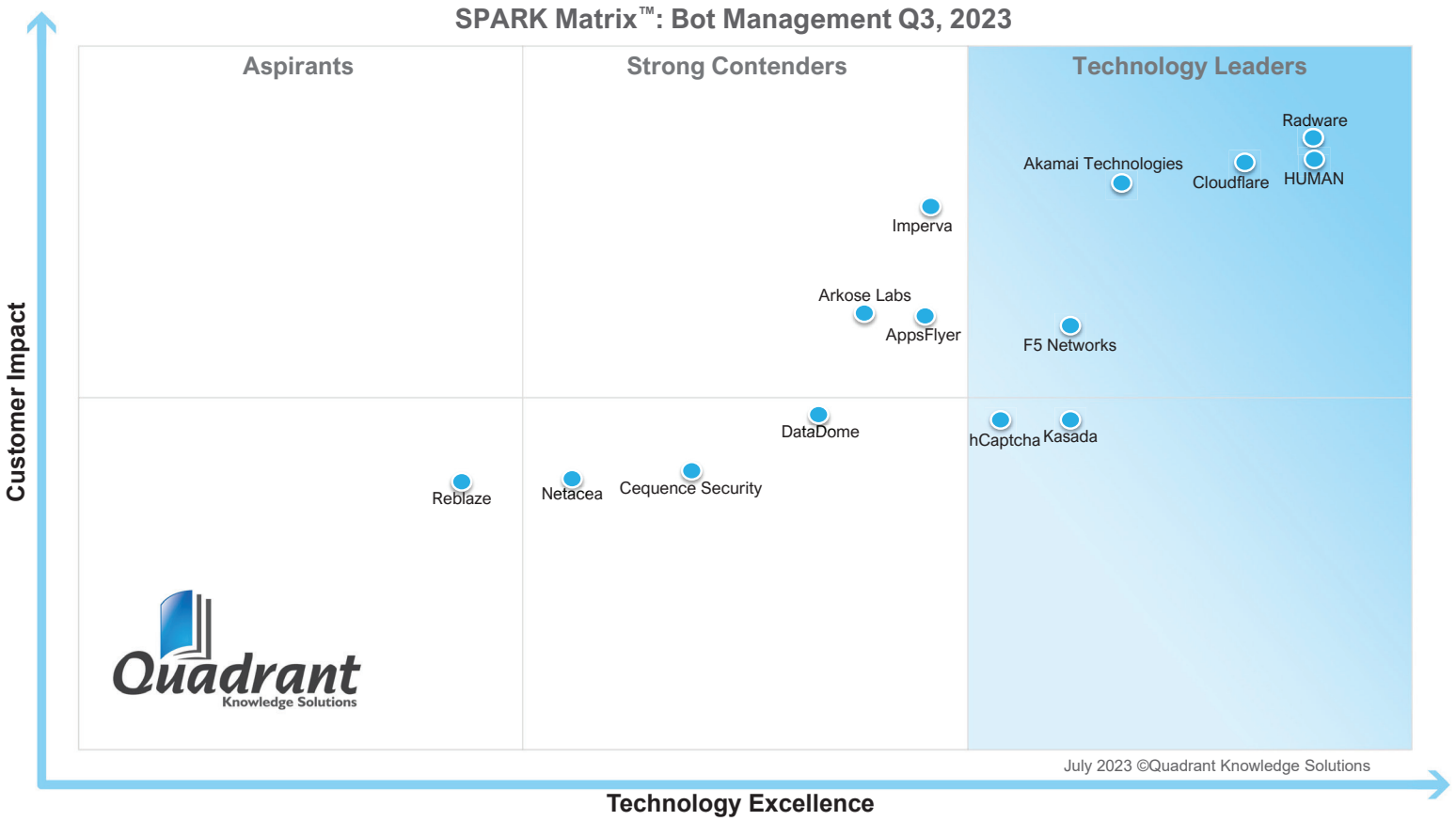
Quadrant Knowledge Solutions conducted an in-depth analysis of the major Bot Management vendors by evaluating their product portfolio, market presence, and customer value proposition. Bot Management Market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary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

Technology Excellence	Weightage
Sophistication of attack detection	20%
Attack Response & Mitigation	20%
Real-time Reporting and Analytics	20%
Threat Intelligence	10%
Competitive Differentiation Strategy	10%
Application Diversity	10%
Integration & Interoperability	5%
Vision & Roadmap	5%

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 MatrixTM analysis of the global Bot Management Market, "The Radware Bot Manager is equipped with proprietary Intent-based Deep Behavioral Analysis (IDBA), semi-supervised machine learning models, along with a robust client and server-side detection engine to identify malicious bots in real-time with highest accuracy. The solution provides different mitigation options, including blockchain-based crypto mitigation. Additionally, it allows users to take actions according to the bot types/signatures as per the organizational internal security needs" Radware, owing to the robust functional capability of its Bot Manager solution, 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 Bot Management Market."

Figure: 2023 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Bot Management Market



Radware

URL: https://www.radware.com

Company Introduction:

Founded in 1997 and headquartered in Tel Aviv, Radware is a prominent vendor of application delivery and cyber security solutions for virtual, cloud, and software defined data centers. The company offers a host of services, including load balancing, monitoring, management, network security, cloud protection, and such others. Radware offers the industry's most advanced application protection suite with a Web Application Firewall, Bot Manager, API protection, and DDoS mitigation.

Product Introduction:

Radware provides API-based 360-degree real-time protection against OWASP-listed automated attacks across different channels, such as web applications, mobile applications, and APIs, through its Bot Manager solution. Radware Bot Manager helps organizations detect, classify, and manage bot activities through its comprehensive capabilities, including intent-based deep behavioral analysis, a variety of mitigation options, granular analytics and reporting, collective bot intelligence, device and browser fingerprinting.

Technology Perspective:

Followings are the analysis of the Radware capabilities in the global Bot Management market:

- Radware Bot Manager offers robust security to web applications, mobile devices, and APIs from automated threats. 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, it helps to protect the customer 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. Radware Bot Manager provides multiple mitigation options, including blocking, CAPTCHA, feeding fake data, complex JavaScript,

throttling, drop request, session termination, redirect loop, tarpit, log only, custom response, and allow. Additionally, Radware Bot Manager provides a unique and differentiated Blockchain-based Cryptographic Challenge as a mitigation option to its customers.

- Some of the key differentiators of Radware Bot Manager includes broad application security coverage, patented intent-based behavioral analysis, API protection, Secure Identity, Integrated Device Authentication, seamless integration via a unified portal with Radware Cloud WAF, as well as integration with Radware Alteon ADC, comprehensive reporting, and analytics to provide detailed information about bots, fully managed end-to-end service, negligible false positives, configurable integration options from the Dashboard portal itself, extensive deployment options, a unique and differentiated blockchain based cryptographic challenge and customizable IAM roles creation.

- Radware Bot Management provides broad attack detection and coverage to secure sensitive information as well as offer edge-to-endpoint API security through its diverse ML modules, which include the graph-based algorithm, invocation context, API flow control, authentication flow analysis and the support for M2M SDKs, fully managed service, and helps to prevent API abuse. Radware Bot Manager's proprietary IDBA algorithm uses a semi-supervised algorithm which allows organizations to reduce false positives and identifies the intent of the sophisticated bots.

- Radware Bot Manager is equipped with proprietary Intent-based Deep Behavioural Analysis (IDBA), semi-supervised machine learning models along with a robust client-side and server-side detection engine to identify the intent of bots with the highest accuracy in real-time. The solution provides different mitigation options including the blockchain based Crypto mitigation, allowing users to take actions according to the bot types/signatures as per the organizational needs. The platform also enables the publisher to show content only to humans and block non-human invalid traffic. Radware Bot Manager's granular reporting and analytics allows classification of different types of bots, and helps to efficiently manage non-human traffic, clearly understand web traffic, and provide visibility of bot intent to the user.

The bot manager can be seamlessly integrated with leading marketing analytics platforms, to help eliminate skewed analytics

- Radware Bot Manager offers the industry's widest mitigation options, including a unique Crypto Challenge which allows legitimate users to navigate without CAPTCHAs. Additionally, . Radware Bot Manager protects native iOS and Android mobile applications against identity spoofing, tampering, replay attacks, and unauthorized access by mobile emulators, modified applications, and modified operating systems. With two new detection layers – Secure Identity and Integrated Device Authentication - added to identify emulators and modifiers faster, Radware provides a much tighter and faster bot protection against various targeted and distributed bot attacks

- Radware collective bot intelligence uses bot data from its global customer base to identify and flag bad bots, share new information with the other websites on new attack patterns and protect internet properties. In addition, the Bot Manager solution leverages cutting-edge technologies such as Kubernetes container orchestration and Kafka to maintain high scalability during peak network traffic hours.

- Radware Bot Manager is integrated with Radware's application protection offering to protect organizations from a variety of threats like web application attacks, DDoS, bot attacks, and advanced malware through a single integrated offering. Radware provides different types of integration with SDKs, JavaScript tags, web server plugins, edge computing platforms, third-party plugins, load balancer, virtual appliance, and through DNS redirection. Additionally, Radware Bot Manager provides virtual appliance-based deployment as well which allows customers to optimally deploy the Bot Manager solution in their existing infrastructure.

- Radware Bot Management provides a superior architecture to enable scalability in order to handle massive amounts of traffic on negligible latency while responding to requests, its proprietary IDBA detects the intention of sophisticated bots which exhibit human-like behavior to evade detection and provides customers with very 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 the industry's widest mitigation options, including CAPTCHA, feed fake data, browser-based challenges, throttle, drop request, session termination, redirect loop, tarpit, log only, and custom response. Radware supports 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.

Market Perspective:

- From the 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 a 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 sectors, and manufacturing.

- From a use case perspective, Radware Bot Manager 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 and other automated attacks. Radware Bot Manager offers specific additional ATO policy enablement to address the ATO scenarios. Radware Bot Manager also offers a very strong solution for API Protection targeted toward organizations relying on APIs for their services. The Radware Bot Manager API protection solution helps protect against bot attacks on APIs and deployed along with Radware's Cloud WAF solution, offers a complete API protection solution.

Challenges

- Radware may face challenges from growing competition from emerging vendors with innovative technology offerings and continued competition from fairly established Bot Management 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 market share in the global Bot Management market.

Roadmap:

- As part of its technology roadmap, Radware is focusing on continuously enhancing and building on its core bot detection engine, support for newer mitigation challenges, enhancing client-side (JS and SDK) detection and providing tighter protection against the new generations of human-like bots, protecting mobile applications from emulators and app modifiers, hence providing a tighter and faster bot protection against various targeted and distributed bot attacks. Radware also adds newer capabilities on the visibility and self-service aspects on the portal which include a new and unique attack-based analytics view, which will give customers clear visibility into when the attack: when it started, when it ended, what were its main aspects, including source, country, information on the attack pattern, etc. Additionally, the company is investing in creating a unique generic identity that can be used across the AppSec portfolio, as well as ML-based modules and use case-based analytics view on the dashboard.

- In terms of the strategic roadmap, Radware is focused on becoming an industry-leading provider of bot management and online fraud detection solution with its multi-layered protection solution for web, mobile, and API channels, along with multiple integration points with a robust management interface completed by strong managed services offering.