KNOWLEDGE BRIEF

Kaspersky is Positioned as 2020 SPARK Matrix Leader in the Endpoint Detection & Response (EDR) Market

KNOWLEDGE BRIEF

BY

Kaspersky is Positioned as 2020 SPARK Matrix Leader in the Endpoint Detection & Response (EDR) Market

Driven by the growing frequency, sophistication, and complexity of cybersecurity attacks, traditional security measures, and legacy antivirus technologies are no longer effective. With the advancements in IT and security technologies, cybercriminals are increasingly utilizing advanced techniques to launch sophisticated, complex, and targeted attacks. For cybercriminals, the integrated power of IoT botnets, automation, and AI and machine learning tools will enable them to cause the next wave of prominent and dangerous cybersecurity attacks, gain unauthorized access to enterprise network, and resources, and steal information. The advanced AI-based hacking tool will help them find and exploit the new vulnerabilities for their target organizations.

Since traditional security models, legacy antivirus, and anti-malware tools are not effective in handling these complex and sophisticated modern attacks, organizations are increasingly looking at adopting advanced threat detection capabilities. Endpoint detection and response (EDR) solutions with an ability to detect sophisticated threats, restrain them at the endpoint level, and help SOC analysts with threat remediation is increasingly becoming popular amongst both SMB and enterprise organizations. EDR vendors are focusing on advancing their threat detection and prevention capabilities leveraging advanced analytics, AI and machine learning to detect and respond to the most sophisticated and targeted threats. Modern EDR tools also offer automated threat response, visualization, threat hunting, and investigation capabilities to improve the speed of threat response and incident investigation efficiency.

Quadrant Knowledge Solutions, recent study "Market Outlook: Endpoint Detection and Response (EDR), 2020-2025, Worldwide" analyzes market dynamics, growth opportunities, emerging technology trends, and the vendor ecosystem of the global market. 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.

The research includes detailed competition analysis and vendor evaluation with proprietary SPARK Matrix analysis. The SPARK Matrix includes ranking and positioning of leading EDR vendors with a global impact. This study provides an analysis of key vendors, including CrowdStrike, Cybereason, Cylance, Cynet, Digital Guardian, Elastic (Endgame), ESET, FireEye,

Kaspersky, McAfee, SentinelOne, Broadcom (Symantec) and VMware Carbon Black.

Market Dynamics and Trends

Endpoint detection and response market is expected to grow significantly during 2020-2025

Endpoint detection and response (EDR) is an emerging security technology that records and stores endpoint behavior and events and uses this information for early detection of breaches, analysis, investigation, and rapid mitigation of potential insider and outsider threats. EDR solutions are typically installed on IT equipment, including domain controllers, database servers, and workstations. EDR solutions use behavior analytics and machine learning techniques to provide in-depth anomaly detection and visibility into a variety of threats. EDR solutions enhance enterprise visibility across endpoints by providing aggregated threat information and help in early detection, investigation and mitigation of all kinds of threats.

Figure: Primary Market Drivers, 2020-2025

Primary Market Drivers
Growing frequency, sophistication, and complexity of cybersecurity attacks are significantly expanding the organization's risk exposure
The growing concern of insider threats and lateral movement of APTs to exploit important resources
Traditional antivirus and anti-malware technologies are not effective to protect against advanced threats
Global regulations and compliance requirements are increasingly becoming complex
The growing sophistication of EDR tools to provide comprehensive discovery and visibility and prevent all attack types and mega-breaches
Improving the efficiency of threat response processes with an increasing need for threat hunting and root cause analysis
Vendor's strategy of offering an integrated platform to cover endpoint protection, detection, response, and investigation capability

The endpoint detection and response market is expected to grow significantly in the next five to six years from the market size of $1.06 billion in 2019 to over $5.20 billion by 2025. The global EDR market is expected to grow at a compound annual growth rate (CAGR) of 30.4% during the forecast period of 2020 to 2025. The primary market drivers include the EDR value proposition of significantly reducing an organization's risk exposure, improving MTTD (Mean time to detect) and MTTR (Mean time to respond), enhancing SOC productivity, ensuring endpoint compliance, and others.

The majority of the popular EDR solutions include the core functionalities of rapid threat detection, guidance for threat response, and threat hunting and investigation. However, the breadth and depth of features may vary between vendors offerings. Some of the key competitive and technology differentiators include sophistication of threat detection against advanced, APT, and targeted attacks; an integrated platform with threat prevention, detection, threat hunting, response, investigation, security analytics capabilities; integration & interoperability; visibility, analytics and reporting; supporting security automation & orchestration; comprehensive threat intelligence feeds; managed detection & response (MDR) services, and others.

Security automation is increasingly becoming important for transforming security operations processes for rapid detection and response. SecOps teams often struggle to keep up with the growing threat landscape and the massive volume of security alerts, resulting in an ever-increasing number of unattended alerts. The lack of security talent and the necessary skills needed for security operations are further adding to the challenges. Therefore, EDR vendors are increasingly improving security automation functionalities or integrating with best-of-breed vendors to effectively automate their threat response processes.

SPARK Matrix™ Analysis of the Endpoint Detection and Response Market

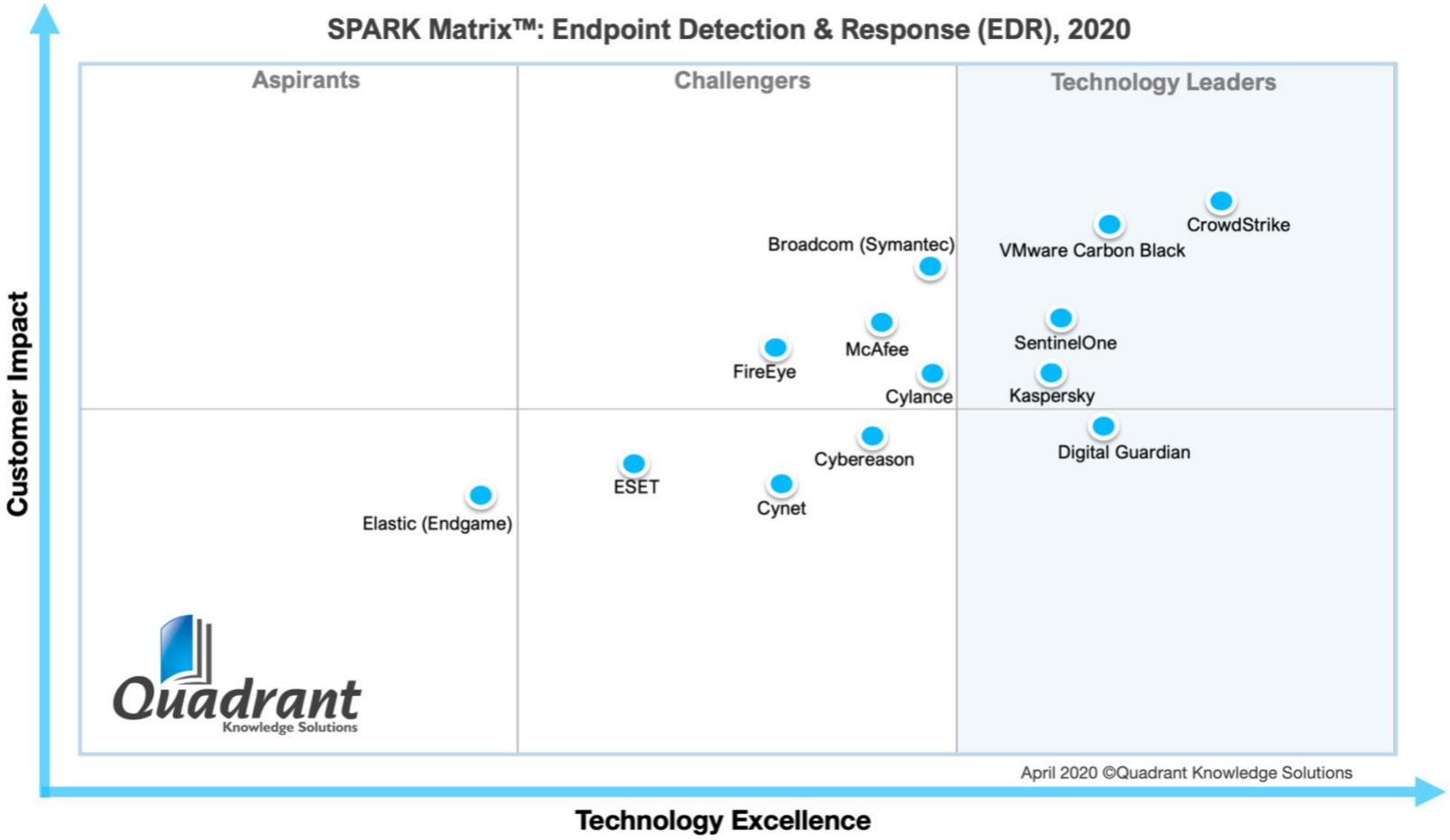
Quadrant Knowledge Solutions conducted an in-depth analysis of the major EDR vendors by evaluating their product portfolio, market presence, and customer value proposition. The endpoint detection and response research provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™.

SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants. It offers strategic insights into how each vendor ranks related to their competitors, taking into account various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for making strategic decisions, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and more. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall endpoint detection and response 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: 2020 SPARK Matrix
(Strategic Performance Assessment and Ranking)
Endpoint Detection and Response (EDR) Market



Kaspersky's Capabilities in the Global Endpoint Detection and Response (EDR) Market

Founded in 1997 and headquartered in Moscow, Kaspersky is a leading vendor of endpoint cybersecurity solutions. In addition to their endpoint security solution, Kaspersky offers a range of cybersecurity products (cloud or on-premise) and services designed to meet the end-to-end needs of customers ranging from SMBs to government bodies, global enterprises and industry-specific organizations. Kaspersky Endpoint Detection and Response (EDR) provides endpoint security through automated threat detection, investigation, hunting and response capabilities.

Kaspersky EDR helps enterprises build defenses against advanced cyberthreats by improving the visibility of all endpoints on the network, boosting detection and investigation capabilities, as well as enabling the automation of routine tasks to discover, prioritize, investigate and neutralize complex attacks. Boosted detection and investigation capabilities through targeted attack analyzer (TAA), Sandbox, MITRE ATT&CK enrichment and a flexible query builder, plus access to the Kaspersky Threat Intelligence Portal knowledge base - facilitate effective threat hunting and fast incident response.

Kaspersky EDR's advanced detection, adaptive threat response and proactive threat hunting capabilities help organizations detect and respond to complex, advanced threats, and targeted attacks. The targeted attack analyzer (TAA) can discover suspicious actions based on enhanced anomaly heuristics, provisioning real-time automated threat hunting capabilities. It supports the automatic analysis of all events and their mapping Indicators of Attack (IoAs) generated by Kaspersky's threat hunters. Kaspersky's web-based interface is an easy-to-use tool for monitoring events, visualizing threat hunting, examining analysis and tracking threat reaction for an effective threat investigation and response.

Kaspersky EDR improves endpoint visibility and threat detection by using advanced technologies like machine learning, sandbox, indicators of compromise (IoC) scan, IoAs analysis and threat intelligence. Kaspersky EDR's advanced sandbox analyses the behavior of an object as it executes for effective threat detection. The Sandbox solution uses several patented detection methods and supports numerous emulation modes to accurately detect the most complex modern threats. Kaspersky EDR enables proactive fast search in real-time and applies retrospective analysis, using a centralized database and IoC scan. This helps organizations proactively scan endpoints to

spot anomalies and breaches. Kaspersky EDR enables ongoing monitoring and visualization of every investigative stage with fast access to centrally stored data, even when the data has been encrypted on the hosts or destroyed by attackers. Kaspersky EDR is integrated with its endpoint protection platform (EPP) – Kaspersky Endpoint Security for Business and offers comprehensive endpoint protection powered by feature-rich EDR capabilities. Kaspersky EDR can also be built into the Kaspersky Anti Targeted Attack (KATA) Platform, combining EDR capabilities and network-level advanced threat discovery to form an Extended Detection and Response solution. IT security specialists have all the tools they need to handle multi-dimensional threat discovery at both endpoint and network levels, applying leading-edge technology, undertaking effective investigations, and delivering a rapid, centralized response — all through a single solution.

Analyst Perspectives and Differentiators

Here Follows analysis of Kaspersky's capabilities in the EDR market:

- Kaspersky's EDR solution, with capabilities for advanced threat detection enriched with threat intelligence, MITRE ATT&CK mapping, threat hunting, and adaptive threat response offers comprehensive EDR functionalities for detecting advanced, targeted threats and their automated response.

- Kaspersky EDR, combined with Kaspersky Anti Targeted Attack (KATA) Platform, offers an effective APT protection platform with extended detection and response capabilities based on its unified server architecture and centralized management. The EDR solution also utilizes Kaspersky Private Security Network (KPSN) – a private cloud-based solution, which is available for organizations with strict privacy policies who are unable to send their data to the global Kaspersky Security Network but still want to benefit from Kaspersky's global reputation database. Organizations with KPSN deployed can also benefit from reputations provided by external intelligence from third-party systems via an API.

- Kaspersky continues to invest in maximizing the automation in detection and response processes to provide superior endpoint defense against complex threats. The company also offer a managed detection & response (MDR) solution, providing benefits to organizations at different stages of IT security maturity. Kaspersky's

long-term product roadmap includes combining its EDR with security orchestration, automation, and response (SOAR) products to offer a comprehensive, unified monitoring and analysis platform.

- While the majority of Kaspersky's customers are from the Middle East region and Europe, the company is expanding its presence in APAC and the North America. The company has a strong presence in the government & public sector, banking & financial services, and e-commerce & retail industries.

- Kaspersky's integrated EDR and endpoint protection platform solution, with its comprehensive technological functionalities along with capabilities that provide a strong customer ownership experience, has received strong ratings across the performance parameters of the technology excellence and customer impact. With overall strong ratings, Kaspersky is positioned amongst the technology leaders in the 2020 SPARK Matrix of the global EDR market.