Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™:

Managed Detection and Response (MDR)

Market Insights, Competitive Evaluation, and Vendor Rankings

September 2022

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global Managed Detection and Response (MDR) solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading Insider Risk Management vendors in the form of 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 its market position.

Market Dynamics and Overview

The concept Quadrant Knowledge Solutions define Managed Detection and Response (MDR) as:

"Quadrant Knowledge Solutions defines Managed Detection and Response (MDR) as a managed solution and service that combines technology with human expertise to offer the ability to immediately detect, analyze, investigate, and actively respond to cyber threats and reduce their impact through threat mitigation and containment in real-time. MDR solutions enable users to gain faster threat defenses across endpoints, networks, hardware systems, applications, OT/IoT, and enterprise assets."

Additionally, MDR solutions provide modern security operations center (SOC) capabilities, 24/7 threat monitoring, turnkey threat detection and response across on-prem, remote resources, cloud services, and OT/ICS environments. MDR enhances cyber agility and resilience against advanced threats with real-time detection and response while leveraging automated threat management solutions powered by AI and ML.

Digital transformation has led to a rise in different kinds of cyberthreats resulting in high volume of security alerts, which are often missed by the organization's security team. MDR acts as a catalyst for these kinds of cyberthreats and security alerts to secure organizational IT assets and helps organizations to presicely configure security policies for better security.

Managed Detection and Response (MDR) comprises of network host and endpoint-based security services, which are outsourced by enterprises and managed by third-party vendors. MDR provides 24*7 security control, rapid incident response, threat discovery, investigates, contains, and eliminates threats to protect and secure organizations' assets and sensitive data. A robust MDR solution provides protection from fileless malware and phishing attacks, defends the business against external and insider attempts to exfiltrate data, quickly responds to a security incident, and validates suspicious activity on endpoints.

MDR providers leverage real attack data to improve the organization's overall security posture by protecting it from threats. A typical MDR solution should provide the capabilities to investigate endpoints and offer the ability to search for historical information about endpoints use indicators of compromise to root out threats on endpoints, and automatically detect threats. A MDR solution also aids organizations in performing root cause analysis for every cyber threat, or any other threat found on an endpoint proactively and deemed important, searches endpoints for signs of threats known as threat hunting, and takes decisive action when a security incident, either potential or in-progress, is identified.

Overall, MDR has a huge significance in transforming strategies for information security for organizations. Additionally, MDR is like a specialized service which is developed to handle complex IT networks and allows organizations to fight against sophisticated vulnerabilities.

Following are the key capabilities of Managed Detection and Response (MDR) solution:

- **Threat Detection:** MDR solutions provide threat detection and intelligence abilities that swiftly identify, protect, detect, respond to, and recover from threats at an early stage through hypotheses based on the tactics and techniques used by attackers before the threats can cause any harm to the organizational system. MDR solutions allow users to discover anomalous activities, root causes of threats, improve threat detection, analysis, and hunting by leveraging human expertise, technology-assisted techniques, and user behavior analytics.

- **Incident Response:** MDR offers incident response capabilities that enable organizations to identify and respond to threats in real-time. MDR enables users to control an incident and eradicate the threat from the network to recover and restore the organizational data by alerting the incident handling team. Additionally, it allows a reduction of the detection time, responds quickly to cyber-attacks and threat actors, and maximizes visibility into the threat landscape. MDR intelligently recognizes advanced cyber-attacks, differentiates between noise and useful reports based on data collected on cyber threats, and converts them into actionable intelligence.

- **Threat Intelligence:** Insider risk management solution offers risk response capability that mitigates threats automatically in real-time. Additionally, it monitors users' activities to application, data, and block automatically or restrict access to an application or privileged data for any unusual behavior. Further, the automated risk response enhances the productivity and efficiency of the Security Operation Center (SOC) team without depending on time-consuming manual investigation or roles.

- **Security Monitoring and Analytics:** With an MDR solution provides greater visibility into all the IT activities associated with the

organization, irrespective of whether these activities occur inside or outside the organizational network. An MDR solution tracks and records data from applications and endpoints, including IoT devices, and analyzes the data to detect inefficiencies or anomalies. Additionally, the solution analyzes application usage and performance data to help organizations configure usage policies and implement the necessary security measures. An MDR solution provides an in-depth analysis of data collected from all endpoints and provides insights through visualization dashboards and custom reports. The solution leverages analytics to track and improve the overall performance and user experience and provides quick access to precise data-driven decisions based on a holistic view of devices and applications.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major vendors of Managed Detection and Response (MDR) by evaluating their offerings, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Managed Detection and Response (MDR) market. This study includes an analysis of key vendors, including Alert Logic, Arctic Wolf, Binary Defense, BlueVoyant, Cisco, Critical Start, CrowdStrike, Cybereason, Deepwatch, eSentire, Expel, WithSecure, Fishtech, GoSecure, Kudelski Security, Kroll, LMNTRIX, Mnemonic, Mandiant, NCC Group, Open Systems, Orange Cyberdefense, Pondurance, Proficio, Rapid7, Red Canary, Secureworks, Sentinel One, Sophos, and Trustwave.

Alert Logic, Arctic Wolf, Blue Voyant, Critical Start, Crowdstrike, Cybereason, eSentire, Kaspersky, Kudelski Security, Mandiant, Pondurance, Proficio, Rapid7, Red Canary, Secureworks and SentinelOne are identified as global technology leaders in the SPARK Matrix: Managed Detection and Response (MDR), 2022. MDR helps detect intrusions malware and malicious activity on the network and eliminate and mitigate those threats with the expert team monitoring the network 24*7. MDR providers leverages real attack data to improve overall security posture of the organizations. A typical MDR solution should have tools that are there in place to investigate endpoints, ability to search for historical information about endpoints, ability to use indicators of compromise to root out threats on endpoints, and ability to detect threat automatically. These companies provide a sophisticated and comprehensive technology platform to protect, detect, analyze, and remediate known and unknown cyberthreats.

Alert Logic delivers white-glove managed detection and response (MDR) with comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Alert Logic's proprietary MDR platform collects data from network traffic and billions of log messages every day to provide outcome-based security. In addition, the platform provides coverage across vulnerabilities and attacks by bringing together asset visibility and security analytics for networks, applications, and endpoints in on-premises, hybrid, and cloud environments.

Arctic Wolf MDR platform includes endpoint threat detection and response, which provides endpoint intelligence and increased threat detection capabilities

to offer Arctic Wolf's security engineers deep, comprehensive visibility into the organization's security posture. Additionally, the platform provides Sysmon event monitoring, which gives users complete insights into threats, including lateral movement, weekly endpoint reporting, and managed containment.

BlueVoyant Core offers cloud native "Elements Platform" that enables organizations to converge cyber defense capabilities into a consolidated platform, which makes easier for BlueVoyant Core to collaborate with internal security and SOC teams to meet specific customer requirements. BlueVoyant Core leverages exclusive data, proprietary automation, and intelligent playbooks to fight against cyberthreats and protects the organizational IT infrastructure. It offers managed threat hunting for Microsoft XDR by designing a customized cyberdefense platform that allows BlueVoyant to build the push detection logic in several client environments and allows organizations to store all EDR data within the customer's console.

CrowdStrike offers an MDR solution through its Falcon Complete product. Falcon Complete enables offloading Falcon endpoint protection to the experienced CrowdStrike staff and assists organizations in deployment and configuration. Moreover, the solution provides 24x7 alert and incident handling with delivering proactive incident triage and containment and allows organizations to effectively handle incident remediation. CrowdStrike Falcon Complete provides transparent management reporting and metrics. CrowdStrike provides threat hunting capabilities, including hypothesis-driven, behavioral, analytic, and adversary-based threat hunts on a regular basis. Additionally, the solution allows organizations to customize these threat hunting capabilities according to their needs.

Cybereason offers a comprehensive MDR solution that protects users from a wide range of threats across all endpoints. Cybereason MDR helps users identify unique, sophisticated threats with the Cybereason Defense Platform's automatic hunting capability, along with MITRE ATT&CK alignment. Cybereason MDR leverages MalOps severity score, which includes the following basic components: a behavioral score that maps MalOps to MITRE ATT&CK and access activity factor of MalOps, expert analysis which aids in root cause verification and investigation, actor attribution and information impact, and customer criticality to adjust the score based on the asset's criticality and their ability to recover.

Critical Start MDR platform includes a Zero Trust Analytic Platform (ZTAP) and Trusted Behavior Registry (TBR) to reduce false positives and MOBILESOC. Critical Start MDR provides complete visibility into the services, service licensing

agreements, security operations center, and application of threat intelligence to the customers. Additionally, it allows users to collaborate with the analysts in real-time from within their iOS and Android mobile app and review their analysis and corrective measures and take direct action immediately. It achieves this with the help of the information gathered in the platform to reduce attacker dwell time.

eSentire offers comprehensive MDR solution that protect critical data and applications from known and unknown cyber threats. Additionally, eSentire provides the Atlas platform, which is built on top of AWS serverless architecture and supports dynamic horizontal and vertical scaling. eSentire deploys its MDR services across all availability zones to ensure uptime exceeding 99.99%. In addition, it runs periodic stress tests that allow the platform to handle a large amount of data and request volume relative to the production payloads.

Mandiant provides its MDR through the Mandiant Managed Defense product, which includes the experience of the Mandiant response team to respond to the most impactful breaches, faster detection and remediation time, access to nation-state grade intelligence collection supported by a well-staffed team of intelligence analysts, and a robust defense with a combination of proprietary technology stack which incorporates Mandiant technology and intelligence.

Kaspersky is a global provider of product and technologies based on threat intelligence, machine learning (ML), cloud services, and global threat intelligence to secure businesses, critical infrastructures, government, and consumers from sophisticated and emerging cyber threats. Kaspersky offers Managed Detection and Response (MDR) service in two tiers for meeting diverse IT security needs and requirements. The first tier is “Kaspersky MDR Optimum,” which provides automated threat hunting. The second, titled “Kaspersky MDR Expert,” provides managed threat hunting to organizational IT systems. Kaspersky Anti-Targeted Attack Platform (KATA) includes network intrusion detection and a sandbox. Kaspersky’s proprietary ML model assists organizations in automating the initial incident triage and reduces the mean time to respond to cyberattacks.

Pondurance is another emerging leader in the MDR market. The Pondurance MDR solution leverages GPUs within their platform to accelerate the processing of data, apply Artificial Intelligence (AI) and threat intelligence, the ability to scale linearly and detect threats allowing Pondurance’s SOCs to respond faster and reduce false positives. The solution’s cloud-native architecture gives full data transparency and access to SOCs. Pondurance offers the dynamic defense methodology to enable

risk-based prevention, detection, and response to monitoring from a different set of vantage points filling the blind spots that are often overlooked.

Rapid7 MDR services and solutions leverage a unique set of threat detection methodologies that include threat intelligence, proactive threat hunting, Network Traffic Analysis, Network Flow data, deception technologies, user behavior analytics, and attacker behavior Analytics, derived from monitoring millions of endpoints. Rapid7 MDR services include security guidance, incident analysis, and remote incident response. Additionally, it offers tailored services based on the requirement of customers and security advisors for security maturation.

Red Canary MDR leverages API-first architecture with access to threat data used in the ticketing system, SIEM, Slack, SMS, and automatically scaling detection engine, propriety analyst workbench to perform hundreds of investigations per day for broader and precise detection coverage. Red Canary also provides a threat intelligence and research team as well as a cyber incident response team (CIRT) to classify confirmed threats. Red Canary MDR allows organizations to execute controlled or active remediation and containment in their network with Red Canary's response engineers.

Secureworks ManagedXDR provides experienced security operations, partnered investigations, and real-time chat with security analysts to protect users against cyber threats. It also provides periodic threat reports and data diversity for threat detection and improved security posture. The company leverages human and machine intelligence, proactive threat hunting for evasive threats, incident response, and provides protection for cloud deployment, which includes AWS, Office 365, and Azure.

SentinelOne offers its MDR services titled Vigilance Respond Pro and Vigilance Respond that adds value by augmenting and reducing the load on security organizations with features including clean dashboards, threat review, escalations for urgent matters only, accelerated threat resolution, proactive notifications, executive reporting, and periodic cadence calls. SentinelOne Vigilance Respond Pro offers all the capabilities of Vigilance Respond and includes intel-driven hunting, digital forensics & malware reversing, containment & eradication, faster SLA, root cause analysis, and post-mortem consultation. Vigilance Respond Pro offers direct access to forensic experts for incident management and IR retainer hours for malcode analysis and IR.

Cisco, Deepwatch, Expel, Kroll, Kudelski Security, NCC group, Orange Cyberdefense, Sophos, Trustwave, and With Secure have been positioned among the primary challengers. These companies provide comprehensive technology capabilities and are gaining significant market traction in the global Managed Detection and Response (MDR) market. These companies are also mindful of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2022 SPARK Matrix include Binary Defense, Fishtech Group, Go Secure, LMNTRIX, Mnemonic and Open Systems

All the vendors captured in the 2022 SPARK Matrix of Managed Detection and Response (MDR) are enhancing their capabilities to protect against known and unknown cyberattacks. Additionally, they help organizations expand their partnership channels and support diverse use cases. Vendors are consistently looking to enhance Managed Detection and Response (MDR) and expand support for easy deployment options. Vendors continue to enhance their offerings to provide robust capabilities, which include providing proactive threat hunting, threat analysis, fast incident response, threat intelligence, security monitoring and analytics, and visualization and reporting. The continuous transformation of MDR services driven by advanced technologies is propelling its market adoption amongst small to medium organizations and large enterprises. MDR vendors provide certain differentiators, including the sophistication of technology capabilities, maturity of AI and ML, integration and interoperability, scalability, and flexibility. Furthermore, vendors are adopting new strategies like automated attack detection and orchestrated mitigation using multiple methods, behavioral-based detection, encrypted attack protection, and others. Additionally, the vendors are focusing on increasing their customer base, geographical presence, different industry verticals, and expanding use case support. Vendors are also looking at expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

The following are the key competitive factors and differentiators for the evaluation of Managed Detection and Response (MDR) solution vendors. While most of the Managed Detection and Response (MDR) solutions may provide all the core functionalities, the breadth and depth of functionalities may differ by different vendors' offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology capabilities and overall value proposition to remain competitive. Some of the key differentiators include:

- **Advanced Security Features:** Users should evaluate the MDR solutions that offer advanced security features to protect against all types of cyberattacks while providing the ability to proactively recognize and detect network breaches and provide timely responses by leveraging various monitoring tools for 24/7 threat monitoring in real-time. Vendors are offering features that include threat analytics which should evaluate network threats based on threat signatures, composition, source, and other threat features. Vendors should also provide timely updates and proactive protection against evolving attacks. Additionally, vendors are also providing threat intelligence to protect users from advanced and zero-day attacks. Vendors are also offering incident investigation, incident validation threat containment, remote response services, and human expertise, including off-site SOC team assistance. Furthermore, vendors are focusing on integrating advance security analytics tools into their MDR services, which offer SIEM, behavioral analytics, forensics, network analysis and visibility, SOAR, and others.

- **Integration and Interoperability:** Users should Seamless integration and interoperability with vendors' existing technologies are among the crucial factors impacting the technology deployment and ownership experience. Vendors are increasingly integrating their solutions with organizations' existing complicated security solutions and ingest their logs and security events data to provide expert threat detection and automatic incident response based on the MITRE ATT&CK methodology. Additionally, vendors should provide out-of-the-box integrations with open API frameworks and integrate security telemetry into the user's technology stack to avoid blind spots. Users should also seek vendors who can integrate with their existing Security Information and Event Management (SIEM) system to increase the capability of their security team. Enterprises should carefully evaluate the vendor's existing

technology capabilities, along with their technology vision and roadmap to improve overall satisfaction and customer ownership experience for long-term success.

- **Vendors Strategy and Roadmap:** Users should consider the vendors' capability to formulate a comprehensive and compelling technology roadmap prior to the adoption of the MDR solution. Vendors are investing in digital transformation, catering to specific-use cases, and minimizing risk exposure. Vendors are continuously investing in R&D for their MDR solutions to take the lead in providing security. Additionally, some of the vendors are investing in innovating their MDR service by implementing cross-vendor XDR capability into their products to create novel detections based on multiple vendor products, adding support and direct integrations for additional sources of security alerts, such as identity, email, OT, cloud applications, enhancing their risk-based security operations, and improving service delivery to seamlessly interact with clients. Vendors are also focusing on improving analysts' productivity through orchestration. They are also focusing on XDR expansion while continuing to lead the MDR industry in broader and deeper MITRE ATT&CK coverage and expanding its product integrations across cloud and emerging security controls. Moreover, vendors are offering support for additional endpoint technology vendors, vulnerability management vendors, and additional Log/SIEM vendors. Vendors are implementing additional technologies with existing MDR solutions to build a robust security solution offering protection from these advanced cyberattacks.

- **Vendor's Expertise and Domain Knowledge:** Organizations should evaluate vendors expertise and domain knowledge in understanding their unique business problems, use case, and industry-specific requirements. Organizations are advised to conduct a comprehensive evaluation of different Managed Detection and Response platforms and vendors before making a purchasing decision. Users should employ a weighted analysis of the several factors important to their specific organization's use cases and industry-specific requirements.

- **Scalability and Flexibility:** An MDR solution vendor should offer a sophisticated solution that can manage, secure, and monitor all types of cyberthreats. The MDR solution should offer the scalability to fulfill the high demands and workloads while ensuring the best experience for employees and less burden on IT/admin resources. Users should look for vendors providing

security event management, security orchestration, incident response and workflow, reporting, and fully operationalized and automated security controls. Additionally, vendors should provide support for full multi-tenancy for large organizations for the deployment of MDR solutions. Users should be able to leverage these services to create a customized security solution to meet their specific business and technology requirements. Users should choose a platform that helps them reduce the risk and protects them from zero-day attacks. Users should look for MDR solution providers with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments.

- **Customized Service Delivery and Pricing Model:** Organizations should look for MDR vendors offering customized service delivery and pricing model in MDR service. Customized service delivery and pricing models deliver personalized MDR services. This model enables clients to pay only for services that they need to strengthen the IT infrastructure of organizations. Additionally, organizations are looking for MDR vendors who enables clients to configure exactly what nature of MDR service they need at a particular point of time like as a full suite of MDR services for network, log, endpoint and cloud or separate component of MDR service and this robust suite of MDR services will also reduce IT operational costs.

- **Data Visibility and Transparency:** Organizations should look for MDR vendors whose products provide data visibility and transparency in user security operations. MDR providers allow organizations to gain data visibility and transparency into their IT activities to ensure that organizations are completely aware of all kinds of security alerts regarding and enables internal security and SOC teams to look at every alert based on priority level. Additionally, organizations are looking for MDR vendors who brings efficient ROI to their MDR investment by providing them productive insights in context to how many attacks are occurring, how many are being stopped, and what risks still need to be considered

- **Incident Response Retainer (IRR):** Users should look for MDR vendors who offer Incident Response Retainer (IRR). An IRR is a service agreement that allows organization to get external assistance for cybersecurity incidents. The IRR service includes incident response preparation, incident response planning, Incident triage and classification, initial response, and SLA (service level agreement). Additionally, organizations are looking for MDR vendors

whose products allow organization to scan, analyze, identify, and remediate threats by leveraging incident response service which includes 24/7 incident response, deep forensic investigations, threat hunting and malware analysis to fight against cyberthreats intrusion into IT system.

- **Single Management Console:** Organizations should look for MDR vendors whose products offer a single management console to consolidate all security policies and reports for seamless management and customer provisioning. A single console enables organizations to perform 24x7 continuous threat monitoring, alert triage, and incident handling in one platform for effective remediation of cyber threats. A single management console enables organizations to create, view, and control all network security management domains from a single console. Additionally, Organizations are looking for MDR vendors offering single security management for VPN, Firewall, IPS, and other protections.

- **Alert Fatigue Minimization:** Organizations are looking for MDR Vendors whose products automatically reduce alert fatigue by Alert prioritization, reasonable alert suppression, unified security tools, visualized alert data and alert grouping. MDR services leverage a logic-based detection engine to trigger the investigation of any abnormal behavior occurs in the IT system. Additionally, organizations are looking for MDR vendors providing a combination of automation and incident response experts for neutralizing and remediating cyber threats.

- **Customized Technology Stack:** Organizations should look for MDR vendors offering customized technology stacks. A customized technology stack allows organizations to perform real-time threat monitoring, detection, investigation, and launch an active mitigating response to existing and potential cyber threats according to their security requirements. A customized technology stack also enables organizations to integrate with cloud service coverage (SaaS and IaaS) and malware analysis, identifying indicators of compromise (IOCs), human-powered threat hunting, threat containment, and specific guidance on remediation.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and similar others.

Each market participants are analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix.

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%

Evaluation Criteria: Technology Excellence

- **The sophistication of Technology:** The ability to provide comprehensive functional capabilities and product features, technology innovations, product/platform architecture, and such others.

- **Competitive Differentiation Strategy:** The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.

- **Application Diversity:** The ability to demonstrate product deployment for a range of industry verticals and/or multiple use cases.

- **Scalability:** The ability to demonstrate that the solution supports enterprise-grade scalability along with customer case examples.

- **Integration & Interoperability:** The ability to offer product and technology platform that supports integration with multiple best-of-breed technologies, provides prebuilt out-of-the-box integrations, and open API support and services.

- **Vision & Roadmap:** Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance:** Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.

- **Market Presence:** The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record:** Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.

- **Ease of Deployment & Use:** The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation and usage experience. Additionally, vendors' products are analyzed to offer user-friendly UI and ownership experience.

- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting,

training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

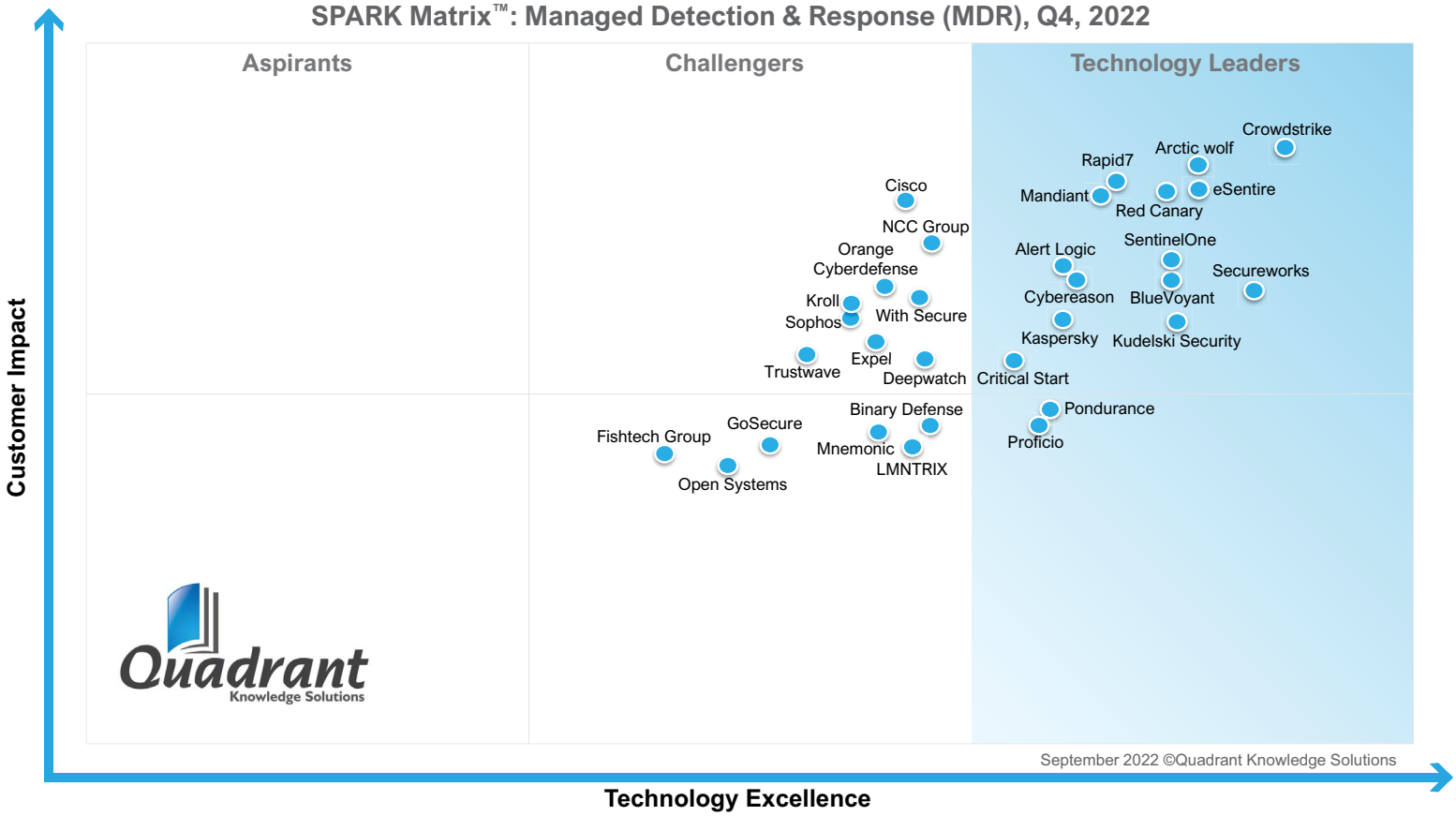
SPARK Matrix™:
Managed Detection and Response (MDR)

Strategic Performance Assessment and Ranking

Figure: 2022 SPARK Matrix™

(Strategic Performance Assessment and Ranking)

Managed Detection and Response (MDR)



Vendor Profiles

Following are the profiles of the leading know your customer solution vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions, regarding know your customer technology and vendor selection based on research findings included in this research service.

Kaspersky

URL : www.kaspersky.co.in

Founded in 1997 and headquartered in Moscow, Russia, Kaspersky is a global provider of products and technologies based on threat intelligence, machine learning, cloud services, and global threat intelligence to secure businesses, critical infrastructures, government, and consumers from sophisticated and emerging cyber threats. Kaspersky offers Managed Detection and Response (MDR) service in two tiers for meeting diverse IT security needs and requirements. The first tier is "Kaspersky MDR Optimum," which provides automated threat hunting. The second, titled "Kaspersky MDR Expert," provides managed threat hunting to organizational IT systems.

Kaspersky Managed Detection and Response (MDR) provides threat intelligence to organizational IT systems. Kaspersky MDR's threat intelligence capability enables services to develop threat hunting techniques, improve threat detection logic to quickly identify cyber threats, prioritize cyber incidents, and decide the best response/mitigation measures. Furthermore, the Kaspersky MDR service leverages many proprietary IoA to hunt for threats and deliver responses to customers.

Kaspersky MDR service comes with built-in Kaspersky EDR optimum, which delivers a centralized response to all incidents detected by the service. Kaspersky MDR enables organizations to automatically detect and analyze security incidents in their IT infrastructure by leveraging telemetry, threat intelligence, advanced machine learning technologies, and human expertise.

Kaspersky MDR publishes its information to Kaspersky Security Center, a single management console for Kaspersky products. It provides complete visibility into all service detections, statuses of the protected assets and delivers incident notifications with comprehensive incident response recommendations.

Analyst Perspective

Following is the analysis of Kaspersky capabilities in the global Managed Detection and Response (MDR) Market:

- Kaspersky MDR enables organizations to leverage their limited in-house resources to protect their IT infrastructure in real-time from an increasing number of complex threats. Kaspersky MDR allows organizations to benefit from fully managed detection, prioritization, investigation, and response to cyber threats and strengthen the organizational SOCs. Kaspersky MDR service enables organizations to detect cyber incidents at all MITRE ATT&CK tactics.

- Kaspersky MDR allows organizations to analyze telemetry from Kaspersky products installed in physical, virtual, and cloud environments. The service validates product alerts to ensure the effectiveness of automatic prevention and proactively analyses system activity metadata for any signs of an active or impending attack. This metadata is collected via Kaspersky Security Network and is automatically correlated in real-time with Kaspersky's threat intelligence to identify the tactics, techniques, and procedures used by attackers. Kaspersky's proprietary ML model automatically processes 35-40% of all alerts right at the moment the data comes helping to minimize MTTD and MTTR.

- Depending on the requirements, the service offers a completely managed or guided disruption and containment of threats while keeping all response actions under the customer's full control. The service can be complemented with a full-scale incident response retainer.

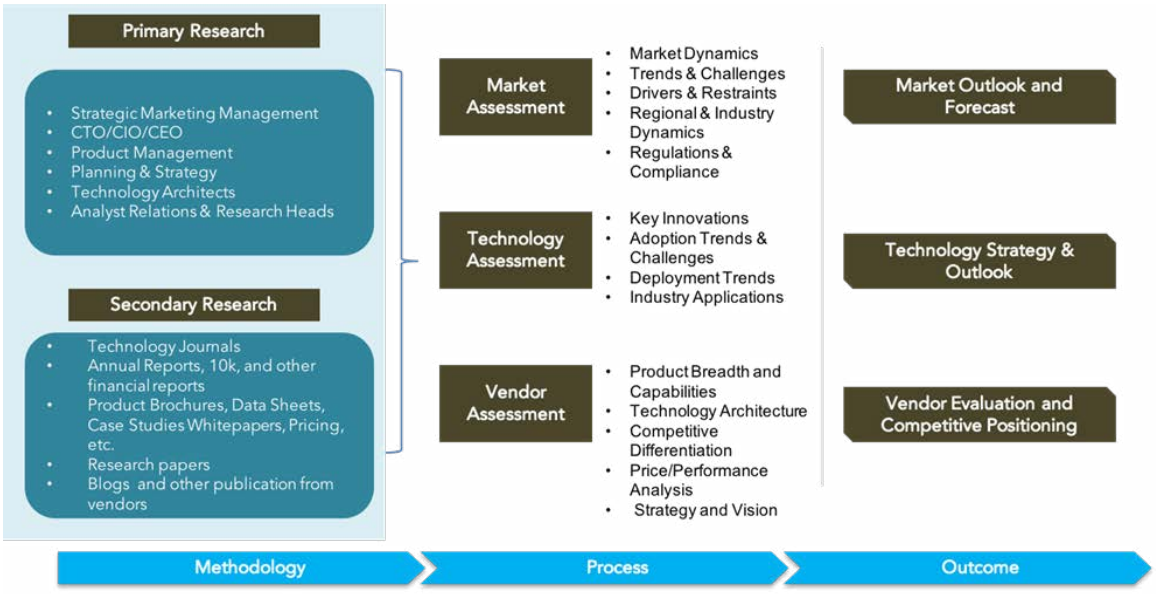
- Regarding geographical presence, Kaspersky has a strong presence in EMEA, and the Americas, followed by the Asia-Pacific. From an industry vertical perspective, while the company has a presence across a wide variety of verticals, its primary verticals include industrial, financial, IT/technology, retail, transportation, and such others. From a use case perspective, the Kaspersky MDR is used for mitigating targeted attacks, malware, vulnerability exploitation, social engineering, and insider threats.

- Kaspersky's primary challenges include the growing competition from emerging vendors with innovative technology offerings. However, with its advanced capabilities like threat intelligence, managed threat hunting, built-in extended detection and response, robust technology differentiators like incident response retainer, detection and prevention technologies, and many others, Kaspersky is well-positioned to maintain and grow its market share in the MDR market.

- As part of its technology roadmap, Kaspersky will invest in establishing regional SOCs with local teams, providing the service with third-party EPP/EDR products. Kaspersky is also evaluating partnership options to offer cyber insurance.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products

- Database of market sizes and forecast data for different market segments
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage

with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis:
Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic scenario, industry trends, and economic dynamics. Finally, the analyst team arrives at the most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix:
Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis and forecasts, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including market forecast; competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at
rmehar@quadrant-solutions.com | www.quadrant-solutions.com