Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Managed Detection and Response (MDR), Q4 2023

Market Insights, Competitive Evaluation, and Vendor Rankings

December, 2023

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of the global Managed Detection and Response (MDR) market dynamic, vendor landscape, and competitive positioning analysis. The study provides a competitive analysis of leading vendors. 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 and competitive differentiation.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines Managed Detection and Response (MDR) as "a third-party managed service that combines technology with human expertise to offer the ability to immediately detect, analyze, investigate, and actively respond to cyber threats." MDR ensures the immediate identification and mitigation of cyber threats by combining advanced technology with skilled threat hunting and incident management experts, thus reducing the impact across various dimensions such as endpoints, networks, hardware systems, applications, OT/IoT, and enterprise IT assets. This process involves analyzing data within the organizations' platforms to provide faster threat defenses and deliver actionable insights.

Additionally, MDR service 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. The MDR service 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.

While digital transformation has led to a rise in different kinds of cyber threats, there are not enough personnel to combat them. The remaining workforces are also battling threats like burnout and stress owing to the ever-evolving threat landscape. Deploying Managed Detection and Response (MDR) services can help organizations ensure that their business remains secure and pivot their security teams to more strategic tasks.

Managed Detection and Response (MDR) comprises 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, and threat discovery; and investigates and eliminates threats to protect and secure organizations' assets and sensitive data. A robust MDR 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. This service automate the supervision and response to security incidents, providing capabilities such as real-time threat detection, incident investigation, and proactive response measures.

MDR providers leverage real attack data to improve the organization's overall security posture by protecting it from threats. A typical MDR service 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. An MDR also aids organizations in performing root cause analysis for every security 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.

MDR providers offer comprehensive security for both cloud-native and on-premises assets of the organization, which enhances the overall security posture and provides a unified and proactive approach to managing and responding to security incidents. Moreover, the integration of the MDR technology stack with the pre-existing organization's security solutions, such as SIEM and SOAR, plays a crucial role in the comprehensive security of the organizational assets.

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

The following are the key capabilities of an Managed Detection and Response (MDR):

- **Threat Detection:** An MDR provides 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 impact the organizational systems. MDR enable the discovery of anomalous activities as well as root causes of threats, and improved threat detection, analysis, and hunting by leveraging human expertise, technology-assisted techniques, and user behavior analytics, which helps identify abnormal activities, such as privileged users accessing unauthorized information or unusual data access patterns.

- **Incident Response:** An MDR provides incident responsibility capability, which enables reduced detection time, quicker response to cyber-attacks and threat actors, and maximizes visibility into the threat landscape. An 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.

- **Managed Threat Hunting and Advisory:** An MDR provides Threat hunting and advisory capability, which involves a proactive strategy of identification of previously unknown or hidden threats or IOCs. This capability allows threat hunters to reduce dependence on pre-established attack patterns and security alerts to indicate potential data breaches. Instead, they actively search for threat patterns that might typically escape the conventional security tools. This forward-looking method of identifying threats empowers threat hunters to uncover and alert clients about potential threats or unknown threats before they impact organizational systems. This proactive threat hunting and advisory allows users to improve their organizational security posture and identify unknown or hidden threats.

- **Threat intelligence:** MDR offers threat intelligence capability that enables the collection of threat data via crowdsourcing and correlating and validating real-time attack data from multiple sources. MDR creates, identifies, and categorizes threat profiles by collecting and analyzing data from several types of cyber threats. Additionally, MDR provides enhanced support to security systems by integrating constant updates of possible risks and vulnerabilities with real-time information about these attack vectors.

- **Security Analytics and Monitoring:** MDR provides greater visibility into all the IT activities associated with the organization, irrespective of the activities' points of origin. The solution tracks and collects data from heterogeneous sources and analyzes the data to detect inefficiencies or abnormal activities. Additionally, MDR analyzes application usage and performance data to help organizations configure usage policies and implement the necessary security measures. In addition, MDR identifies, analyzes, and prevents zero-day threats before they can reach the enterprise IT system in real-time. Also, It provides meaningful insights into threats and the security landscape through interactive reports.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Managed Detection and Response (MDR) vendors 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 Arctic Wolf, Binary Defense, Bitdefender, BlueVoyant, Booz Allen Hamilton, Cisco, Critical Start, CrowdStrike, Cybereason, Cyderes, Cyberoo, Deepwatch, eSentire, Expel, Fortra, Group-IB, Integrity360, IBM, Kaspersky, Kudelski Security, Kroll, Mandiant, Mnemonic, NCC Group, Obrela Security, Ontinue, Optiv, Orange Cyberdefense, Pondurance, Proficio, Quorum Cyber, Rapid7, Red Canary, Secureworks, SentinelOne, Sophos, Trustwave, and WithSecure.

Arctic Wolf, BlueVoyant, Critical Start, CrowdStrike, eSentire, Fortra, Group-IB, Kaspersky, Kudelski Security, Proficio, Rapid7, Red Canary, Secureworks, and SentinelOne have been identified as global technology leaders in the SPARK Matrix™: Managed Detection and Response (MDR), 2023. These companies provide a sophisticated and comprehensive technology platform to protect, detect, analyze, and remediate known and unknown cyberthreats.

Arctic Wolf's MDR offers endpoint threat detection and response, which provides endpoint intelligence and increased threat detection capabilities to allow Arctic Wolf's security engineers to gain deep, comprehensive visibility into the user organization's security posture. Additionally, the Arctic Wolf's MDR provides Sysmon event monitoring, which gives users complete insights into threats, including lateral movements, weekly endpoint reporting, and managed containment.

BlueVoyant Core offers the cloud-native "Elements Platform," which enables organizations to converge cyber defense capabilities into a consolidated platform, enabling easier collaboration between BlueVoyant Core and clients' internal security and SOC teams to meet specific customer requirements. BlueVoyant Core leverages exclusive data, proprietary automation, and intelligent playbooks to fight cyberthreats and protect the organizational IT infrastructure. ICrowdStrike offers an MDR through its Falcon Complete product. Falcon Complete enables offloading of endpoint protection to the experienced CrowdStrike staff and assists organizations in deployment and configuration. Moreover, the solution provides

24x7 alert and incident handling, along with proactive incident triage, and containment and allows organizations to effectively handle incident remediation. CrowdStrike Falcon Complete provides transparent management reporting and metrics, as well as threat-hunting capabilities, including hypothesis-driven, behavioral, analytic, and adversary-based threat hunts on a regular basis. Additionally, the service allows organizations to customize these threat-hunting capabilities according to their needs.

Critical Start's MDR 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 apps, review their analysis and corrective measures, and take direct action immediately. It achieves this with the help of the information gathered to reduce attacker dwell time.

eSentire offers a comprehensive MDR capabilities that protects 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 service to handle a large amount of data and request volume relative to the production payloads.

Fortra delivers white-glove managed detection and response (MDR) with comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Fortra's proprietary MDR collects data from network traffic and billions of log messages every day to provide outcome-based security. In addition, the service 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.

Group IB's MDR consists of comprehensive technology that includes endpoint protection, threat intelligence, sandboxing, and other capabilities. Group-IB MDR operates its own SOC, which includes a wide range of Managed Services, including 24x7 Managed Detection, Managed Response, and Managed Threat Hunting. This SOC is also certified as a Computer Emergency Response Team (CERT) and plays a pivotal role in supporting all Group-IB's cybersecurity activities, such as threat hunting and detection. Group-IB's managed threat hunting takes a

proactive approach to identifying unfamiliar threats, advanced attacks, and APTs. Expert threat hunters use XDR alerts as a basis for investigating hypotheses. This capability serves to both safeguard the system against threats and gather valuable threat-related information.

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.

Kudelski Security provides next-generation detection, prevention, and deception technologies to protect endpoints and prevent the intrusion of cyber attackers into organizational IT systems. Kudelski MDR service for endpoints detects malicious activity, contains threats, and accelerates incident response measures to tackle cyber threats. Kudelski Security's 24/7 MDR service, powered by the FusionDetect™ platform, collects security-related data from organizational IT environments to support internal security teams to effectively investigate cyberthreats intrusion into the organizational IT systems. Additionally, it provides complete visibility across IT, cloud, endpoints, and OT/ICS. Kudelski Security FusionDetect™ platform collects relevant data, including security-related data, and alerts internal SOC and security teams related to cyberattacks. It also offers rich contextualization by providing the latest MITRE ATT&ACK techniques to prioritize cyber threats in terms of their ability to intrude into IT systems.

Proficio offers MDR through its ProSOC MDR service. ProSOC MDR provides threat detection analytics and threat intelligence platform integration features. Additionally, Proficio ProSOC MDR offers the ProView security management portal to organizations by delivering real-time visibility into IT infrastructure, incident case management, security gap assessment, and scorecard and peer comparison. Also, Proficio ProSOC MDR offers managed endpoint detection and response (MEDR), which allows organizations to mitigate risk through consistent monitoring of critical endpoints.

Rapid7's MDR services 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 requirements 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, an automatically scaling detection engine, and a 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 as well as incident response, and provides protection for cloud deployment, which includes AWS, Office 365, and Azure.

SentinelOne's MDR services, titled Vigilance Respond Pro and Vigilance Respond, add value by augmenting and reducing the load on security organizations through features like clean dashboards, threat review, escalations for urgent matters, accelerated threat resolution, proactive notifications, executive reporting, and periodic cadence calls. SentinelOne Vigilance Respond Pro offers all the capabilities of Vigilance Respond as well as 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, IBM, Cybereason, Mandiant, Booz Allen Hamilton, Orange Cyberdefense, NCC Group, Kroll, Sophos, WithSecure, Bitdefender, Quorum Cyber, Optiv, Expel, Trustwave, Integrity360, Trustwave, Mnemonic, Pondurace and Cyderes have been placed as strong contenders. 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 2023 SPARK Matrix™ include Obrela Security Industries, Cyberoo, Ontinue, and Binary Defense.

All the vendors captured in the 2023 SPARK Metrist 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 proactive threat hunting, threat analysis, fast incident response, threat intelligence, security analytics and monitoring, 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) vendors. While most of the Managed Detection and Response (MDR) 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 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 evaluates 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 advanced security analytics tools into their MDR services, which offer SIEM, behavioral analytics, forensics, network analysis and visibility, SOAR, and others.

Integration and Interoperability: 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 ingesting 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. This synergy enables faster, more informed decision-making, continuous improvement, and adaptability

to unique organizational needs. 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.

Vendor Strategy and Roadmap: Users should consider the vendors offering a comprehensive and compelling technology roadmap prior to the adoption of the MDR service. 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 service 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 technology stack to build a robust security service offering protection from these advanced cyberattacks.

Scalability and Flexibility: Users should look for MDR service vendors offering a sophisticated solution that can manage, secure, and monitor all types of cyberthreats. The 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. The MDR service should be flexible to easily integrate with diverse IT environments, support various security protocols, and adapt to emerging threats and technologies. 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 service. 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 service that helps them reduce the risk and protects them from zero-day attacks. Users should look

for MDR service providers with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments.

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 and enable internal security and SOC teams to look at every alert based on priority level. This visibility and transparency also help organizations with regulatory compliance. Additionally, organizations are looking for MDR vendors who bring 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). The IRR service includes incident response preparation, incident response planning, Incident triage and classification, initial response, and SLA (service level agreement). Also, as many privacy and consumer protection regulations require swift response and timely notification for cybersecurity incidents, this service also helps organizations with compliance management. Additionally, organizations are looking for MDR vendors whose products allow scanning, analyzing, identification, and remediation of 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 systems.

Single Management Console: Organizations should look for MDR vendors who 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 24/7 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.

Customized Technology Stack: When selecting an MDR service, organizations should look for MDR vendors that demonstrate a strong capability in delivering a customized technology stack that offers hyper-personalized security services. This includes the ability to customize threat detection algorithms and adapt response

strategies to the organization's specific risk profile. 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-making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Each market participant is 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
Managed Detection	15%
Managed Threat Hunting and Investigation	15%
Case Management and Incident Response	15%
Threat Intelligence	10%
Technology Stack and Platform Capabilities	15%
Skills, Expertise and Experience of Security Analysts	10%
Security Analytics and Reporting	10%
Competitive Differentiation Strategy	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%

Evaluation Criteria: Technology Excellence

- **Managed Detection:** The ability to use advanced technologies, such as threat intelligence, behavioral analysis, and machine learning, to identify potential security threats.

- **Managed Threat Hunting and Investigation:** Managed Threat Hunting and Investigation focuses on proactively searching for and investigating potential security threats within an organization's IT environment.

- **Case Management and Incident Response:** The ability of the solution to organize and handle security incidents and investigation through proper response.

- **Threat Intelligence:** The ability involves collecting, analyzing, and leveraging information about potential and existing cyber threats.

- **Technology Stack and Platform Capabilities:** The combination of hardware and software technologies along with their functionalities.

- **Skills, Expertise and Experience of Security Analysts:** The ability of the analysts to detect and respond to threats.

- **Security Analytics and Reporting:** The ability to deliver insights and recommendations based on the data collected.

- **Competitive Differentiation Strategy:** USPs and competitive advantage.

- **Vision & Roadmap:** Key Planned enhancement to offer superior products/technology.

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.

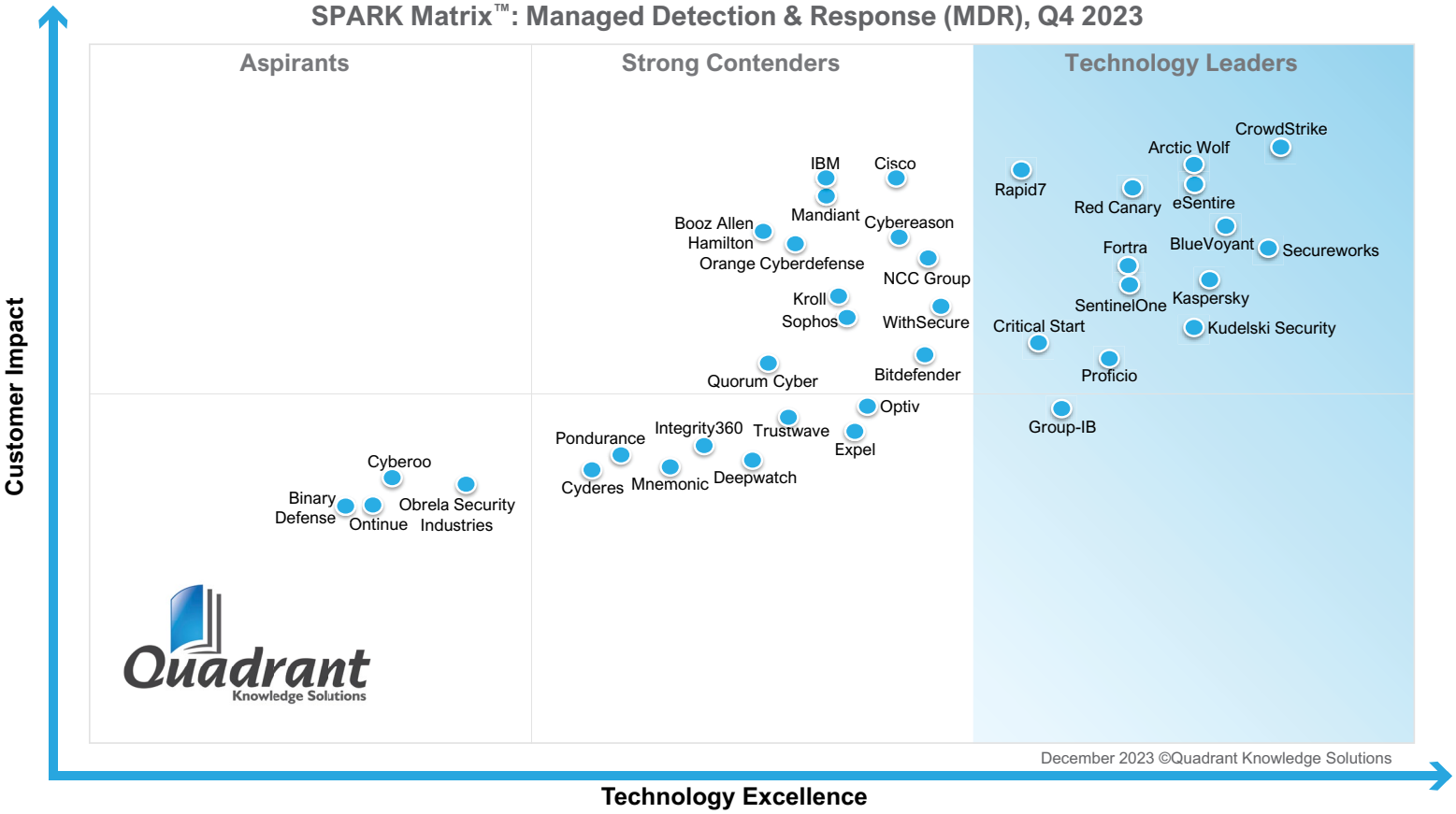
- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **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: 2023 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Managed Detection and Response (MDR) Vendors



Vendor Profile

Following are the profiles of the leading Managed Detection and Response (MDR) 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 Managed Detection and Response (MDR) and vendor selection based on research findings included in this research service.

Kaspersky

URL: https://www.kaspersky.co.in

Company Introduction:

Founded in 1997 and headquartered in Zurich, Switzerland. Kaspersky is a provider of cybersecurity and digital privacy products. Kaspersky offers Managed Detection and Response (MDR) service in two tiers to meet the 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.

Product Introduction:

Kaspersky Managed Detection and Response (MDR) provides threat intelligence to organizational IT systems. Kaspersky MDR's threat intelligence capability enables organizations 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, Kaspersky MDR's managed threat-hunting capability enables organizational security teams and SOC teams to hunt TTPs (Techniques, Tactics, and Procedures) to develop Indicators of Attack.

Kaspersky MDR offers built-in Endpoint Detection and Response (EDR), which enables organizations to use only the functionalities required at a specific point in time to remediate cyber threats by strictly monitoring and controlling endpoints. Kaspersky MDR enables organizations to automatically detect and analyze security incidents in their IT infrastructure by leveraging telemetry and advanced machine learning technologies.

Kaspersky Managed Detection and Response provides a plug-in for Kaspersky Security Center Web Console and Cloud Console in organizational IT systems and is updated with enhanced MDR Health functionality that improves the interface of MDR Health and provides organizations with a list of assets of all statuses.

Technology Perspective:

Following is the analysis of Kaspersky's 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 manage and customize the detection of cyber threats, prioritization, investigation, and response of cyber threats, and strengthening the organizational SOCs. Kaspersky MDR service enables organizations to detect cyber incidents at several phases of access or at different stages of IT operations. The initial access is covered by the Kaspersky anti-targeted attack platform (Kaspersky MDR expert), which detects phishing and social engineering attacks, resource development, execution stage, lateral movement where cyber incidents of high severity are detected, command and control where low and medium severity incidents are detected and discovery stage.

- Kaspersky Threat Intelligence integrates various intelligence sources, threat data feeds, and internal research to provide an extensive perspective on the worldwide threat environment. Kaspersky's team of experts analyzes this information to offer actionable insights, empowering organizations to safeguard themselves against cyber threats. Kaspersky MDR and Kaspersky Compromise Assessment provide threat-hunting services to uncover previously unknown threats.

- Kaspersky MDR provides telemetry analysis from various sensors for up to 1 to 3 months, including endpoints (EPP/EDR), network intrusion detection systems (IDS), and sandbox. 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.

- Kaspersky MDR's incident response retainer allows organizations to launch Incident response, which provides a detailed analysis of the incident with storage up to 1 year. Kaspersky MDR enables organizations to track the incident investigation and response cycle, which includes incident response and evidence collection, to identify and launch an appropriate mitigation

plan. Additionally, Kaspersky Industrial CyberSecurity (KICS for networks) integrates with Waterfall Security Solutions to strengthen security for industrial networks.

- Kaspersky also offers Global and localized MDR services. In the global team, MDR analysts are available on a follow-the-sun basis. Kaspersky also offers complimentary digital forensics and malware analysis as add-on features. Kaspersky also offers supporting products like an anti-targeted attack platform with Endpoint Detection and Response, digital forensics, and security awareness training.

Market Perspective:

- Regarding geographical presence, Kaspersky has a strong presence in Europe and the Asia Pacific, followed by the Americas. From an industry vertical perspective, while Kaspersky has a presence across a wide variety of industry verticals, its primary verticals include BFSI, Govt and Public sector, food and beverages, manufacturing, healthcare, transportation and media, retail, IT, education, construction, as well as travel and hospitality.

- From a use case perspective, Kaspersky's primary use cases include mitigating targeted attacks, 24*7 human-led protection, threat-hunting, endpoint security, real-time visibility with detailed reporting on security performance metrics, compliance with regulations, and APT detection.

Challenges:

- 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.

Roadmap:

- As a part of its technology roadmap, Kaspersky plans to enhance the efficiency, quality, and expertise of services, the creation of services tailored for Industrial Control Systems (ICS) and Operational Technology (OT), and the advancement of features in Managed Detection and Response (MDR).

- The strategic initiatives involve the establishment of regional Security Operations Centers (SOCs) with local teams and data storage capabilities. This includes offering Managed Detection and Response (MDR) services in conjunction with third-party Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) products. Furthermore, the company plans to evolve the service into a managed Extended Detection and Response (XDR) solution, supporting not only Kaspersky technologies but also integrating third-party products.

Arctic Wolf

URL: https://arcticwolf.com/

Company Introduction:

Founded in 2012 and headquartered in Eden Prairie, MN, Arctic Wolf offers a cloud-native security operations platform to eliminate cyber risk. Arctic Wolf offers a portfolio of solutions that include managed detection and response (MDR), managed risk, cloud detection and response, cloud security posture management (CSPM), managed security awareness, and incident response. Arctic Wolf MDR enables organizations to detect, respond, and recover from modern cyber-attacks in real-time.

Product Introduction:

The Arctic Wolf MDR solution collaborates with the user's current technological stack to provide comprehensive visibility into the network environment by finding and profiling assets, as well as collecting and analyzing data and security event observations from a diverse set of sources. Additionally, the MDR allows organizations to perform 24*7 network, endpoint, and cloud environment monitoring and helps detect sophisticated threats. The Arctic Wolf MDR solution integrates machine learning with adaptive tuning to deliver proactive threat hunting, advanced threat detection, and remote forensic analysis for increased detection efficiency and scale. Most customers receive on average an alert per day, which dramatically reduces alert fatigue and allows for the optimization of security strategies and assets.

Technology Perspective:

Following are the analysis of Arctic Wolf's capabilities in the global Managed Detection and Response market:

- The Arctic Wolf Managed Detection and Response (MDR) solution provides 24×7 monitoring of networks, endpoints, and cloud environments to detect, respond, and recover from modern cyber-attacks. Arctic Wolf's MDR solution

addresses critical cybersecurity challenges, including modern evolving threats, increasing costs, and retention of experienced security professionals. Additionally, Arctic Wolf provides a Concierge Security Team (CST) that works directly with users to execute threat hunting, alert triage and prioritization, incident response and guided remediation, as well as provide strategic suggestions particular to the user's cloud environment requirements.

- Arctic Wolf MDR offers guided remediation to validate threat remediation and neutralization. The MDR leverages its root cause analysis capability to provide an in-depth probe of any security incident. The MDR also promotes the creation of customized rules and workflows that lead to the formation of a robust security posture for organizations. It also offers personalized engagement to improve the overall security for users optimized for their organizational environment.

- Arctic Wolf MDR solution provides an investigation of suspicious activities, and its managed investigations capability eliminates alert fatigue and false positives for faster response. Moreover, the solution provides unrestricted log retention, wherein the platform automatically gathers, standardizes, analyzes, and preserves log data from current networks, systems, and applications. This feature provides users with insight-based reporting and makes compliance with regulations easier. Arctic Wolf MDR is built as an open, vendor-agnostic tool and it integrates with the user's existing systems through an API for faster threat detection, response, and recovery without the need to alter the existing infrastructure.

- Arctic Wolf MDR solution's incident response capability identifies and prevents critical security incidents in minutes. Arctic Wolf's IR JumpStart Retainer is a proactive incident response retainer that provides incident response planning with 1-hour SLA.

- Some of the unique differentiators of Arctic Wolf MDR include endpoint threat detection, which provides endpoint intelligence and increased threat detection capabilities. These capabilities give Arctic Wolf's concierge security experts deep, comprehensive visibility into the organization's security posture. The MDR also comes with Sysmon event monitoring, which gives users complete insights into threats, including lateral movement, weekly endpoint reporting, and managed containment.

Market Perspective:

- Arctic Wolf has a presence in the North America, Europe, Africa and Asia/ Pacific regions. From an industry vertical perspective, the primary verticals for Arctic Wolf include agriculture, construction, education, energy, entertainment, finance, government, healthcare, legal, manufacturing, real estate, services, and technology industries.

- From a use case perspective, Arctic Wolf's key use cases include 24*7 human-led protection, threat hunting, endpoint security, real-time visibility with detailed reporting on security performance metrics, compliance with regulations, and APT detection.

BlueVoyant

URL: https://www.bluevoyant.com/

Company Introduction:

Founded in 2017 and headquartered in New York, NY, BlueVoyant is a provider of an end-to-end cyber defense platform that fights internal and external cyber threats.

Product Introduction:

BlueVoyant offers robust MDR service through its cyber defense platform. The services protect the organizational networks from all kinds of cybersecurity vulnerabilities and strengthen the IT infrastructure. The cloud-native "Elements Platform" enables user organizations to converge cyber defense capabilities into a centralized platform, which makes it easier for BlueVoyant to collaborate with internal security and SOC teams to meet specific customer requirements. The BlueVoyant platform integrates technology, telemetry, and security excellence to help user organizations respond to zero-day attacks and new threats by leveraging analytical and unique/exclusive data sets. BlueVoyant provides integrated security, threat, and risk capabilities to organizations to offer them a robust integrated experience while minimizing risk. These capabilities allow organizations to provide actionable intelligence to their client.

Technology Perspective:

Followings is the analysis of BlueVoyant's capabilities in the global Managed Detection and Response (MDR) Market:

- BlueVoyant utilizes exclusive data, proprietary automation, and intelligent playbooks to actively combat cyber threats to secure organizational IT infrastructure. The company employs threat analytics supported by Microsoft security technology to effectively reduce the risk for user organizations. Integration with Splunk enables BlueVoyant to promptly address critical vulnerabilities, minimize alert fatigue, and offer comprehensive visibility into IT assets and vulnerabilities, facilitating cyber threat investigations. BlueVoyant

also extends MDR services to endpoints, enabling automatic blocking of cyber threats, investigation of cyber incidents, and swift threat containment.

- BlueVoyant's responsiveness capability allows organizations to engage BlueVoyant rapidly during the start of the security breach. BlueVoyant's precision scoping allows the organization to investigate only specific cyber incidents, saving time and cost for the affected organization. BlueVoyant deploys the client data on its IT infrastructure, which allows it to fully control the data in real-time. Additionally, BlueVoyant monitors organizational Security Operations Centers (SOC) with automated alerting and remote incident response to cyber threats.

- BlueVoyant MDR provides managed third-party risk and digital risk protection services to the organizational IT system as EDR or SIEM managed detection and response. BlueVoyant offers managed threat hunting for Microsoft XDR by designing a customized cyber defense platform that allows BlueVoyant to build push detection logic in client environment and allows organizations to store all EDR data within the customer's console. BlueVoyant metrics and reporting focus on data advisory metrics which are focused on SIEM content and ROI, as well as MITRE mapping and SOC KPI metrics, which are outcome oriented.

- BlueVoyant's MDR provides supply chain defense that provides risk assessment, vulnerability identification, cyber defense, risk mitigation, and high-volume monitoring services. BlueVoyant provides 24*7 SOC-as-a-service with expert staff who help deploy, maintain, and improve the security features of the platform. This service includes detection, alerting, and response.

- From a differentiator point of view, BlueVoyant's key differentiators include focus on third-party and supply chain risk services and organized threat intelligence.

Market Perspective:

- From the geographical presence perspective, BlueVoyant has a strong presence in North America, particularly the US, followed by Canada, Europe, the Middle East & Africa, Asia Pacific, and Latin America. From an industry perspective, the company has a presence across a wide variety of industry verticals,

such as banking & financial services, private equity, automotive, healthcare, government, retail and e-commerce, legal, insurance, manufacturing, oil and gas, gaming and leisure, food and beverage, pharmaceutical, and telecom.

- From a use case perspective, BlueVoyant's primary use cases include platform maintenance and curation of security, a fully managed XDR, combining capabilities of managed third-party risk, digital risk protection, data leak protection, digital brand protection, accelerated SIEM deployment, and endpoint protection.

Challenges:

- The primary challenges for BlueVoyant include the competition from emerging vendors with innovative technology offerings. However, owing to its functional capabilities such as responsiveness, elements platform, inside and outside SOC, the flexibility of service delivery, robust technology differentiators such as security content creation and delivery, curated log ingestion and optimization, and excellent robust customer value proposition, BlueVoyant is well-positioned to maintain and grow its market share in the Managed Detection and Response market.

Roadmap:

- Regarding the technology roadmap, BlueVoyant is focusing on investing in unifying MDR, third-party risk monitoring, digital risk protection, and attack surface monitoring. Moreover, it will also invest in security content syndication of custom detection logic and cloud-native incident response.

Critical Start

URL: https://www.criticalstart.com

Company Introduction:

Founded in 2012 and headquartered in Plano, TX, Critical Start is a network security consulting firm. The company's MDR solution portfolio includes end-to-end Professional Services, Managed Detection and Response (MDR), and cyber security consulting services. Critical Start's MDR leverages a ZTAP platform with Trusted Behavior Registry (TBR), 24x7 human-led end-to-end monitoring, investigation and remediation of alerts, and on-the-go threat detection and response capabilities to prevent alert fatigue.

Product Introduction:

The Critical Start MDR service offers transparency by design using a Zero Trust Analytics Platform (ZTAP) that provides complete visibility as well as access to every alert with full investigation details as well as every action taken. All of it is auditable and reportable. Additionally, the Critical Start MDR service provides the user with visibility across the entire security ecosystem. This view provides the user with a better understanding of the security tools' performance, and the MDR services, which helps validate the ROI. Additionally, with contractual SLAs for Time to Detect (TTD) and Median Time to Resolution (MTTR), Critical Start states that it guarantees that it will triage every alert in minutes with a 1-hour SLA.

Technology Perspective:

Following is the analysis of Critical Start's capabilities in the global MDR market:

- Critical Start offers a robust MDR service titled Critical Start Managed Detection and Response Services. The service protects users from a wide range of threats across all endpoints. The service is integrated with industry leading EDR and SIEM technology to monitor every event, resolve every alarm, and respond to breaches in real-time. The MDR service auto-scales and auto-heals using AWS native tools and uses AWS services across

multiple regions to provide continuity. It also supports full multi-tenancy for larger organizations that need the separation of entities to focus on enhancing organizational security. Critical Start also provides Cyber Threat Intelligence (CTI) to better understand the threat landscape.

- The Critical Start MDR service also provides a two-person review process titled SCREVIEW that enables organizations to maintain the quality of playbook designation and alert investigation. The company also provides the Critical Start MOBILESOC app, which allows users to investigate, escalate, and remediate security incidents from iOS or Android devices. It also offers services that adapt to the unique differences of each customer. Additionally, its MDR services offer contractual investigation SLAs to ensure action is taken to isolate endpoints and stop attacks in progress with 1-hour Time to Detect and 1-hour Median Time to Resolution for every alert, regardless of priority.

- Critical Start's Security Operations Center (SOC) for MDR is a fully managed, cloud-based Security Operations Center (SOC) with a team of cyber security professionals providing 24x7 monitoring of the user's network environment. The SOC consists of L1, L2, and L3 analysts (including shift leads and tier 2-3 escalation/evaluation of alerts). Critical Start also provides a threat intelligence application that adds behavioral detections, additional Indicators of Compromise (IOCs), threat hunts, and correlation rules into the integrated security tools by combining internally created threat intelligence from previous SOC investigations, Red Team investigations, and external threat intelligence feeds (both paid and free). This combination enhances the efficacy of detection through profound threat intelligence, detection engineering, and aligning detections with the MITRE ATT&CK® Framework for better response.

- Critical Start SOC provides security event management, security orchestration, incident response and workflow, reporting, and fully operationalized and automated security controls. Organizations can leverage these services to create a customized security service that meets their specific business and technology requirements. Critical Start provides insights into the existing security stance through Quick Start Risk Assessments.

- Critical Start integrates with Microsoft Defender for Endpoint, Microsoft 365 Defender, Microsoft Sentinel, Trend Micro, CrowdStrike, Blackberry, VMware, Splunk, and Cortex's products as a part of its security technology integrations.

- Some of the key differentiators of the Critical Start MDR service include Zero Trust Analytic Platform (ZTAP) and Trusted Behavior Registry (TBR) to reduce false positives, MOBILESOC, providing customers with complete visibility into the services, service licensing agreements, security operations center, and application of threat intelligence. Users can collaborate with the analysts in near real-time from within their iOS and Android mobile apps and can review their analysis and corrective measures and take direct action immediately with the help of the information gathered in the platform to reduce attacker dwell time. The deployment options of Critical Start MDR service include endpoint, SIEM, and XDR.

Market Perspective:

- Critical Start has a strong presence in the USA. From the industry vertical perspective, Critical Start's primary verticals include manufacturing, retail, government, healthcare, financial services, energy, and education.

- From a use case perspective, Critical Start's primary use cases include cybersecurity performance management, cybersecurity risk management, rationalized cybersecurity spending, offloading security workloads, and security tool effectiveness.

CrowdStrike

URL: https://www.crowdstrike.com

Company Introduction:

Founded in 2011 and headquartered in Sunnyvale, CA, CrowdStrike is a global cybersecurity company offering cloud-native next-generation endpoint protection and services. CrowdStrike offers next-generation antivirus (AV), endpoint detection and response (EDR), and a 24/7 managed hunting service via a single lightweight agent. CrowdStrike offers its MDR services through its Falcon Complete platform, which allows organizations to detect and stop threats in real time.

Product Introduction:

The CrowdStrike Falcon Complete platform offers layers of expertise, which include security professionals for incident handling, incident response, forensics, SOC analysis, and IT administration with 24/7 coverage of network and endpoints. Additionally, the company possesses experts who provide advanced protection with native threat intelligence and proactive threat hunting and provides 24/7 human threat-hunting in near real-time. The ingestion of both native and third-party telemetry enhances customers' visibility across different domains and streamlines end-to-end remediation, offering a comprehensive and efficient approach to eradicating threats.

Technology Perspective:

Followings is the analysis of the CrowdStrike's capabilities in the Managed Detection & Response market:

- The CrowdStrike Falcon platform offers single lightweight-agent architecture and leverages cloud-scale artificial intelligence (AI), real-time protection and visibility, deep link analytics to deliver robust XDR, EDR, next-gen AV, device control, and firewall management across the enterprise to prevent attacks on endpoints and workloads on or off the network. Falcon Complete provides the technology, platform, actionable intelligence, and skilled expertise required to

provide a comprehensive endpoint security lifecycle solution that takes care of all aspects of endpoint security, which also includes remote remediation of incidents.

- Falcon Complete offers offloading Falcon endpoint protection to experienced CrowdStrike staff and assists organizations in deployment and configuration. Moreover, it also provides 24x7 alert and incident handling, as well as delivering proactive incident triage and containment that allows organizations to effectively handle incident remediation. CrowdStrike Falcon Complete ensures transparent management reporting and metrics. CrowdStrike provides threat hunting capabilities, including hypothesis-driven, behavioral, analytic, and adversary-based threat hunts that occur on a regular basis. Falcon Cloud Workload Protection safeguards organizational cloud-native stack on any cloud, whether it is private, public, or hybrid, across all workloads, containers, and Kubernetes applications. Falcon Cloud Workload Protection key integrations enable organizations to support continuous integration/continuous delivery (CI/CD) workflows which allows them to protect IT workloads at the speed of DevOps. Additionally, it allows organizations to customize these threat-hunting capabilities according to their needs.

- The platform offers fully cloud-native next-generation endpoint protection. The platform provides full visibility into every endpoint through propriety threat graphs. It also offers customers implementation, platform management, response and remediation services for advanced threats. It also offers fast protection of endpoints from threats while capturing and recording endpoint activities and transparent and secure collaboration between organizations and Falcon Complete team through the CrowdStrike message center.

- The platform's Falcon OverWatch team and CrowdStrike human threat detection engine also enable organizations to continuously monitor, discover, and prevent the most sophisticated hidden threats. CrowdStrike Falcon Complete leverages vast cloud-scale data and mines it in real-time to detect signs of intrusions. Additionally, it offers 24/7 active monitoring and response and investigates all critical, high, medium, and low-severity detections in a timely manner to ensure quicker intrusion discovery, di with an average time of fewer than 10 minutes to respond to threats.

- CrowdStrike, with its surgical remediation, can be combined with the Falcon platform's capabilities to help remove malware persistence mechanisms

surgically, halt active processes, and clear other latent artifacts. Falcon Complete returns systems to their pre-intrusion state without the cost and disruption of reimaging. With less than 60 minutes of remediation time, Falcon Complete can often perform remediation without the user being aware that it has happened. Additionally, the company offers executive dashboards which provide visibility into daily activities, including trends and actionable insights.

- From a differentiator point of view, CrowdStrike's incident response services help in threat detection, uniform customer experience because of the absence of tiered security operations model.

Market Perspective:

- From a geographical perspective, CrowdStrike has a strong presence in the US, followed by Canada, the UK, the Middle East, Turkey, Africa, Australia, and New Zealand. From the industry vertical perspective, the primary verticals for CrowdStrike include financial services, retail, public sector, hospitality, telecommunications, hospitality, retail, IT services, manufacturing, health, education, automotive, energy and utilities and transportation industries.

- From a use case perspective, CrowdStrike supports bridging visibility gaps through proactive threat hunting and enriched threat intelligence, optimizing slow operations through threat eradication, overcoming the skill shortage through its 24*7 SOC services, automated response, real-time protection and visibility.

eSentire

URL: https://www.esentire.com/

Company Introduction:

Founded in 2001 and headquartered in Waterloo, Canada, eSentire provides information security solutions that enable organizations to detect, investigate, and eliminate cyber threats before they harm their business. eSentire services mitigate business risk and enable security at scale by combining cutting-edge machine learning XDR technology, 24/7 threat hunting, and security operations leadership. eSentire's managed detection and response (MDR) services protect organizations' critical data and applications from known and unknown cyber threats. eSentire MDR service provides various key features & functionalities, including Atlas XDR cloud platform, multi-signal visibility, multi-signal response, eSentire's TRU team, and incident response.

Product Introduction:

eSentire offers MDR service through the Atlas XDR cloud platform that can investigate thousands of customers' data to identify common patterns of threat vectors and deliver a significant advantage over single company datasets. The platform can integrate with the client's existing technology stack, such as EDR, network security, email security, VPN providers, and web gateways, to provide continuous monitoring, proactive threat hunting, and multi-signal visibility. This visibility and threat-hunting capability helps provide full threat visibility with investigating capability and deeper correlation, strengthening the response and time-to-contain across networks, endpoints, logs, and insider threat attacks.

Technology Perspective:

Following is the analysis of eSentire's capabilities in the MDR market:

- eSentire offers a comprehensive MDR service that protects critical data and applications from known and unknown cyber threats. Additionally, eSentire offers 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 three availability zones to ensure uptime exceeding 90 percent. In addition, the company runs periodic stress tests that allow the platform to handle a large amount of data and request volume relative to the production payloads.

- eSentire MDR service's multi-signal response capability helps disrupt, isolate, and contain the threats in the network, endpoints, and identity levels before they impact business operations. The company also provides an eSentire Threat Response Unit (TRU) team that develops, or curates threat intelligence, analytics, and response methods being fed to the Atlas platform and shares the same with the customers. eSentire's end-to-end managed 24*7 SOC cyber analyst support helps reduce security gaps and resource constraints while minimizing and quantifying risks with managed risk, threat disruption and containment, digital forensics, and IR expertise.

- eSentire offers rapid incident response with the help of proven tools and processes, including digital forensics, remote access, investigation and response tools and techniques, visibility and remote triage for forensic analysis, evidence capture, and incident recovery across network servers and endpoint workstations. eSentire also offers end-to-end incident response lifecycle coverage to stop attackers and supports remediation and recovery that ensures root causes are fixed, and the chance for recurrence is eliminated.

- eSentire's Atlas XDR platform leverages patented AI and machine learning to automatically detect threats with signatures, Indicators of Compromise (IOC), and IP addresses. These detections are mapped to the MITRE ATT&CK framework. This mapping helps users respond to threats in real-time.

- eSentire provides the InSight Portal access, which offers real-time visualizations with operational reporting and peer coverage comparisons. This portal helps organizations improve their security strategy through competitor analysis and support in business reviews and continuous improvement planning.

- The key differentiators of eSentire include Atlas Extended Detection and Response (XDR) to analyze data from different customers to detect common patterns and provide huge advantages over a single company data set, Threat Response Unit (TRU) to provide threat intelligence, analytics, and response methods to the users, on-demand 24/7 incident response, operationalized

threat intelligence through the eSentire AMP service, and AI & ML-based applications such as Blue Steel and Malkara to detect malicious PowerShell activity and usual VPN connections at scale.

Market Perspective:

- Concerning geographical presence, eSentire has a strong presence in North America, Europe, the Middle East, Africa, and Asia-Pacific regions. From the industry vertical perspective, the primary verticals for eSentire include Banking and Financial Services, Healthcare and Lifesciences, IT and Telecom, Manufacturing, Energy & Utilities, Media & Entertainment, Travel & Hospitality, Retail & eCommerce, and Govt & Public Sectors.

- From a use case perspective, eSentire supports cost savings through security consolidation, ransomware prevention, third-party risk, increasing security coverage, improving threat visibility, faster threat detection and response, increasing operational efficiency, and sensitive data protection.

Fortra

URL: https://www.fortra.com/

Company Introduction:

Founded in 1982 and headquartered in Eden Prairie, MN, Fortra is the industry's first SaaS-enabled managed detection and response (MDR) provider. Fortra protects organizations and mitigates all kinds of cyber threats with the help of its purpose-built technology and a white-glove team of MDR security experts. Fortra acquired Alert Logic, a well-known leader in managed detection and response (MDR) services to strengthen its cybersecurity portfolio.

Product Introduction:

Fortra's Alert Logic MDR solution addresses threats detected in a pre-and post-breach environment to minimize the attacks' likelihood of attacks' recurrence and overall impact. This solution protects all the systems irrespective of where they are hosted. Fortra's Alert Logic MDR solution also provides critical context about the organization's risk regarding exposure and exploitation to allow for the most appropriate event response. Fortra security experts use industry data, continuous research from the Fortra threat intelligence team, and machine learning from aggregated data from thousands of customers in their global Security Operations Centers (SOC) to get better visibility into various types of threats for remediation in real-time.

Technology Perspective:

Following are the analysis of Fortra's capabilities in the managed detection & response (MDR) market:

- Fortra's Alert Logic MDR solution alerts and notifies users through telephone, Email, and API integration after the report and analysis are ready. It also provides internal and external vulnerability scanning, remediation activities, log collection and search, log data monitoring, web log analytics, file integrity monitoring, cloud configuration exposures, and compliance status. It also allows

users to focus on prioritized threats requiring additional triage, drill down into threats to act on or mitigate exposure and provide intuitive risk visualization. Fortra MDR's Intelligent Response™ capability leverages embedded SOAR capabilities with workflows, which enables them to execute response actions across networks, endpoints, and cloud environments to allow organizations to reduce the impact of a cybersecurity breach.

- Fortra also provides an MDR concierge, who is a single point of contact and an expert in the delivery of Fortra's MDR solution and understands each customer's business needs to provide the best possible service and security. The Fortra MDR solution also provides a designated security expert at the Fortra Security Operations Center (SOC). This expert provides personalized protection and customized incident response plans. Fortra offers the flexibility to select the most appropriate level of protection for any asset, ensuring that users have the necessary coverage and achieve the desired security outcome at an optimum cost.

- Fortra's MDR platform is suitable for any cloud environment, web applications, network, system, endpoints, and compliance requirements, thus managing the organization's security posture. Fortra's Managed Detection and Response (MDR) platform provides the adaptability needed for an integrated infrastructure, ensuring security and compliance throughout the user's environment. It also provides threat management, security monitoring, web application firewall, network intrusion detection system (IDS), vulnerability scanning and assessment, and log management. It also provides AWS user behavior anomaly detection, AWS outpost management, and extended endpoint protection in hybrid environments.

- Fortra delivers white-glove managed detection and response (MDR) with comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Fortra's proprietary MDR platform collects data from network traffic and billions of log messages every day to provide outcome-based security. It analyses the collected data by leveraging correlational and behavioral analytics technologies to gain insights that help provide 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. Fortra has formed a strategic partnership with TD SYNNEX to strengthen its incident response capabilities and improve its clients' cybersecurity postures.

- Some of the unique features offered by Fortra MDR solution include cloud-based security expertise, intelligent response, white-glove customer experience, comprehensive coverage, and 24/7 threat detection & management with global SOC experts. Additionally, it offers a 15-minute escalation SLA, emerging threat response, on-demand tuning & sensor optimization, and extended security investigations.

Market Perspective:

- From a geographical perspective, Fortra has a presence in North America, Latin America, Europe, and Asia-Pacific regions. From an industry vertical perspective, the primary verticals for Fortra include healthcare and life sciences, advertising/media, hospitality, transportation, technology, consulting, manufacturing, banking & financial services, e-commerce, and retail.

- From a use case perspective, Fortra's primary use cases include log management and analysis, network threat detection, web application security, 24*7 human-led threat protection, cloud security, compliance, and vulnerability management.

Group-IB

URL: https://www.group-ib.com/

Company Introduction:

Founded in 2003 and headquartered in Singapore, Group-IB provides cybersecurity products aimed at countering cyberattacks, eradicating fraud, and protecting its clients. Group-IB offers a portfolio of services that include enterprise email security, managed detection and response, ransomware protection and response, phishing protection and response, bot protection. Group-IB is also a member of the European Cybercrime Centre's Advisory group.

Product Introduction:

Group-IB's MDR solution provides comprehensive visibility into network environments by collaborating with the user's current technological stack to find and profile assets, as well as collecting data and security event observations from a variety of sources. Additionally, the solution allows organizations to monitor networks, endpoints, and cloud environments 24/7 and helps detect sophisticated threats. Group-IB MDR service delivers proactive threat hunting and remote forensic analysis for increased efficiency and scale by integrating machine learning with adaptive tuning. Group-IB claims to provide threat containment in 15 minutes and an initial report in 24 hours. They also claim to have more than 55 certified analysts and that 95 percent of the alerts are analyzed within 60 minutes.

Technology Perspective:

Following is the analysis of Group-IB's capabilities in the global Managed Detection and Response market.

- The Group-IB MDR solution offers a comprehensive technology suite that spans email security, endpoint protection, network traffic analysis, and sandboxing solutions. This integrated stack simplifies the process of incorporating and implementing these security measures.

- The Group-IB MDR solution offers a diverse range of human security experts that are available 24*7. These experts include Incident Responders, Security Analysts, Security Operations Center (SOC) Consultants, Threat Hunters, Investigators, Forensic Analysts, Malware Analysts, Penetration Testers, Red Teamers, Fraud Analysts, Threat Intelligence Analysts, Security Auditors, and numerous other professionals. This extensive team plays a crucial role in safeguarding user data confidentiality. assisting users in assessing and pinpointing significant alerts and offering practical guidance about responding to pertinent threats. These global specialists aid in swiftly stopping attacks, reducing the time needed to recover, and safeguarding an organization's infrastructure, network, and data. This threat response process includes identifying, containing, and eliminating threats.

- Group-IB's managed threat hunting takes a proactive approach to identifying unfamiliar threats, advanced attacks, and APTs. The company's expert threat hunters use XDR alerts as a basis for investigating hypotheses. This capability serves to both safeguard the users' system against threats and gather valuable threat-related information.

- Group-IB MDR operates its own SOC, which encompasses a wide range of Managed Services including 24x7 Managed Detection, Managed Response, and Managed Threat Hunting. This SOC is also certified as a Computer Emergency Response Team (CERT) and plays a pivotal role in supporting all of Group IB's cybersecurity activities.

- Group-IB MDR's key differentiators include Digital Forensics, eDiscovery, and incident response services as a bundle. This bundling of MDR and DFIR services provides users with holistic and enhanced security.

Market Perspective:

- Group-IB has a presence in APAC, EMEA, LATAM regions. From an industry vertical perspective, primary verticals for Group-IB include E-commerce, BFSI, Entertainment, Food and Beverages, Gaming, Govt and Public sector, Healthcare, Manufacturing, Transportation and Media, Retail, Telecommunication.

- From a use case perspective, Group IB supports managed detection, managed threat hunting and investigation, case management and incident response, threat intelligence and Security analytics and reporting.

Roadmap:

- As a part of the technology roadmap, Group-IB plans to upgrade its EDR services by introducing local network scanners for network inventory. The company also plans to upgrade its email security solution by introducing time-of-click URL analysis, computer vision for URL analysis, employee inventory and risk index. For its network traffic analyzer, Group IB plans to introduce built-in attack surface management, and detection of unusual behavior for the remote workforce.

Kudelski Security

URL: https://kudelskisecurity.com/

Company Introduction:

Founded in 2012 and headquartered in Switzerland, Kudelski Security, a division of the Kudelski Group, provides security solutions and managed services to ensure technology stack optimization and robust organizational security posture management. Kudelski Security provides advisory teams for security, security technology optimization, managed security, managed detection and response (MDR), advisory on emerging security technology, and incident response.

Product Introduction:

Kudelski Security offers an advanced MDR service called MDR One Resolute. The service is based on its FusionDetect™ XDR platform, which incorporates a comprehensive stack of security solutions alongside artificial intelligence and an advanced analytics tool for threat detection and quick response. MDR One Resolute offers various features, including high-density threat data collection and retention, advanced analytics for threat detection, integration with MITRE ATT&CK framework for deep threat hunting and identification of blind spots, AI-driven incident management and response, and resilience guidance for security posture management. This comprehensive set of security tools enables full-stack threat detection, faster threat response, and a high-density knowledge pool. MDR One Resolute also offers guidance on building resilience with an emphasis on continuous improvement, empowering the user to be more proactive and regain control.

Technology Perspective:

Following is the analysis of Kudelski Security's capabilities in the global Managed Detection and Response (MDR) Market:

- MDR One Resolute offers a high-performance data lake that allows for ingestion and retention of large quantities of data. Kudelski Security also offers advanced analytics along with the hot data lake, which allows users

to perform historical event analysis and longitudinal analysis to gain deep insights into the threats and their attributes for improved threat response and data prevention. Kudelski security's large data retention policy enables users to manage large quantities of data without additional storage costs. This feature provides the user organization with unlimited raw data telemetry, better scalability, and reduced time in onboarding and tuning to meet the organizational requirements.

- MDR One Resolute provides risk-based threat detection, hunting, and investigation features, which analyzes threats through its priority-based risk score, context-based attack stories, and human-led threat hunting. The threat detection engine leverages its expert-led hunting capability to enable faster threat detection and response, resulting in the reduction of mean time to identify and resolve threats across the entire IT stack. This feature allows the analysts to enrich the context regarding the threats and improve their threat intelligence, enabling faster correlation with attack stories to detect and respond to threats. MDR One Resolute enables accelerated response through its integrated SOAR platform. Through its risk prioritization algorithm, it provides a faster and guided incident response. This reduced the mean time to response (MTTR), thus improving the effectiveness of the service.

- Analysts and threat hunters at Kudelski's Cyber Fusion Center (CFC) employ Fusion Detect for the triage, investigation, and identification of threats and breaches. This threat hunting provides proactive security. MDR One Resolute also provides threat exposure management which improves the organization's cyber resilience.

- MDR One Resolute provides a threat navigator feature, which leverages MITRE ATT&CK framework to provide enhanced visibility, allows identification of gaps and blind spots that are susceptible to threats, and offers methods to collect data for faster detection. This feature allows for deep inspection and threat hunting to improve the overall security posture of the organization and comply with standard requirements.

- MDR One Resolute allows users to have visibility and transparency into the threat management landscape. This transparency and visibility allow users to gain insights regarding the threat management, attack stories, and threat analysis performed. Also, Kudelski Security provides users with access to the FusionDetect XDR platform, allowing them to run queries, manage data sources, perform deep analysis, and perform threat hunting.

- Kudelski Security offers an intuitive client portal with 24/7 access to dashboards, reports, security trends, incidents and their responses, benchmarks for security posture, and guidance to security resilience. Also, it offers resiliency guidance, which allows users to minimize vulnerabilities and rectify misconfigurations to avert potential future security breaches.

- MDR One Resolute offers high-quality incident escalation, which leverages AI to perform deep investigations through risk scoring and prioritization. This feature escalates incidents based on priority and provides actionable insights and steps for remediation through its detailed investigation and analysis.

- MDR One Resolute leverages real-time threat intelligence with its Fusion Detect™ XDR platform which adapts detection rules dynamically, thus optimizing analyst focus and driving immediate security gains.

- Kudelski Security differentiates through its unlimited data ingestion, visibility into threat management operations, hot data lakes for longitudinal analysis, and enhanced client collaboration features. These features allow for reduced storage cost of data, transparency, real-time understanding of the threat aversions, and improved security resilience.

Market Perspective:

- From a geographical presence perspective, Kudelski Security has a presence in North America, Europe, and Asia-Pacific regions. From an industry vertical perspective, the primary verticals for Kudelski Security include financial services, government, manufacturing, healthcare, energy and utilities, retail, software, and internet services.

- From a use case perspective, Kudelski Security's primary use cases include improved cybersecurity strategies, faster threat detection and response, secured cloud journey, reduced response time, secured Microsoft 365 modern workplace, reduced attack surface, secure OT-ICS networks, secure IOT ecosystems, and blockchain security.

Proficio

URL: https://www.proficio.com/

Company Introduction:

Founded in 2010 and headquartered in Carlsbad, CA, Proficio is a Managed Security Services Provider (MSSP) offering 24×7 security monitoring and advanced data breach prevention services to organizational IT systems at the global level.

Product Introduction:

Proficio offers an automated Managed Detection and Response (MDR) service titled "PROSOC MDR," which rapidly detects Indicators of Compromise (IOC) to fight against intruded cyber threats. The ProSOC MDR includes comprehensive capabilities like Integrated Threat Intelligence, artificial intelligence (AI)-based threat hunting, MITRE ATT&CK framework, expert investigations and guided remediation, Managed Endpoint Detection and Response, automated and semi-automated containment, risk-based vulnerability management, and insight to security posture and risk.

Technology Perspective:

Following is the analysis of Proficio's capabilities in the global Managed Detection and Response (MDR) market:

- Proficio offers MDR services through its solution titled "ProSOC MDR." The services strengthen the user's internal security and help organizational SOC teams safeguard their IT systems against various types of threats. Proficio ProSOC MDR leverages AI and Multi-Vector threat detection analytics, threat intelligence platform integration, and machine-driven analyst verified threat hunting, to allow user organizations to detect threats. Additionally, Proficio ProSOC MDR offers the ProView security management portal, which delivers real-time visibility into IT infrastructure, incident case management, security

gap assessment for vulnerability management and scorecard and peer comparison to better understand the threat landscape.

- Proficio "ProSOC MDR" offers cloud solutions that imbibe capabilities like infrastructure monitoring, CloudTrail integration, GuardDuty monitoring, office 365 monitoring, managed security services, support for GCP projects, and many others. It offers threat intelligence profiler to the organization, which consists of real time threat intel database for providing standard threat feeds, premium feeds, Proficio threat research, and client logs. Additionally, Managed Detection and Response (MDR) vendors provide log management, use case library, threat intelligence, threat analyst investigation, actionable incident alerting, case management, active defense response, and ProView portal.

- Proficio ProSOC MDR also offers an enhanced threat intelligence and discovery feature that enhances the user's understanding of IT activities and identifies and defends assets against cyber threats. The feature allows organizations to integrate security use cases and threat intelligence data to examine security events through data correlation from vital log sources. Moreover, it empowers security analysts to scrutinize unusual user behavior by utilizing the MITRE ATT&CK framework and employing AI-based threat models for proactive cyber threat hunting. Proficio's Managed EDR utilizes a comprehensive technology stack to continuously monitor endpoints and search for threat attack methods aligned with the MITRE ATT&CK framework. Proficio MDR utilizes a variety of tools that include industry-leading threat feeds and compliance monitoring to remediate cyber threats. Proficio ProSOC MDR enables threat Intelligence teams to constantly monitor the threat landscape to detect new cyberattacks, critical vulnerabilities, and the behavior of cybercriminals and other adversaries.

- Proficio ProSOC MDR provides a managed endpoint detection and response (MEDR) solution that allows organizations to minimize risks through continuous monitoring of crucial endpoints. Proficio's MEDR service enables real-time risk detection through features such as device audits, analyst investigations, and automated response capabilities for swift identification of cyber threats. Proficio MEDR allows organizations to monitor security and ticket status in real-time through its ProView portal. The portal also provides recommended remediations for cybersecurity threats. Additionally, Proficio PROSOC MDR's risk-based vulnerability management capability allows organizations to prioritize vulnerabilities based on exploitable risks. Proficio PROSOC MDR provides automated response technology that enables organizations to orchestrate responses to security incidents.

Market Perspective:

- From the geographical presence perspective, Proficio has a strong presence in North America, particularly the USA, followed by APAC and EMEA. From an industry perspective, the company has a presence across a wide variety of industry verticals, including BFSI, eCommerce, entertainment, food and beverages, govt and public sector, healthcare, manufacturing, transportation, media, retail, and legal services.

- From a use case perspective, the company's primary use cases include breach preparation, attack detection, alert validation and triage, incident response, attack isolation, threat hunting, and threat remediation.

Challenges:

- The primary challenges for Proficio include the competition in the MDR market from well-established vendors. Additionally, as a part of company expansions, the company may face competition from big vendors while tapping new markets. However, with its comprehensive functional capabilities like artificial intelligence (AI)-based threat hunting, MITRE ATT&CK framework, risk-based vulnerability management, and an excellent customer value proposition, the company is well-positioned to maintain and grow its share in the MDR market.

Roadmap:

- Regarding its technology roadmap, Proficio is focusing on enhancing its updates to both its core SIEM platform and on-prem virtual machines. It also plans on continuing the development of SOAR capabilities and machine learning. As a part of its strategic roadmap, the company plans to enhance ease of use and accessibility for its MDR platform experience, delivering security and expertise through complete and well-defined alerting.

Rapid7

URL: https://www.rapid7.com

Company Introduction:

Founded in 2000 and headquartered in Boston, MA, Rapid7 provides a security operations platform that delivers cloud-native extended detection and response (XDR) capabilities, characterized by a superior signal-to-noise ratio, early threat detection, and expedited response measures. The company excels in recognizing advanced threats, preempting attackers before they initiate attacks, and bolstering organizational security through its Managed Detection and Response (MDR) Services and Solutions.

Product Introduction:

Rapid7's MDR solution employs advanced methods, including proprietary threat intelligence, behavioral analytics, Network Traffic Analysis, and human-led threat hunting to detect threats and swiftly stop attacks in real-time. This solution is designed to not only stop ongoing attacks but also promptly contain threats targeting users and endpoints while speeding up the improvement of overall security programs. The solution includes a dedicated security advisor, 24*7 Security Operations Center (SOC) monitoring, real-time incident detection and validation, immediate response actions, access to Rapid7's threat intelligence and research, proactive threat hunting, full utilization of InsightIDR and cloud SIEM, behavioral analytics, network traffic detection, incident management and response support, zero data costs, and unrestricted event source integration.

Technology Perspective:

Following is the analysis of Rapid7's capabilities in the managed detection & response (MDR) market:

- Rapid7 MDR solution and service provides a comprehensive product that combines hands-on 24/7 monitoring, proactive threat hunting, effective response support, targeted security guidance, and a team of active response

professionals to stop malicious activities and help enterprises accelerate their security maturity. Additionally, it offers 24/7 end-to-end detection and response with three layers of analysts for full coverage and near-zero false positive rates. Rapid7 MDR helps organizations minimize false positives to enable their internal security teams and SOC teams to achieve faster MTTD (Mean time to detect or discover) and MTTR (mean time to recovery or mean time to restore). The Rapid7 MDR Solution & Service leverages machine learning to provide real-time event correlations at scale and provide visibility into on-prem and cloud environments.

- Rapid7's MDR solution is designed as a multi-layered approach, incorporating proprietary threat intelligence and research, as well as utilizing a cloud-based SIEM titled InsightIDR for analyzing network and endpoint data to uncover potential threats. This approach encompasses a well-defined threat detection methodology, the operations of the Rapid7 SOC, incident investigation, and active response, all provided as part of a 24/7 end-to-end MDR service. Additionally, it includes a program for advancing threat detection and response capabilities. Within the Rapid7 MDR solution, detection methodologies encompass proactive threat hunting, which involves using Insight Agent data and specialized views to conduct both scheduled and ad-hoc threat hunts across the organizational environment. This approach ensures real-time identification of unusual running processes, risky user behavior, and malicious activities, granting users comprehensive visibility across their network, even extending to remote workers and cloud services. The Rapid7 SOC relies on User Behavior Analytics (UBA) indicators to dynamically prioritize and assess alert criticality based on the presence or absence of notable behaviors.

- Rapid7 MDR services and solution leverages a unique set of threat detection methodologies, including 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 to enable better security. Rapid7 MDR services include security guidance, incident analysis, and remote incident response. Additionally, it offers tailored services based on the requirements of customers and security advisors for security maturation.

- Rapid7's Managed Threat Complete platform offers unlimited incident response with Digital Forensics and Incident Response (DFIR) professional service as part of its core MDR. The platform offers customers unrestricted access to its cloud-native XDR technology and extensive threat detection

library. This access enables users to gain clear visibility into the activities of their Rapid7 MDR partners.

- Rapid7 MDR offers Security Orchestration Automation and Response (SOAR) for better automation and accelerated DFIR as add-ons to its MDR product.

- Rapid7's MDR solution takes advantage of distinctive threat intelligence derived from research, past investigations, monitoring outcomes, and external sources. The MDR Threat Intelligence team manages this intelligence and works closely with SOC analysts to ensure its consistent application across all MDR customer environments.

Market Perspective:

- From a geographical presence perspective, Rapid7 has a strong presence in North America, particularly the US and Canada, followed by Europe and Asia-Pacific. From an industry vertical perspective, the primary verticals for Rapid7 include healthcare, manufacturing, technology, finance, communications, media, education, services, real estate, retail, transportation, government, and hospitality.

- From a use case perspective, Rapid7 supports total threat coverage, accelerated program maturity, faster threat detection, unlimited incident response, 24*7*365 SOC, endpoint protection, and alert fatigue minimization.

Challenges:

- Rapid7's primary challenges include the growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to mid-market organizations and are among the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Rapid7 is well-positioned to maintain and grow its market share in the MDR market.

Red Canary

URL: https://redcanary.com

Company Introduction:

Founded in 2013 and headquartered in Denver, CO, Red Canary is a provider of cloud-based security services. The company's products enable organizations to work smoothly without the fear of cyberattacks. Red Canary offers outcome-focused solutions for security operations teams and helps to analyze and respond to enterprise telemetry, manage alerts across the network, and provide cloud environment runtime threat detection. Red Canary offers its MDR solution with its MDR for endpoints and MDR for infrastructure.

Product Introduction:

Red Canary MDR for endpoints offers 24/7 detection, investigation, and remediation capabilities like expanded visibility, which analyzes all endpoint telemetry and alarms through its cloud-based detection engine, which is made up of hundreds of behavioral analytic use cases. Red Canary MDR offers advanced detection through its comprehensive security operations platform, which covers all attack techniques and analyzes potential threats.

Technology Perspective:

Following is the analysis of the Red Canary's capabilities in the Managed Detection & Response market:

- Red Canary MDR for endpoints provides a quick response to the confirmed threats and provides a detailed threat report with customized automated response actions. Red Canary also offers a dedicated ally for security consulting and incident response (IR) support when they need it. Red Canary MDR leverages propriety detection, analytics, and automation technology to help organizations eliminate evolving threats. Additionally, it offers robust protection within minutes, automation-as-a-service to boost incident response and reduce mean time to respond (MTTR) and addresses real threats with its

cyber incident response team (CIRT). Its built-in automation and orchestration of playbooks allow users to automate the incoming threat resolutions and notify the respective teams immediately. Red Canary MDR for endpoints offers features like cross-platform integration, expert response engineers, and threat research.

- Red Canary MDR for Infrastructure extends MDR to the users' on-premises and cloud infrastructure with deep Linux threat detection expertise and experience. The MDR also protects the Linux environment from threats through modern, purpose-built infrastructure optimized for Linux. It also provides security measures such as Linux first detection during runtime and runtime threat detection through continuous monitoring and collection, as well as behavioral-based analysis mapped to MITRE ATT&CK.

- Red Canary MDR offers dashboarding and reporting features that allow users to gain a better understanding of the threat landscape. This feature allows users to gain data-driven insights into the security posture and performance metrics such as Mean Time To Respond (MTTR) and Return On Investment (ROI), thus providing improved transparency.

- Red Canary MDR solutions offer security expertise and technology to detect, investigate, and remediate threats in real-time. Red Canary offers 24/7 monitoring, added capacity, and expertise according to organizations' needs. Red Canary MDR allows the processing of raw telemetry from big cybersecurity companies to enable organizations to implement in-house analytics into their IT system for effective and quick identification of existing and potential cyber threats. Additionally, it provides a threat intelligence team that hunts globally for adversaries.

- Red Canary MDR also provides adversary intelligence that offers insights into the threat actor's operational patterns and methods of operation. This information aids the users in comprehending the strategies employed by adversaries and equips them with the knowledge needed to effectively detect and counteract them. It also provides expanded and evolved detection, consultation on security strategies and allows organizations to investigate every threat, reduce false positives, automate response actions, and improve organizational security measures. It also provides personalized explanations with conclusions following the confirmation of a threat or the elimination of a false positive.

- 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. Additionally, the solution includes proactive guidance on security architecture, engineering, or overall strategy. Additionally, Red Canary MDR integrates with Microsoft Defender for Endpoint (MDE), which allows organizations to stop cyber threats across endpoints, identity, and email threats across organizations and the Microsoft ecosystem.

- Some of the features of MDR for infrastructure include complete visibility and support across cloud and on-premises infrastructure, efficiency, safety, and performance while ensuring minimal resource impact, proactive performance monitoring, and easy deployment. Red Canary MDR's key differentiators include better threat detection and customer support.

Market Perspective:

- Regarding geographical presence, Red Canary has a presence in the U.S. From the industry vertical perspective, the primary verticals for Red Canary include healthcare and life sciences, education, banking & financial services, and retail.

- From a use case perspective, Red Canary supports zero-day attack protection, lower MTTR, 24/7 human-led threat monitoring, personalized reporting with insights through documents and dashboards, better protection across endpoints, proactive performance monitoring, and regulatory compliance.

Secureworks

URL: https://www.secureworks.com

Company Introduction:

Founded in 1999 and headquartered in Atlanta, GA, Secureworks offers a unique combination of a cloud-native, SaaS-based security platform and an intelligence-driven security solution with threat intelligence and research. The company offers Taegis ManagedXDR, an MDR service delivered on their extended detection and response platform, Taegis XDR.

Product Introduction:

The Taegis ManagedXDR solution offers intelligent XDR that provides organizations with deep cyber security expertise to protect against suspicious activities and threats in realtime. The solution provides proactive threat hunting and unlimited incident response, to prevent threat breakouts. Secureworks Taegis ManagedXDR solution also offers an easy-to-use user interface that allows organizations to easily investigate suspicious events, share data between their teams, and chat with Secureworks specialists in real-time to reduce mean time to resolution.

Technology Perspective:

Followings are the analysis of Secureworks' capabilities in the global Managed Detection & Response market:

- Secureworks offers comprehensive MDR services via Taegis ManagedXDR delivered on top of its Extended Detection and Response platform, Taegis XDR. The services allow users to detect, hunt, and respond to advanced threats across endpoints, networks, and cloud environments. Additionally, the platform also offers softwaredriven detection speed & precision, diverse threat data and research, proactive threat hunting, and full support of incident response.

- Taegis ManagedXDR provides experienced security operations, partnered

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

- Taegis ManagedXDR offers two response configurations: Proactive Response Actions (PRAs) and Authorized Response Actions. PRAs allow Secureworks pre-authorization to initiate predetermined and configured containment and mitigation actions through Taegis. This proactive approach reduces risk by enabling Secureworks analysts to take immediate response actions against threats with a single mouse click. On the other hand, Authorized Response Actions involve consulting with customers before implementing any response. Larger customers with their own 24x7 teams may prefer this latter approach, which allows them to collaborate with Secureworks and conduct their own Level 2 analysis. Secureworks takes customer preferences into account to provide tailored response recommendations in investigation findings. The company enables communication with analysts through in-app chat and phone, ensuring prompt execution of authorized response actions. Customers can also execute response actions directly from the Taegis console.

- Secureworks provides “Unlimited Response,” where the Incident Response team collaborates with the customer to comprehend and contain the threat throughout the environment, regardless of the time required. Additionally, Taegis ManagedXDR offers services such as remediation, recovery, ransomware negotiation, on-site support, and privileged engagement for a comprehensive response to incidents.

- The Taegis platform can integrate data from organizations’ existing security tools and leverage an analytics engine and threat intelligence for detection of known and unknown threats. It also provides analysis mapped to the MITRE ATT&CK framework to provide robust detection and integrated response, which helps improve the organizations’ security posture. The Taegis platform also offers` behavioral threat analytics, which is combined with machine learning and deep learning trained by using proprietary threat intelligence and customer data. The platform includes built-in detection based on use cases, simple investigative workflows, and automated containment actions.

- Taegis detections work across the customers' IT and OT endpoint, network, cloud, and business system environments. Secureworks provides 24*7 threat monitoring supported by a team of security experts. The Secureworks MDR team consists of security analysts, threat hunters, threat researchers, threat engagement managers, security engineers, and incident responders working together to deliver a comprehensive MDR experience to customers.

Market Perspective:

- Regarding geographical presence, Secureworks has a strong presence in North America, particularly the USA, followed by Europe and Australia. From the industry vertical perspective, the primary verticals for Secureworks include BFSI, professional services, manufacturing, SLED, technology, retail, and utility industries.

- From a use case perspective, Secureworks provides risk reduction and third-party compliance, 24*7 human-led protection with security expertise, holistic threat monitoring, detection, and response across IT and OT environments, maximized value from existing technology investments such as Microsoft and other third-party vendors.

Challenges:

- Secureworks' primary challenges mainly include the growing competition from emerging vendors with innovative technology offerings. These vendors are successful in gaining a strong market position with increased penetration amongst small to midmarket organizations and are among the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and customer value proposition, Secureworks is well-positioned to maintain and grow its market share in the Managed Detection and Response market.

Roadmap:

- As a part of its technology roadmap, Secureworks plans to expand security coverage through additional event types, event sources, & connectors along with meaningful technology alliance partners. It also plans to continue innovation on its OT-based offering with new integrations, detections, response actions, and incident readiness capabilities. Additionally, the company plans to build on its out-of-the-box report capabilities with additional broad and business-level reporting. The company also plans to launch a new Risk & Exposure Management-based service offering to complement MDR and help customers reduce risk and improve their security posture.

SentinelOne

URL: https://www.sentinelone.com/

Company Introduction:

Founded in 2013 and headquartered in Mountain View, CA, SentinelOne provides cybersecurity products that detect, prevent, and respond to attacks across endpoints, data centers, and cloud environments. SentinelOne offers its MDR services through its AI-based solution titled SentinelOne Vigilance Respond, which provides 24*7 threat detection and response.

Product Introduction:

The Vigilance Respond offers 24/7 MDR and Digital Forensics and Incident Response (DFIR) service through security analysts and response preparation. The solution helps organizations reduce the mean time to detect and respond. The company also provides SOC team augmentation that offloads day-to-day operationalization and threat hunting to SentinelOne's MDR experts to help the organizations focus on more critical functions. Vigilance Respond also provides threat-hunting through its WatchTower services to fight against attacker techniques and dangerous cyber threats. The service consists of two tiers. WatchTower offers hypothesis-based behavioral threat hunting, analysis, and containment to optimize the security posture of the organization. WatchTower Pro offers customized threat hunting, compromise assessments, and premium hunting support.

Technology Perspective:

Following is the analysis of SentinelOne's capabilities in the Managed Detection & Response (MDR) market:

- SentinelOne offers a comprehensive AI-based titled Vigilance Respond to detect, respond, prevent, and remediate threats in real time. The solution's AI-based Vigilance Respond detects emerging threats, which helps user organizations detect cyber incidents, supply chain attacks, major zero-day vulnerabilities, and other emergent threats.

- The Vigilance Respond also provides access to analysts to perform deep dives into threats and incidents post-classification. The Threat Insight feature interprets these console incidents, ensuring user awareness. Vigilance automatically mitigates and resolves threats, initiating proactive escalation when necessary.

- SentinelOne Vigilance Respond also offers an Incident Response Retainer that assigns IR case managers that allow organizations to investigate cyber incidents, followed by actively containing and eradicating cyber threats, then reporting the incident to the IT systems. Vigilance Respond helps reduce alerts by adding a human context to Storyline™ technology to save time spent on aggregating, correlating, and contextualizing alerts. SentinelOne analysts triage and prioritize events based on unique user requirements, acting as an extension to the user's security team. Additionally, it provides documentation and reporting regarding every identified threat in the environment and incorporates it as a part of ongoing reporting.

- Vigilance Respond also offers DFIR that enables incident lifecycle management. The company also offers security consultations. Sentinel One Vigilance Respond leverages AI to help security analysts detect, prioritize, and triage threats. This service allows analysts to perform forensic investigations, root cause analysis, malware reverse engineering, and threat hunting. Vigilance Response Pro leverages analysis and technology, including RCA for infection vectors, exfiltration & breach determination, incident-driven threat hunting, threat intel enrichment & contextualization, malware reversing, memory analysis, and malicious code de-obfuscation to offer insights from a comprehensive investigation of threats.

- Sentinel Vigilance Respond also provides proactive IR preparation with IR assessment, which helps organizations evaluate their ability to respond to breaches, identify evidence sources in their environment, create emergency response plans, and provide On-Call IR. Vigilance Response also offers tailored reporting and guidance to organizations for long-term success.

- SentinelOne offers its MDR service with 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 additionally provides

intel-driven hunting, digital forensics & malware reversing, containment & eradication, faster SLA, root cause analysis, and postmortem consultation. Vigilance Respond also offers direct access to forensic experts for incident management and offers IR retainer hours for malcode analysis and IR. Additionally, SentinelOne Vigilance Respond helps organizations extend their threat monitoring, detection, and response capabilities across all their IT operations.

Market Perspective:

- Regarding geographical presence, SentinelOne has a strong presence in the USA. From an industry vertical perspective, the primary verticals for SentinelOne include services, agriculture, media and entertainment, education, transportation, non-profit, energy, fintech, government, hospitality, automotive and healthcare industries.

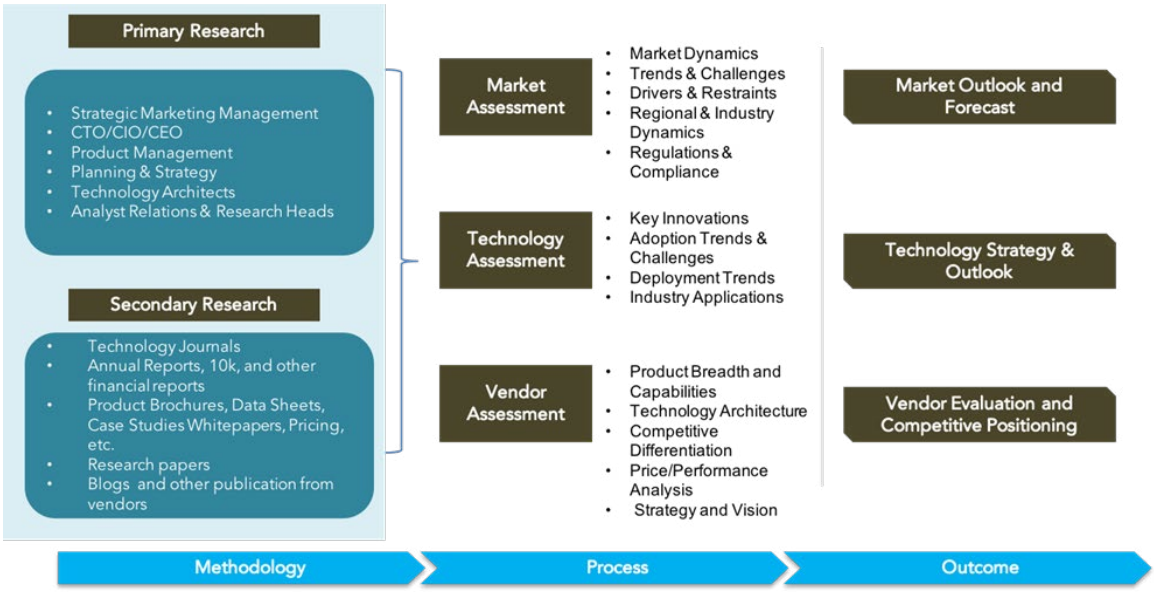
- From a use case perspective, SentinelOne supports 24*7 human-led detection, hypothesis-driven threat hunting, organized threat intelligence, robust reporting through dashboards, incident lifecycle management, real-time analytics, faster SLA, and threat containment.

Roadmap:

- As a part of its technology roadmap, SentinelOne plans to launch Mandiant's threat intelligence in its Singularity platform through partnership. This addition will help to improve SentinelOne's threat intelligence, which facilitates proactive monitoring of emerging threats in nearly real-time, allowing organizations to minimize risk promptly and swiftly identify adversaries within their operational space.

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
- 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.

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.

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 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.

Final Report Preparation

After finalization of market analysis, 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 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

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com