Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Managed Security Services (MSS), Q4 2022

Market Insights, Competitive Evaluation, and Vendor Rankings

December 2022

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of global Managed Security Services market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading managed security service providers in the form of SPARK Matrix™. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors capabilities, competitive differentiation, and its market position.

Market Dynamics and Overview

Organizations are increasingly moving to SaaS-based cloud environments owing to the popularity of cloud services and rapid digital transformation in the market. This has driven the need for Managed Security Services (MSS) to enhance the security management services within an organization. Organizations select MSS because of the increasing risk posture of cybersecurity and rigorous government regulations. Emerging cloud technologies in the IT domain have led organizations to use various services, including malware as a service, storage as a service, and database as a service, which offer benefits in terms of high scalability, availability, and resource sharing along with maintaining the balance between benefits & security threats and challenges in the adoption of cloud technology. MSS platforms emphasizing security operations make it easy for an organization to ensure an effective balance between the adoption of cloud technologies and security concerns.

Usually, MSS offers 24/7 monitoring of security technology with threat response capabilities by integrating it with a central log management tool, such as security information and event monitoring (SIEM). However, with technological advancements, vendors are offering managed services that can independently run on an endpoint detection and response (EDR) platform and network detection and response (NDR) without integrating with SIEM. Additionally, MSS vendors compete with managed detection and response (MDR) providers by offering capabilities such as security assessment, vulnerability management, and log management to deliver enhanced supporting services, including the MDR solution in its marketplace for customers.

MDR helps organizations to detect threats, incidents, and events that may occur in the future, protect critical data from unauthorized users, and control all mobile devices across an organization, which helps organizations implement coverage and control measures for maximum uptime and minimum disruption. It also offers insights to respond to those threats effectively by providing visibility and context in delivering and maintaining services while alerting customers, thus reducing organizational security risks.

Most large organizations utilize MSS services to maintain their complex technology environments with both customized and standardized offerings. MSS also provides flexibility to use the existing security technology by integrating it with

other advanced monitoring and management technologies, reduce deployment time, and deliver full operational capabilities.

Quadrant Knowledge Solution's definition for MSS is as follows:

"Managed Security Services provide organizations with continuous monitoring of security assets and systems, which enables security and risk managers to respond to security events by identifying, advising, responding, and providing remedial action to protect devices from threats, exposures, and other vulnerabilities occurring in the IT environment.".

Following are the key capabilities of EFM a Managed Security Service Provider:

- **Managed Detection and Response:** MSS vendors offer integrated MDR services built into their own detection and response operations rather than outsourcing these services. The service enables users to gain faster threat defense across endpoints, networks, hardware systems, applications, OT/IoT, and enterprise assets. MDR also integrates with SIEM, AI/ML tools, and big data analytics. Moreover, it also 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. Additionally, incident response services enable organizations to identify the incident in real time through strongly encrypted authenticated access to the portal. Soon after, the incident response service alerts the incident handling team to initiate a procedure to bring the incident under control and eradicate the threat from the network to recover and restore the business data.

- **Threat Detection and Intelligence Services:** MSS providers offer threat detection and intelligence abilities integrated into their service offerings to allow users to identify, protect, detect, respond to, and recover threats promptly, which depends on the global networking of the providers. The vendors offer the sharing capability across networks, endpoints, and open telemetry tools to make data intelligence more insightful for industry verticals, geographic locations, tactics, procedures, and consulting tools. Additionally, the threat detection and intelligence services improve data analysis to better identify modern threats. The unified security management (USM) platform

combines multiple security capabilities for comprehensive threat coverage, including asset discovery, adding context with vulnerability assessment, intrusion detection, and SIEM event correlation. The threat intelligence service analyzes the different types of attacks, emerging threats, vulnerabilities, and exploits.

- **Managed Vulnerability Management:** Vendors offer vulnerability management features, such as asset discovery and inventory from a global hybrid IT environment — on-premises, cloud, and containers. They also offer internal and external vulnerability management, threat contextualization, policy compliance scanning, web application scanning, and patch management. Moreover, vendors also offer web application scanning, malware detection, PCI vulnerability scanning, cloud security assessment, continuous monitoring, container security, and file integrity monitoring, and they host self-updated, centrally managed, remotely deployable agents. Additionally, vendors provide automated scanning, remediation tracking, and actionable reporting to manage digital assets. They also offer application security assessment services, DevSecOps services, and security consulting services with automated tool-based scanning, manual checks, and treating vulnerabilities identified in applications to align with industry benchmarks.

- **Enhanced Visibility:** Vendors provide a complete visibility across the organizational security platform to detect and respond to vulnerabilities. They add more capabilities to ingest data from several data sources into a single platform. As organizations migrate from on-premises to the cloud infrastructure, the vendors are also adding the internet of things (IoT) and operational technologies (OT) to collect and analyze data. Moreover, they are incorporating AI/ML technologies to support advanced threat detection and mitigation capabilities.

- **Customer Experience Services:** Vendors offer customer reporting portal services to enhance and support real-time customer experience with ticketing and workflow analysis. They also offer enhanced visualization and analytical tools, reporting capabilities, risk metrics, self-service, live support, and user authentication to drive better customer experience. This helps organizations to find

new growth opportunities, launch new products or ventures, and redesign omnichannel purpose-driven customer services. It also optimizes marketing, sales, and service activities across organizational ecosystems. Vendors also offer customer experience services management tools, such as user experience, web content, digital commerce, digital content & process management, and marketing analytics.

- **Security Device Management:** MSS vendors provide security device management services, including device troubleshooting, hardware management replacement, device backup, device restoration, asset management, critical security software patches, and upgrades. Security device management can be deployed on-premises or on third-party cloud-service devices. Device management services should be purchased with health and policy management services to monitor the overall health of the organizational security devices. Some vendors also offer project managers to the customer for understanding device management services in the business.

- **Consulting Services:** MSS vendors are offering security consulting services through advisory and assessment services, incident response, testing, application security testing, red team testing, threat hunting assessment, incident response, and readiness retainer. The vendors assess organizations' security maturity levels, identify the current state, and define the target state to develop a security roadmap with expert guidance. Additionally, vendors also provide cloud security consulting by reviewing cloud configuration and architecture assessment. Moreover, vendors provide consulting on security assessment and regulatory compliance to focus on the relevance of security controls, time, and budget on the device to assess and map the existing security controls against regulatory frameworks and industry standards to prioritize corrective action. They also provide guidance to meet Payment Card Industry Data Security Standards (PCI DSS) requirements.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major managed security services vendors by evaluating their products, 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 MSS market. This study includes an analysis of key vendors, including Ackcent, Alert Logic, Arctic Wolf, BlueVoyant, Cipher, Control Scan, Cyberproof, Delta Risk, Encode, eSentire, Herjavec Group, Integrity 360, Proofpoint, Kaspersky, Kudelski Security, Nuspire, Open Systems, Proficio, Rapid7, Stratozen, Trustwave, and WithSecure.

Managed Security Services are provided by a variety of vendors with different technological expertise. The market is highly fragmented. Non-security specific vendors such as Network services/Telecommunication and System integrators, IT outsourcing, and Consulting firms commonly offer implementation and management services. Some pureplay security vendors offer MSS as a standalone service, while others offer it as a platform-based service with the functionality to customize or use it as a standard service. SaaS security capabilities have become a priority for buyers, and this has significantly reduced the preference to utilize a third-party provider for maintaining the security requirements of organizations.

The demand for dedicated security service providers with a high focus on offering functionalities such as threat hunting, threat intelligence, detection of anomalies, cyber-attacks, breaches while offering recovery solutions, and recommendation services are on the rise. These vendors utilize their internal IP and tools in their capabilities. They are focused on implementing existing and advanced security capabilities to reduce running costs and leverage automation with AI/ML technology. They are also focused on incorporating 5G security technology, integrating with informational and operational technology and managing security operation centers (SOC) while maintaining a zero-trust approach.

Most of these dedicated security service providers are based out of the North American and European regions.

BlueVoyant, Cyberproof, Integrity 360, Proofpoint, Kaspersky, Kudelski Security, Nuspire, Proficio, Rapid7, and WithSecure are identified as the leaders in SPARK Matrix: Managed Security Services and they offer the highest value proposition in terms of technology and service and have a good customer base with a

considerable number of deployments. These vendors provide all the required capabilities of a managed security service provider, along with exceptional support and service. Some of the key factors of differentiation for the leaders are the sophistication of their technology platforms, network of partners, geographic presence, past deployments, type of service delivery approach to MSS, and region-specific solution offerings.

Alert Logic, Arctic Wolf, Cipher, eSentire, Herjavec Group, Open Systems, Stratozen and Trustwave have been positioned among the primary challengers. These companies provide comprehensive service capabilities and are gaining significant market traction in the global MSS market. These companies are also mindful of the upcoming market trends and have outlined a comprehensive roadmap to tap into future growth opportunities. The other key vendors captured in the 2022 SPARK Matrix include Ackcent, ControlScan, Delta Risk and Encode.

There have been a few acquisitions in the past year in the MSS space. Proofpoint acquired Intelisecure to offer MSS, in addition to their recognized security and compliance platforms. Rapid7 acquired the threat intelligence firm IntSights to further improve Rapid7's security operations platform and provide end-to-end external and internal threat detection, automation, and remediation capabilities. Obrela Security Industries acquired Encode to expand its footprint in the global MDR market.

The MSS market is tech-driven, and the attacker TTPs are constantly evolving. The potential of AI in MSS will enable users to gain visibility with tools such as behavioral-based detection which predicts, detects, and prevents breaches and insider threats before they occur while providing real-time analytics. Behavioral-based analytics, when integrated with end-point data, user data, user security, and network flow, will identify suspicious activity and correlate data while spotting policy violations and remediating threats. The integration of AI technology into MSS also offers better IT infrastructure management services, which include workforce management, resolving privacy theft, better decision making, and enhanced functionalities of automated systems and robots. Furthermore, MSS vendors are focusing on implementing business process hyper-automation such as RPA, AI, ML, and process mining to automate and speed up tasks for various business and IT processes and improve operational efficiency & resilience for organizations. AIOps, application performance monitoring (APM), infrastructure visibility, and the observability platform will be integrated with managed security service providers to detect incidents and provide real-time root cause analysis.

Another trend in this space is the continued wariness for MSSPs, owing to various factors including the scale of services offered. As a result, multiple companies have switched vendors before the expiration of contracts. To mitigate this issue, MSS vendors are offering cloud-based SaaS platforms for their clients to operate their own fully managed operational services and provide deep visibility. Cloud-based visibility services allow organizations to identify infrastructure assets that may have escaped from the sight of the IT team and shadow IT problems for the organizations. Moreover, cloud-based MSS vendors are offering a pay-as-you-go model, faster response times, 24/7 monitoring, and full ownership of network performance and management. SMBs with a smaller budget can choose cloud based MSS for their services. Additionally, organization verticals such as banks and telecom dealing with a large amount of sensitive data and compliance restrictions are moving toward co-managed services. MSS provides flexibility to organizations that allow their employees to work remotely by providing around-the-clock cybersecurity protection, distributed cloud models, and the ability to scale security services up and down as per their requirements. The MSS vendors are also offering zero trust architecture to gain visibility across cloud infrastructure activity, users' activity, devices, networks, applications, and data. Furthermore, MSS vendors provide services such as cloud security posture management (CSPM) to automate security systems across diverse cloud infrastructure, secure access service edge (SASE) to secure remote workforce and cloud applications, and public key infrastructure (PKI) to automate, manage, and secure cloud platform by minimizing costs, reducing downtime, and minimizing resource wastage.

All the vendors captured in the 2022 SPARK Matrix of Managed Security Services are emphasizing on improving their capabilities to detect and respond to threats, manage vulnerabilities, monitor, and secure devices. They are also emphasizing on minimizing the complexity of the security stack, protecting against unauthorized access to sensitive data and digital assets, expanding the partnership channels and supporting diverse use cases.

Key Competitive Factors and Technology Differentiators

While most of the leading MSSPs provide the key capabilities off-the-shelf, good customer experience, service excellence, seamless integration, and the flexibility of deployment and the degree of increase in organizational security posture may differ by different vendors offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology and service capabilities and overall value proposition to remain competitive. Following is some of the key competitive factors and differentiators to evaluate the vendors:

- **Sophistication of Technology & Broad Portfolio:** Organizations should look for vendors offering all the key capabilities of a managed security service, and they should evaluate the solutions based on the sophistication of the technology platform and the strength of its detection and response, threat intelligence, and vulnerability management capabilities. Buyers can also consider vendors with a broad portfolio to evaluate how MSS can be combined with their complementary security services to address the organization's IT security needs.

- **Service Capabilities:** Organizations are advised to conduct a comprehensive evaluation of the different MSS vendors before making a purchase decision. Users should employ a weighted analysis based on their specific organization's needs in terms of providing 24/7 monitoring and visibility to the organizational security networks and platforms. An organization's key MSS vendor services requirements may differ based on the industry vertical, consulting services, compliance requirements, co-managed services, customer experience, and end-user size. Users should also look for MSS vendors with a history of successful large-scale deployments and carefully analyze the existing case studies of those deployments. Users should also consider vendors offering dedicated SOC analysts who continuously monitor, protect, and offer security even to the most evolved threats and incidents. Vendors also offer a customized alert system to ensure reduced time for remediation while limiting potential damage to the infrastructure in the future, which is carried out without the engagement of internal teams. The users should examine vendors offering the follow-the-sun capability by delivering 24x7x365 services to analyze and potentially respond to incidents for better outcomes.

- **Competitive Strategy and Use Cases:** Users should employ weighted analysis of the various parameters required for their industry needs and look for quick time to value, industry-specific use cases, including event analysis & correlation, network/endpoint & application, solution usability, event collection, and environmental security. The user should also look for vendors who provide seamless integration, business & technical value, analytics & automation, incident management process, reporting capabilities, compliance, and R&D services. Moreover, users with one or more specific requirements are advised to evaluate MSS by considering vendors' differentiating strategies that may include customized services, requirement management, and cloud-based platform. Users must carefully examine vendors that provide visibility and reporting for various layers of organizational security infrastructure.

- **Industry Experience and Domain Knowledge:** Users should evaluate vendors based on their specific domain knowledge to provide threat detection, monitoring, and security consulting and position themselves as the provider of a wide range of use cases and industry verticals. Users are also advised to consider the vendor's service of offering advanced technological tools such as AI/ML into their platform. Vendors also offer use cases such as endpoint security, process automation, legacy application monitoring, data privacy, and a unified real-time security dashboard. Users must carefully examine vendors by their offering of security device management to manage hardware devices, troubleshoot, provide recovery and data backup, and control software upgrades. Additionally, organizations can choose vendors that offer third-party cloud-based security device management, provide security service advisors (SSA) for their customers, and offer a 24x7 accessible customer portal.

- **R&D Investments:** Users are advised to select vendors who offer emerging technologies to advance the threat detection process. They should invest in MSS R&D services to understand the solutions required to keep the customers safe from incidents and threats occurring on the cloud or the on-premises-based platform. MSS vendors help organizations understand their needs and invest in the right technologies, such as cloud-based security and IoT/OT infrastructure. The security service can detect incidents from unknown malware and anomalous activity in real time using advanced correlation, complex

event processing, and machine learning (ML). It also helps users to reduce the mean time to respond and provide effective KPI, which is a crucial requirement for an organization. Users are advised to evaluate the provider based on current and future investments.

- **Region Specificity:** While buyers can look for vendors with a wide geographical presence, organizations who are concerned with the level of control over the data or have policies aimed at eliminating international data transfer risk can look for vendors offering region-specific solutions that provide tailored solutions with varying levels of control over the storage of data, resources, and operations.

- **Integration of Orchestration and Automation:** MSS vendors focus on the orchestration and automation of services while integrating advanced technologies into their platforms. Users are advised to carefully examine vendors providing AI/ML technologies to help SOC analysts easily and quickly prioritize, analyze, and respond to threat events. With the help of automation, users can utilize the results from analytical tools through real-time reporting and reduce the mean time-to-detect and mean time-to-respond to threats with greater efficiency. Thus, users are advised to select vendors that reduce the onboarding time and standardize & automate the security process.

- **Vision and Roadmap:** Users are advised to evaluate each vendor's service vision and roadmap by considering vendors offering a complete set of features that include threat detection, managed detection & response, threat intelligence services, vulnerability management, SOC, customer experience portal, device management, and consulting services. Additionally, users should evaluate MSS platforms that can adjust their features and functionalities by understanding organizations' KPIs to provide maximum outcomes from the organization's budget. Organizations should focus on vendors who broaden their managed security services by incorporating automation by utilizing AI and ML into their service capabilities to reduce the mean time to recovery (MTTR) and rapidly resolve the incidents occurring in the security networks.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Managed Security Services vendors by evaluating their service portfolio, market presence, and customer value proposition. The cloud native application development services market research provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants. It provides strategic insights on how each vendor ranks related to their competitors based on their respective service excellence and customer impact parameters. The evaluation is based on primary research, including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall managed security services market.

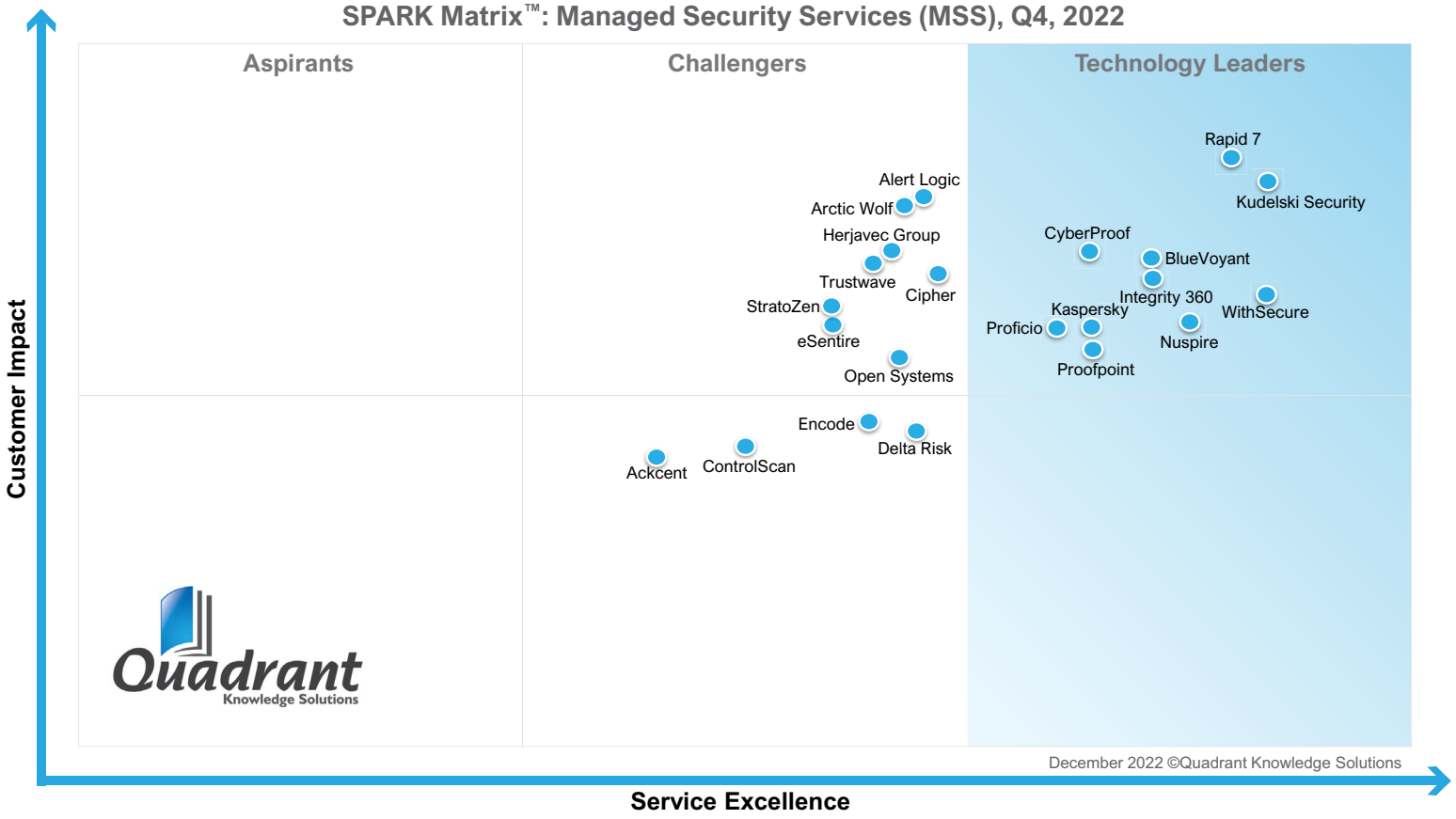
Service Excellence	Weightage
Sophistication of Service Capabilities	25%
Competitive Differentiation Strategy	25%
Industry Experience & Domain Knowledge	25%
Global Reach & Service Capabilities	15%
Vision & Roadmap	10%

Customer Impact	Weightage
Diversity of Client Base	25%
Market Presence	25%
Proven Record	25%
Customer Service Excellence	15%
Unique Value Proposition	10%

SPARK Matrix™: Managed Security Services (MSS), Q4 2022

Strategic Performance Assessment and Ranking

Figure: 2022 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Managed Security Services (MSS) Market



Vendor Profile

Following are the profiles of the leading MSSPs 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 MSSPs based on research findings included in this research service

Kaspersky

URL : www.kaspersky.co.in

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats.

Kaspersky provides Managed Security Services through a bundled service that combines managed detection & response, endpoint security, targeted attack discovery, and cybersecurity trainings.

Analyst Perspective

Following is the analysis of Kaspersky's capabilities in the global managed security services market:

- Kaspersky takes an integrated approach to MSS and the service includes technologies and services required to implement a complete cycle of protection against targeted attacks including Preparation, Detection/Investigation, Data Analysis and Automated Protection.

- Kaspersky experts/analysts offer round-the-clock monitoring and continuous analysis of threat data to ensure the timely and accurate detection of non-malware attacks, cyber espionage attempts, or cybercriminal campaigns. The threat data is accumulated from workstations, servers, SIEM systems, and all other equipment in the customer's infrastructure and is for any signs of an active or impending attack. In addition, Kaspersky analysts conduct a retrospective analysis of the data to analyze incidents, threats, and their impact on the network infrastructure, providing the initial response recommendations in the case of an event.

- Compromise assessment can be delivered in the form of a threat hunting process. The final report includes details about threats, indicators of compromise (IoC), a description of attack sources and network components, and remediation recommendations.

- MSS leverages Kaspersky's threat intelligence platform and Kaspersky's threat intelligence services are enabled by its patented technologies and in-house team of researchers and analysts, which helps them differentiate themselves from other vendors. These services include Threat Data Feeds, CyberTrace, APT Intelligence Reporting, Crimeware Intelligence Reporting, Digital Footprint Intelligence, Threat Lookup, Threat Attribution Engine, and Cloud Sandbox. These tools contextualize information collected from internal Kaspersky monitoring systems, Kaspersky Security Network, Botnet Monitoring service, spam traps, research teams, partners, and underground cybercriminal communities to help analysts operationalize threat intelligence for conductive effective alert triage and initial response.

- In addition, Kaspersky delivers separate training services to improve the expertise of client organizations' in-house digital forensics and incident response teams to fill the skill gaps in threat hunting and threat intelligence. Kaspersky also offers Incident Response Services separately. These services are performed by highly experienced cyber-intrusion detection analysts and investigators. The services can be delivered on a subscription basis or in response to a single event. Additionally, the company offers security assessment services to conduct penetration testing and identify weak points in the network, avoid financial and operation losses, and comply with government, industry, or internal corporate standards.

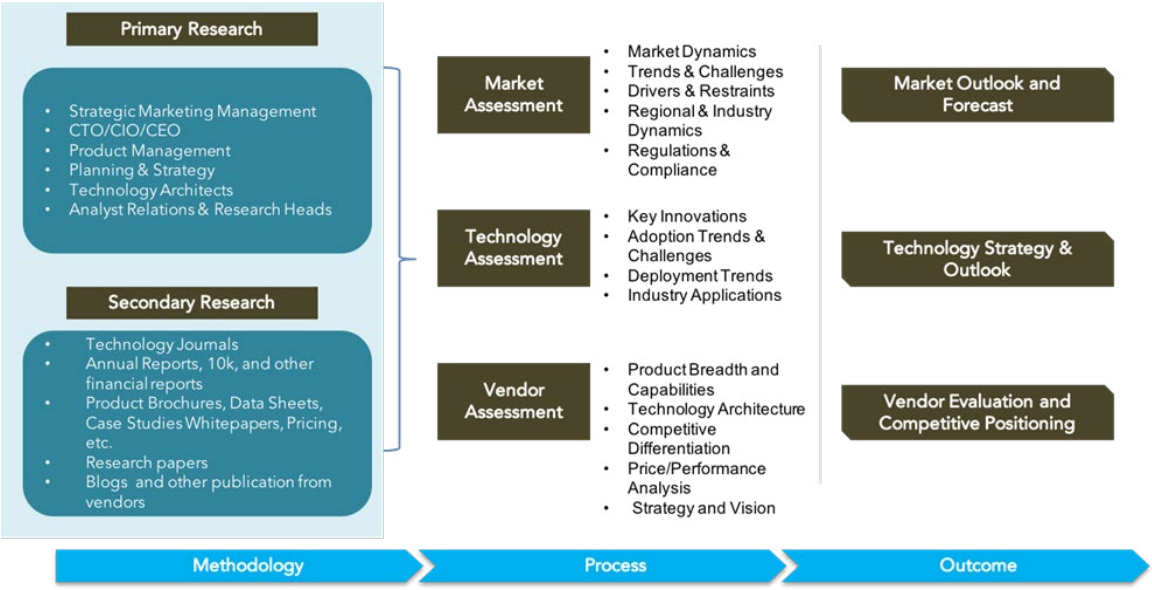
- Kaspersky offers a wide range of products & services to tackle each and every security incident in an enterprise. Kaspersky has individual offerings designed to cater to specific business sizes and types. Kaspersky has access to large amounts of data from different countries, which helps them achieve high detection rates and accuracy.

- Kaspersky invests significantly in its R&D division and its Global Research & Analysis Team (GReAT) is an elite group of IT security experts employed by the company to contribute to threat hunting and analysis.

- Regarding geographical presence, Kaspersky has a strong presence in Europe, Middle East, and Asia Pacific, followed by Latin America, and North America, particularly the US and Canada. From an industry vertical perspective, while Kaspersky has a presence across a wide variety of industry verticals, its primary verticals include industrial, financial, IT/technology, retail, transportation, healthcare, finance services cybersecurity, and more.

Research Methodologies

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



Secondary Research

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

Quadrant's Internal Database

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

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

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

Literature Research

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

Inputs from Industry Participants

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

Primary Research

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

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

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

with client personnel in one of the following functions:

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

Feedback from Channel Partners and End Users

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

Data Analysis: Market Forecast & Competition Analysis

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

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

SPARK Matrix: Strategic Performance Assessment and Ranking

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

Final Report Preparation

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

Client Support

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