Knowledge Brief

Quadrant Knowledge Solutions

Pondurance is a Leader in SPARK Matrix: Managed Detection and Response (MDR), 2021

Quadrant
Knowledge Solutions

2021
SPARK MATRIX
LEADER

Managed Detection and Response (MDR)

An Excerpt from Quadrant Knowledge Solutions
“SPARK Matrix: Managed Detection and Response (MDR), 2021”

Pondurance is a Leader in SPARK Matrix: Managed Detection and Response (MDR), 2021

Managed Detection and Response (MDR) comprises of network host and endpoint-based security services, which are outsourced by enterprises and managed by third-party vendors. MDR provides 24*7 security control, rapid incident response, threat discovery, investigates, contains, and eliminates threats to protect and secure organizations' assets and sensitive data. A robust MDR solution provides protection from fileless malware and phishing attacks, defends the business against external and insider attempts to exfiltrate data, quickly responds to a security incident, and validates suspicious activity on endpoints. MDR providers leverage real attack data to improve the organization's overall security posture by protecting it from threats. A typical MDR solution should provide the capabilities to investigate endpoints and offer the ability to search for historical information about endpoints use indicators of compromise to root out threats on endpoints, and automatically detect threats. A MDR solution also aids organizations in performing root cause analysis for every cyber threat, or any other threat found on an endpoint proactively and deemed important, searches endpoints for signs of threats known as threat hunting, and takes decisive action when a security incident, either potential or in-progress, is identified.

The ongoing COVID-19 pandemic is driving organizations and enterprises to accelerate their digital transformation journeys and migrate to the cloud. The accelerated digital migration, the increased usage of unsecured mobile and IoT devices, and remote working have extended the attack surface and are creating new vulnerabilities. Different types of attacks like ransom attacks and multi-vector attacks have become even bigger and more complex during this time, targeting multiple organizations across multiple locations. A majority of the MDR vendors have claimed that there has been a substantial rise in cyberattacks employing more and more attack vectors compared to the pre-COVID era. MDR vendors are continuously making efforts to combat these complex attacks through advanced solutions while constantly improving their capabilities based on the attack types. Vendors are adopting new strategies like automated attack detection and orchestrated mitigation using multiple methods, behavioral-based detection, encrypted attack protection, and others.

The key value proposition of MDR services includes providing proactive threat hunting, threat analysis, fast incident response, threat intelligence, security monitoring and analytics, and visualization and reporting. The continuous transformation of MDR services driven by advanced technologies is propelling its market adoption amongst small to medium organizations and in large enterprises. MDR vendors provide certain differentiators, including the sophistication of technology capabilities, maturity of AI and ML, integration and interoperability, scalability, and flexibility.

Quadrant Knowledge Solutions' 'SPARK Matrix: Managed Detection and Response (MDR), 2021' research includes a detailed analysis of the global market regarding short-term and long-term growth opportunities, emerging technology trends, market trends, and future market outlook. This research provides strategic information - for technology vendors to better understand the existing market, support their growth strategies, and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

The research includes detailed competition analysis and vendor evaluation with the proprietary SPARK Matrix analysis. SPARK Matrix includes ranking and positioning of leading MDR vendors with a global impact. The SPARK Matrix includes analysis of vendors, including CrowdStrike, Arctic Wolf, eSentire, Red Canary, Rapid7, FireEye, Sophos, Alert Logic, Secureworks, Sentinal One, Cybereason, Expel, Critical Start, Pondurance, Cisco, NCC Group, Orange Cyberdefense, F-Secure, Kudelski Security, Trustwave, Deepwatch, Binary Defense, Mnemonic, BlueVoyant, Fishtech, GoSecure, Open Systems, Proficio, and LMNTRIX.

Market Dynamics and Trends

The following are the key research findings of Quadrant Knowledge Solutions Managed Detection and Response (MDR) research:

- The market drivers for the growth of MDR solutions include the growing frequency, sophistication, and complexity of cyberattacks that are significantly expanding organizations' attack surface and the continued disruption in the technology landscape, which is driving emerging business models and leading to the wave of emerging MDR trends.

- The market drivers also include continued investments in digital transformation projects leading to increased online availability across verticals, increase in remote working, increased use of unsecured mobile and personal devices, and pandemic-related increase in different types of cyberattacks. All these factors are driving the need for efficient MDR solutions that combine sophisticated technical capabilities with an in-house expert team to provide advanced threat detection and remediation with an improved and hassle-free experience for organizations.

- Security technology solutions that were once stand-alone are now becoming part of more comprehensive managed detection and response solutions. Firms offering MDR services have begun to add SIEM, CASB, XDR, expand threat intelligence, and other elements, previously available as a stand-alone product, as a component to their MDR platforms.

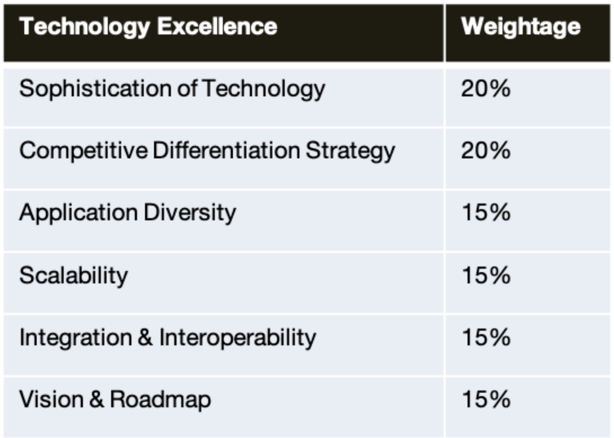
- As the attacks grow more sophisticated, expanding the attack surface, MDR vendors are keeping pace by expanding their capabilities beyond just endpoint protection to provide complete visibility into the entire network, which includes BYOD, IoT devices, etc., and protect and respond to threats to identity, cloud, and emails.

- As developers realize the importance of managed detection and response services for their customers, security is becoming a team effort, as some vendors are developing channel sales models to promote development in collaboration with the service providers.

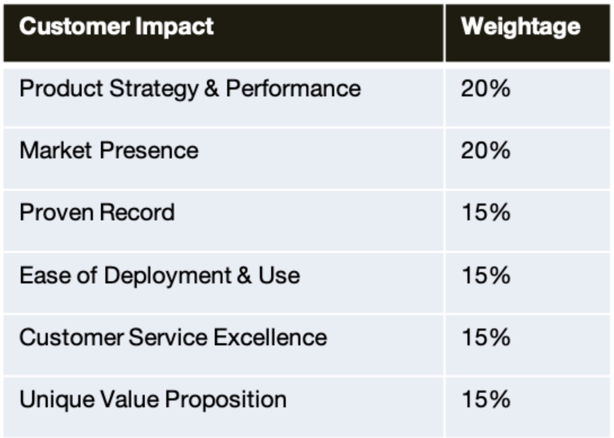
- The distinction between MSSP and MDR is beginning to blur as Managed Security Service Providers, and niche Managed Detection and Response service providers are taking up each other’s roles. While MSSPs have been responding to buyers needing help with threat detection and response, MDR providers are beginning to expand beyond MDR to have a more comprehensive portfolio of consulting-type services, including incident response, vulnerability management as a service, penetration testing, etc.

SPARK Matrix Analysis of the Managed Detection and Response (MDR) Market

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Managed Detection and Response (MDR) vendors by evaluating their product portfolio, market presence, and customer value proposition. MDR market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix^{TM}. 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 technology excellence and customer impact parameters. The evaluation is based on primary research including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall MDR market.



Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%



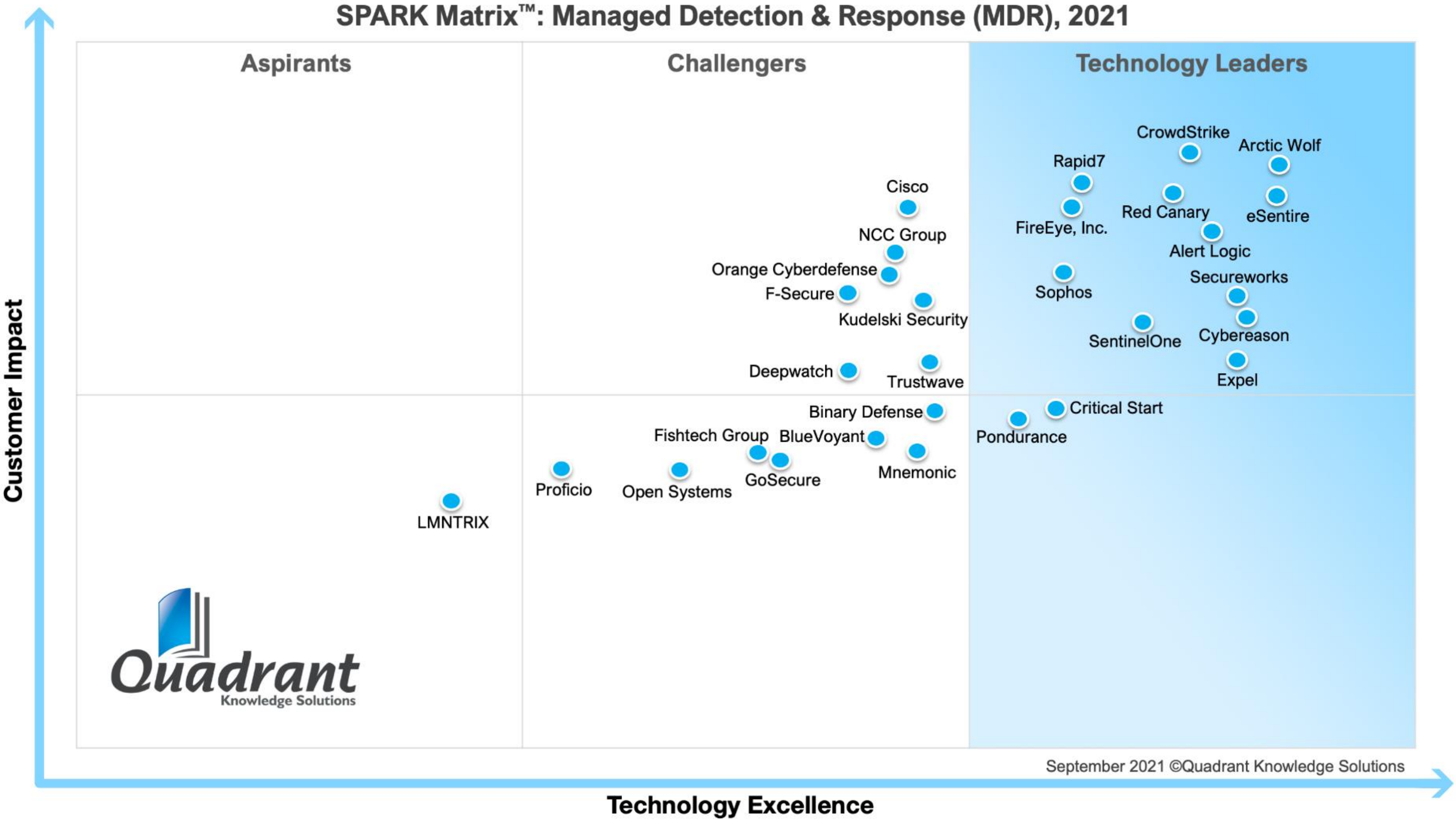
Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

According to the SPARK Matrix analysis of the global MDR market, “Pondurance, with a robust functional capability of its MDR services has secured strong ratings across the performance parameters of technology excellence and customer impact and has been positioned amongst the technology leaders in the 2021 SPARK Matrix of the Managed Detection and Response (MDR) market.”

Figure: 2021 SPARK Matrix

(Strategic Performance Assessment and Ranking)

Global Managed Detection and Response (MDR) Market



Pondurance Capabilities in the Managed Detection and Response (MDR) Market

Founded in 2008 and headquartered in Indianapolis, IN, USA, Pondurance is a cybersecurity company offering technology-enabled security services. Pondurance detects and responds to advanced threats in real-time through its Managed Detection and Response (MDR) services that allows organizations to secure data and assets by stopping cyber threats in real-time. The Pondurance MDR solution offers various key features and functionalities, including 360-degree visibility, 24/7 expertise and advisory, consulting services, and incident response services.

Pondurance MDR offers 360-degree visibility with best-in-class Extended Detection and Response (XDR) across networks with fully-managed and monitored Network Traffic Analysis (NTA) sensors, endpoints with fully-managed EDR solutions, logs with fully managed SIEM as a service platform, and cloud infrastructure, including AWS, GCP and Azure. The MDR service also offers US-based Security Operations Centres (SOCs), which act as extensions of the organization, providing monitoring, proactive threat hunting, and investigation of sophisticated threats while tracking down and unveiling zero-day vulnerabilities.

Pondurance MDR offers a customer-facing XDR and communication platform titled Scope, which allows users to view findings and recommendations, securely communicate and collaborate. Pondurance Scope leverages a multi-tenant architecture that provides comprehensive platform access to Pondurance, while ensuring that unique instances of the portal are available to each client. Additionally, Pondurance provides consulting services like risk management, compliance and audits, cybersecurity programs, and vCISO. Pondurance MDR also offers closed-loop incident response, which helps organizations and users reduce the time it takes to respond to emerging cyberthreats through instant triage and integrated Incident Response services.

Analyst Perspective

Following is the analysis of the Pondurance’s capabilities in the Managed Detection and Response (MDR) market:

- Pondurance MDR solution integrates an advanced platform with an experienced team of analysts including seasoned security operations analysts, digital forensics, and incident response professionals, as well as compliance and security strategists, to continuously hunt, investigate, validate, and contain threats. Pondurance offers always-on services capability to its customers for broader visibility, faster response, containment, and more unified risk management services. Pondurance MDR leverages a 4-dimensional detection strategy to enable better detection, lower false positives, and less manual analysis to keep up with a dynamic enterprise environment.

- Pondurance's methodology and platform integrate vulnerability management, managed detection and response, and incident response capabilities. Some of the key differentiators for Pondurance’s MDR solution includes leveraging GPUs within their platform to accelerate the processing of data, apply Artificial Intelligence (AI) and threat intelligence, and ability to scale linearly and detects threats allowing Pondurance’s SOCs to respond faster and reduce false positives, and their cloud-native architecture that gives full data transparency and access. Pondurance offers Dynamic Defense Methodology to enable risk-based prevention, detection, and response to monitoring from a different set of vantage points filling the blind spots that are often overlooked.

- Concerning geographical presence, Pondurance has a strong presence in the US. From the industry vertical perspective, the primary verticals for Pondurance include healthcare and life sciences, IT & telecom, manufacturing, education, banking & financial services, retail & e-commerce, energy & utilities, and government & public sectors. From a use case perspective, Pondurance offers its solutions to minimize risk of attacks, address insufficient cybersecurity resources, reduce budgetary costs, and enable regulatory compliance.

- Pondurance’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 amongst the primary targets for mergers and acquisitions. However, with its comprehensive functional capabilities, integrated partnership, compelling customer references, and robust customer value proposition, Pondurance is well-positioned to maintain and grow its market share in the Managed Detection and Response market.

- As part of its technology roadmap, Pondurance is focusing on enhancing its position in risk-based security operations and improving service delivery to seamlessly interact with clients. The company is also focusing on improving analysts' productivity through orchestration, on XDR expansion while continuing to lead the MDR industry in broader and deeper MITRE ATT&CK coverage, and on expanding its product integrations across cloud and emerging security controls.