Knowledge Brief
Quadrant Knowledge Solutions

Critical Start 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”

Critical Start 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

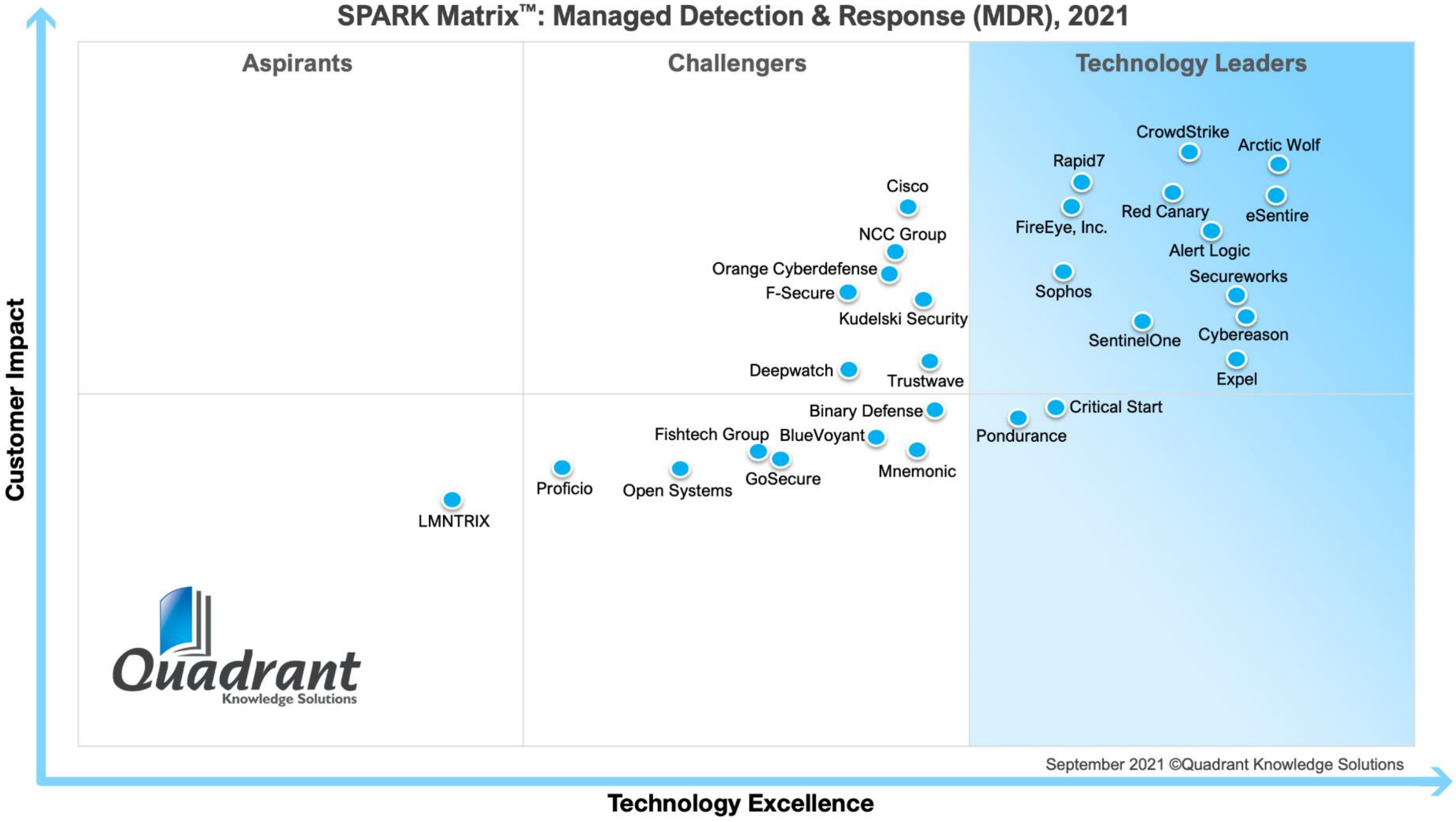
Quadrant Knowledge Solutions conducted an in-depth analysis of the major Managed Detection and Response (MDR) vendors by evaluating their product portfolio, market presence, and customer value proposition. MDR market outlook provides competitive analysis and a ranking of the leading vendors in the form 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, “Critical Start”, 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



Critical Start Capabilities in the Managed Detection and Response (MDR) Market

Founded in 2012 and headquartered in Plano, Texas, USA, Critical Start™ is a managed detection and response (MDR) services company that focuses on protecting customers from cyber-attacks. The company's services portfolio includes end-to-end Managed Detection and Response (MDR) services and Red Team and Blue team services to further help customers prepare their organization for real-world threats. Services include threat hunting, incident response retainers and readiness services, Penetration Testing, and Vulnerability Management as a Service, to name a few.

The Critical Start MDR service protects companies from breaches by leveraging the Zero Trust Analytics Platform (ZTAP) featuring the 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. Critical Start leverages ZTAP to collect, understand, and resolve every alert. ZTAP features the Trusted Behavior Registry (TBR). It's the industry's only purpose-built registry of known good alerts or false positives. The TBR auto-resolves false positives – the largest volume of alerts – at scale. We take every alert and match it against the TBR. If there is a match, the alert is automatically resolved. If there is no match, the Critical Start Security Operations Center (SOC) will triage and investigate the alert to ensure the escalation of the alerts that really require the attention of customer security teams.

Critical Start offers an MDR solution that is transparent by design. Customers have complete visibility and access to every alert with full investigation details, every action taken, and all of it can be audited and reported on. Additionally, the Critical Start MDR solution provides the user with visibility across the entire security ecosystem. This view provides the user with a better understanding of how the security tools are performing and the ability to validate returns on those investments. Additionally, with contractual service licensing agreements (SLAs) for Time to Detect (TTD) and Median Time to Resolution (MTTR), Critical Start states that it guarantees it will triage every alert in minutes with a 1-hour SLA.

The Critical Start Security Operations Center (SOC) is SOC-2 Type 2 certified and is a fully managed, cloud-based Security Operations Center (SOC) with a team of cyber security professionals providing 24x7x365 monitoring, investigation, and response to alerts. The SOC consists of L1, L2, and L3 analysts, which include shift leads and tier 2-3 escalation/evaluation of alerts, a different approach from others. Every one of the analysts must complete 200 hours of training at hiring and another 40-80 hours of annual training. To ensure the integrity of the Trusted Behavior Registry, Critical Start employs two-person integrity on every playbook they implement.

A key component of the Critical Start MDR service is the team of expert threat detection engineers and researchers. Behind the scenes, the Critical Start Cyber Research Unit curates original and third-party threat intelligence to enable quick detection and investigation of threats. Critical Start manages, maintains, and curates out-of-the-box detections and Indicators of Compromise (IOCs) leveraging the Critical Start Threat Navigator. The Critical Start detection engineering team enhances out-of-the-box detection capabilities by developing and adding proprietary IOCs and behavioral detections from curated threat intelligence, previous SOC investigations, Red Team investigations, and external threat intelligence feeds. Detection content is also mapped to the industry-leading MITRE ATT&CK™ framework.

The company also provides the Critical Start MOBILESOC™ application, which allows users to investigate, escalate, and remediate security incidents from iOS or Android devices. The mobile application also allows the customer to collaborate and communicate with the security analyst in real-time.

Customer engagement starts with onboarding. Each customer is assigned a dedicated project manager who will manage the implementation and ensure the solution is installed and operationalized for the customer's environment. The Critical Start implementation team provisions and configures ZTAP to meet the customer's specific needs. They help configure and tune supported security tools and add Critical Start Indicators of Compromise (IOCs) to enhance their detection capabilities. After transitioning to live monitoring, the customer is handed off to the Customer Success Management (CSM) team; they serve as the primary point-of-contact.

Analyst Perspective

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

- Critical Start offers a robust portfolio of Critical Start Managed Detection and Response services, Red Team and Incident Response services to protect users from a wide range of threats. The platform behind the MDR service is bi-directionally integrated with industry-leading Endpoint Detection and Response (EDR), Security and Information and Event Management (SIEM), and Extended Detection and Response (XDR) technology to monitor every event, resolve every alert and respond to breaches in real-time. The ZTAP platform behind the service auto-scales and auto-heals and uses AWS services across multiple regions to provide continuity. It also supports full multi-tenancy for larger organizations that need this separation of entities from the main for business, IT, security, etc.

- Some of the key differentiators of Critical Start include Zero Trust Analytic Platform (ZTAP) and Trusted Behavior Registry (TBR), which automatically resolves 99% of alerts, the MOBILESOC for on-the-go threat detection and response, and 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 app 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.

- Critical Start SOC Investigates and responds to every alert received, taking action to contain threats and applying automation to adapt their service to the business. Organizations can leverage these services to achieve operational security controls monitored and responded to 24x7.

- Concerning geographical presence, Critical Start has a strong presence in the USA. From the industry vertical perspective, the primary verticals for Critical Start include financial services, healthcare, energy & utilities, retail & e-commerce, and manufacturing.

- Critical Start 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. Additionally, the company might face challenges in expanding its presence in some regions, including Europe, the Middle East and Africa, Asia Pacific, and Latin America regions due to the dominance of other well-established players in these regions. However, with its comprehensive functional capabilities, compelling customer references, and robust customer value proposition, Critical Start is well-positioned to maintain and grow its market share in the Managed Detection and Response market.

- As part of its technology roadmap, Critical Start is investing in further refining its solutions to improve the solutions' threat detection and response capabilities and minimize customer OPEX. It is innovating its MDR service by leveraging ZTAP and implementing cross-vendor XDR capability into the ZTAP platform to create novel detections based on multiple vendor products and adding support and direct integrations for additional sources of security alerts, such as identity, email, OT, cloud applications.