

F R O S T & S U L L I V A N

2024

COMPETITIVE
STRATEGY LEADER

*IN THE GLOBAL
MANAGED DETECTION
AND RESPONSE
INDUSTRY*

F R O S T & S U L L I V A N

BEST
2024 PRACTICES
AWARD



Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each Award category before determining the final Award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. DeepSeas excels in many of the criteria in the MDR space.

AWARD CRITERIA	
<i>Strategy Innovation</i>	<i>Customer Impact</i>
Strategy Effectiveness	Price/Performance Value
Strategy Execution	Customer Purchase Experience
Competitive Differentiation	Customer Ownership Experience
Executive Team Alignment	Customer Service Experience
Stakeholder Integration	Brand Equity

Competitive Intensity Builds as MDR Adoption Increases

As a direct result of its ability to alleviate the main pain points in the cybersecurity industry, Managed Detection and Response (MDR) is currently experiencing success across all regions and verticals. A typical MDR service promises comprehensive 24/7 monitoring, detection and response, threat hunting, and incident response across the environment to deal with the onslaught of sophisticated cyberattacks that enterprises endure. A core aspect of MDR is that it allows customers to harness the experience, knowledge, and resources of the provider’s own security team, enhancing their own internal SOC or avoiding the need to invest in one in the first place. In this way, Frost & Sullivan appreciates how MDR services addresses the scarcity of cybersecurity personnel and the increasing complexity of the threat landscape at the same time.

MDR’s effectiveness and rapid adoption have led to a fiercely competitive market, with vendors from various spaces converging on the space. To stand out against other vendors, providers focus on different aspects of the overall MDR promise. Some seek to cover particular environments such as identity, OT and IoT security, or containers to deliver industry-specific visibility. Others provide different types of adjacent security services that increase the coverage and depth of their MDR service to broaden the service’s suitability. There are dozens of other examples, including providers anchoring their service on collaboration, enhanced incident response, AI-powered technology, and more. Additionally, MDR faces competition from XDR vendors that try to address similar use cases with a different approach - even if many of these players offer both MDR and XDR as part of their security solution portfolio.

Even in a green-field market that is ripe for growth, Frost & Sullivan points out that ferocious competition means that MDR providers must differentiate themselves and demonstrate the benefits of their value proposition to potential customers. This requires a strategy that builds on the synergy between innovation and growth and considers the many facets and advantages of managed security.

DeepSeas – A Well Anchored Growth Strategy

Headquartered in San Diego, California, DeepSeas is one of the top competitors in the MDR market. DeepSeas is the result of the 2022 acquisition of Booz Allen Hamilton’s commercial managed threat services (MTS) by Security On-Demand. The company properly leverages the experience, market share, and expert teams of both parts of this union, enabling impressive growth that puts it ahead of many other competitors in the space.

DeepSeas is primarily focused on the North American market, with the bulk of its revenue stemming from its business in this region; a smaller portion comes from Latin America, EMEA, and APAC. The company’s customers are found across all industries, with government, healthcare, and manufacturing organizations as top revenue contributors. North American organizations in these sectors have advanced use cases, challenging DeepSeas to establish a comprehensive strategy to deliver effective MDR security outcomes for its customers.

DeepSeas has made two key acquisitions this year – testament to the company’s commitment to growth in the highly competitive MDR market. The first was the acquisition of RedTeam in July 2023, which extended its penetration testing capabilities; this was quite essential for strengthening cyber resilience and providing valuable feedback for MDR services. The second was the acquisition of GreyCastle Security in December 2023, which expanded DeepSeas’ professional services repertoire, including audit readiness, CISO advisory services, and incident response readiness.

This inorganic growth is an essential part of DeepSeas’ MDR strategy since it synergizes with the MSSP pedigree and professional service focus that the company inherited from Booz Allen Hamilton and Security On-Demand. The acquisitions of RedTeam and GreyCastle contribute to an expanded portfolio of tools that bolster the provider’s MDR service. Adjacent services such as vulnerability management, penetration testing, virtual CISO, and security assessments – all of which are part of DeepSeas’ arsenal – are increasingly essential to help organizations develop and deploy a cutting-edge security strategy. As the company continues to spearhead the combination of MDR and professional services, it will be able to address a growing number of customer use cases.

Technology and Innovation to Unlock a Deep Connection with the Customer

DeepSeas provides MDR services through its Cyber Defense Platform – a unified platform and command center for customers’ security needs, including 24/7 monitoring, detection, incident response, security planning, and numerous other tools and services. To provide strategic flexibility and maximize its customers’ return on investment, DeepSeas focuses on an open approach to MDR – achieving excellence through the integration of disparate security solutions and data sources. This emphasis on providing a vendor-agnostic service empowers organizations that are placed anywhere on the security maturity spectrum, as it allows analysts on the customer team to work with the tools and solutions with which they feel comfortable.

Apart from providing untold value for customers that can leverage existing investments, Frost & Sullivan appreciates how concentrating on third-party integration allows DeepSeas to have unfettered visibility across the environment. The Cyber Defense Platform extends its telemetry, correlation, and actionability across the endpoint, network, cloud, IoT, OT, and other attack surfaces, allowing it to address the needs of customers with diverse environments. This third-party telemetry, consisting of over 140 data sources, is enhanced by DeepSeas' threat intelligence to protect business-critical data through effective synergy.

DeepSeas ensures that customers enjoy even further flexibility by providing two different ways of delivering incident response. The first mode, called "little r", is ideal for organizations that seek a less involved approach (or for any of the multiple IR service provider partners that work with DeepSeas). By opting for this mode, customers handle security responsibilities with their own hands, with DeepSeas only providing alerts and response support. The second mode, called "big r", involves comprehensive hands-on-keyboard approaches where DeepSeas will take care of all critical tasks, and fits quite well with enterprises that prefer to fully outsource their security operations.

DeepSeas also provides customers with co-analysis opportunities, enabling customer teams to participate in investigation, threat hunting, and incident response processes together with the provider's security team by integrating them into the analysis platform. This feature extends the effects of both response modes, sharing the expertise and knowledge of DeepSeas' team and rapidly increasing maturity and security best practices adoption across the customer team in an organic way.

Automation, machine learning, and artificial intelligence also play a significant role in enabling analysts of all skill levels to realize their full potential and become more efficient. These technologies underpin the prediction, correlation, detection, and response capabilities of the Cyber Defense Platform. Technologies such as the AI Safety Net tool (which flags an alert when the triage decision differs significantly from a predetermined AI prediction), or the AI Smart Filter (which filters alerts according to a scoring system) enhance decision-making and further improve threat hunting and incident response. With a keen understanding of megatrends, DeepSeas is also investing in LLM-based technology to provide a better experience for both its own analysts and customers.

The common denominator of DeepSeas' MDR strategy is the unquenchable conviction that technology is an essential tool in the cybersecurity company's arsenal – one that is best used to empower analysts, the most important asset that organizations have at their disposal. Moreover, DeepSeas understands that MDR does not necessarily mean completely replacing the customer's security team; it means creating a unique two-way relationship that multiplies value and aligns with the very specific needs and use cases of each customer.

Conclusion

Through its inorganic growth efforts, DeepSeas continues to extend its portfolio to address additional customer use cases and respond to their needs, spearheading the development of technology and innovation in the MDR market. DeepSeas harnesses integration, visibility, flexibility, and smart R&D investments to magnify cyber resilience and empower security analysts, producing deeper and more valuable business relationships.

With its strong overall performance, DeepSeas earns the 2024 Frost & Sullivan Global Competitive Strategy Leadership Award.

What You Need to Know about the Competitive Strategy Leadership Recognition

Frost & Sullivan's Competitive Strategy Leadership Award recognizes the company with a stand-out approach to achieving top-line growth and a superior customer experience.

Best Practices Award Analysis

For the Competitive Strategy Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Strategy Innovation

Strategy Effectiveness: Effective strategy balances short-term performance needs with long-term aspirations and overall company vision

Strategy Execution: Company strategy utilizes Best Practices to support consistent and efficient processes

Competitive Differentiation: Solutions or products articulate and display unique competitive advantages

Executive Team Alignment: Executive team focuses on staying ahead of key competitors via a unified execution of its organization's mission, vision, and strategy

Stakeholder Integration: Company strategy reflects the needs or circumstances of all industry stakeholders, including competitors, customers, investors, and employees

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

