DEEP seas

2025 TECHNOLOGY INNOVATION LEADER

Enhancing Customer Impact Through Powerful Technology Integration

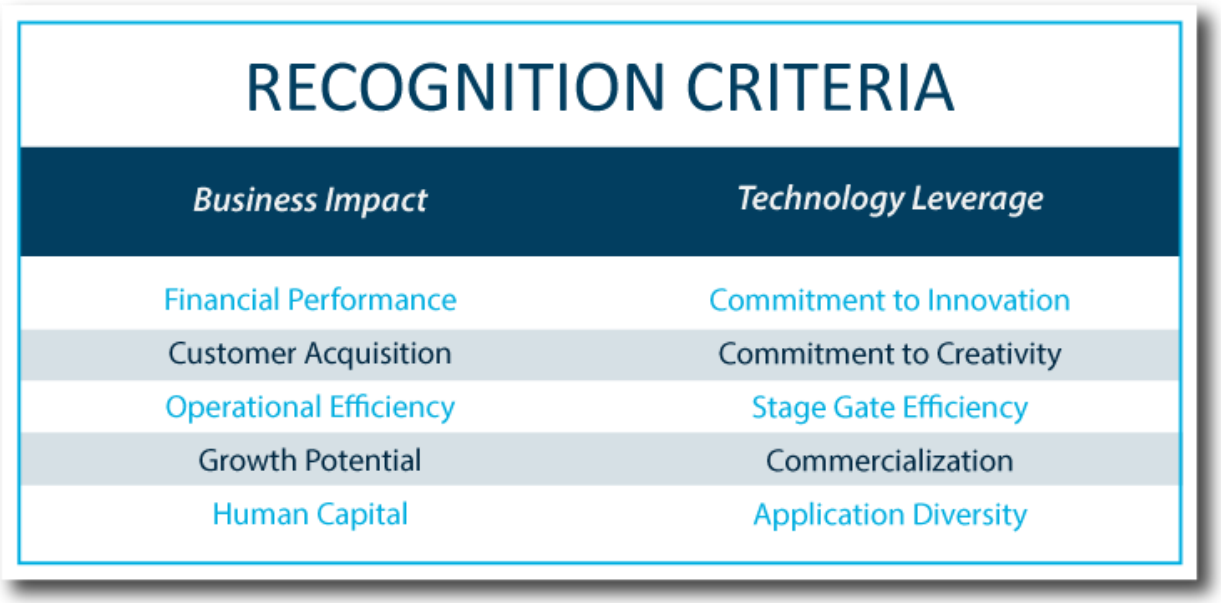
RECOGNIZED FOR BEST PRACTICES IN THE GLOBAL MANAGED DETECTION AND RESPONSE INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition 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.



The Transformation of the MDR market

Organizations continue to face relentless challenges that threaten their ability to protect business-critical data. Technologies that drive efficiency and growth—such as cloud, IoT, OT, containers, and AI—also multiply risks. Attackers now exploit advanced tools, including generative and agentic AI, to automate malicious campaigns, craft deepfake phishing, or write polymorphic code, enabling them to scale attacks with unprecedented sophistication and speed.

The result is stark: cyberattacks are more numerous, more costly, and more disruptive than ever. IBM's Cost of a Data Breach 2025 report found that the average global breach now costs $4.44 million. Even if this represents a 9% decrease from the 2024 figure, it remains a massive complication for most organizations. Beyond direct financial losses, Frost & Sullivan research highlights severe repercussions: waste of productivity, loss of trust, brand erosion, and higher customer churn following successful incidents.

Meanwhile, the cybersecurity talent shortage continues to plague organizations. ISC2's 2024 Cybersecurity Workforce Study reports a global gap of 4.8 million professionals. This dearth of personnel leaves many enterprises unable to build or staff modern, 24/7 security operations centers (SOCs). As environments grow more complex thanks to the proliferation of hybrid and multi-cloud architecture, coupled with remote work models, and the use of IoT/OT, CISOs are under pressure to cover an ever-expanding attack surface with limited resources.

Managed detection and response (MDR) has emerged as a strategic, holistic response to these issues and needs. By combining advanced analytics, threat intelligence, and AI/ML with the expertise of seasoned SOC analysts, MDR enables continuous monitoring, threat hunting, and rapid incident response. The most advanced MDR services are currently evolving with additional proactive capabilities, becoming prevention-oriented to complement their reactive tools. World-class providers are integrating agentic AI to automate investigations, extending visibility across non-traditional environments and security controls, and leveraging the continuous threat exposure management (CTEM) approach to identify, prioritize, and mitigate risks before they materialize.

Sustained MDR value for customers comes from establishing a cycle of continuous innovation to stay one step ahead of attackers. Leading MDR providers make sure to broaden integrations for fuller attack stories, deepen agentic AI capabilities for autonomous triage and remediation, and layer complementary services to address new use cases. Competitors that sustain this loop while maintaining transparency, global support, and excellent service will continue to triumph in the rapidly evolving MDR market.

DeepSeas: An Innovation Leader in the MDR Space

Headquartered in San Diego, California, DeepSeas has a long history in the managed security space dating back to 2013. The company offers a full portfolio of cyber solutions, including MDR, CISO Advisory, offensive security testing, governance/risk/compliance, incorporating threat intelligence, attack surface mapping, and monitoring.

DeepSeas' MDR service provides 24/7 monitoring, detection, threat hunting, and incident response with a vendor-agnostic platform that spans endpoints, servers, identities, SaaS/cloud, TCP/IP networks, and IoT/OT.. The core pillars of its approach to MDR include environment visibility, threat contextualization, advanced threat detection, and threat response, reinforced by a battle-tested team of cybersecurity professionals and a focus on transparency to foster collaboration and communication with customers.

The firm has a significant footprint in the cybersecurity industry, with over 225,000 endpoints under management, dozens of active incident response engagements at any time, and Devo-based, multi-tenant SIEM deployments in the US and Latin America. DeepSeas has an extensive customer base in multiple industries, including high-stakes sectors with advanced security requirements such as government, healthcare, finance, and manufacturing. Its commercial success is evidenced by acquisitions such as GreyCastle Security and RedTeam Security, which expanded DeepSeas' capabilities significantly in GRC and advisory.

Since taking the DeepSeas name in 2022, the firm has built significant brand awareness and equity thanks to its MDR service, earning a spot as an innovation leader in two editions of the Global MDR Frost Radar. DeepSeas continually invents and operationalizes new capabilities, committing to an approach that combines advancements across platform, analytics, and service delivery.

Addressing Diverse Use Cases with Scale and Integration

Among the core aspects of security operations platforms such as XDR and MDR is the need to provide visibility and actionability across diverse customer environments. Additionally, these platforms should be

able to leverage existing security investments, ingesting data and alerts from multiple sources and tools. DeepSeas' VISION platform is underpinned by these two promises.

The platform is deliberately open and vendor-agnostic, integrating over 400 third-party sources across detection and response. Such breadth provides flexibility for customers seeking to empower best-of-breed security strategies and allows analysts to work with their preferred tools, boosting cyber resilience. DeepSeas harmonizes telemetry from these disparate tools, closes visibility gaps, and orchestrates multi-layered responses— speeding time-to-value and avoiding lock-in while addressing multiple use cases and delivering effective security outcomes.

Understanding Modern Risk and Delivering Synergy with an Extensive Adjacent Portfolio

Beyond its approach to integrating the security portfolio, DeepSeas has developed capabilities to match the security needs of modern attack surfaces and risks.

Firstly, its identity threat detection and response (ITDR) solution provides continuous monitoring, pre-built analytics, and dashboards (e.g., high-risk identities, suspicious logins), enhancing detection and response capabilities of the VISION platform with proactive security. This shows that DeepSeas understands the megatrends in the MDR space, as prevention is quickly becoming a must-have in the world of innumerable, sophisticated, AI-powered attacks.

DeepSeas also helps whittle down the number of alerts, which is increasingly essential for overextended security teams. It achieves this through a combination of adjacent tools and services offered alongside MDR, including but not limited to:

- Devo-powered multi-tenant SIEM operations (and continued support for Microsoft and Splunk SIEM when customers prefer it).
- Email MDR with enterprise-wide deep phishing analytics driven by a purpose-built AI engine.
- NDR capabilities strengthened by the firm's partnership with Corelight.

To solidify its world-class technology offering, DeepSeas also offers IR Overwatch, a rapid, autonomous deployment option to resolve active incidents. The service expedites investigations and transforms emergency responses into comprehensive, long-term resilience initiatives and improvements by supplementing the DFIR activities of its partners with the firm's expertise in threat defense. It includes live forensics, which helps understand the when, why, and how of the incident, as well as offering guidance on how to prevent them in the future.

Overall, these tools, alongside others in DeepSeas' arsenal, help organizations craft a highly sophisticated security strategy that comprises multiple layers. Such services provide feedback for DeepSeas and the customer's security teams, building a positive feedback loop and enhancing cyber resilience significantly through proactive and reactive security.

Leveraging A Broad Portfolio To Deliver Disruptive, Pre-Built Security Programs to the Middle Market

The Q4 launch of the DeepSeas Complete portfolio marks a comprehensive approach to delivering enterprise-grade security to the mid-market. The portfolio comprises three security programs designed to address some of the most critical needs facing these clients under a single vendor contract:

- *Advisory* comprises DeepSeas' CISO Advisory, Pen Testing and Vulnerability Scanning services
- *Foundations* comprises all the elements of *Advisory* plus MDR for Endpoint
- *Complete* comprises all the elements of *Foundations,* plus MDR for SIEM and Vulnerability Management

The DeepSeas Complete program enables clients to stand up an enterprise-grade security program within 30 days, without the time and money required to recruit security practitioners or build a 24/7 monitoring program. Just as importantly, DeepSeas Complete unifies the key elements of an advanced security program (i.e., strategy, testing, and continuous monitoring) within a single contract priced per user, resulting in a simple, easily procurable security program that can be rapidly deployed.

Embedding AI from the Beginning to the End of the Journey

As attackers increasingly leverage both GenAI and agentic AI tools to scale up their speed, reach, deception, and sophistication, organizations demand AI-enabled SOCs that can strengthen security. However, veteran and highly knowledgeable MDR security teams remain the X factor of the service, as both critical decision-making and last-mile cybersecurity delivery remain tasks best left to humans.

With an understanding of organizational needs, DeepSeas embeds agentic AI directly into the VISION platform in multiple ways. As a first step, the firm's AI participates in the detection and investigation pipeline from the start, reducing alerts proactively at the front door by analyzing data during the ingestion phase. This speeds up identification and classification of threats, freeing up the time for analysts of all tiers to work on more critical parts of the process. The system also performs automated threat dispositioning, flags probable false positives using historical case data, and generates analyst-ready courses of action, further cutting time-to-respond and lowering total cost of ownership.

Beyond its own models, DeepSeas operationalizes AI features from trusted enterprise platforms: Swimlane's investigation assistant and ServiceNow's LLM-powered summarization help analysts move faster to keep up with threats without losing rigor. DeepSeas' focus on skill, people, and know-how ensures AI augments practitioner judgment and decision-making, preserves transparency, and improves security posture. Such data is available through dedicated dashboards, including a metrics and reporting app, ensuring CISOs and customer stakeholders have deep visibility into the processes that protect their business-critical data.

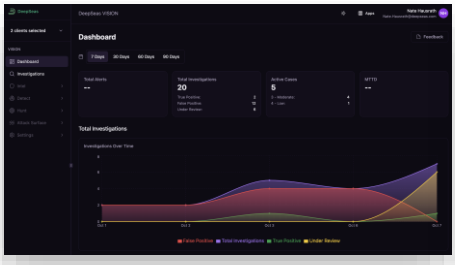
Finally, the combination of AI and technology integration drives differentiated engineering for DeepSeas: its Detection-as-a-Service Engine programmatically pushes proprietary detection logic into third-party customer tools, creating a positive feedback loop that enhances the detection and response processes. Furthermore, DeepSeas harnesses the capabilities of its Threat Response Engine to subsequently orchestrate vendor-agnostic actions across endpoints, networks, identities, and cloud. Through these engines, customers gain faster, AI-powered containment, improved co-analysis options with DeepSeas' 24/7 team, and auto-disposition for high-confidence events, all while maintaining architectural freedom.

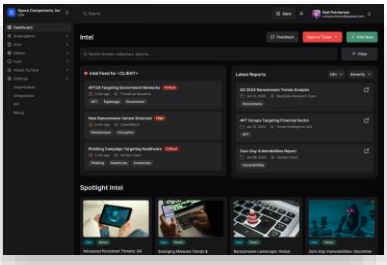
Next on the Horizon: A Roadmap for Evolved Resilience

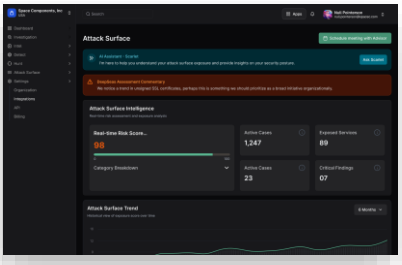
DeepSeas' roadmap prioritizes human risk management, which goes beyond ITDR to make proactive security a top priority, improving MDR beyond detection and response. The development of a quantum

threat defense solution acknowledges the potential risk of quantum attacks, which could mean that encrypted, long-shelf-life data stolen from organizations today might be decrypted in the future.

Additionally, DeepSeas' near-term releases include expanded agentic AI features, a next-gen client portal with AI-enabled reporting (shown below), federated search (hunt without forced centralization), security posture management-as-a-service (Cloud and AI SPM), and packaged "Unified Cyber Resilience" offers that deliver preparation, prevention, and protection. The plan signals a clear view of where MDR is headed and builds toward it methodically.







Conclusion

In a highly advanced cybersecurity space, DeepSeas stands out for its leading AI-powered MDR platform, its vendor-agnostic approach, and the diversity of its complementary tools and services. Together, these elements provide a value far greater than the sum of their parts, delivering effective security outcomes for customers across a wide variety of high-risk industries. DeepSeas understands the current and future promises of MDR, as well as customer needs, and has carefully crafted its roadmap in consideration of this. With its strong overall performance, DeepSeas earns Frost & Sullivan's 2025 Global Technology Innovation Leadership Recognition in the MDR market.

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Technology Innovation Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Leveraging innovative technology characterizes the company culture, which enhances employee morale and retention

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)