S&P Global
Market Intelligence

DeepSeas offers MDR program built to mature, transform midmarket and global enterprise clients

Analysts - Scott Crawford

Publication date: Friday, May 10 2024

Introduction

In 451 Research's 2024 Voice of the Enterprise: Information Security, Budgets & Outlook survey, the improvement of cybersecurity risk management was the most frequently reported strategic objective among survey respondents, but organizations face obstacles to its achievement. Threat detection was ranked among the top pain points among these same respondents. Finding the expertise to manage this critical aspect of security strategy is a further source of pain.

Managed detection and response (MDR) has emerged as a segment specifically focused on optimizing threat detection and response, leveraging provider expertise and investment in technology to combine diverse telemetry and response tools and processes with a provider's expertise and technology for making security posture assessment, detection and response more effective. DeepSeas has succeeded with an approach that targets the upper midmarket with a combination of enterprise-class distinctives and tailored expertise gained through serving large multinational organizations.

The Take

DeepSeas has a distinctive focus on the upper midmarket. It caters to those that need offerings developed for the midtier organization, but whose requirements may be more enterprise-like in the need for tailoring an approach to unique business and technical requirements — such as industry-specific IT and OT, environments where access and management pose distinctive challenges — and other business needs. It has reported significant customer acquisitions (its top four customers average $22 billion in revenue) and revenue growth in a very busy field, where it must compete against a range of established managed security service providers (MSSPs) and consultancies, as well as more recent MDR entrants and technology vendors offering their own MDR services.

Context

The foundation of DeepSeas was laid when midmarket private equity firm Nautic Partners acquired MSSP Security On-Demand and formed its parent, Advanced Threat Response Holdings, in January 2022. To shape the new entity's mission of providing cybersecurity services for highly regulated industries, industry veteran Chris Esemplare was named CEO, bringing more than 18 years' worth of experience with IBM Corp., where he most recently served as the general manager of global security services. With the company's acquisition of Booz Allen Hamilton Holding Corp.'s commercial Managed Threat Services business in December 2022, the combined entity was named DeepSeas.

Security On-Demand gave the new entity a managed security services platform to provide fast search, low-cost indexing and behavioral analytics for security logs, laying a technology foundation for the business. The former Booz Allen Hamilton business added experienced tradecraft, robust detection and more full-featured security operations (SecOps) capabilities. Since its formation, DeepSeas made two additional acquisitions in 2023, picking up security testing expertise with RedTeam Security in July and augmenting its professional security services with GreyCastle in December.

Strategy

The founders of DeepSeas recognized that there was a sizeable gap in mature MDR offerings serving the upper midmarket. Many of these organizations confront the same threats faced by larger or more complex organizations, but frequently lack the resources or expertise of an enterprise. While DeepSeas supports many smaller organizations in concert with its channel partners, solutions targeting SMBs may not suffice among midtier (500-1,500 personnel) and large midtier (1,500-15,000) organizations that represent DeepSeas' primary direct sales targets. DeepSeas has tailored its approach to fill this need, but its appeal has also led to an expansion of its customer base among large enterprises since its debut, with proportionately larger revenue opportunities in the enterprise segment.

DeepSeas claims 300% growth in revenue, with nearly 300 employees serving nearly 1,000 customers in health and life sciences, manufacturing, oil and gas, transportation, retail and hospitality, financial services, state and local government, and higher education. Esemplare continues as DeepSeas CEO, with company headquarters based in San Diego, Calif. While the company's core operations are in the US, it has global customers served from security operations centers in the UK, Costa Rica and India, and a data science team based in Poland.

Offerings

The DeepSeas Cyber Defense Platform supports deployments to organizations having 100-200,000 endpoints. It balances this technological and operational ability to scale with an emphasis on what it terms "personalized innovation." Large midtier organizations and enterprises often have, for example, areas of their operations requiring specialized needs. These last-mile challenges often require specialized adaptations for specific organizations. Environments may be difficult to access or manage — not uncommon, particularly when OT is part of the customer's landscape. Detailed knowledge of decision-makers and the customer's own personnel may be required, especially when swift response is critical. DeepSeas emphasizes its ability to address these requirements to help its clients implement continuous transformation of their cyber readiness in response to an ever-evolving threat landscape, and practice persistent defense.

DeepSeas MDR+ is augmented by pillars of strategic advisory and professional services, penetration testing, and attack surface management. DeepSeas MDR+ features a range of approaches, from alerting and proactive response to the more direct involvement of DeepSeas

analysts in outsourced engagements. While the company has key partnerships with security technology vendors including Microsoft Corp., Devo, Broadcom Carbon Black, SentinelOne Inc., Splunk (acquired by Cisco Systems Inc.), Claroty, Nozomi Networks and Palo Alto Networks Inc., DeepSeas MDR+ offers a vendor-agnostic security platform, and runbooks developed are aligned to the customer's security priorities and business needs. The DeepSeas Cyber Defense as a Service offering is a more fully outsourced program, with dedicated resources and shared services on the back end. Cyber Defense as a Service customers include some of DeepSeas' largest engagements, and it represents a focus of innovation for the company's approach to personalized service tailored to the customer's needs.

The strategic advisory and professional services portfolio centers on assessment as well as expertise. The company's rapid assessment model seeks to differentiate from approaches that laboriously develop voluminous findings, which can be difficult to translate into action. DeepSeas leverages specialized technology and experience to emphasize immediacy of results and help organizations focus as quickly as possible on remediation, growth and maturation of their cyber posture. In terms of personnel and expertise, its CISO Advisory program offers senior practitioners to help organizations cost-effectively develop security programs at the executive level, as well as experienced cybersecurity subject-matter experts to augment risk mitigation, policy development and technical transformation.

DeepSeas extends its approach to rapid and actionable assessment with its Attack Surface Management 360 offering, which includes baseline vulnerability assessments of network, web application, Active Directory/Microsoft Entra, AWS and physical environments. Automated penetration testing allows customers to perform as-needed testing using a credit-based pricing model. Augmented by its RedTeam Security acquisition, penetration testing may target internal and external networks, web applications and APIs, and wireless and physical assets. The company offers a single point of contact and direct communication with security testing personnel, as well as a cloud-hosted portal to request tests and explore findings.

Competition

DeepSeas has staked out strategic priorities for 2024 that are intended to help it differentiate from a flourishing field of MDR competitors. Among those priorities are identity threat detection and response, expanded protection for hybrid cloud environments (IaaS, PaaS and SaaS), automation and AI, a growing spectrum of regulatory requirements, and the impact of cyber insurance on security strategy and management among its customers.

Focus in these areas may help further distinguish DeepSeas from four primary fields of contenders:

- MDR specialists such as Arctic Wolf, Binary Defense, BlueVoyant, Critical Insight, Critical Start, Cyderes, Deepwatch, eSentire, Expel, Fortra (formerly HelpSystems, which acquired AlertLogic in 2022), Open Systems' Ontinue business, Pondurance, Red Canary and others.
- Broader MSSPs, particularly those with an MDR emphasis such as AT&T Cybersecurity, Atos, IBM, Kyndryl, NCC Group, Optiv, Orange Business Services, Proficio, ReliaQuest, SecureWorks Corp., Trustwave, Verizon Business, Wipro Ltd. and others.
- Security technology vendors with MDR offerings including BitDefender, Broadcom Inc., Cisco, CrowdStrike, Forescout, Google Cloud (Mandiant), Microsoft, Palo Alto Networks, Rapid7 Inc., SentinelOne Inc., Sophos, Trend Micro Inc., Xcitium and others.
- Cybersecurity consultancies such as Deloitte, EY, Kroll and many more.

Additional contenders include vendors with a regional MDR focus, which have become potential acquisition targets for a range of potential bidders looking to increase their global penetration. MDR players targeting the SMB, such as Huntress, may be less competitive given DeepSeas' emphasis on the upper midmarket, as well as on those customers whose unique requirements

favor a more personalized approach, its vertical market emphasis arising from OT deployments, or the specialized expertise available through the company's acquisitions and focus areas.

SWOT Analysis

Strengths	Weaknesses
DeepSeas has succeeded with the distinction of its upper midmarket focus: Its personalized approach and rapid assessment strategies help to make its services more immediately actionable and relevant for this class of customer.	While most of DeepSeas' market is in the US, it has a global presence that it could expand to counter multinational and regional competitors. Other MDR contenders also see this opportunity, and may see regional providers as potential acquisition targets.
Opportunities	**Threats**
MDR continues to be a growing segment, and DeepSeas' targeted customers remain underserved where gaps in competitive coverage exist between enterprise and SMB offerings. Global expansion also represents greenfield opportunities for MDR providers.	The competitive landscape of MDR is very wide, and DeepSeas will have to maintain differentiation among its most targeted clients from other MDR providers, as well as broader MSSPs, consultancies, and the "co-opetitive" landscape of technology vendors whose products MDR providers often manage, but that also offer their own MDR.

Source: 451 Research.