MARKETSANDMARKETS™

MANAGED DETECTION AND RESPONSE (MDR) MARKET

GLOBAL FORECAST TO 2027

BY SECURITY TYPE (NETWORK, ENDPOINT, CLOUD), DEPLOYMENT MODE (ON-PREMISES AND CLOUD), ORGANIZATION SIZE (SMES AND LARGE ENTERPRISES), VERTICAL, AND REGION

Report Code: TC 5752

www.marketsandmarkets.com

MarketsandMarkets™ is the world's largest revenue impact company, serving over 7500 customers. 80% of top 2000 companies globally rely on us for identifying new high growth and niche revenue opportunities. In the face of constant technology innovation and market disruption, we help organizations plan and operationalize their future revenue mix decisions by identifying over 30,000 high growth opportunities ranging from $1B to $500B across 90+ industry trends and markets. Organizations choose MarketsandMarkets™ to stay ahead of the curve and accelerate their revenue decisions and implementations by 6 – 12 months, giving them a unique, first-mover advantage. Our revenue impact methodology provides quantified and actionable insights on converged, granular, and connected market eco-systems that result from disruptive technologies and high-growth markets. We provide an extended lens on not only what will impact our client's revenue but also what will impact their clients' revenues, continually uncovering latent opportunities.

We work across all major B2B industries with C-level executives in functions such as Strategy, Marketing, Sales, R&D, Product, and M&A. MarketsandMarkets™ brings exclusive high-growth markets intelligence generated by over 850 SMEs and analysts along with its proprietary Revenue Impact platform (Knowledge Store).

EXECUTIVE SUMMARY

Enterprises are highly dependent on Information and Communications Technology (ICT), making them vulnerable to cybercrimes. Cyber threats are growing rapidly, with adversaries becoming more professional and experts in breaking the barriers established via traditional security measures. It is critical for an organization to manage the huge data produced from thousands of devices, including servers, desktops, gateways, and firewalls.

MDR is a modern approach to proactively detect threats and cyberattacks and respond to them, accordingly, thereby helping enterprises protect their cyberinfrastructure from attacks. Additionally, increasing complications in Information Technology (IT) infrastructure and cyberattacks and the rise in distrust in Managed Security Service Providers (MSSPs) have forced organizations to reconsider and adopt MDR to tackle the sophisticated cyberattacks on their IT infrastructure. MDR service providers offer real-time protection to organizations and help reduce the risks of potential attacks.

MDR essentially evolved out of Managed Security Services (MSS) and possessed improved detection and response capabilities. MSS became available in the market for all regions and verticals in 1997 and offered enterprises security solutions and services, thus helping them reduce the burden of capital investment in security equipment and dedicated resources. The evolution of cloud or hosted deployment aided the adoption of security services due to the reduction in the installation cost of on-premises IT infrastructure to support security services. However, with the evolution of the threat landscape, MSS fell short in protecting the business-critical cyberinfrastructure. This led to the introduction and growth in adopting innovative MDR services to tackle Advanced Persistent Threats (APT) and other vulnerabilities. MDR service enables immediate notification of any threat or vulnerability, allowing cybersecurity experts to help an enterprise deal with the problem and provide advice. MDR helps save businesses a significant amount of time and money that otherwise would have been spent dealing with issues after suffering an attack.

Growing instances of cyberattacks, shortage of skilled security practitioners, stringent government policies, and the need for compliance will drive the MDR market over the next five years. Moreover, technological proliferation and increasing adoption of Internet of Things (IoT) and connected devices across industrial applications have led to a steep increase in security vulnerabilities, thereby increasing the demand for solutions and services safeguarding such applications. With MDR service providers integrating conceptual technologies, such as AI, ML, and pattern recognition into their MDR offerings, it has opened a wide range of growth avenues for various service providers in the industry. However, the lack of trust in third-party applications and the absence of modern IT infrastructure across organizations are anticipated to affect the market growth over the coming years.

The scope of this report covers the MDR market by security type, deployment mode, organization size, vertical, and region. The Banking Financial Services and Insurance (BFSI) vertical is expected to dominate the market with the largest market share during the forecast period. This is due to the increasing use of web-based applications and processes across the banking sector and targeted cyberattacks. Additionally, the increasing compliance requirements for enterprises operating in the vertical are expected to push the adoption of such advanced cybersecurity services. North America is expected to hold the largest share of the MDR market during the forecast period due to various MDR service providers in this region. Asia Pacific offers significant growth opportunities due to the increasing demand for hosted MDR services across Small and Medium-sized Enterprises (SMEs) and the growth of the IT industry in the region that caters to a global clientele.

OPPORTUNITIES

Introduction of ML/AI-powered MDR services

As the dynamicity in the enterprise, IT environment is unprecedented, cyberattacks occur at an increasing rate and with a growing level of complexity. Traditional MSSPs fail to adapt to the changing conditions and effectively handle new and complex attacks. Next-generation cybersecurity services integrated with advanced technologies, such as ML and behavioral analytics, to provide cutting-edge threat protection to combat APTs, by integrating real-time contextual awareness, automating intelligent security, and providing rapid response and low cost of ownership. Such next-generation MDR services leverage advanced technological concepts, such as ML and AI, to proactively determine the root cause of the threat and help protect critical information at networks, endpoints, and application layers. Vendors are deploying the concepts of AI, ML, and pattern recognition to automatically update the set of security rules to effectively protect an enterprise's cyberinfrastructure from advanced threats and vulnerabilities.

Increasing adoption of MDR across SMEs

MSSPs currently dominate SMEs due to their capability to provide cost-effective services over a range of security service areas. Although popular MSSPs protect several different vulnerabilities and advantages such as low costs, not all processing can be combined, as some protection methods rely on different inspection techniques. It offers a significant opportunity for MDR vendors to develop innovations to provide these enterprises with cost-effective, consistent, and MDR services with enhanced functionalities to extend their foothold in the SMEs segment. Moreover, increasing distrust among organizations and bad experiences from MSSPs have led SMEs to adopt an advanced MDR services instead of an MSS to protect the business from security vulnerabilities. Hence, it is expected to drive the adoption of MDR services across SMEs in various verticals.

CHALLENGES

Lack of modern IT infrastructure

IT framework typically comprises diverse segments, for example, complex servers, business applications, system and security environments, tools, and databases. Each of these segments frames the center of each business. However, managing them is quite challenging. Most organizations keep up their tools and aptitudes to keep the IT foundation up and running. In contrast, others require innovative partners to deal with the pressure to bring down the increasing maintenance and administration costs.

With systems becoming more dispersed, customizable, and heterogeneous, the quantity of data collected regarding security services is vast. The data collected from various components of the infrastructure keeps increasing and hence the segregation of important data becomes a challenge for any IT department. As organizations grow, so does the volume and variety of the data, which attracts even more diversified threats for which firms are unprepared. Thus, modern-day MDR vendors focus on a shared technology framework that can address such issues.

Potential cyberattacks on MDR service provider's infrastructure

Large enterprises regularly have structural difficulties that other smaller businesses typically do not experience. These include a broadly diverse customer base, numerous products and services, discrete internal divisions or hierarchical units, and essentially more outsourced business information. Considering large players in the MDR market, it is difficult to maintain and secure the data to provide security services. MDR and security service providers are aware of threats and allocate resources toward information security, faster response times, and recovery after threat detection. To protect the security services of a provider's IT infrastructure from viruses, malware, and other cyber-security threats, most of the MDR vendors use a unified approach to manage security, which is a viable solution for growth-orientated companies.

KEY COMPANY EVALUATION QUADRANT

The company evaluation quadrant provides information about the key players in the managed detection and response market. It outlines the findings and analysis based on how well each market vendor performs within the predefined company evaluation quadrant criteria. Vendor evaluations were based on two broad categories: strength of product portfolio and business strategy excellence. Each category carries various criteria based on which vendors were evaluated. The evaluation criteria considered under the strength of the product portfolio include breadth and depth of product offerings, feature/functionality, the focus of product innovations, and product quality and reliability. The evaluation criteria considered under business strategy excellence include geographic footprint, breadth of applications or verticals served. CrowdStrike, Rapid7, Proficio, Red Canary, Arctic Wolf, Kudelski Security, SentinelOne, Expel, Secureworks, Alert Logic, Trustwave, Mandiant, Binary Defense, Sophos and eSentire are the key players operating in the managed detection and response market.

FIGURE 33 MANAGED DETECTION AND RESPONSE MARKET: KEY COMPANY EVALUATION QUADRANT

Source: Press Releases, Expert Interviews, and MarketsandMarkets Analysis

PROFICIO

Business overview

Proficio is a leading MDR service provider delivering 24/7 security monitoring and various solutions, including automated and semi-automated response, managed endpoint detection and response, AI-based threat hunting, Identity Threat Detection and Response, threat intelligence, managed cloud security, and SOCaaS. They apply advanced analytics to telemetry from a large number of log sources. Proficio's services can be deployed as fully managed, hybrid, and co-managed solutions via a cloud or on-premises infrastructure. In addition, Proficio helps clients meet compliance mandates such as HIPPA, PCI, and GDPR.

TABLE 280 PROFICIO: BUSINESS OVERVIEW

Founded	2010
Country	United States
City	Carlsbad, California
Ownership	Private

Source: Company Website

Proficio's MDR service provides continuous monitoring and alerting with actionable alerts and includes their proprietary threat intelligence platform – Threat Intelligence Profiler (TIP). TIP adds contextual information from multiple threat feeds and enriches log data for more accurate event detection and alerting. Their MDR service uses the MITRE ATT&CK framework to analyze attacks as a set of behaviors, to respond faster, and always stay ahead of adversaries. They have a dedicated team of security experts in San Diego, Singapore, and Barcelona SOC, which monitors security events and hunts for targeted attacks. Proficio also offers Risk-Based Vulnerability Management (RBVM) services to prioritize vulnerabilities based on the likelihood of exploitation and the criticality of the assets at risk, and Active Defense service to automate the response to high fidelity security events. Proficio caters to various verticals, including financial services, healthcare, manufacturing, law firms, government, and retail. The company has offices in North America, Europe, and Asia Pacific.

Products/solutions/services offered

TABLE 281 PROFICIO: PRODUCT/SOLUTION/SERVICE OFFERINGS

PRODUCT TYPE	PRODUCT/SOLUTION/ SERVICE	DESCRIPTION	APPLICATION
Managed Services	MDR	▪ Threat detection, and automated incident response at the perimeter, cloud, identity layer, and endpoint ▪ Ransomware Protection ▪ 24/7 security monitoring and alerting ▪ Includes MITRE ATT&CK framework ▪ Managed security for endpoints, security devices, and SIEM ▪ Integrated threat intelligence ▪ AI based threat hunting ▪ Risk-based Vulnerability Management ▪ Cyber Risk Scoring	▪ Financial Services ▪ Insurance ▪ Healthcare ▪ Manufacturing ▪ Technology ▪ Law firms ▪ Government ▪ Retail

Source: Company Website