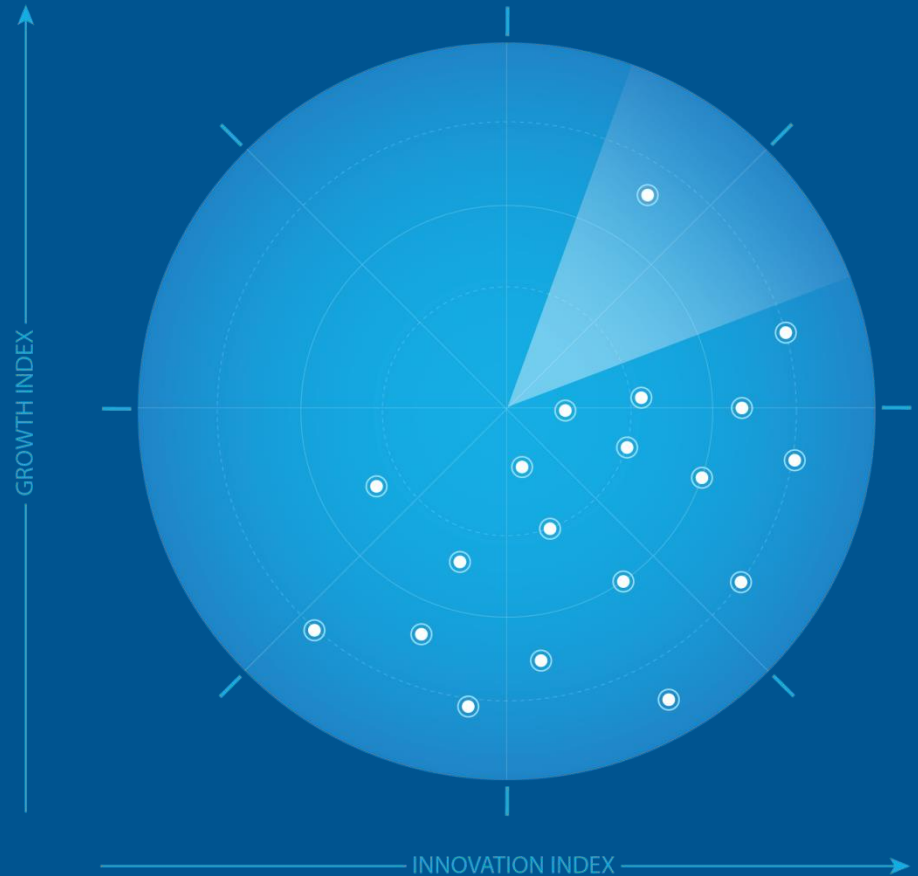# FROST & SULLIVAN

Frost Radar™: Global Managed Detection and Response Market, 2022

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines

Global Security Research Team at Frost & Sullivan

Strategic Imperative and Growth Environment

Strategic Imperative

- The lack of security professionals is becoming more pronounced with each passing year. In the US alone, nearly half a million cybersecurity jobs were unfilled by August 2021.

- Lacking access to professionals and unable to effectively protect their businesses, organizations turn to managed services to cover their security needs. MDR service providers have experienced professional teams that can support organizations in the form of threat detection and response.

- Organizations seeking to upgrade their threat detection and response capabilities will increasingly make use of MDR services, relying on the service providers' vast knowledge, expertise, and monitoring capabilities. Due to this, they will be able to allocate their resources to other, more strategic tasks.

- In the next five years, as the Everything-as-a-service model spreads further, organizations will escalate investment and deployment of MDR services.

- In light of the shortage of cybersecurity professionals, organizations are looking for ways to automate the process of threat detection and response. The new generation of solutions and services promises to deploy machine learning and artificial intelligence, automating decision-making to improve the overall performance of the security stack.

- But meaningful automation is still in the early stages of development. Organizations are aware that technologies provide limited benefits right now, and seek alternative paths to success.

- Organizations looking to boost the limited capacities of current automation technologies can lean into MDR for their needs. Highly trained security professionals can complement machine learning algorithms and AI for unmatched incident response.

- In the next five years, while MDR providers continue to develop and perfect meaningful automation, security services and solutions that provide a combination of human teams and automation will thrive in the market.

Strategic Imperative (continued)

- Over the past decade, security incidents have increased in frequency and sophistication. An increasing number of cyberattacks are sponsored by nation-states, while the attack surface continues to expand in a time of rapid digitalization.

- Due to the sophisticated nature of the threats, organizations find it increasingly difficult to keep up to date with new developments in cybersecurity and to secure their business assets efficiently relying on in-house experts.

- On February 24th, 2022, Russia began an invasion of Ukraine with a wide-ranging attack on multiple fronts. The destruction of the country's infrastructure, devastating loss of life of both military personnel and civilians, as well as the displacement of millions of people will have long-lasting consequences at a global scale.

- A new divide between West and East will bring about a profoundly different global geopolitical context, and this will have implications for the cybersecurity industry as a whole. Attacks sponsored by nation-states were already on the rise. After the economical and political sanctions that the US and the EU (backed by the majority of the world's nations) are imposing on Russia, these types of attacks may increase.

- A silver lining for the cybersecurity industry, organizations will need security solutions and services to provide comprehensive protection of their environments. MDR's 24/7 monitoring, threat hunting, incident response, and professional guidance will be essential for both large enterprises and SMBs of all regions looking for an edge over the new threat. MDR's promise will resonate with organizations for the foreseeable future.

Growth Environment

- MDR is a relatively new solution in the cybersecurity market. While some vendors have been providing services similar to MDR in the form of SOC-as-a-service or various MSS offerings, the inception of MDR goes back to 2018 for the earliest competitors. The novelty of the solution means that the market is just passing the early adopters stage – MDR is starting to be picked up by an early majority of customers in 2021.

- Growth rates for the market show a decrease, from 79.8% growth in 2020 to 60.8% in 2021. However, the CAGR is still very high at 34.0%. There is ample room for growth across all regions, and in every industry vertical or company size.

- The MDR market is currently receiving an influx of new competitors. Some are pure-play cybersecurity companies, coming from the XDR or EDR space, adding a managed component to turn the solution into a service. MSSPs have also developed their own MDR services, looking to establish a long-lasting relationship with their customers, and deepening the threat detection and response they can provide. Furthermore, there are also professional services firms, and other security vendors jumping at the opportunity to increase their already broad portfolios with an MDR offering.

- In the long term, the scarcity of cybersecurity professionals will boost the MDR market growth, as the issue will persist (and possibly deepen) for the rest of the forecast period. MDR currently offers a solution to the most pressing limitations and complications with the cybersecurity industry, and Frost & Sullivan expects this will ensure the success of the service in the next three years.

- Additionally, the market may grow due to an even larger influx from XDR vendors. Frost & Sullivan's study on XDR uncovered the three promises of XDR. The most underdelivered of these promises is that of meaningful automation. The managed component of MDR and managed XDR allows vendors to bypass the need for true automation. As more vendors try to carve out a niche in the market, they may resort to turning their solution into a service in this way.
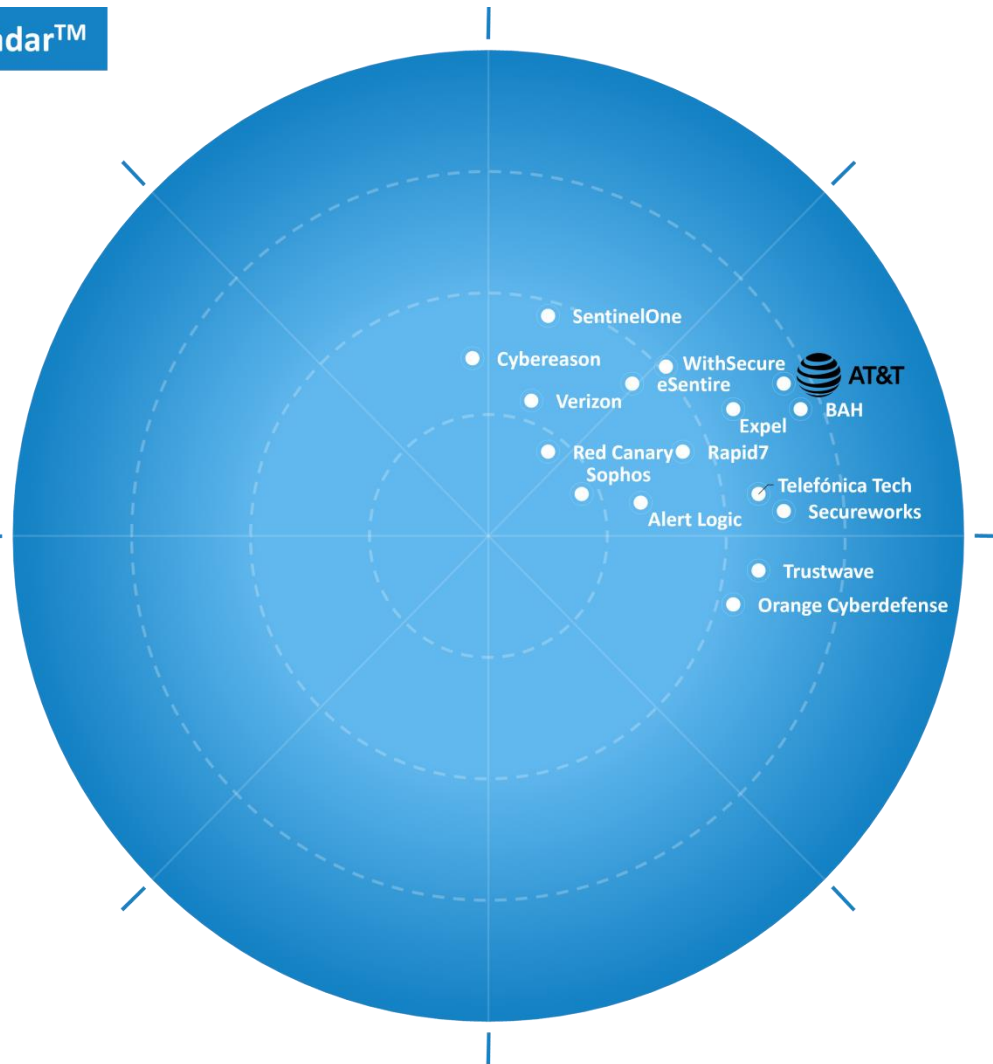
Source: Frost & Sullivan
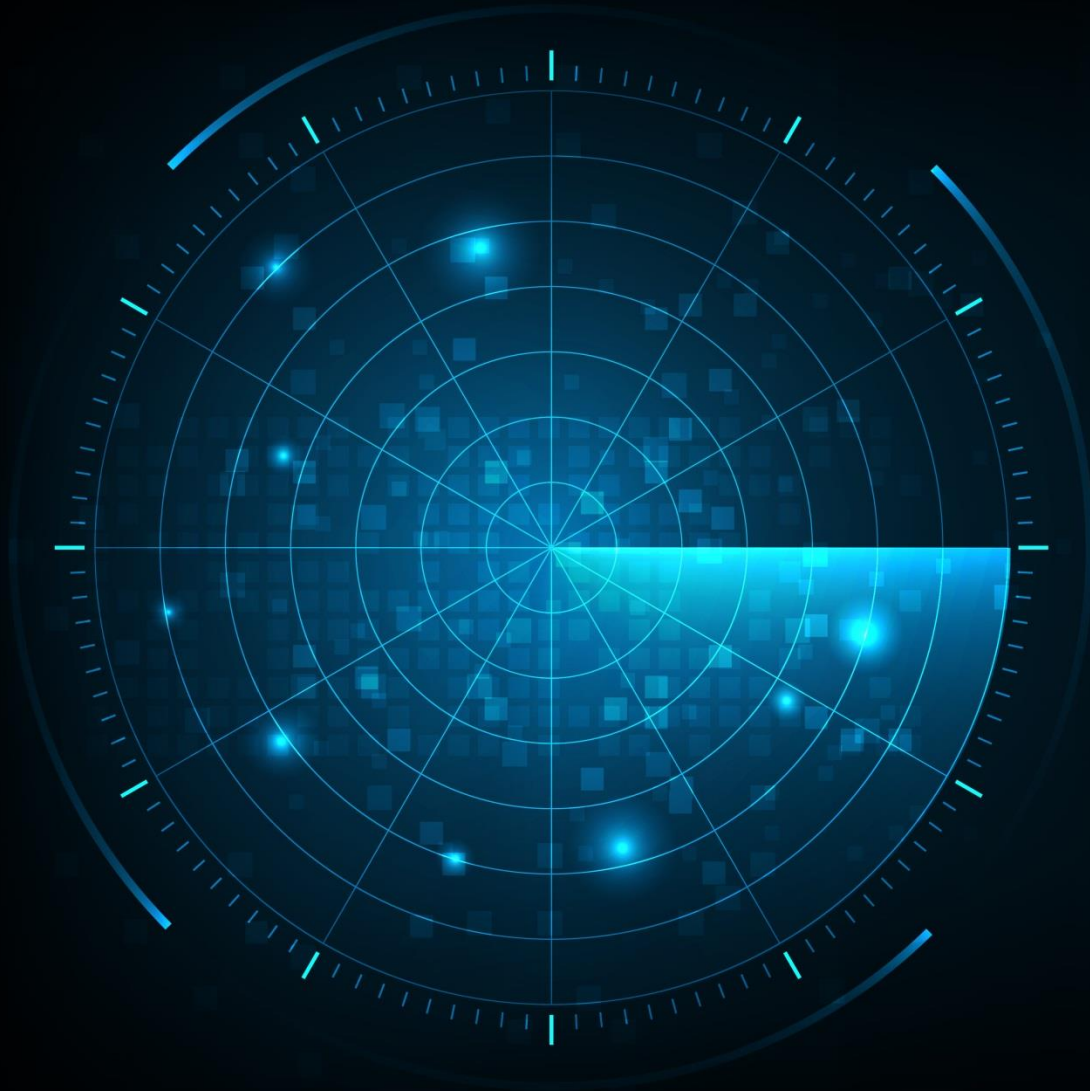
FROST & SULLIVAN

Frost Radar™

Managed Detection and Response

Frost Radar™: Global MDR Market

Frost Radar™

GROWTH INDEX

INNOVATION INDEX

- SentinelOne
- Cybereason
- WithSecure
- eSentire
- AT&T
- Verizon
- BAH
- Expel
- Red Canary
- Rapid7
- Sophos
- Telefónica Tech
- Secureworks
- Alert Logic
- Trustwave
- Orange Cyberdefense

Key: AT&T Cybersecurity appears as AT&T in the image;

Source: Frost & Sullivan

Frost Radar™: Competitive Environment

- The global Managed Detection and Response market is fragmented, highly competitive, and one of the most innovative in the cybersecurity industry. Frost & Sullivan selected and plotted the top 15 out of over 70 market participants in this Frost Radar™ analysis.

- Unlike other cybersecurity competitive environments, no single vendor can get close to a 10% of the global MDR revenue share. A factor that contributes to the share allocation is the relative novelty of the market, leading to players growing within their niches without directly taking revenue from each other.

- An additional factor is the combination between the **Highly Innovative** nature of cybersecurity in general, and MDR in particular, with the varied use cases, industry verticals, company sizes, and maturity levels of prospect customers. Both established vendors and recent entrants into the market will invest in developing MDR modules that best align with their vision, and the use cases of their customers. As a consequence, two MDR players might be doing the same R&D investments, and fully focusing on innovation, while reaching separate target customers.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action
Companies to Be Considered First for
Investment, Partnerships, or Benchmarking

AT&T Cybersecurity

INNOVATION

- AT&T is an innovation and growth leader in the MDR Frost Radar.

- The company's acquisition of AlienVault in 2018, and its continued investment in Alien Labs (threat intelligence) and USM AlienApps (telemetry and orchestration) enhance the capabilities of its MDR service.

- With 8 global SOCs, the vendor provides extended coverage for its MDR solution. AT&T works with the customers' existing security stack, integrating over 500 AlienApps through the AT&T AlienApps ecosystem to increase telemetry.

- Furthermore, AT&T provides integrations with best-of-breed XDR solutions such as SentinelOne, Crowdstrike, Palo Alto Networks Cortex, and more.

- Cross-portfolio integration with AT&T SASE solutions and AT&T Risk Management bestow the service with increased visibility over critical sections of the customer environment.

GROWTH

- AT&T relaunched its MDR service in 2019. Since then, the company has managed to carve out its niche in the highly competitive MDR market.

- The vendor's size, its position as an MSSP, and its keen awareness of the trends that permeate the MDR space give it a unique advantage to unlock future growth in the market.

- USM AlienApps constitutes a powerful growth differentiator. As the company continues to develop and increase the number of integrations, the value proposition of AT&T's MDR service will grow exponentially for current and potential customers.

- AT&T's 8 global SOCs and strong MSSP channels are also instrumental in the vendor's growth strategy. By leveraging its infrastructure and positioning, the company will take advantage of increased MDR adoption in those regions in the future.

FROST PERSPECTIVE

- AT&T is one of the leading competitors in Frost & Sullivan's MDR Frost Radar.

- The firm should continue to invest in USM AlienApps to widen the scope of MDR and improve the customers' security posture through data ingestion. USM Anywhere as a whole is a powerful differentiator that sets AT&T apart from other service providers in the MDR space.

- AT&T's current focus is on North America, and while the region will continue to grow at a rapid pace for the next few years, other regions will outpace its growth rate. Leveraging its global SOCs, AT&T should try to break into the European MDR market and establish a foothold through the power of its massive number of integrations.

- AT&T should also consider investing in visibility over OT environments, as vendors from the manufacturing and utility industries will demand such capabilities soon.

Source: Frost & Sullivan

Strategic Insights

Strategic Insights

1 MDR providers should focus on **Extending the Value of their Platforms by Integrating with Additional Security Controls and Feeds** outside of the traditional integrations. Including additional modules will also accelerate the adoption of non-traditional industry verticals for cybersecurity (i.e. manufacturing, utilities,). MDR vendors should add or further develop visibility for OT and IoT devices, Vulnerability Management like BAS or Penetration Testing, integration with Zero Trust / SASE, and support for AWS, Azure, or SaaS apps, among other innovations.

2 While North America is the indisputable leader in terms of cybersecurity technology adoption, MDR vendors will have to expand into the EMEA, APAC, and Latin American regions to maintain current growth. **EMEA Constitutes the Most Accessible Opportunity**, especially in the European market. Due to the current geopolitical developments, after the invasion of Ukraine by Russian forces, European SMBs and large enterprises will need support to improve their security posture. MDR providers can offer top-tier guidance and supplement the lack of security personnel in the region

3 Machine learning, automation, and artificial intelligence are underused as a part of MDR and managed XDR services. Most vendors have developed playbooks to enable basic automation, but the service needs to exploit these technologies further to stay ahead of threat actors. **MDR Vendors Should Acquire or Develop Further ML and AI Capabilities:** chatbots that categorize and automate customer queries to provide immediate assistance, checking for false alerts, responding appropriately to threats already discovered in a different customer's environment, automated reports, and more.

Source: Frost & Sullivan

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

GROWTH INDEX ELEMENTS

VERTICAL AXIS

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline™ system; and effective market, competitor, and end-user focused sales and marketing strategies.

- **GI1: MARKET SHARE (PREVIOUS 3 YEARS)**
  This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

- **GI2: REVENUE GROWTH (PREVIOUS 3 YEARS)**
  This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.

- **GI3: GROWTH PIPELINE™**
  This is an evaluation of the strength and leverage of a company's growth pipeline™ system to continuously capture, analyze, and prioritize its universe of growth opportunities.

- **GI4: VISION AND STRATEGY**
  This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

- **GI5: SALES AND MARKETING**
  This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

INNOVATION INDEX ELEMENTS

HORIZONTAL AXIS

Innovation Index (II) is a measure of a company's ability to develop products/services/solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets, and are aligned to customers' changing needs.

- **II1: INNOVATION SCALABILITY**
  This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

- **II2: RESEARCH AND DEVELOPMENT**
  This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

- **II3: PRODUCT PORTFOLIO**
  This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

- **II4: MEGA TRENDS LEVERAGE**
  This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.

- **II5: CUSTOMER ALIGNMENT**
  This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Legal Disciaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan

3211 Scott Blvd., Suite 203

Santa Clara, CA 95054