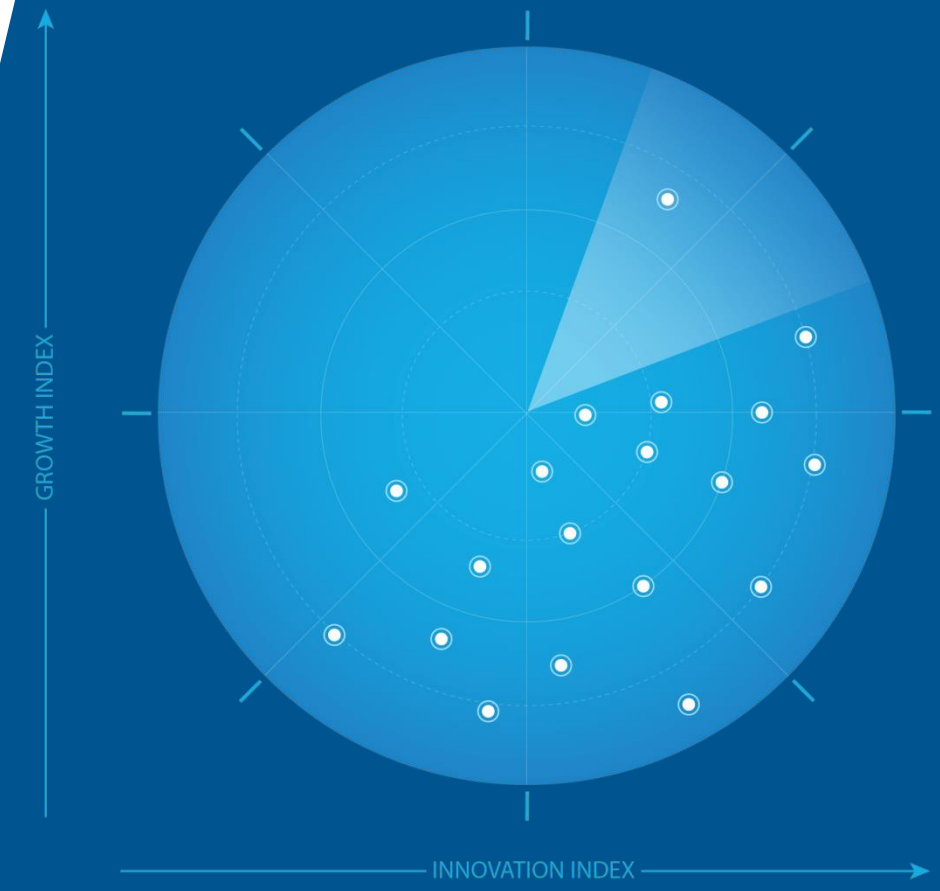
FROST & SULLIVAN

Frost Radar™: Managed Detection and Response, 2024

Authored by: Lucas Ferreyra

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



March 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment



Strategic Imperative

Factors Creating Pressure on Growth

- The dearth of cybersecurity professionals continues to shape the industry, becoming a thorn in global organizations' side as they try to secure their growing environments.
- Faced with a lack of access to professionals and an inability to protect their business-critical data effectively, organizations are outsourcing to alleviate the issue.
- MDR service providers can offer top-tier security across the environment, delivered by experienced professional teams that partner with and support organizations in establishing effective security perimeters.
- In the next three years, organizations will continue investing in outsourced security through MDR services as it enables them to focus personnel on the core business instead of building internal security operations centers (SOCs).
- AI, ML, and automation have become increasingly integral to cybersecurity solutions. These technologies enhance detection and response and allow SOC analysts to focus on what's important instead of chasing down false alerts.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- But automation cannot replace human analysts just yet, as organizations cannot trust AI to handle complex decision-making beyond detection and response.
- As organizations seek alternative ways to cope with the shortage of security analysts, they will adopt solutions that leverage ML and AI in combination with the ever-important human factor.
- As a result, security services such as MDR will continue to thrive in the next three years while security providers invest in developing and enhancing automated security assistants.
- Due to the sophisticated nature of the latest cyberattacks, the growing incidence of nation-state-sponsored threats, and the increasing number of cybersecurity incidents, there's an arms race between threat actors, security solutions, and service providers.
- Organizations are caught in the middle, with the pressure to understand, invest in, and keep up with the latest developments in the cybersecurity industry to protect their environments.
- As digital transformation continues and geopolitical conflicts around the globe progress, organizations will continue to be targeted by complex cyberattacks and data breaches.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- MDR's promise to bolster an organization's security posture with 24/7 monitoring, state-of-the-art detection and response, and incident response capabilities will resonate with global organizations for the foreseeable future.

Source: Frost & Sullivan

Growth Environment

- According to Frost & Sullivan's 2023 Voice of the Enterprise Security Customer survey, 36% of global organizations were using MDR at the beginning of 2023, with a further 26% of them planning to invest in the service by 2024.
- MDR has witnessed widespread adoption in 2023, with a growth rate of 35.2% and a compound annual growth rate (CAGR) of 25.3% expected from 2023 to 2026. MDR has made significant waves in the cybersecurity industry thanks to its ability to address many of global organizations' most pressing pain points.
- The dearth of security talent and the rapid increase in the number and sophistication of threats generate the perfect conditions for MDR to thrive. These driving factors are not expected to diminish soon and will continue to push organizations to outsource their security, either partially or completely.
- The growth rate and customer adoption of MDR services will remain high for the foreseeable future, as the platform's drivers far outweigh its restraints and limitations.

Source: Frost & Sullivan

Growth Environment

- The lion’s share of MDR revenue and adoption comes from North America, but Europe, the Middle East, and Africa (EMEA) is a close second. These regions' higher maturity and cybersecurity focus and increased government involvement in guiding organizations toward effective security strategies and compliance make MDR a great option for businesses in both regions. They will continue growing rapidly for the next three years and remain high-priority investments for MDR providers.
- As with most high-end cybersecurity solutions and services, Latin America (LATAM) and Asia-Pacific (APAC) account for smaller contributions to MDR revenue. Nonetheless, these regions have a higher potential for growth, as the CAGR is higher for the 2023–2026 period, showing that adoption is expected to ramp up for local organizations. The new MDR message, with extended incident response and adjacent services that increase maturity and awareness, resonates with regional companies. Highly involved MDR partners could leverage their competitive differentiators to expand into these regions in the next few years.

Source: Frost & Sullivan

Growth Environment

- Organizations across various company sizes consider MDR a worthwhile option to secure their business-critical assets. While enterprises with more than 10,000 employees account for less revenue and growth, it is to be expected from companies that have already invested in their SOCs and have experienced analysts working with them.
- The highest-spending industry verticals for MDR are finance, government, manufacturing, and technology & telecommunications. Overall, adoption is high across every sector, with every MDR provider focusing on different integrations, providing visibility into distinct environments, and delivering multiple adjacent services. Such specialization means most organizations can find an MDR partner that meets their needs and use cases.



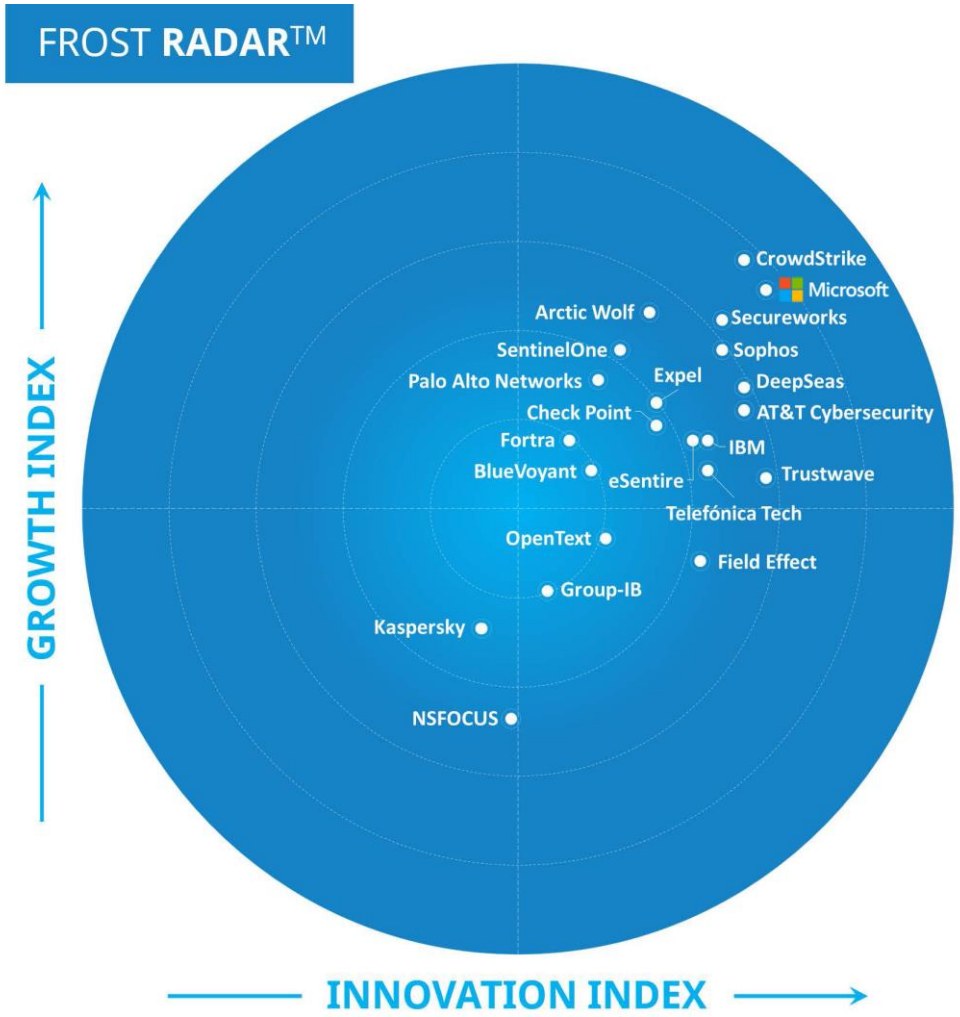
Source: Frost & Sullivan

FROST & SULLIVAN



Frost Radar™ Managed Detection and Response, 2024

Frost Radar™: Managed Detection and Response, 2024



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- In a rapidly growing field of more than 150 industry participants with revenue greater than $1 million, Frost & Sullivan independently plotted 22 growth and innovation leaders in the MDR space in this Frost Radar analysis.
- Over the last few years, MDR providers have developed solutions to deliver extensive visibility over the environment, advanced detection of the most pervasive threats, and a veteran team of expert security analysts supported by AI, ML, and automation capabilities. MDR has become the primary way of delivering SOC services, unifying capabilities such as detection and response, investigation, threat hunting, and more under a single platform.
- Because of this, the MDR sector will continue to see an influx of new competitors from very different spaces, including endpoint detection and response (EDR) and extended detection and response (XDR) vendors, players with extensive coverage and portfolios, and managed security services providers (MSSPs) wanting to leverage their ample service offerings.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- MDR providers will face fierce competition from XDR vendors and MSSPs that do not provide managed XDR or an MDR platform. These spaces seek to provide organizations with comprehensive and centralized security that enables and empowers the customers' analysts via many of the same features.
- The most significant innovations of highly successful MDR platforms and services include implementing threat detection across a wide range of environments to address multiple use cases, leveraging world-class threat intelligence and ML features to empower analysts, providing a synergistic portfolio of complementary managed and professional services to multiply the value of the MDR service; integrating third-party telemetry sources to augment flexibility; and developing and implementing large language models (LLM) tools and generative AI security assistants to ramp up the effectiveness of new analysts and facilitate the lives of experienced ones.



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Microsoft is one of the innovation leaders in the MDR Frost Radar. The company's focus on AI and ML, especially the development of Copilot for Security, coupled with its top-tier threat detection and response capabilities, allows it to maintain an innovation edge over other world-class competitors. Microsoft is a recent entrant in the MDR space but has carefully exploited its advantages to deliver a robust growth strategy and obtain rapid revenue growth.



Source: Frost & Sullivan

FROST & SULLIVAN



Companies to Action:

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

Company to Action: Microsoft

Innovation

- Microsoft provides cross-domain MDR services through its Microsoft Defender Experts for XDR solution, with visibility over endpoints, email, cloud, and identity. The company delivers 24/7 monitoring, detection and response, and proactive threat hunting, combined with its world-class threat intelligence, security posture assessments, access to its expert team, and compliance management.
- Microsoft is heavily focused on developing and leveraging AI and ML for all its security solutions, and MDR is no exception. Microsoft Copilot for Security is an AI assistant that empowers security analysts by summarizing data signals, providing insights, helping with detection, and adding context to alerts and incidents. This tool supports junior analysts who are still gaining experience as well as experts by allowing them to make fully informed decisions.
- Microsoft Defender Experts for XDR can take action on a customer's behalf and provides one-click managed response functionality where customers can get additional details and take any pending actions on assets they may have decided to exclude from the Defender Experts for XDR service scope. Additionally, the service has an embedded chat experience integrated with Microsoft Teams to enable customers to directly interact with Microsoft Defender Experts, promoting collaboration and increasing security maturity for customers' teams.

Source: Frost & Sullivan

Company to Action: Microsoft

Innovation

- Microsoft's MDR service includes Defender Experts for Hunting, a threat-hunting service with on-demand expert support. Microsoft Incident Response Retainer is sold separately as an add-on for customers who need incident response services.
- Microsoft spends a significant part of its R&D budget on the development of Copilot for Security and LLM-based technology, expanding the scope of its service for the government sector, extending the coverage of its MDR service to Defender for Cloud, and providing additional integration with third-party data sets.

Source: Frost & Sullivan

Company to Action: Microsoft

Growth

- Microsoft is a newer player in the MDR space, but in a short time, the company has carved out a significant presence in the sector. Such rapid expansion is possible thanks to its brand name and varied and successful solution portfolio, which create numerous upselling and cross-selling opportunities for Microsoft's MDR service.
- The company serves the needs of every industry vertical, region, and across all company sizes and maturity levels. However, its approach to MDR is better suited for medium to large enterprises.
- For added flexibility, Microsoft has extended the Defender and Sentinel platforms with API and multi-tenant support for over 40 verified managed XDR (MXDR) service partners that can provide MDR services through the platform. This partnership initiative is highly beneficial for both parties, as it provides growth opportunities, increases brand equity, and extends the reach of Microsoft's technology.

Source: Frost & Sullivan

Company to Action: Microsoft

Frost Perspective

- Microsoft's foray into the MDR sector is recent, but the company is already making waves as one of the most innovative in the space. Microsoft's overall focus on automation, ML, and AI outside the cybersecurity industry has helped the company develop its Copilot for Security Assistant as an extremely valuable tool that enables and empowers analysts. The company's threat intelligence, embedded chat feature, and extensive threat detection and response capabilities augmented by ML ensure an effective MDR service.
- Thanks to the broad security portfolio and brand equity that Microsoft brings to the table in conjunction with its partnership initiative and wide-reaching distribution, the company's rapid growth will continue for the foreseeable future.
- Microsoft doesn't support third parties yet, but the company is investing in integrating third-party sources and expanding visibility. Microsoft's R&D focus on flexibility and AI is aimed in the right direction for success in the MDR sector. Microsoft should continue developing its MDR platform with both factors in mind to maintain its competitive differentiators.

Source: Frost & Sullivan

FROST & SULLIVAN



Key Takeaways

Key Takeaways

1

MDR can benefit any organization and enjoys high adoption across many industry verticals; it caters to the needs of diverse global organizations with different use cases and maturity levels.

2

Frost & Sullivan's 2023 Voice of the Enterprise Security Customer survey revealed that 1in 2 organizations that spend money on security services, such as managed security services (MSS), professional security services (PSS), MDR, threat intelligence services, and SOC monitoring, used MDR in early 2023. A further 36% of these enterprises plan to add MDR by 2024.

3

The percentage of MDR adopters out of all organizations is also significant, with 36% using it by 2023 and 26% planning to deploy it by 2024.

Source: Frost & Sullivan

Key Takeaways

4

Collaboration or outsourcing: MDR providers have different approaches as to how the service should be delivered. Some are at their best when collaborating with customer security teams, increasing their maturity over time and performing threat hunting and investigations as a unified group. Other providers prefer to take care of everything themselves, sending periodic reports to customers and allowing them to focus their resources elsewhere. MDR can completely replace or assist and empower your cybersecurity team and everything.

5

Environment visibility: Top-tier MDR players can provide visibility across various environments, from the classic trio of endpoint, network, and cloud to email, identity, containers, OT and IoT devices, and others. However, focus can also be a good choice. If your organization only needs to cover a few specific environments, looking for a specialized vendor that provides the deepest visibility across fewer security controls is better.

Source: Frost & Sullivan

Key Takeaways

6

Adjacent service offering: A comprehensive portfolio of additional synergistic tools and services will make MDR a more flexible solution than it already is, empowering your organization with additional capabilities at a fraction of the cost. Those tools, however, are as varied as MDR providers. MSSPs with cutting-edge MDR solutions can usually provide a wider set of adjacent managed tools and professional services. However, leading pure-play vendors are heavily investing in providing these as well. If you seek to advance your organization's security maturity and develop your security team, consulting engagements, assessments, and penetration tests can be a worthy addition to MDR.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics



Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

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.

GROWTH INDEX ELEMENTS

- **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

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.

INNOVATION INDEX ELEMENTS

- **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 Disclaimer

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: permission@frost.com

© 2023 Frost & Sullivan. All rights reserved. This document contains highly confidential information and is the sole property of Frost & Sullivan.
No part of it may be circulated, quoted, copied, or otherwise reproduced without the written approval of Frost & Sullivan.