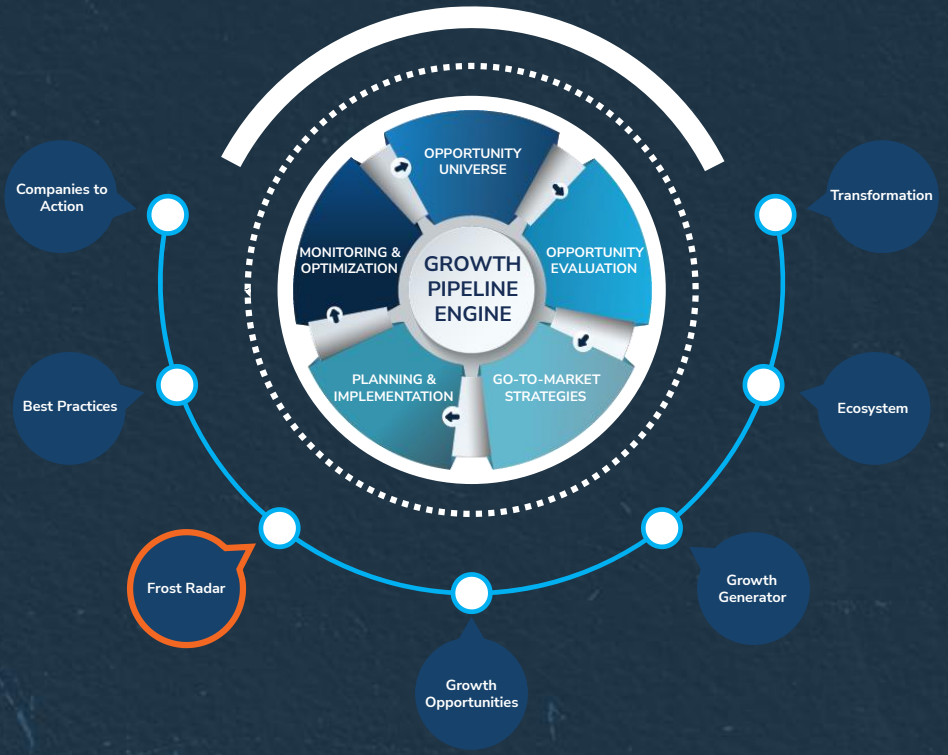
FROST & SULLIVAN

Frost Radar™: Managed Detection and Response, 2025

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



KB57-74
July 2025

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

- Cybersecurity outsourcing remains a top priority for many organizations because it enables them to address the scarcity of cybersecurity professionals and the associated costs of building and staffing a modern security operations center (SOC). Governments and businesses need 24/7 security monitoring, which multiplies the cost of effective SOCs and underscores the benefits of partnering with security service providers to protect business-critical data.
- Managed detection and response (MDR) providers can deliver highly effective and advanced security across the environment, leveraging experienced teams of cybersecurity professionals and SOCs with global footprints and reach.
- In the next 3 years, organizations will continue to invest in outsourced security through MDR services while they focus personnel on the core business instead of building internal SOCs.
- Artificial intelligence (AI) and machine learning (ML) are integral aspects of modern cybersecurity. The sophistication and speed of attacks require faster-than-human responses; however, attackers also leverage these tools, making it even more essential for organizations to harness them in their cybersecurity strategies.
- While increasingly advanced, AI tools are not designed to replace human analysts, but to complement them and aid them in their strategic cybersecurity decision-making.
- Cornered by sophisticated threats, with fewer analysts at their disposal and attackers that leverage AI tools to target them, more and more organizations are adopting AI-powered, human-supervised security services and platforms to increase their cyber resilience. Advanced security services, such as MDR, will continue to thrive as providers invest in agentic AI and combine it with human expertise.

Strategic Imperative (continued)

- Geopolitical tensions continue to mount, with a growing number of conflicts around the world, including the Russo-Ukrainian War, the India-Pakistan crisis, and wars in the Middle East. Such conflict fuels state-sponsored cyber threats, increasing the number of attacks across the globe and resulting in an arms race between threat actors and cybersecurity solutions and service providers. Organizations can be collateral damage and are under tremendous pressure to understand, invest in, and keep up with the latest developments in the cybersecurity industry to protect their environments.
- As geopolitical tensions continue to churn, one thing is clear: organizations will continue to be targeted by highly complex cyberattacks and data breaches, and critical infrastructure will remain a prime target for state-backed cybercriminals.
- MDR's capabilities, including 24/7 monitoring, incident response, threat hunting, and a focus on proactively securing customer environments, will enjoy high adoption from organizations seeking the best tools a provider can offer.

Growth Environment

- The MDR market continues to expand rapidly, showing a projected growth of 24.8% in 2025 and a compound annual growth rate of 20.7% in the 2024–2027 period. This is healthy for a market that has entered a more mature phase in which buyer confusion tends to be less of an issue and adoption continues to be significant across all regions, industry verticals, and company sizes.
- The rapid growth stems from rising complexities, resource constraints, and digital transformation as organizations face more pressure to secure evolving and complex environments. Hybrid cloud and multicloud infrastructure is now the norm, and organizations must secure vast numbers of endpoints and mobile devices as remote work arrangements remain commonplace.
- Operational technology (OT) and the internet of things (IoT) are prevalent across mission-critical organizations and those that leverage them to enhance productivity. However, these tools expand the attack surface and make environments harder to secure. MDR addresses these issues, providing essential visibility and swift response capabilities across these complex environments.
- The number and sophistication of attacks are also on the rise, driven by multiple factors, including geopolitical instability and war, ransomware-as-a-service, AI-powered cyberattacks (including deepfake technology for more effective phishing, AI-generated malicious code, and potential agentic AI frameworks), and infrastructure vulnerability. Organizations short on cybersecurity personnel are overwhelmed by alert fatigue and demand expert-driven threat hunting, rapid incident response, comprehensive visibility, and automated remediation to protect their business-critical data.
- MDR continues to thrive because it combines the most advanced analytics that extended detection and response (XDR)/security operations platforms can provide with proactive threat hunting, integrated threat intelligence, and 24/7 SOC analyst expertise, giving organizations peace of mind.

Source: Frost & Sullivan

Growth Environment (continued)

- Another factor contributing to the significant growth of the MDR market is organizations' need for consolidation. Beyond its correlation capabilities and ability to piece together the entire attack story, MDR can also unify first- and third-party security solutions. Multiple providers in the market focus on one or the other, and organizations are not starved for choice when it comes to finding one that fits their needs and vision.
- Initially, MDR was primarily the service of choice for organizations with limited internal cybersecurity expertise or budgets insufficient for comprehensive, in-house SOC capabilities. However, innovations related to AI, ML, agentic AI, customizable automation playbooks, intuitive graphical interfaces, the increasing involvement of threat intelligence, and the focus on proactive security capabilities have made MDR accessible to all types of businesses and even more appealing to organizations with mature security teams. As a result, adoption across company sizes is similarly high, although enterprises in the mid-market still contribute a larger share of MDR revenue globally.
- North America accounts for the lion's share of MDR revenue, thanks to the region's high security maturity and adoption of technology. The EMEA region (particularly Europe), closely follows North America in terms of adoption because of regulatory environments mandating advanced security practices. These regions are home to numerous digital organizations with complex infrastructure and advanced security needs and will continue to be strongholds for MDR growth for the foreseeable future.
- Latin America and Asia-Pacific are increasingly relevant for MDR providers. The most mature countries in these regions are establishing regulatory frameworks that, coupled with the accelerating digital transformation of local organizations, have led to greater awareness of cybersecurity threats. Organizations here want MDR providers that can help them build their security strategy and protect their assets from the most pervasive and advanced threats. Vendors are expanding their presence in these regions through local partnerships, vertical-focused offerings, and region-specific SOC expansions.

Source: Frost & Sullivan

Growth Environment (continued)

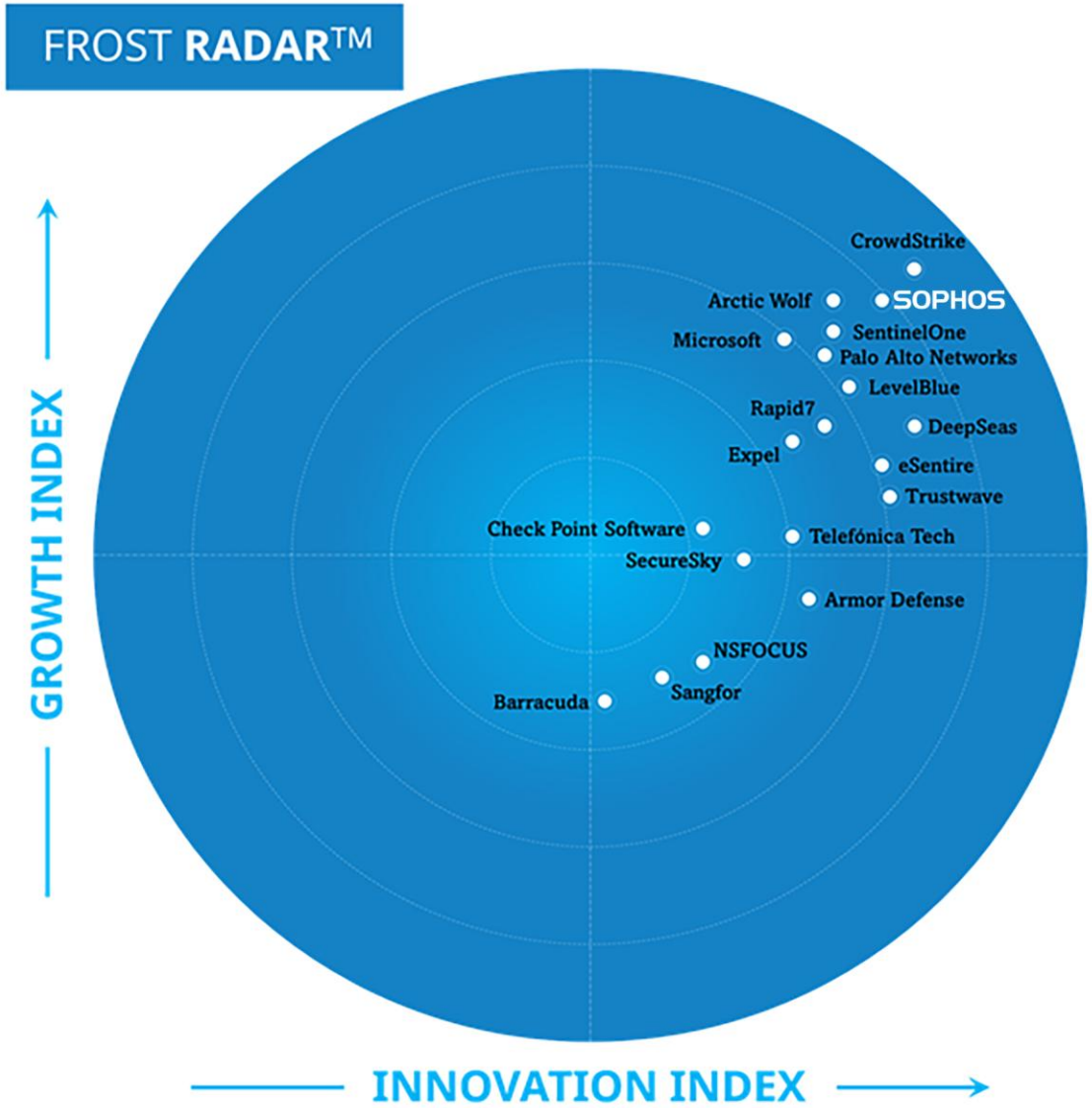
- MDR’s can provide actionability and visibility across multiple environments (including endpoint, network, cloud workloads, OT, IoT, and mobile). Financial services organizations, traditionally early adopters of the most advanced cybersecurity tools and solutions because of their high standards and security maturity, remain the leading MDR customers, and will continue to be for the foreseeable future. Manufacturing, healthcare, technology, and telecommunications companies and government organizations also can benefit greatly from MDR's holistic and proactive security capabilities and will continue to adopt it at a slightly higher rate than other industry verticals.

FROST & SULLIVAN

Frost Radar™

Managed Detection and Response

Frost Radar™: Managed Detection and Response



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- From a rapidly growing and increasingly competitive field of more than 120 industry participants with revenue greater than $1 million, Frost & Sullivan independently benchmarked 19 of the leading MDR providers for this Frost Radar™ analysis.
- The number of MDR providers continues to increase; while many have modest success, some are thriving, evident by their sizable revenue and consistent growth. MDR is now a staple of cybersecurity and the primary way of delivering SOC services, unifying capabilities such as detection and response, in-depth investigation, threat hunting, proactive and autonomous security, and more under a single platform.
- Rating the complexity, variety, and effectiveness of all the innovation and growth approaches to MDR is challenging. Frost & Sullivan considered the main aspects of MDR, including but not limited to detection and response capabilities, data correlation and analysis, incident response, threat hunting, teams that deliver the various services offered, integration of GenAI and agentic AI as part of the service and platform, adjacent services (including add-on services and those included as part of any tier of service that the provider has), first- and third-party integrations, visibility and actionability across security vectors and environments, usability and collaboration features that foster partnership with customers, threat intelligence, inclusion of proactive security capabilities (such as behavioral analysis and identity threat detection and response), adequacy of strategy to target customers, R&D spending, revenue share and growth, and sales and marketing.
- Frost & Sullivan also conducted interviews with customers of these services, asking questions about the services that they are using or have used in the recent past and gaining insights on customer satisfaction, customer alignment, and intangible factors that contribute to the overall customer experience.

Frost Radar™ Competitive Environment (continued)

- In the cybersecurity industry, MDR, XDR, and managed security service providers (MSSPs) have a similar goal: to provide clients with comprehensive and centralized protection across complex ecosystems, and to augment SOC analysts with additional resources, such as automation, support from external analysts, and complementary services. Because of this, MDR providers are not only facing competition from each other, but from adjacent cybersecurity spaces: vendors that offer an XDR platform, managed XDR services, or MSSPs that do not provide MDR.
- Most market players can be categorized as either pure-play MDR firms that rely on customer-focused service delivery and their long history of providing the service; MSSPs that have developed MDR platforms and services, harnessing their extensive managed and security service offerings to multiply value for customers; and cybersecurity vendors that leverage their extensive portfolios for coverage, detection and response excellence, and growth. However, each MDR provider is unique, and many are somewhere in between two or even three categories in one way or another.
- To stand out in an increasingly crowded market, MDR providers have been heavily investing in innovation and technology. The most advanced developments of successful MDR providers are constant improvements to detection and response accuracy and speed, leveraging ML, AI, threat intelligence, behavior analysis, indicators of compromise (IOCs), and more. The integration of security assistants powered by GenAI and agentic AI accelerates the development of junior analysts, frees up time for senior analysts, and improves resilience with automated investigations and threat hunts.
- Providers continue to extend third-party integration across hundreds of security solutions and tools, securing the attack surface effectively, providing flexibility for organizations to embrace a best-of-breed approach to cybersecurity. Increasing the number and synergy of adjacent, complementary security services can provide additional information to improve security strategies, deliver insights into a customer's security posture, and multiply the value for clients.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Proactive cybersecurity capabilities move the focus to prevention and help mitigate or even stop threats before they materialize. Several MDR leaders are evolving their solution in line with the Continuous Threat Exposure Management (CTEM) approach, a structured program that focuses on proactivity and prevention, including risk prioritization, vulnerability assessments, and anomaly detection.
- In a market with so many successful cybersecurity companies competing against each other, the differences between top players are relatively small, and mostly depend on implementation timings and strategic approaches. As a result, every vendor appearing on this Frost Radar™ might be an ideal partner to fit the needs of different types of customers according to their approach and environment coverage.
- CrowdStrike is the Frost Radar™ Growth and Innovation leader. As one of the market share leaders, with an effective go-to-market strategy and a well-developed growth pipeline, CrowdStrike secured the top position on the Growth Index. The firm provides fast and accurate detection and response capabilities backed by one of the most developed AI assistants in the market, Charlotte AI, and complemented by multiple adjacent services and a team of battle-tested cybersecurity professionals.
- With the acquisition of Secureworks, Sophos has multiplied its capabilities, showing that the resulting organization is greater than the sum of its parts. As the firm works on integrating services and solutions together, it continues to be one of the top competitors in the MDR market thanks to its focus on proactive security, ample coverage of the environment, and multiple adjacent services.
- Arctic Wolf has a vast market presence and a customer-focused approach that does not dwindle even with the scale of its operations across the globe. The firm is investing in all the right trends and leveraging its know-how and history in the space to thrive in the MDR market, achieving a good position across both Frost Radar™ axes.

Frost Radar™ Competitive Environment (continued)

- SentinelOne, Palo Alto Networks, and Microsoft have exploited the breadth of their security coverage, delivering effective MDR solutions complemented by many services and relying on advanced GenAI and agentic AI systems to address the needs of customers across all major industries and regions. SentinelOne and Palo Alto Networks have expanded their presence and coverage in the last few years and carved out significant MDR mindshare, which presents many future growth opportunities.
- LevelBlue is among the Growth Index leaders, leveraging its significant resources and investments in managed security in general to provide an advanced service with one of the most comprehensive ecosystems of third-party integrations. While it is slightly behind other leaders in terms of agentic AI investments, its coverage of the environment and portfolio of adjacent services allows it to multiply value for customers.
- Rapid7 and Expel are pure-play MDR providers that have found success in their customer-focused service strategies. Both are somewhat behind leading competitors in agentic AI developments, but they rival or overcome them in service delivery. Their roadmaps are solid and show an understanding of the essential aspects of MDR, and they will continue to be among the top players in the market as they follow through by adding capabilities and improving their service.
- DeepSeas, eSentire, and Trustwave are among the most advanced firms in the market and are Innovation Index standouts on the Frost Radar™. These providers have significant vendor-agnostic integration capabilities, providing comprehensive security across complex customer environments as well as many proactive security capabilities that increase customers' cyber resilience as AI-powered attacks become more common. DeepSeas and eSentire have developed tight integrations with AI as part of their workflow, embracing agentic AI as essential elements in their toolkits. Trustwave is behind the other two on agentic AI features, but it is about to even the score and features other value-multiplying tools and services that significantly enhance its value proposition.

Frost Radar™ Competitive Environment (continued)

- Telefónica Tech relies on its MSS pedigree, consulting strength, know-how expertise on multiple industries, and complementary services to deliver effective MDR to its customers in Europe and Latin America. While its small presence in North America affected its Growth Index position, it is actively investing in expanding across the region (e.g., its partnership with the Levan Center of Innovation in Florida), and it is only a few roadmap items away from reaching the Innovation Index leaders.
- SecureSky is among the most unique firms in the market, having embraced a CTEM-powered approach that fully focuses on proactively addressing threats while maintaining regular MDR capabilities, such as threat hunting and incident response. As SecureSky continues to invest in its unconventional approach, the firm has good potential for growth and could become a significant innovator in the space.
- Armor Defense offers an approach focused on transparency, collaboration, and proactive protection in the form of risk assessment and reduction. The firm ticks all the boxes for MDR megatrends, and while it is slightly behind top competitors in innovation, it has potential to be among the innovation leaders if it follows through on its roadmap.
- Check Point Software has a slower approach to the use of AI, third-party integration, and coverage of the ecosystem. However, if it continues to leverage the power of its excellent XDR solution, invest in MDR R&D, and enhance its service with agentic AI, it will improve its Frost Radar™ position significantly.
- NSFOCUS, Sangfor, and Barracuda are ahead of the average MDR provider, but behind the leading competitors in both growth and innovation. These firms lack the ecosystem of integrations and coverage of the environment that leaders have but are focusing on expanding them as well as their additional services and other capabilities. While their services and platforms embed AI to improve workflows, they lack deeply autonomous capabilities that other top players in the market already have. NSFOCUS and Sangfor are limited by their lack of presence in profitable North America and Europe, but they are leveraging growth opportunities in other fast-growing regions.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Several providers, including Fortra, Group-IB, IBM, and ReliaQuest, were considered for this Frost Radar™, but chose not to participate in the research process and were not included because of the lack of sufficient information for benchmarking. OpenText was not included because the firm was undergoing a significant transformation of its MDR service at the time of the research.

FROST & SULLIVAN

Frost Radar

Companies to Action

Sophos

INNOVATION

- Sophos MDR integrates natively with Sophos's own broad portfolio (endpoint, firewall, cloud, email, ZTNA, and more) and with more than 350 third-party solutions, enabling open-platform delivery and ensuring deep visibility and control across diverse environments, including Microsoft and Google Workspace ecosystems.
- Sophos MDR's core service includes unlimited, human-led incident response at no extra charge—a differentiator that gives customers peace of mind. Sophos offers vulnerability and attack surface management, threat hunting, exposure management, NDR, backup and recovery monitoring, and other complementary services that round out its MDR offering. All services are bolstered by Sophos X-Ops, its expert research unit with more than 500 professionals from different cybersecurity domains.
- In February 2025, Sophos completed its acquisition of Secureworks, another major player in the MDR and XDR spaces. The fusion between the two companies has caused major waves in the market and has provided Sophos with additional solutions and services that multiply the value for customers. Secureworks has boosted and expanded Sophos's capabilities in several ways: bringing in its identity threat detection and response solution; providing OT visibility and security, an expanded third-party ecosystem of integrations, dark web monitoring, and posture management; and including the proprietary threat intelligence from Secureworks' Counter Threat Unit. Sophos is consolidating the Secureworks and Sophos solutions into the Sophos Central platform, providing SIEM-style capabilities and enhancing custom playbooks and threat hunting with more tailored responses.

Sophos (continued)

INNOVATION

- The solution offers flexible response modes with different levels of involvement that work for organizations across the security maturity spectrum: just notifying customers, collaborating as a team, or fully authorizing Sophos to perform response and remediation actions on their behalf. This allows customers to fully outsource operations, augment internal teams, or engage in a hybrid model.
- Sophos has its own AI security assistant, which guides end-to-end investigations. Analysts can interact with it via natural language prompts and queries, and it provides capabilities such as querying endpoints, enriching investigations and alerts with threat intelligence, summarizing cases, and recommending next steps. It also uses AI to analyze and explain potentially malicious command lines, and analysts can leverage it to search the Sophos Data Lake for faster alert triage.
- While a large part of Sophos's roadmap is shaped by the Secureworks fusion and the integration of its tools, which will enable the firm to truly unify and synergistically leverage the advantages of both companies and their respective security stack, Sophos is also investing considerably in R&D initiatives. A key focus area for the firm in this regard is AI, which includes general improvements to automated triage for faster and more intelligent responses, additional agentic AI capabilities, and more. Sophos also is expanding third-party integrations and enhancing its dashboard and reporting capabilities.

Sophos (continued)

GROWTH

- Sophos provides MDR services to organizations of all sizes and industry verticals but has traditionally had a strong grip on SMBs and the mid-market. Secureworks, on the other hand, was focused on the enterprise market, and its acquisition will enable Sophos to serve a broader range of customers, covering the entire range of business sizes.
- The firm's 100% channel-driven model leverages more than 60,000 global partners, including MSPs and MSSPs, to expand reach and accelerate adoption. The recent strategic alliance with Pax8 significantly broadens its exposure to more than 40,000 MSPs, fueling expansion in the SMB space. Today, Sophos MDR protects more than 30,000 organizations globally, providing them with massive insight into different attack patterns and threats across industry verticals and locations, expanding its threat intelligence and feeding its detection engine.
- Sophos's go-to-market strategy involves targeting companies in specific verticals and organizational maturity levels with tailored content, self-assessment tools, and industry reports. For example, the company aims its ransomware-focused campaigns at education, manufacturing, and healthcare, and includes localized resources in multiple languages. Its field CISO program and vertical-focused sales overlays offer strategic guidance aligned with regulatory and operational needs. Sophos's presence and brand equity in many other cybersecurity markets create growth opportunities from customer organizations wanting to expand their partnership with the vendor.

Sophos (continued)

GROWTH

- Sophos offers two tiers of service—Sophos MDR Essentials and Sophos MDR Complete—in addition to Secureworks' Taegis MDR offerings. Sophos MDR Essentials is aimed at organizations with internal cybersecurity capabilities, as Sophos does not perform full remediation on the customer's behalf. This tier still provides 24/7 monitoring and detection, support for third-party telemetry, threat hunting, reporting, threat intelligence briefings, and more. Sophos MDR Complete adds full-scale incident response on top of these features, a dedicated incident response lead, and a $1 million breach protection warranty. These two tiers allow Sophos to target all kinds of organizations, provide versatility for customers, and allow for the possibility of customers moving from one tier to the other depending on their security maturity evolution.

Sophos (continued)

FROST PERSPECTIVE

- Sophos's acquisition of Secureworks is one of the most important deals in the history of MDR. As a result, Sophos has gained in technology, strategy, processes, and people, enriching its capabilities to become something better than the sum of both companies' parts. Sophos MDR, already a powerhouse in the market, will continue to evolve as the firm builds up this synergy piece by piece, leading to numerous growth opportunities. As Sophos continues to find a delicate balance in this process, the company's future in the MDR space looks bright.
- Sophos provides extensive visibility across complex environments, features multiple AI-powered capabilities, and can multiply the value of its MDR services with numerous adjacent services. The firm's strategy of bundling unmetered IR within its MDR Complete tier is a powerful differentiator that multiplies customer value. To extend its MDR solution's coverage and provide additional use cases, Sophos should consider expanding its dark web monitoring capabilities into a stand-alone solution. This would provide an early threat detection boost, improve threat hunting and threat intelligence capabilities, and offer cross-selling opportunities. It would pair extremely well with the firm's breach warranty, as cyber insurance increasingly has dark web monitoring as a requirement.
- From an AI perspective, Sophos is moving in the right direction. The firm should continue to evolve its AI assistant, because achieving a higher degree of agency and automation is important to remain competitive in the MDR market. Sophos should integrate its adjacent services and the valuable insights that it can obtain with its AI to deliver better recommendations and drive automated investigations, contextualization, and responses.

Sophos (continued)

FROST PERSPECTIVE

- Sophos has a strong alignment with proactive security measures and the CTEM approach to cybersecurity, which is becoming important for platforms at the center of the SOC, such as XDR and MDR. Sophos should embed CTEM capabilities directly into its platform, leveraging its threat intelligence, Sophos Managed Risk, and exposure management to deliver proactive security as a continuous lifecycle. Dashboards and reporting options with the result of these assessments in combination with other KPIs and security posture items would showcase the firm's value proposition. This would align with multiple elements in Sophos's strategy, including its customer focus, flexibility, and adaptive defense, and drive growth for its MDR service.

FROST & SULLIVAN

Best Practices & Growth Opportunities

Best Practices

1. Successful MDR vendors are rapidly integrating generative and agentic AI to enhance analyst productivity and scale services. GenAI enables natural language threat hunting, automated reporting, and investigation summaries, while agentic AI autonomously handles detection, triage, and response with minimal analyst input. Automation via pre-built playbooks remains essential for consistent responses. This AI-driven automation focus boosts efficiency across analyst tiers and expands MDR's scope.

2. Leading MDR providers are shifting toward proactive security by integrating identity threat detection and response to spot credential misuse and behavior anomalies. Combining identity analytics with threat intelligence, risk assessments, attack simulations, and CTEM tools enables the blocking of emerging threats. This convergence transforms MDR from reactive to proactive, providing holistic protection, stronger cyber resilience, and an improved security posture for customers.

3. MDR services are typically built on cybersecurity platforms, such as XDR with SIEM and SOAR capabilities. Customers expect this type of integration by now. To excel, MDR providers should expand third-party integrations for greater flexibility, visibility, and actionability across complex environments. Adjacent services, such as automated penetration testing, red/blue team exercises, and compliance, vulnerability, and risk assessments enhance value for stakeholders and strengthen customer security.

Growth Opportunities

1 High-stakes finance, healthcare, manufacturing, utilities, and government organizations are prime cyberattack targets. MDR providers can better serve them by integrating vertical-specific AI and ML models trained on industry data, threat intelligence, workflows, and regulations. This improves detection accuracy, automates tailored responses, and reduces response times. Such specialized offerings create growth opportunities and position MDR vendors as domain experts in these critical industries.

2 Expanding SOC infrastructure in regions with low MDR adoption but high growth potential, such as Latin America and Asia-Pacific, enables compliance with local data regulations and provides localized support. Regional SOCs improve cultural alignment, language compatibility, and trust with customers—key for MDR success. This local presence becomes a competitive differentiator, helping providers invest in regional staff and facilities to outperform global competitors in these markets.

3 To scale efficiently and expand regionally and across industries, MDR vendors should partner with MSPs, MSSPs, other MDR providers, and cloud ecosystems. White-labeling MDR platforms offers additional growth opportunities without direct service delivery, though it may not suit all strategies. Flexible MDR solutions attract third-party providers by covering diverse attack surfaces, accelerating expansion, diversifying go-to-market channels, and reaching SMBs and organizations with lower security maturity.

FROST & SULLIVAN

Frost Radar™ Analytics

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

Growth Index

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.

Source: Frost & Sullivan

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

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) 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

MEGATRENDS 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 megatrends 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.

Source: Frost & Sullivan

FROST & SULLIVAN

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders

Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Frost Radar™ Empowers the CEO's Growth Team

STRATEGIC IMPERATIVE

- Growth is increasingly difficult to achieve.
- Competitive intensity is high.
- More collaboration, teamwork, and focus are needed.
- The growth environment is complex.

LEVERAGING THE FROST RADAR™

- The Growth Team has the tools needed to foster a collaborative environment among the entire management team to drive best practices.
- The Growth Team has a measurement platform to assess future growth potential.
- The Growth Team has the ability to support the CEO with a powerful Growth Pipeline™.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

Source: Frost & Sullivan

Frost Radar™ Empowers Investors

STRATEGIC IMPERATIVE

- Deal flow is low and competition is high.
- Due diligence is hampered by industry complexity.
- Portfolio management is not effective.

LEVERAGING THE FROST RADAR™

- Investors can focus on future growth potential by creating a powerful pipeline of Companies to Action for high-potential investments.
- Investors can perform due diligence that improves accuracy and accelerates the deal process.
- Investors can realize the maximum internal rate of return and ensure long-term success for shareholders
- Investors can continually benchmark performance with best practices for optimal portfolio management.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

Source: Frost & Sullivan

Frost Radar™ Empowers Customers

STRATEGIC IMPERATIVE

- Solutions are increasingly complex and have long-term implications.
- Vendor solutions can be confusing.
- Vendor volatility adds to the uncertainty.

LEVERAGING THE FROST RADAR™

- Customers have an analytical framework to benchmark potential vendors and identify partners that will provide powerful, long-term solutions.
- Customers can evaluate the most innovative solutions and understand how different solutions would meet their needs.
- Customers gain a long-term perspective on vendor partnerships.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar™ Benchmarking System**

Frost Radar™ Empowers the Board of Directors

STRATEGIC IMPERATIVE

- Growth is increasingly difficult; CEOs require guidance.
- The Growth Environment requires complex navigational skills.
- The customer value chain is changing.

LEVERAGING THE FROST RADAR™

- The Board of Directors has a unique measurement system to ensure oversight of the company's long-term success.
- The Board of Directors has a discussion platform that centers on the driving issues, benchmarks, and best practices that will protect shareholder investment.
- The Board of Directors can ensure skillful mentoring, support, and governance of the CEO to maximize future growth potential.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Source: Frost & Sullivan

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

Source: Frost & Sullivan

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