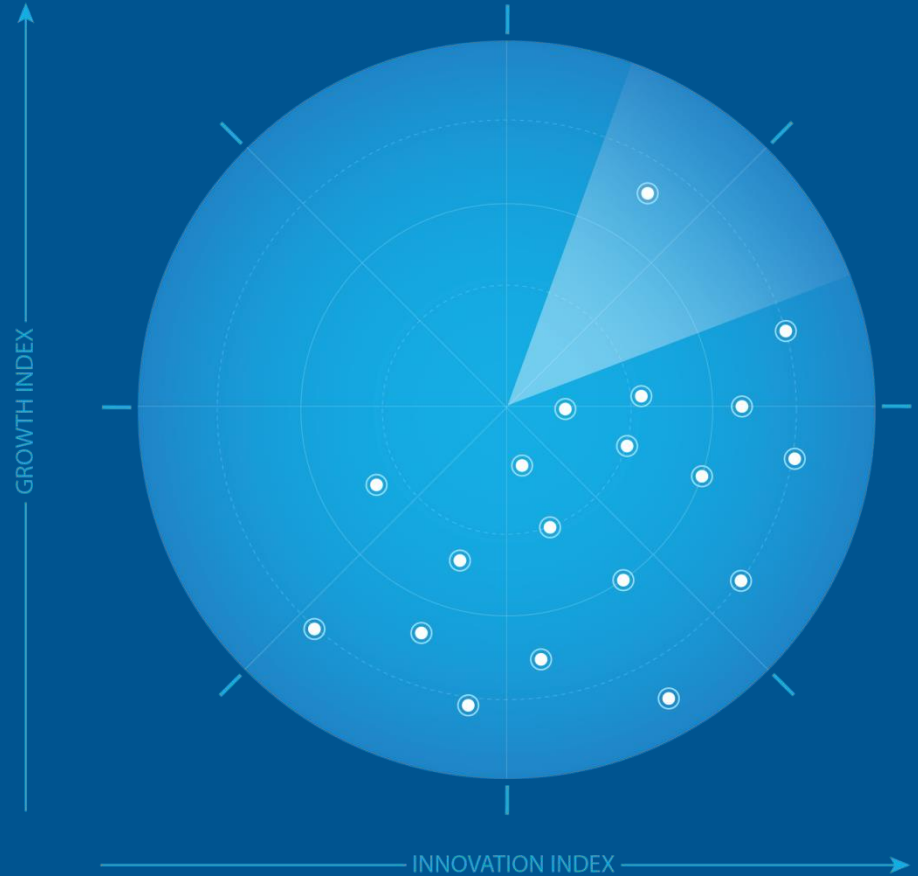


Frost Radar™: Extended Detection and Response, 2023

Authored by: Lucas Ferreyra

With contributions by: Jared Carleton and Adrian Drozd

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



August 2023

Strategic Imperative

- Big Data, ML, and AI have redefined application design, delivery, and user and environment interaction. Almost all industries and disciplines are taking advantage of these technologies.
- Cybersecurity is not an exception: security providers can leverage these tools to analyze the growing amounts of threat information, consequently boosting threat detection, response, and the ability to react to previously unseen attacks and zero-day threats.
- In the next five years, the importance of analyzing vast amounts of data and allowing software to learn from it will continue to increase. As a result, the XDR industry will flourish as it addresses organizational needs of automation, robust analytic capabilities, and data-driven security, spearheading the new generation of single-pane-of-glass cybersecurity solutions.
- Most organizations are still in the midst of digital transformation. Enterprise and government attack surfaces continue to grow as they establish cloud strategies and adopt new security controls and tools to protect their hybrid environments.
- The growing number and sophistication of cyber threats and the lack of cybersecurity professionals in most regions make securing business-critical assets difficult.

Source: Frost & Sullivan

Strategic Imperative (continued)

- An effective security strategy in the post-perimeter world requires close coordination between security controls and the dismantling of cybersecurity silos. As a unifying tool, XDR can ease organizations into reshaping their security posture and help them focus on the most important issues thanks to its overarching visibility of the environment. The dearth of skilled personnel will continue to increase the need for easy-to-use tools that can make lives easier for overburdened security analysts.
- Cybersecurity is a fast-changing and innovative industry. The growing number and sophistication of threats coupled with broader technological and social trends call for a generation of security solutions that are more effective and easier to use. In this environment, vendors must continuously innovate to maintain a competitive edge. XDR is a great example of the competitive nature of the cybersecurity market, with vendors aiming to go above and beyond to meet customers' needs.
- These factors have made XDR an essential tool in the arsenal of many security vendors. But its ubiquity does not mean that all XDR solutions address similar use cases: each vendor provides specific integrations and features that make its solution stand out. The evolution of XDR will further increase competitive intensity and influence additional developments.

Source: Frost & Sullivan

Growth Environment

- XDR is showing impressive revenue growth in the cybersecurity industry in 2023 after a 66.5% increase in 2022 and a projected compound annual growth rate of 31.2% from 2022 to 2025. Such success is a testament to XDR's capabilities and how they address many pain points of cybersecurity customers.
- XDR's ability to satisfy organizations' demands for visibility, integration, analytics, flexibility, and automation, allows it to stand out in the extremely competitive cybersecurity industry. Over the last three years, vendors have updated their strategies to offer more competitive solutions and deliver high-end security to their customers.
- Even with a more conservative assessment of XDR's potential, the growth rate will remain above average for the industry for the next three years as the early majority, late majority, and finally the laggards adopt the solution.
- Finance, government, tech, and retail are usually the top spenders for cybersecurity solutions, and XDR is no exception. Manufacturing and utility companies also are spending considerable amounts on securing business-critical assets, and XDR provides them with the visibility they need to secure OT and IoT devices.

Source: Frost & Sullivan

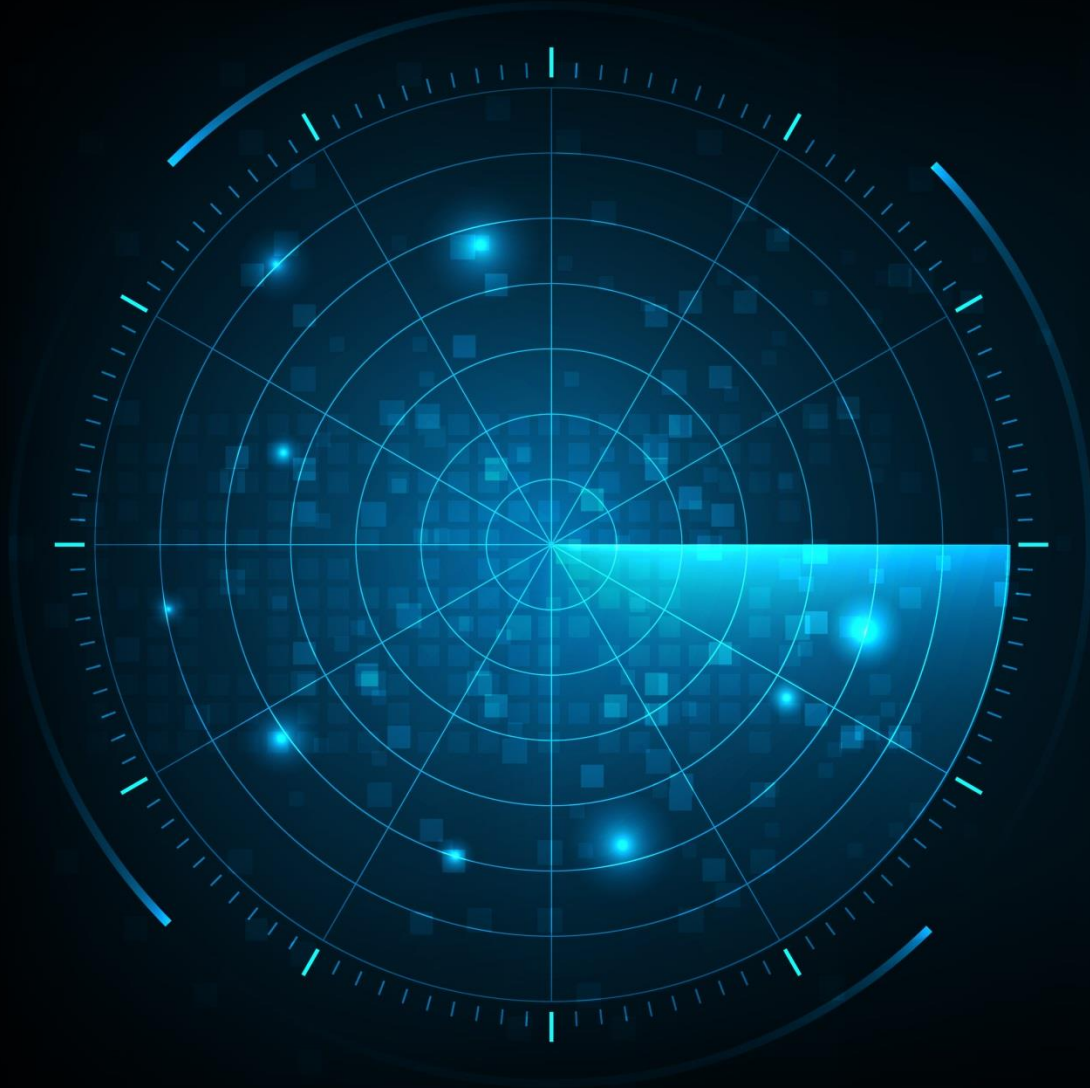
Growth Environment (continued)

- Shortly after its development, only corporations and enterprises with a high employee count had in-house cybersecurity teams large enough to manage a complex XDR solution. Automation used to be the most underdelivered out of the three XDR promises and limited the technology's use. Today, large and medium enterprises remain the biggest XDR spenders, but these customer groups are no longer the fastest-growing.
- Thanks to the push for further automation and ease of use, smaller businesses are investing in XDR as well. As vendors continue to design XDR in line with AI and ML developments and add features that let non-experts handle analytical tasks and threat investigation, XDR use will continue to soar.
- As is the case with most cybersecurity technology, XDR had a fast adoption rate and success in North America first, followed closely by the EMEA (Europe, the Middle East, and Africa) region. Revenue in both regions continues to grow at a rapid pace as the early majority of organizations invest in the solution.

Source: Frost & Sullivan

Growth Environment (continued)

- Latin America and Asia-Pacific contribute considerably less revenue but will grow at a faster rate for the foreseeable future as more companies realize the benefits of XDR. While these regions have lower security maturity levels, the new XDR trends will disproportionately affect how smaller and less mature organizations interact with the solution, and how they can leverage it to protect their evolving environments during a digital transformation.

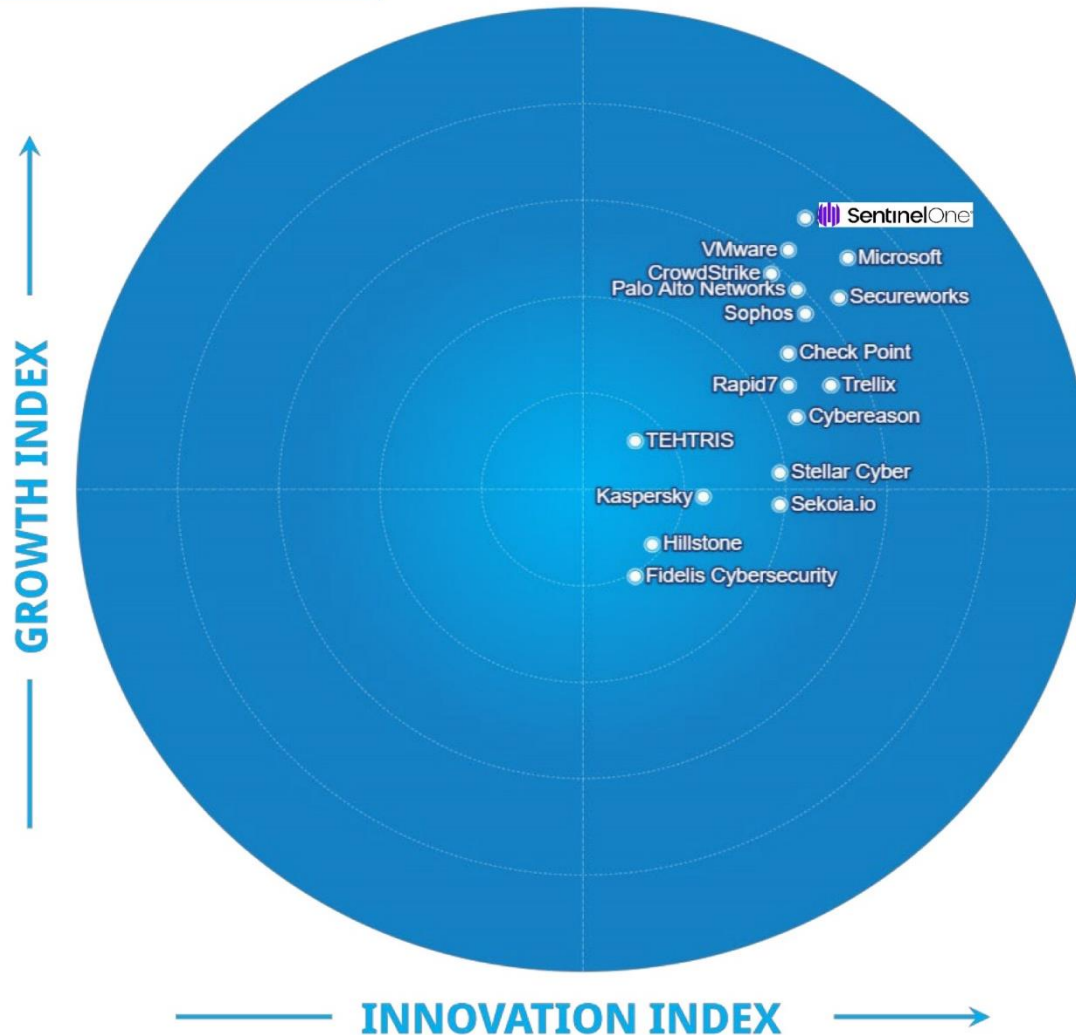


Frost Radar™

**Extended Detection
and Response, 2023**

Frost Radar™: Extended Detection and Response, 2023

FROST RADAR™



Source: Frost & Sullivan

Frost Radar™

Competitive Environment

- In an extremely competitive and fast-growing field of more than 70 industry participants with revenue greater than \$1 million, Frost & Sullivan independently plotted 17 leaders in growth and innovation in the XDR space in this Frost Radar analysis.
- As a first look into the competitive environment, it is essential to understand the three approaches to XDR: open (focused on third-party integrations and open architecture to provide more flexibility to customers), native (focused on providing native integrations with the vendor's own—usually comprehensive—security stack to improve detection and response), and hybrid (combining both approaches while keeping a smaller focus on native integrations, allowing customers to decide which works better for them). Frost & Sullivan has taken the three key promises of XDR as the basis for Innovation Index scoring, consisting of a solution's capabilities for integration (particularly third-party, vendor-agnostic integration), meaningful automation, and cross-layered threat detection and response.

Source: Frost & Sullivan

Competitive Environment (continued)

- Several of the largest XDR players have transitioned from a purely native approach to XDR integration to a hybrid one, providing more flexibility through third-party integrations while realizing the vision of a vendor-agnostic tool. Some of these companies have partnered with competitors to provide specific integrations with best-in-breed solutions and have formed alliances that foster integration between the security stacks of its members. These vendors' third-party telemetry may consist of just a few curated, out-of-the-box integrations to dozens or hundreds of security controls. A group of these vendors has created the XDR Alliance that fosters a more open approach to XDR among its members, demonstrating the increasing interest in providing a vendor-agnostic solution. Top competitors that fit the hybrid category either by succeeding in their transition through one of these strategies or by taking this approach from the start include Check Point Software, CrowdStrike, Fidelis Cybersecurity, Kaspersky, Microsoft, Palo Alto Networks, SentinelOne, Sophos, TEHTRIS, Trellix, and VMware.

Competitive Environment (continued)

- As a general trend, vendors taking every approach to XDR continue to make the solution easier to use, configure, and manage, making it more accessible for organizations with varied use cases. Offerings and roadmaps that include automation and ML capabilities, graph tools that show the complete story of an attack, collaborative tools that allow organizations to increase security maturity while enhancing cyber resilience, additional third-party and native integrations, and more beginner-friendly and intuitive features are on the right track in this rapidly developing market.

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.

Source: Frost & Sullivan

Companies to Action: SentinelOne

INNOVATION

- SentinelOne Singularity XDR seeks to deliver hybrid XDR through a mixed set of native and third-party partner technology integrations. The solution provides customers with the option for a fully on-premises or cloud-delivered multitenancy SaaS to address different use cases.
- The Singularity Marketplace shows integration with 65 cybersecurity vendors and their technologies and a curated group of premier partners that SentinelOne deeply integrates and supports within Singularity XDR.
- SentinelOne recently introduced its Singularity Security DataLake data platform at the core of Singularity XDR. It enables easier visibility into the security ecosystem, enhancing the ingestion and analysis of external data sources.

GROWTH

- SentinelOne is an XDR market leader with a track record of significant business growth quarter by quarter over the past few years.
- The company has leveraged its renown in the EDR space and its presence across all regions, industry verticals, and company sizes to succeed in the XDR market.
- SentinelOne makes significant investments in marketing, engaging potential customers in advertising, global public relations campaigns, email campaigns, trade shows, and—most importantly—thought leadership through its blog, webinars, and SentinelLabs, where the company's experts share their latest findings with the cybersecurity community.

FROST PERSPECTIVE

- SentinelOne is the Growth Index leader of the XDR Frost Radar. The company has transformed its significant innovation efforts and success across other cybersecurity spaces into growth opportunities.
- SentinelOne's commitment to flexibility is a great way of increasing market penetration and succeeding in the highly competitive XDR space. The company's fully on-premises and cloud-delivered multitenancy approaches, its go-to-market strategy with channel partners, and the large catalog of integrations with its solution tell a great story. They will enable SentinelOne to continue growing in the foreseeable future.

Source: Frost & Sullivan

Companies to Action: SentinelOne

INNOVATION

- SentinelOne's analytics and data aggregation process is the patented Storyline technology. Singularity XDR leverages its telemetry to link, map, and index behaviors in the environment to consolidate everything into a unified timeline of related entities. This process helps analysts reduce false positive alerts and provides immediate containment, remediation, and investigation options.
- The vendor's roadmap shows additional investments into automation through third-party vendors, including automated correlations and response actions. SentinelOne also offers several options for remediation and incident response automation through predefined triggers.

GROWTH

- SentinelOne delivers Singularity XDR through a network of more than 6,000 partners that cast a wide net over the cybersecurity market.
- The company offers multiple product tiers, allowing customers to pick and choose what they need, including data ingestion and retention options for threat hunting. SentinelOne's portfolio contains additional services on top of Singularity XDR, such as MDR and DFIR, to increase value for customers that need a more hands-on approach from their cybersecurity vendor.

FROST PERSPECTIVE

- SentinelOne should continue to invest in different ways of automating workflows, detections, and responses within Singularity XDR. Automation capabilities will be an increasingly important competitive differentiator as the number of unfilled cybersecurity positions continues to increase and organizations look for a way to mitigate the problem through XDR.
- Increasing the already large number of integrations and the list of premier partners will help SentinelOne capitalize on additional growth opportunities, especially because these curated, out-of-the-box integrations represent a valuable midpoint between the open and native approaches. SentinelOne's membership in the XDR Alliance is a great stride with third-party integration in mind.

Source: Frost & Sullivan

Frost Radar™

Key Takeaways



Key Takeaways

1

More than 3.4 million cybersecurity job openings went unfilled in 2022, according to the (ISC)² Cybersecurity Workforce Study, meaning a worrying lack of security personnel. XDR is a traditionally complex solution requiring the expertise of a well-trained cybersecurity team to leverage its capabilities and advantages fully. While automation, AI, and ML alleviate these issues somewhat, XDR vendors are finding other ways to support organizations affected by the shortage of security professionals.

2

Top XDR competitors include simple ways of performing threat investigations through interfaces, drag-and-drop menus, and pseudo-code. They also augment XDR solutions with intuitive user interfaces, graphic representations, charts, and networks that show the entire attack chain and the software's automated steps to prevent a threat. These features are essential to making XDR more accessible to customers while enabling and empowering inexperienced security analysts, setting them up for success.

3

Third-party integration within an XDR solution provides many advantages for customers: the choice of which solutions to deploy, no vendor lock-in, and the ability to maintain legacy solutions during a digital transformation with the knowledge that XDR is keeping business-critical assets secure.

Source: Frost & Sullivan

Key Takeaways

4

Open and hybrid approaches to XDR are in demand, and most of the top vendors that delivered a purely native solution have been including more third-party integrations, moving away from the concept of XDR as a portfolio integrator. Sometimes this transition involves vendor alliances that aim to deliver deep integrations between the members' security stacks.

5

The threats that put organizations at risk become more numerous and sophisticated with every passing day, with zero-day threats that exploit vulnerabilities being among the most dangerous. XDR provides many ways to offset these attacks, including recommendations, suggestions, vendor-provided playbooks, complex detections aligned with MITRE ATT&CK techniques, and threat investigation processes.

6

One of the most powerful tools in the XDR arsenal is the ability for customers to create their own playbooks, automate threat investigation in some way, or employ coding/pseudo-coding processes to improve detection and response.

Source: Frost & Sullivan

Key Takeaways

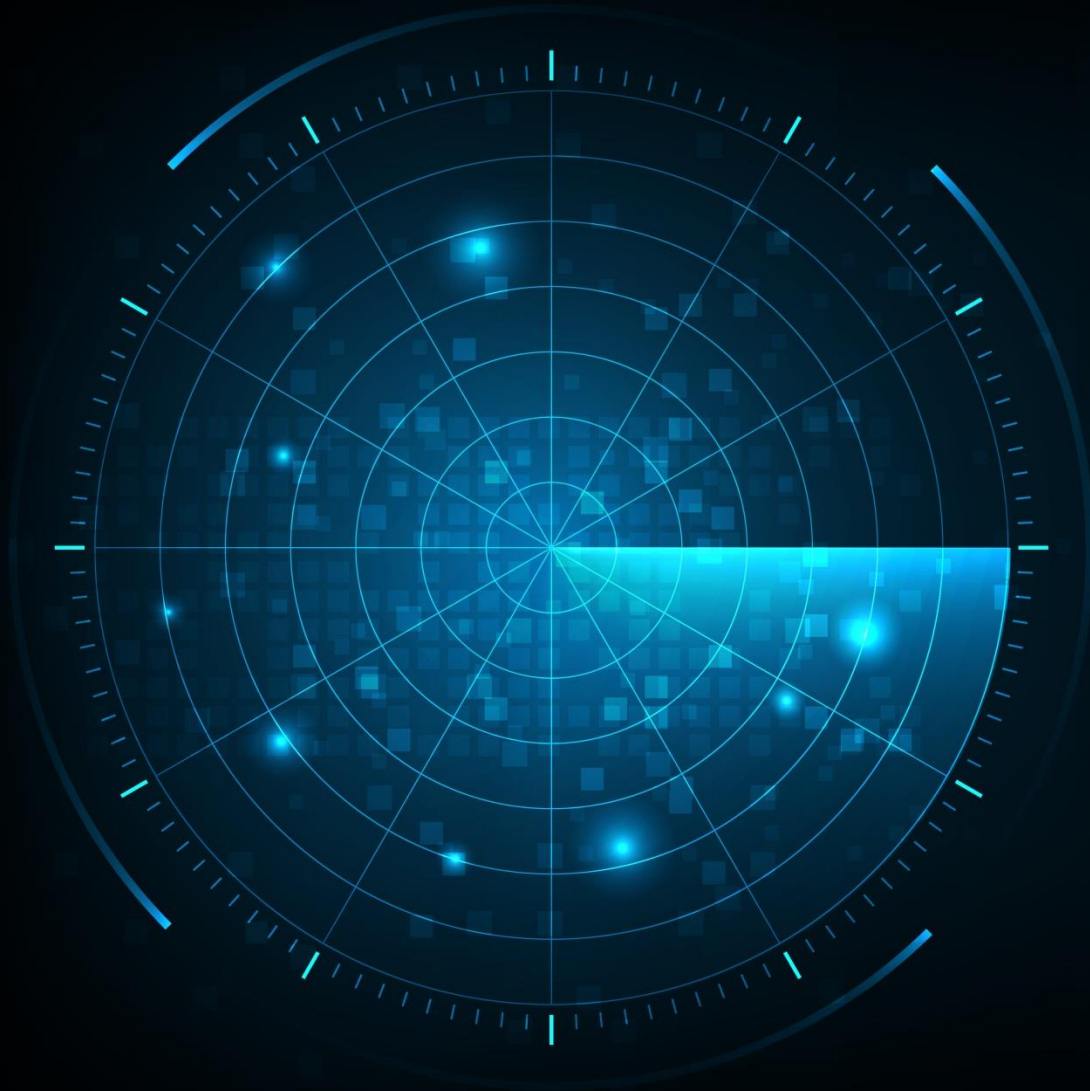
7

Some of the most innovative XDR vendors are already enhancing the value of their solutions by allowing customers to share their content with each other, enabling anyone to take advantage of other analysts' work. This greatly enhances detection and response, bolsters the entire cybersecurity community, and makes XDR easier to use.

Source: 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.