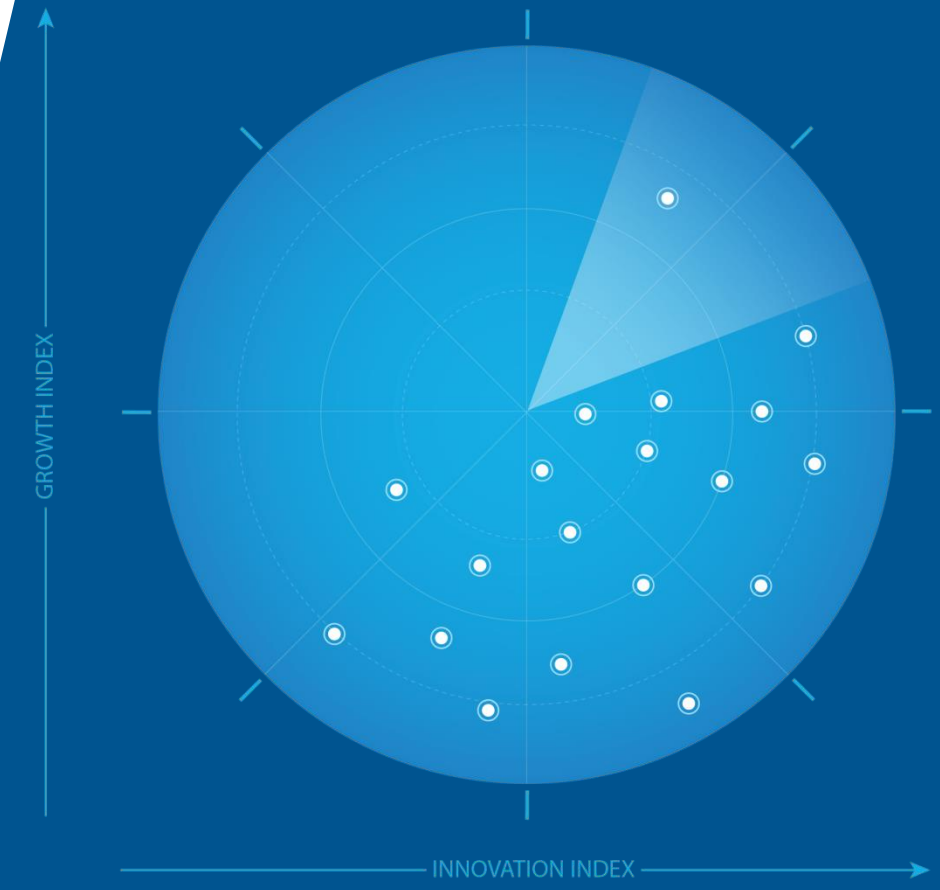
FROST & SULLIVAN

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.

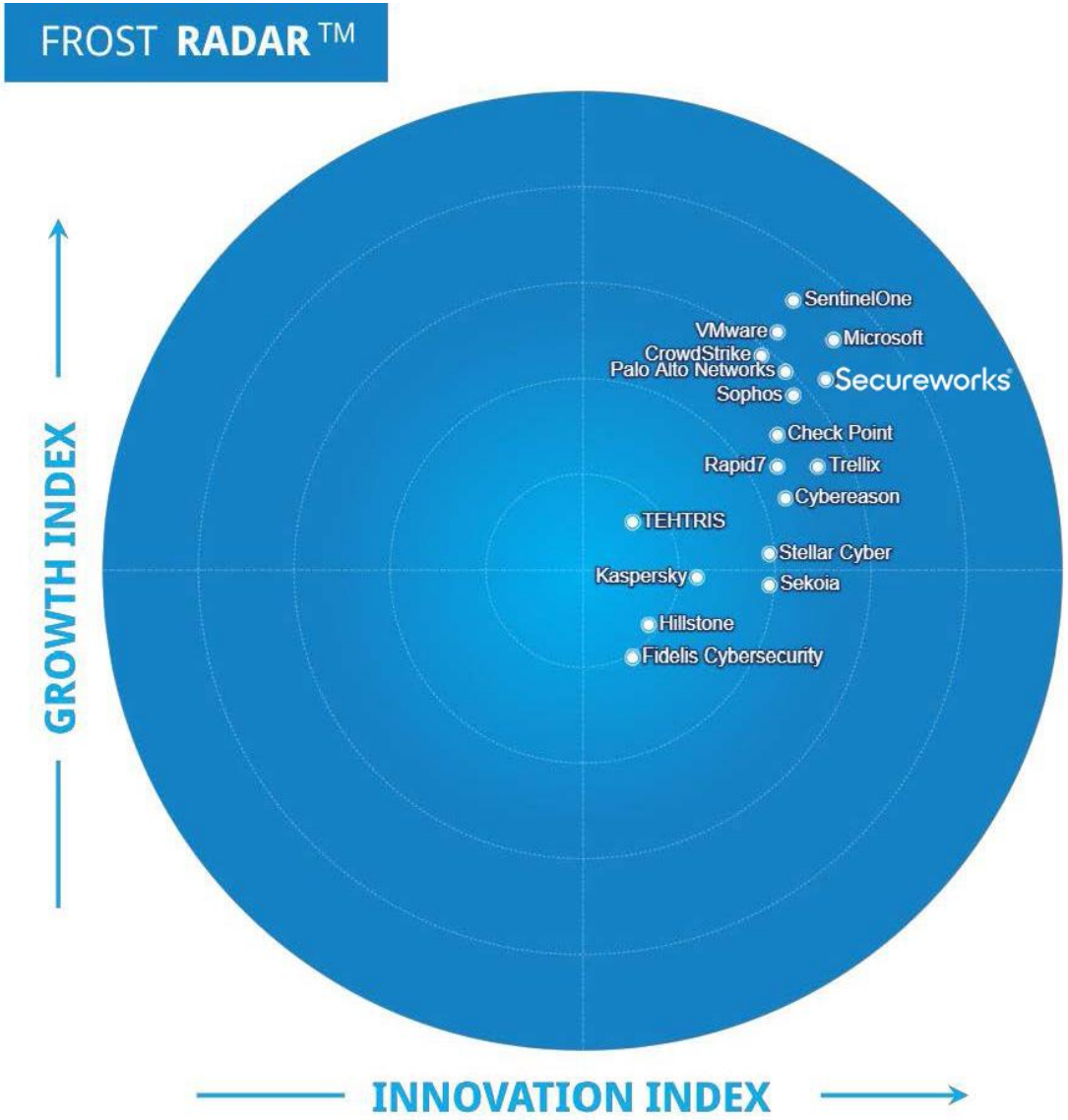
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Extended Detection and Response, 2023

Frost Radar™: Extended Detection and Response, 2023



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

Frost Radar™

Competitive Environment (continued)

- Secureworks has earned the second-highest score on the Innovation Index overall and the top innovation spot in the open XDR category. Secureworks delivers advanced threat detection and response augmented by extensive third-party integration, automation, and effective built-in collaborative features that provide a significant competitive advantage.

Source: Frost & Sullivan

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: Secureworks

INNOVATION

- Secureworks delivers open XDR and managed XDR through its Taegis™ platform. The solution integrates over 100 endpoint, network, cloud, and data collection integrations, from both Secureworks and third parties. Customers can create their own integrations through Secureworks' API and SDK, extending the visibility of the solution even further.
- Taegis XDR parses and normalizes data into event types, automatically generates graphs that correlate and map relationships between hosts, users, IPs, domains, and more to improve context and awareness. It employs machine learning algorithms to prioritize alert information (both native and third-party) and prioritize targets for analysts.

GROWTH

- Secureworks continues to grow faster than the market average, adapting its strategy as the XDR market evolves and changes. The company's main region is North America, with EMEA as a close second.
- Secureworks' market strategy involves selling Taegis directly to mature large enterprises that can leverage all the features of XDR; adding MDR or managed XDR on top of it for less mature customers, and offering its product through the MSSPs channel to widen its reach and market penetration.

FROST PERSPECTIVE

- Secureworks is the second most innovative company in the XDR market, thanks to its impactful collaborative features, wide vendor-agnostic integrations, and extensive threat detection and response capabilities across customer environments.
- Secureworks continues to support the open approach to XDR by allowing its customers to create custom integrations through an SDK and its open API. This is coupled with the vendor's normalizing and parsing capability to provide enhanced visibility throughout the ecosystem. Supporting these initiatives will drive sales and multiply growth opportunities in the foreseeable future.

Source: Frost & Sullivan

Companies to Action: Secureworks (continued)

INNOVATION

- The solution leverages all this data to create Investigation Timelines, allowing analysts to visualize threats across all environments. It also includes 79 pre-built playbooks, MITRE ATT&CK framework alert mapping, and more than 30 natively supported connectors to automate the investigation and response process.
- Taegis XDR's roadmap includes additional integrations with SentinelOne endpoint, TrendMicro, Workday, SalesForce, ForcePoint, and others; further automation and machine learning capabilities to enhance the investigation and threat-hunting processes; and extra features for service providers.

GROWTH

- Secureworks complements this strategy with its Partner First approach, which has been rolling out since 2021. The idea behind such an approach is to work in unison with tech alliance partners (AWS, Mimecast, NetSkope, and others) to build high-quality integrations between solutions and adopt joint market strategies.
- Secureworks is also focusing on and investing in many markets, from regional ones like Asia-Pacific to high-growth industries in the cybersecurity space like manufacturing. Recognizing the importance of the European market, Secureworks has made a new Taegis instance available in the EU for compliance with local data storage regulations. Similarly, the company has localized Taegis XDR and made it available in the Japanese market.

FROST PERSPECTIVE

- Secureworks has shown a historical understanding of the XDR market since the solution's inception. First, realizing that automation was a difficult promise to fulfill and augmenting its capabilities with managed security in the form of managed XDR to address the solution's use cases. The company continues to invest in automation improvements that will benefit small, large, high, and low maturity companies alike, provide localized service to several regions, and add features to support MSSPs delivering excellence through Secureworks' solution. The vendor's go-to-market strategy shows once again that its spot as one of the leading XDR companies in the market is well deserved.

Source: Frost & Sullivan

Companies to Action: Secureworks (continued)

INNOVATION	GROWTH	FROST PERSPECTIVE
• Secureworks was among the first vendors to include managed capabilities on top of XDR, allowing the solution to supplement automation with the service of human experts. Even outside of its managed offering, Taegis XDR provides customers with a chat feature included in the platform that delivers 24x7 access to a SOC analyst in 60 seconds or less. Users can ask for advice beyond basic support, such as questions about alerts or investigations.		

Source: Frost & Sullivan

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 & 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