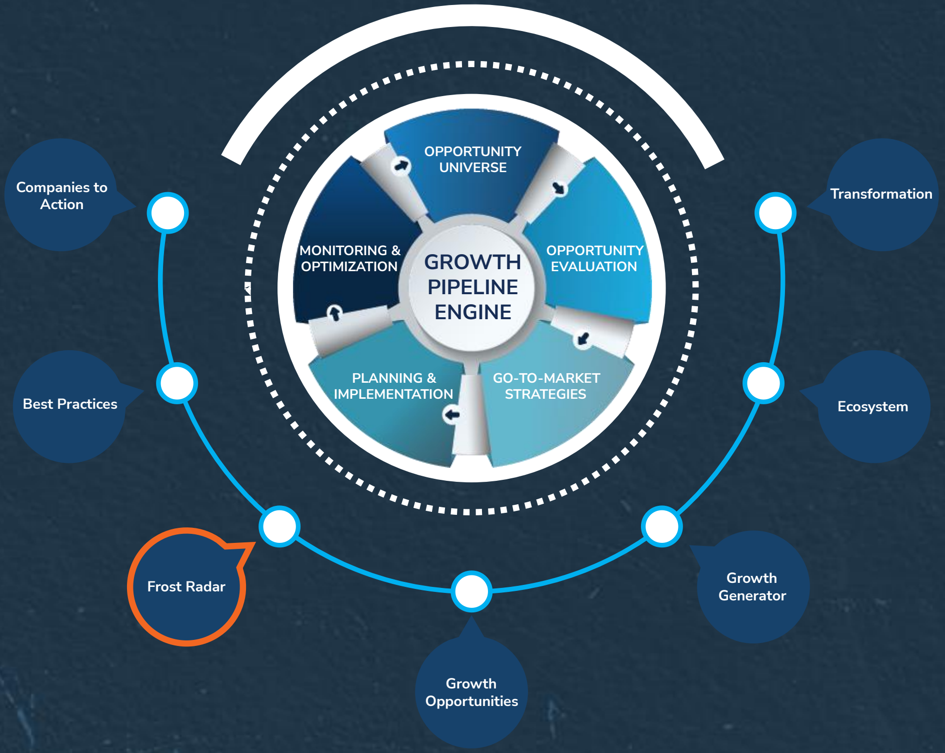
F R O S T & S U L L I V A N

Frost Radar™: Extended Detection and Response, 2024

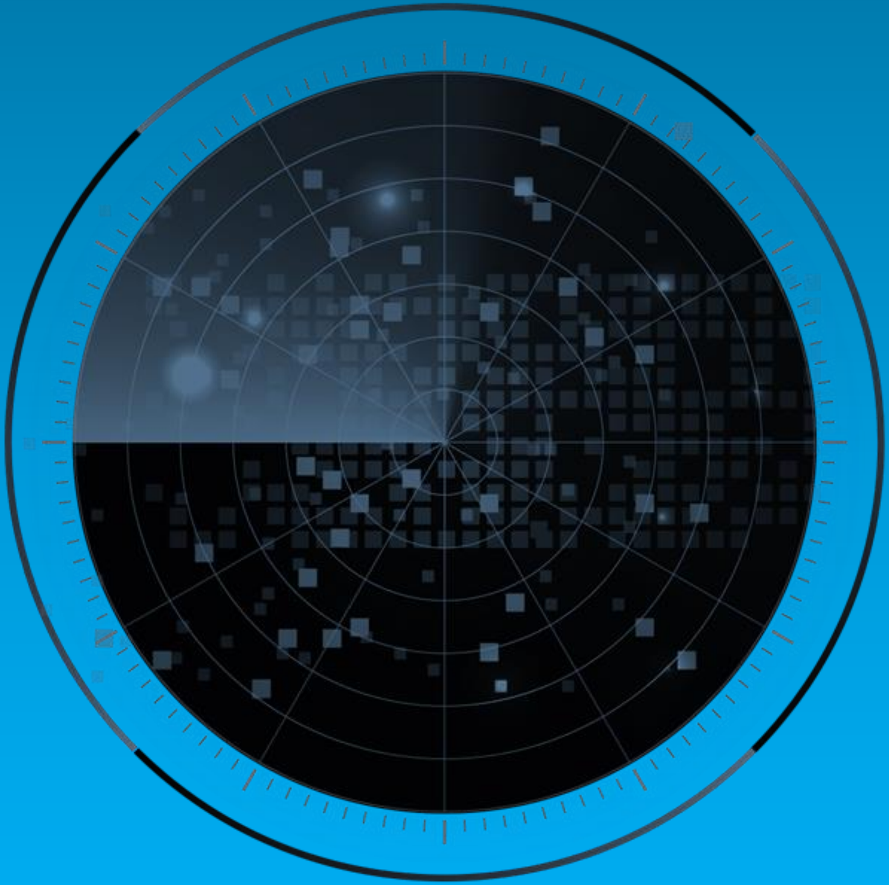
A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines

Authored by: Lucas Ferreyra
Contributor: Jarad Carleton



KAAF-74
December 2024

Strategic Imperative and Growth Environment



Strategic Imperative

- Machine learning (ML), artificial intelligence (AI) and generative AI (GenAI), and big data have redefined technology design, delivery, and user and environment interaction. Almost all industries and disciplines are taking advantage of at least some of them.
- Cybersecurity is not an exception: security providers consistently leverage these tools to analyze the growing amounts of threat information, consequently boosting threat prevention, detection, response, and the ability to react to previously unseen attacks and zero-day threats. For the foreseeable future, the importance of analyzing vast amounts of data and allowing software to learn from it will continue to increase.
- Organizations will need solutions that can provide automation, robust analytic capabilities, and data-driven security to prevent threats in addition to detect and respond to them. Extended detection and response (XDR) will continue to flourish because of the solution's core capabilities as well as integration with threat intelligence.
- Across the world, many organizations are still undergoing a digital transformation. Enterprises and governments' attack surfaces continue to grow and become more complex 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, coupled with the lack of cybersecurity professionals in most regions, makes securing business-critical assets a challenge.
- 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.

Source: Frost & Sullivan

Strategic Imperative (continued)

- XDR vendors are slowly but surely filling ecosystem niches through different integrations and core capabilities, which will result in specific solutions that provide visibility over the most varied environments.
- Cybersecurity is a fast-evolving and innovative industry. Broader technological and social trends call for a generation of security solutions that are more effective and easier to use. In such an environment, vendors must continuously innovate to maintain a competitive edge. XDR is a great example of this competitive nature, with vendors aiming to go above and beyond to meet customers' needs.
- XDR has become an essential tool in many security vendors' arsenals, but its ubiquity does not mean that all XDR solutions address similar use cases; in fact, each vendor provides specific integrations and features that make its solution stand out.
- XDR vendors are not only competing among themselves, but also with managed detection and response (MDR) and managed security service (MSS) providers that can deliver on the promise of comprehensive security in a different way. Because of this, XDR will continue to evolve to deliver end-to-end security in a fiercely competitive context.

Source: Frost & Sullivan

Growth Environment

- The XDR market is fast-growing, even compared with other markets in the cybersecurity industry. Its revenue growth rate for 2024 is expected to be 38.7%, and its compound annual growth rate (CAGR) for the 2024–2027 period is anticipated to be 24.9%—an impressive percentage even before considering that XDR is now a more mature security solution.
- Organizations going through a digital transformation need to secure increasingly complex environments. Work-from-home and hybrid work models are here to stay, meaning that hybrid cloud and multicloud environments that include massive mobile device fleets are becoming more common across the board. Additionally, a growing number of enterprises and government organizations are leveraging operational technology (OT), and internet of things (IoT) devices to multiply efficiency, but these tools are vulnerable to attacks and are high-potential and -reward targets for cybercriminals.
- The number and sophistication of attacks continue to increase each year as threat actors collaborate among themselves through processes such as ransomware-as-a-service; use AI to gather data for phishing attacks and to write malicious code; and occasionally count on nation-states to back them. Because of this, organizations demand visibility and actionability across these opaque environments; integration to simplify the management and the development of a solid security posture; correlation and analytics to detect complex threats; ML, AI, and automation capabilities to allow security analysts to focus on important alerts and decisions; and high-quality threat intelligence to prevent threats and increase cyber resilience. XDR delivers on these capabilities, allowing it to succeed in an extremely competitive environment.

Source: Frost & Sullivan

Growth Environment (continued)

- For a long time, XDR's complexity meant that only organizations with extensive cybersecurity budgets or with sizeable teams of experienced security analysts could leverage the solution effectively. However, advancements in automation, ML, AI (including GenAI and security assistants), improvements to the user interface (UI), additions of graphical representations of the environment to follow the attack story, and effectiveness of the solution to significantly reduce the number of alerts that reach analysts have made XDR platforms useful for smaller organizations and teams. Large organizations and the mid-market continue to be the highest revenue contributors for XDR, but SMBs are the fastest growing in 2024.

- North America leads the adoption of XDR and EMEA is a close second because of the regions' high security maturity. Organizations in these locations have complex use cases and understand the need for highly developed cybersecurity strategies. North America and EMEA will remain greenfields for growth for the foreseeable future.

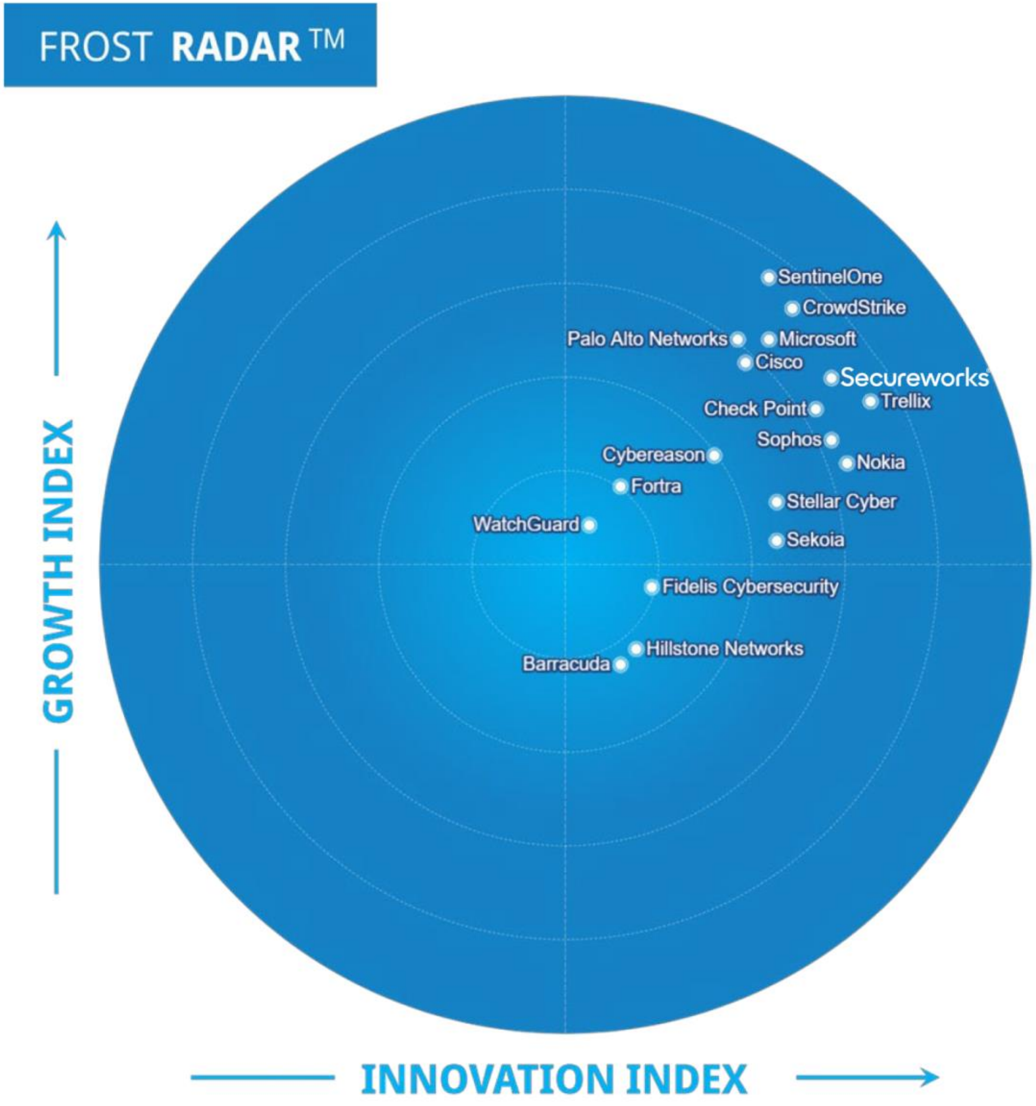
- Latin America and Asia-Pacific contribute considerably less revenue but will grow at significantly faster rates as more companies realize the benefits of XDR. While these regions have lower security maturity levels, the latest XDR trends (including GenAI, additional third-party integration, and usability features) are disproportionately affecting 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.

- XDR's visibility over multiple and heterogeneous environments such as OT, IoT, and containers is attractive to manufacturing, utilities, technology, telecommunications, transportation, and government organizations, although financial organizations' demand for effective and sophisticated security still means they lead the adoption of XDR and will continue to do so for the foreseeable future.

Source: Frost & Sullivan

Frost Radar™: Extended Detection and Response, 2024

Frost Radar™: Extended Detection and Response, 2024



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- From a fiercely competitive field of more than 80 industry participants with annual revenue exceeding $1 million, Frost & Sullivan independently plotted 18 growth and innovation leaders on this Frost Radar™.
- Organizations are looking to consolidate their security, simplify the management of increasingly complex environments and security controls, augment their resilience against the onslaught of sophisticated threats, and make their security budgets and investments count. While XDR can certainly address these issues effectively, it is not the only solution category or market to do so: adjacent markets, such as MDR (especially those players that leverage XDR technology to offer the service), and comprehensive approaches like those of MSSPs can do so as well. Because of this, competition transcends the XDR space, and, in the eyes of consumers, XDR players are pitched against many others outside the space, creating a highly competitive cybersecurity industry megaspace. In addition, many XDR players deliver managed XDR or MDR services, many MSSPs leverage XDR/MDR as part of their managed offering, and some XDR players partner directly with MSSPs to reach SMBs and other tough customer groups.
- XDR approaches continue to be as varied as players in the market, and the traditional divide between native (vendors integrating only their own, usually comprehensive, portfolio), hybrid (vendors requiring or preferring a few native integrations but being open for everything else), and open (vendors focused on third-party integration and open architectures), has become muddled. Top competitors in the space overwhelmingly provide at the very least a few third-party integrations, and they are hybrid or open, although some retain a strong native-first focus.
- The three core promises of XDR continue to be integration (particularly third-party, vendor-agnostic integration), meaningful automation (that includes GenAI capabilities), and cross-layered threat detection and response across a wide range of security vectors. The value of ingesting data from various environments continues to increase, as several vendors focus on providing visibility across OT, IoT, container, and many other uncommon or specific signals and deployments.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Threat intelligence and identity sources are more important than ever as XDR slowly shifts from a reactive to a proactive security approach. Simplification features beyond automation (e.g., intuitive UI, threat investigation graphs, comprehensive attack stories, and collaboration tools) can boost security teams when AI and ML alone are not enough; because of this, many XDR vendors are improving these value-multiplying features of their solutions. Alleviating the shortage of cybersecurity personnel and supporting AI features through threat intelligence and identity-focused approaches and usability improvements will likely become another core aspect of XDR.

- It is extremely challenging to rate the complexity, variety, and different approaches of all XDR vendors and their solutions. Frost & Sullivan considered the core promises of XDR, considering first- and third-party integrations, visibility across multiple security vectors, security operations processes, usability and collaboration features, threat intelligence capabilities, inclusion of identity threat detection and response capabilities, ML and AI capabilities, development and integration of GenAI tools, adequacy of strategy to target customers, R&D spending, revenue share and growth, sales and marketing, and myriad other factors. Frost & Sullivan also conducted interviews with customers of these solutions, asking questions about the vendors they are using or have used in 2024 and gaining insights about customer satisfaction, customer alignment, and intangible factors that contribute to the overall customer experience.

- Ultimately, the differences between top competitors are relatively small, which makes every vendor appearing on this Frost Radar^{TM} an ideal partner to fit the needs of different types of customers according to their approach and environment coverage.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Frost Radar^{TM} Growth Index leaders SentinelOne, CrowdStrike, Microsoft, Palo Alto Networks, and Cisco have managed to exploit the breadth of their security coverage to deliver generalist XDR solutions that can address the needs of customers across all major industries and regions.
- SentinelOne and CrowdStrike leverage their incredibly solid growth pipelines and marketing strategies to obtain the highest market shares and revenue growth in the market. Both are investing in many of the most important industry developments and market trends, and the robustness of their detection and response capabilities will continue to drive revenue growth for the foreseeable future.
- The strong positions of Microsoft, Palo Alto Networks, and Cisco reflect their ability to succeed in an incredibly competitive space. Microsoft's greatest differentiator lies in its AI, ML, and GenAI capabilities, as well as the massive amounts of threat data that increases customers' cyber resilience. Palo Alto Networks has top-tier threat intelligence and a large ecosystem of integrations through Cortex XSOAR, in addition to excellent detection and response capabilities. Cisco is a relatively new market entrant, but it has carved out a niche in the XDR market thanks to a more open approach to the solution than the other Growth Index leaders and its visibility across the ecosystem.
- The Innovation Index standouts include Trellix, Nokia, Secureworks, Sophos, and Check Point Software. What groups these vendors together is not their heterogeneous market shares or growth pipelines, but their incredibly robust R&D initiatives and their willingness to push the boundaries of XDR to address the needs of more targeted groups of customers.
- Trellix is the overall Innovation Index leader, thanks to its massive, out-of-the-box ecosystem of integrations; advanced orchestration, automation, and GenAI capabilities; comprehensive visibility across threat vectors; high-quality threat intelligence; and more.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Nokia has the second-highest score on the Innovation Index. The vendor has a smaller market share than other innovation and growth leaders but effectively delivers on all the promises of XDR via a comprehensive platform focused on addressing the needs of telecommunications, government, and mission-critical organizations with highly complex environments that include enterprise OT.
- Secureworks relies on its open approach to XDR including 350 integrations, APIs, and SDKs, and combines it with intuitive investigation timelines, third-party threat intelligence, automation, and integration with vulnerability and identity threat detection and response to add preventive capabilities and deliver comprehensive security.
- Check Point Software and Sophos have hybrid approaches, offering both native and third-party integrations and leveraging their presence across other spaces in the cybersecurity industry. Check Point Software has a proactive approach, delivered by integration with its ITDR solution and threat intelligence with personalized recommendations. Sophos offers more third-party integrations, very high visibility across complex customer environments, and several features related to prevention. Both players leverage sophisticated GenAI tools to reduce investigation time and empower analysts.
- Stellar Cyber and Sekoia may not have the large market shares of the other top players, but they are growing rapidly thanks to their platform-based, fully open XDR approach. Both have large ecosystems of integrations and partnerships with other cybersecurity leaders as well as the option for customers to request new integrations at will. They are the most flexible players in the market, and they are incredibly close to becoming innovation leaders in the space.
- Cybereason has an established market presence coupled with differentiators as an XDR solution: its patented detection engine and its open capabilities. However, the firm is still developing the most advanced features that other top competitors already have, such as GenAI. Nonetheless, it is well positioned to grow across both indexes as it continues to focus and invest in this space.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Fortra and WatchGuard provide effective XDR capabilities to address most use cases and customer pain points. Their solutions still need to mature, as they lack either the highly advanced GenAI capabilities, the large ecosystems of third-party integrations and visibility, or the forward-looking preventive tools of other top XDR solutions. They are, however, well established in terms of revenue and are poised to improve their Frost Radar^{TM} positions as they invest in additional XDR innovations.

- Fidelis Cybersecurity offers some innovative capabilities as part of its XDR solution, including high-speed, real-time traffic decryption to detect threats in nested files and encrypted traffic and a growing ecosystem of integrations that includes APIs for custom ones. However, the solution is still behind other top players in terms of innovation. As the firm continues to invest in R&D, its future looks promising.

- Barracuda and Hillstone Networks offer solid XDR solutions with use case differentiators but exhibit lower growth than other leading competitors. These players still need to drive revenue growth by expanding vertically and regionally and continue developing their products with additional AI and GenAI capabilities, integration, prevention, and visibility to establish themselves more firmly in the market.

- Several key vendors (including ReliaQuest, VMware, Rapid7, Fortinet, and Trend Micro) were considered for this Frost Radar^{TM} analysis but chose not to participate. Because of the lack of sufficient secondary information for benchmarking, they were not included.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

Secureworks

INNOVATION

- Secureworks delivers XDR through Taegis™, an open, cloud-native platform that features more than 350 first- and third-party integrations with security controls that provide visibility over the endpoint, network, cloud, email, identity, application, and OT environments. In addition to these out-of-the-box integrations, Taegis XDR has built-in APIs and SDKs that enable customers to build their own integrations easily, amplifying visibility and actionability and enhancing the flexibility of the platform.

- Taegis XDR focuses on improving the investigation process and allowing analysts to prioritize alerts through automation and correlation. After ingestion, Taegis XDR parses and normalizes data into event types, stores the information in a data lake, and automatically generates entity graphs that correlate and map relationships between hosts, users, IPs, and domains to improve context and awareness. The platform uses a newly introduced, AI-powered model to correlate the data and generate a threat score for prioritization. The model is trained with more than 750 billion events ingested into Taegis daily and reduces alert noise significantly beyond the regular XDR process of analyzing events.

- On top of this, and among many other features, Taegis XDR provides automatically created investigation timelines that show the timeline and progression of an attack, mapping of the alerts to the MITRE ATT&CK framework; customizable, automated investigations with GenAI summaries; native SOAR capabilities with more than 230 pre-built playbooks; over 60 connectors for alert enrichment including third-party threat intelligence; the ability for customers to add their own customized playbooks and connectors; and a game-changing, built-in, direct access to a SOC analyst with a 90-second response time as a chat feature within the platform, which provides amazing, immediate support for analysts.

Source: Frost & Sullivan

Secureworks (continued)

INNOVATION

- Taegis XDR also has integration with Taegis VDR (vulnerability detection and response), which provides a way to bring in vulnerability data (including third parties') into the threat detection and response workflow, increasing its prevention capabilities. To increase synergy, Taegis XDR highlights new vulnerabilities and ranks them to improve security posture.
- Secureworks' roadmap is focused on adding correlation and integration with its newly released Taegis IDR, the company's ITDR solution providing more comprehensive protection at the identity level; continuing to develop its AI capabilities to augment the detection, investigation, and response process; improving exposure management and attack surface coverage with additional integrations; and enhancing reporting.

Source: Frost & Sullivan

Secureworks (continued)

GROWTH

- Secureworks' XDR revenue continues to soar. It has become one of the fastest-growing companies in the XDR space, which is already one of the more rapidly expanding cybersecurity markets. The vendor's core region is North America, but it has a significant presence in EMEA and a minor one in Asia-Pacific. Many of its customers are in the manufacturing and finance verticals, resulting in a good mix of customers that understand the importance of cybersecurity and need advanced solutions to secure their shifting environments.

- Secureworks' 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 MSSPs to widen its reach and market penetration.

- Secureworks complements this strategy with its Partner First approach, which the company has been rolling out since 2021. The idea behind it is to work in unison with tech alliance partners including AWS, Mimecast, SentinelOne, and Netskope to build high-quality integrations between solutions and adopt joint market strategies. Secureworks and its partners also offer channel incentives, such as higher margins for the distributors when both companies' products are sold together, or referral arrangements to drive additional revenue.

- Secureworks' pricing model is based on the number of endpoints of an organization and works in tiers, meaning it is transparent, and customers can plan with it in consideration. The basic price includes support for all integrations, deployment of the Taegis EDR on all endpoints, one year of data storage, full Taegis XDR functionality, threat intelligence, onboarding, and support.

Source: Frost & Sullivan

Secureworks (continued)

FROST PERSPECTIVE

- Secureworks continues to spearhead the innovation of XDR with its open architecture and rapidly growing ecosystem of integrations (growing from more than 100 in 2023 to more than 350 in 2024), its approach to investigations and detection and response including the recent addition of the AI-powered threat score, the inclusion of GenAI to improve SOC analysts' workflow, and many other innovations that were already in the roadmap. Secureworks also shows a keen understanding of megatrends in the cybersecurity industry and has a good sense of the future development of XDR: its integration between Taegis XDR, Taegis VDR, and Taegis IDR will augment the platform with prevention capabilities. Secureworks should continue to prioritize this investment, because prevention will be increasingly important and become a core aspect of XDR in the short term.

- Customers having direct access to one of Secureworks' analysts via a built-in chat feature continues to be a significant differentiator that emphasizes the vendor's customer focus, even if it's not completely unique anymore. While the feature might be difficult to maintain or scale up as Secureworks continues to expand across the XDR market, the firm should find a way of keeping it, as it is a value multiplier.

- Secureworks should consider extending its presence in Asia-Pacific and expanding its small foothold in Latin America. Taegis XDR's high number of integrations, coupled with the analyst-boosting features in its investigation workflow and its AI improvements, can upscale any SOC analyst regardless of experience level. They will be extremely useful in both of these (comparatively) low security maturity regions that have trouble hiring and retaining experienced cybersecurity personnel. Partnering with local MSSPs and distributors, offering higher cuts and additional support, could lead to a rapid expansion in both regions.

Source: Frost & Sullivan

Best Practices & Growth Opportunities

Best Practices

1 From its inception, XDR unified and merged technological capabilities and leveraged correlation, analytics, and data from disparate security controls to deliver comprehensive detection and response. As threats become more sophisticated, XDR must shift its paradigm and include proactive security measures. Successful vendors are including integration with identity environments, ITDR capabilities, threat intelligence feeds and recommendations, and more to deliver on the most advanced use cases that organizations are demanding.

2 Vendors should shift away from native-first approaches and continue to broaden their scope and coverage by including more third-party integrations. This can be done through partnerships (as many vendors with comprehensive portfolios do), via out-of-the-box and built-in integrations embedded into the platform, through SDKs and public APIs; or leveraging integration with SIEM solutions. Flexibility needs to be at the core of what XDR brings, together with detection and response, automation, and prevention.

3 GenAI assistants are a force multiplier that provide several advantages to security operations, including the upleveling and upscaling of security analysts. Organizations that are not yet investing in this technology should reconsider their GenAI strategy, while those that are should continue to look for additional use cases to apply this technology effectively in ways that enhance cyber resilience.

Source: Frost & Sullivan

Growth Opportunities

1 XDR's integration capabilities mean that it can provide visibility across even the most opaque environments. Because of this, XDR vendors must extend their coverage and detection and response capabilities across the environment, and especially consider OT, IoT, containers, and identity. The development of specific connectors and sensors, as well as the training of ML and AI models on data sets that contain precise information on attacks against companies in underserved verticals, will allow players to find their niche.

2 SMBs and the Asia-Pacific and Latin American regions had been underserved, but the development of automation capabilities in XDR will increase their adoption of the solution. Continuing the development of GenAI security assistants; adding multitenancy support and centralized management; improving usability with intuitive UIs, attack story maps and graphs, simplified threat hunting, and DFIR processes; and leveraging channel partners will enable XDR vendors to expand into these markets more easily.

3 Frost & Sullivan's Voice of the Enterprise Customer survey found that nearly 3 in 5 organizations consider the changing regulatory landscape crucial or very important in driving their security strategy. Cybersecurity regulations are numerous, especially across North America and Europe. XDR vendors would benefit from developing or enhancing features that help organizations meet regulatory compliance requirements with detailed reports and automatic compliance checks.

Source: 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 (continued)

Innovation Index

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

II1

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

II2

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

II3

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

II4

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

II5

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

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

Source: Frost & Sullivan