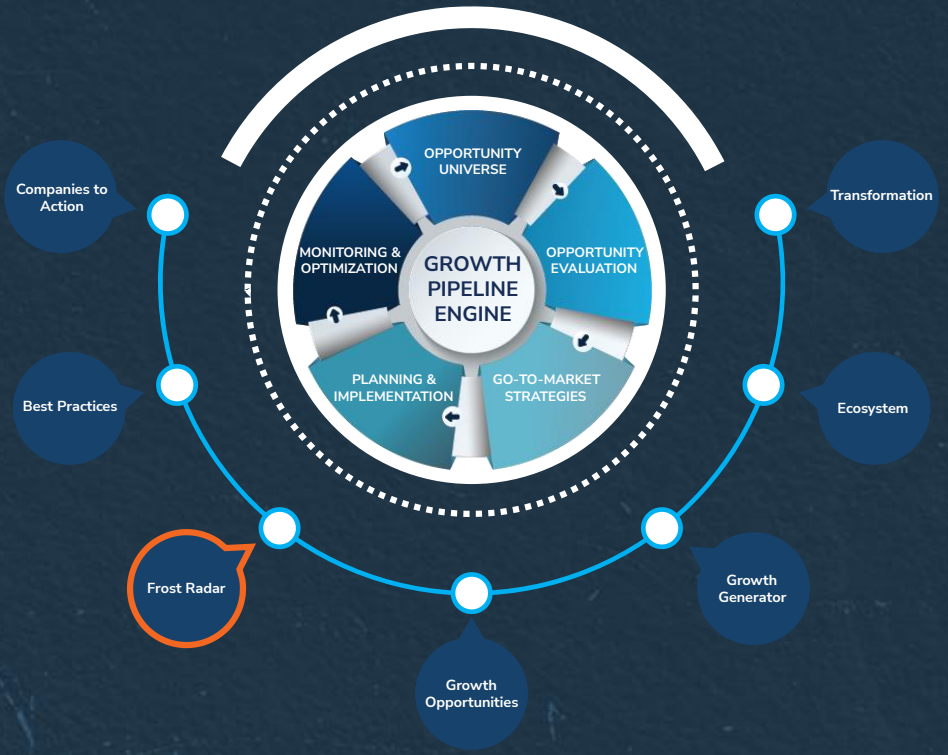
FROST & SULLIVAN

Frost Radar™: Modern Security Information and Event Management, 2024

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

Authored by: Georgia Edell
Contributor: Jarad Carleton



PFN8-74
December 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Source: Frost & Sullivan

Strategic Imperative

- Organizations face enormous pressure and challenges to proactively respond to new and various threats from exponentially growing data. The increasing use of generative AI and machine learning (ML) as a part of the digitalization trend across the industry has resulted in an overwhelming volume of data for personnel to manage underneath security measures.
- The complexity of network infrastructure in the modern environment and the strict implementation of security measures within an organization increased the number of security solutions in use, hence increasing the number of security alerts. The use of multiple, layered security solutions presents a risk of missing important events or tickets that may require in-time management.
- As organizations face a growing cybersecurity skill gap, including the shortage of skilled experts coupled with increasing demand for sophisticated security solutions, modern security information and event management (SIEM) solutions can alleviate the burden by offering a scalable and efficient approach to security operations. By proactively detecting potential threats and triggering automated responses, modern SIEM empowers organizations to effectively manage and respond to cyberattacks.
- It is imperative for an organization's CISO and the security team to acknowledge that cybersecurity is no longer a mere technical issue but something that has a significant impact on overall strategies and policies and will require a proactive approach and actions in response to evolving threats.
- As the use of AI prevails, cyberattacks become more sophisticated and aggressive. Cybersecurity solutions that can quickly respond to complex threats and comply with regulatory frameworks have become imperative. With modern SIEM, organizations can expect agile responses to security threats with automated alert systems that can significantly reduce the response time and minimize the damage caused by a security breach.

Source: Frost & Sullivan

Strategic Imperative (continued)

- As threats have evolved, so must SIEM solutions, which are now leveraging new technologies to protect organizations from the latest vulnerabilities associated with emerging technologies. Modern SIEM allows for add-on features, such as user and entity behavior analytics (UEBA) and security orchestration, automation, and response (SOAR) on the same platform, in addition to traditional SIEM functionality for cloud and on-premises infrastructure.
  - UEBA is a powerful cybersecurity solution that monitors traffic patterns from network communication devices, servers, endpoints, applications, and other sources. It identifies malicious behavior by distinguishing between normal network traffic/user actions and abnormal traffic patterns, promptly alerting administrators.
  - SOAR is designed to enhance efficiency and automation in security operations. Specifically, it aggregates logs and events collected by SIEM from various sources, such as personal computers, proxies, servers, firewall appliances, and security products, and visualizes this information. Based on predefined rules, SOAR automatically responds when specific actions occur. In other words, it reduces the workload for security administrators.
- While the use of SIEM varies among organizations, the need is becoming more prominent as the interest in real-time monitoring of security events, early detection of cybersecurity breaches, and compliance with complex regulatory frameworks increases to maintain a trustful and flexible environment.
- Large enterprises have already adopted modern SIEMs to efficiently manage complex operational environments. Smaller enterprises are showing an interest in implementing modern SIEM on cloud resources.

Source: Frost & Sullivan

Growth Environment

- SIEM has been undergoing a dramatic change as AI and ML shift systems to the next phase. The industry is attempting to maintain its strategic imperatives on new technologies and infrastructure.
- Frost & Sullivan expects modern SIEM market revenue to grow from $6.3 billion in 2023 to $12.1 billion by 2028 at a compound annual growth rate of 14.0%. North America will remain the largest revenue contributor, yet Asia-Pacific (APAC) and the region encompassing Europe, the Middle East, and Africa (EMEA) are projected to experience robust growth, fueled by the strict European Union regulations and rising security concerns in China.
- In the cloud era, organizations have expressed a desire for shared resources and access by large numbers of users. IT security solutions for infrastructure proliferated to eliminate security loopholes; hence, the cloud-based SIEM market is poised for growth at a faster pace than on-premises SIEM in line with the overall digitalization trend.
- Demand for on-premises SIEM will remain stable, however, driven by banking, financial services, and insurance (BFSI), government, and healthcare organizations in which stringent data protection requirements necessitate direct control of IT infrastructure.
- SIEM has long been considered a key tool to respond to modern cybersecurity threats, but cutting-edge malware allows active incursion into systems to achieve an illegal objective in a digital environment. Modern SIEMs are expected to harness the power of advanced technologies, such as AI and ML, to automate threat detection of possible attacks and response processes.

Source: Frost & Sullivan

Growth Environment (continued)

- SIEM vendors are transforming in response to organizations' demand for real-time detection and access management tools. The industry is rapidly reorganizing with the recent trends of M&As among large players indicating a maturing market in which established companies seek to enhance their capabilities and become indispensable to clients navigating an increasingly complex cybersecurity landscape. Major cybersecurity companies have been introducing new capabilities utilizing AI assistance and integrating various security and IT elements for efficient and effective outcomes.

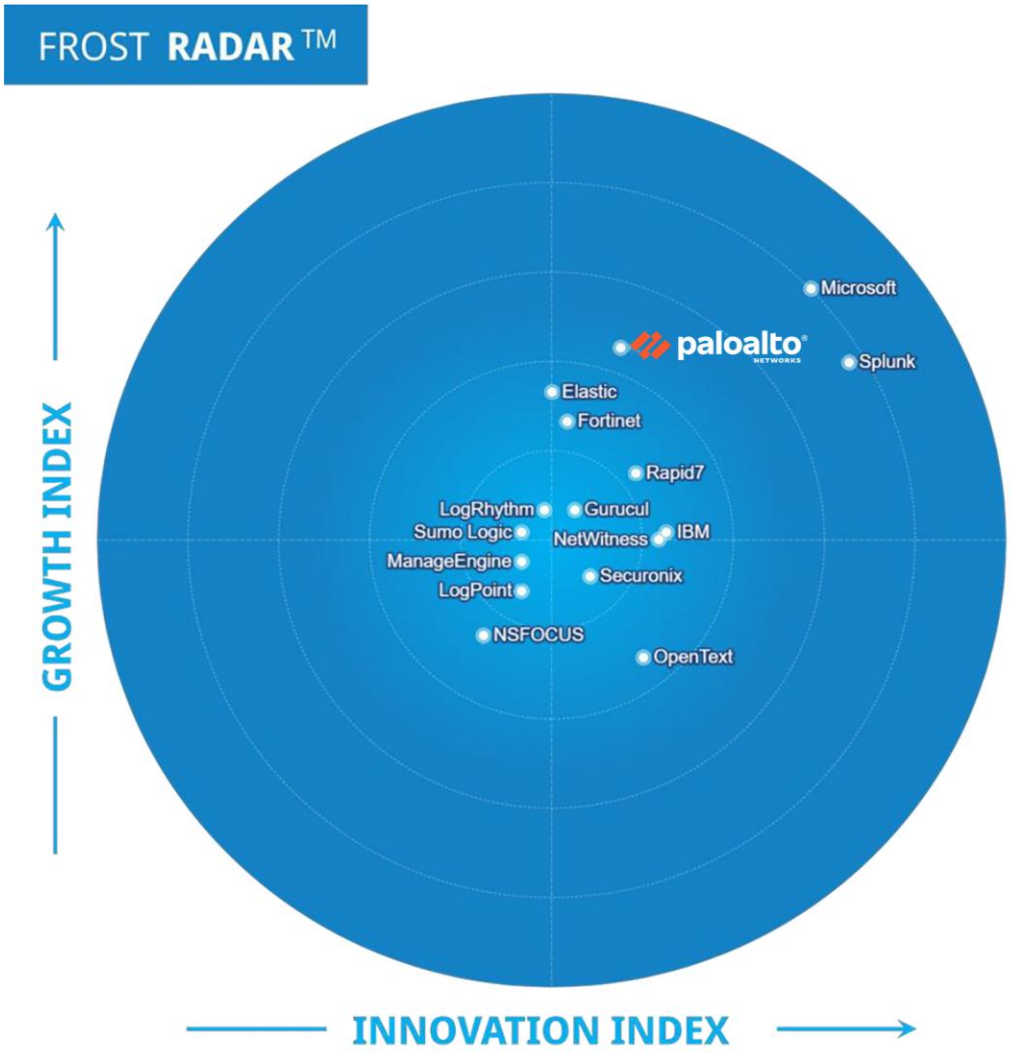
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Modern Security Information and Event Management, 2024

Source: Frost & Sullivan

Frost Radar™: Modern Security Information and Event Management, 2024



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- As cybersecurity threats evolve, organizations are seeking more advanced security measures, and expectations for SIEM products are increasing. Modern SIEM vendors are developing strategies to serve as comprehensive solution providers. The integration of UEBA and SOAR tools on top of a SIEM solution has become an important differentiator.
- The modern SIEM market is expanding, with numerous new vendors intensifying competition. Frost & Sullivan evaluated the top 10 vendors (based on revenue in 2023) and other notable companies that met inclusion criteria, ultimately benchmarking 16 companies on the Frost Radar™: Splunk, Microsoft, IBM, Elastic, LogRhythm, Rapid7, Fortinet, Sumo Logic, NetWitness, Securonix, OpenText, Palo Alto, ManageEngine, NSFOCUS, Gurucul, and Logpoint.
- Frost & Sullivan based all quantitative data points on calendar year 2023 and insights on information available and market condition as of 2023 and 2024. Vendors that met the inclusion criteria but could not share detailed insights into their solution were excluded to ensure fair scoring and comparison.
- Splunk and Microsoft are the leaders on both the Growth and Innovation Indexes for their excellent business performance and commitment to expanding their modern SIEM solution capabilities.
- Splunk became an attractive acquisition to Cisco, offering market-leading security observability solutions and comprehensive experience to customers. Splunk's strategic initiatives of continuous innovation and new functions that enhance its comprehensive security analytics tool position it as a market leader.
- Microsoft stands out with a cloud-native SIEM platform that leverages AI and ML and seamlessly integrates with both Microsoft and non-Microsoft environments. Its unified platform approach addresses the market trend toward consolidation.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Palo Alto Networks also is Growth Index standout. Its platformized Cortex Extended Security Intelligence and Automation Management (XSIAM) solution highlights its future-focused strategies to thrive in the evolving threat environment. Palo Alto Networks announced the acquisition of IBM's software-as-a-service (SaaS) business in September 2024, expecting to migrate those customers to the XSIAM platform.
- IBM sold the SaaS cloud-based segment of its QRadar business to Palo Alto Networks, but the on-premises part remains an important component of its cybersecurity portfolio and its strategic focus. Its strong foothold in on-premises infrastructure and expertise in AI make it a convincing choice for organizations with significant on-premises infrastructure.
- Rapid7's detection-centric SIEM solution is purpose-built for the cloud-first era, allowing seamless data collection and analysis across the hybrid environment. Rapid7 created an integrated security operations platform with its InsightIDR offering, providing customers with a comprehensive security ecosystem.
- Elastic and Fortinet are also prominent on the Frost Radar™ Growth Index.
- Elastic experienced good growth with its desirable open-source design that allows for flexible and scalable use. Elastic's recent introduction to generative AI-assisted analytics and search capabilities and the use of ML in anomaly detection provide limitless visibility to drive foreseeable growth in an organization's network.
- Fortinet has strategically expanded and differentiated its cybersecurity portfolio, focusing on the delivery of an integrated solution. FortiSIEM provides embedded generative AI assistance that enhances incident investigation and response. Fortinet is taking a proactive approach to strengthen its market position by refining its product portfolio and enhancing customer engagement, such as establishing experience centers and training programs through Network Security Expert Fortinet.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Gurucul distinguishes itself with its advanced analytics and ML to deliver comprehensive visibility and threat detection. Gurucul's next-gen SIEM features a standout capability of automatic data ingestion and interpretation from any source, optimizing time, money, and resources as a unified security analytics platform.
- LogRhythm's case management features, embedded in the full SIEM solution, provide users with enhanced security operational capabilities. LogRhythm announced a merger with Exabeam in July 2024, with the aim of strengthening the security operation platform.
- Sumo Logic's Cloud SIEM solution leverages advanced AI and cloud-based machine data analytics to detect and respond to threats across hybrid and multicloud environments. Sumo Logic is emerging as a key player in cloud-native security analytics to drive innovation and meet evolving customer needs.
- Securonix focuses on AI-enhanced SIEM technology, which utilizes ML to deliver a comprehensive SIEM platform that empowers organizations with advanced threat detection and response capabilities. Securonix's United Defense SIEM streamlines security operations by consolidating threat detection, investigation, and response (TDIR) functions into a single platform, enhancing visibility and operational efficiency for security teams.
- NetWitness' approach of integrated SIEM on a comprehensive security platform allows seamless and efficient data management and analysis. Unlike SIEM solutions that rely on logs, NetWitness captures full network packet data, enriching it with metadata across all data types. The comprehensive data set enables the detection of threats that traditional log-based systems might miss, providing deeper insights into security incidents.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- OpenText successfully expanded its business, significantly bolstering its cybersecurity offerings through the strategic acquisition of Micro Focus in 2023. OpenText ArcSight, formerly a part of Micro Focus, offers its robust SIEM capabilities and native SOAR functions that enable automation, guidelines, incident management, and analytics of security operation centers (SOCs), which empower security teams with essential automation and incident management capabilities.
- Log360, a unified SIEM solution of ManageEngine, integrates multiple security functions into a single platform, combining traditional SIEM capabilities with data loss prevention (DLP) and cloud access security broker (CASB) functionalities. To meet the evolving demand of security teams, ManageEngine has been continuously innovating to further improve Log360 features.
- Logpoint is a leading cybersecurity provider in EMEA, offering a unified platform for end-to-end security solutions. Logpoint's SIEM solution comes with built-in SOAR capabilities, with other features available as add-ons. Logpoint provides a flexible and scalable solution that can be tailored to each client's specific security and compliance needs.
- NSFOCUS has a prominent presence in China with solid capabilities in SOAR. Its Intelligent Security Operation Platform (ISOP) incorporates SIEM functionalities with other capabilities for security analysis and operation. The modular architecture is flexible and customizable to various environments, and AI-driven algorithms for intelligent alert and noise reduction prioritize high-risk incidents that require immediate attention.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

Source: Frost & Sullivan

Palo Alto Networks

INNOVATION

- Launched at the end of 2022, Palo Alto Networks' Cortex XSIAM platform is receiving widespread favorable reception. The platform received the Hot Company in Cybersecurity AI award by *Cyber Defense Magazine* during the RSA Conference in 2024 and was identified as a Leader and Outperformer in GigaOm's 2023 Radar Report on Autonomous SOC. Cortex XSIAM goes beyond traditional SIEM.
- The platform is AI driven, incorporating out-of-the-box AI models to connect event data across various sources. XSIAM works in real time to accurately detect and stop threats at scale for organizations of all sizes. The algorithms are continuously learning and improving over time to encourage more accurate predictive analytics.
- Cortex XSIAM also introduces Bring Your Own Machine Learning (BYOML) with Jupyter Notebooks, unlocking the full potential of Cortex XSIAM as a primary data platform.
- The unified platform approach boasts centralized data storage and combines the roles of SIEM, SOAR, TIP, extended detection and response (XDR), and more. It collects logs from XDR, cloud, and identity and analyzes and responds to the events, providing enhanced protection. This unification of capabilities and skill sets is an important introduction into the modern SIEM market.
- The platform is designed to help the modern security operations center (SOC). Palo Alto Networks recognizes that an AI-driven, autonomous SOC is the future of incident and event management. The XSIAM platform embeds automation and analytics in order to reduce SOC costs where possible.

Source: Frost & Sullivan

Palo Alto Networks (continued)

GROWTH

- Palo Alto Networks announced that the Cortex XSIAM pipeline was over $1 billion in November 2023, its first year of release. Cortex XSIAM is said to have captured over $80 million from QRadar-to-XSIAM transitions after Palo Alto Networks acquired QRadar in September 2024.
- The potential for growth is immense, and the company recognizes it. XSIAM was highlighted as one of the standout offerings in Palo Alto Networks' fiscal fourth quarter results, with approximately $500 million in XSIAM bookings. This indicates the performance of the platform is contributing to Palo Alto Networks' overall performance.
- Palo Alto Networks is partnering with other security providers, such as managed detection and response provider Red Canary, to offer Managed XSIAM to accelerate SOC modernization. This is intended to support midsize by delivering AI-powered security to help stop breaches with expert-led managed services.
- As a new offering, Palo Alto Networks is at the start of its journey with XSIAM. The company is putting a lot of effort behind the solution, and already customers are giving feedback. One services company experienced an improvement in median time to resolution of 270 times, while an oil and gas company enjoyed a 75% reduction in incidents requiring investigation through the elimination of false positives and duplicates.
- With the backing of the major security player that is Palo Alto Networks, this offering is sure to grow significantly and continue to challenge the incumbents in the modern SIEM space.

Source: Frost & Sullivan

Palo Alto Networks (continued)

FROST PERSPECTIVE

- As a new entrant to the modern SIEM market, it is yet to be seen how Cortex XSIAM will evolve to support third-party integration. Palo Alto Networks is generally considered to play well with others, offering capabilities to integrate with various security and IT systems. This should be an area of consideration with respect to XSIAM, ensuring ease of integration to encourage further adoption.
- The AI-driven approach is important in the security landscape, and vendors that can offer strong, tested, AI solutions will be important to watch. Palo Alto Networks' Precision AI system is designed to achieve near 100% accuracy in detecting and preventing cyber threats, including sophisticated threats. The evolving security landscape is making AI integration an attractive way to address complex security problems through analysis of massive amounts of data.
- While Palo Alto Networks XSIAM offers powerful automation and analytics capabilities, it may require a significant shift in an organization's security stack. Replacing point products with the XSIAM platform can reduce complexity but requires some adjustment by organizations and can take time to move over. This can deter some organizations from adopting just yet. Allowing for integration with other solutions and gradual deployment of all features can allow for training and upskilling that may be required for staff along the way.
- Frost & Sullivan recognizes the competitive edge of Palo Alto Networks' XSIAM offering, leveraging AI capabilities. As a new addition to the market, user feedback is limited, but the company has made a strong debut in the space.

Source: Frost & Sullivan

Best Practices & Growth Opportunities

Source: Frost & Sullivan

Best Practices

1. Modern SIEM vendors should continue to proactively incorporate evolving technologies, such as AI and ML, that can accelerate the expansion of their security coverage and capabilities. Advanced analysis and automated incident response functions are becoming key competitive points where vast data are generated every day.

2. A unified SIEM solution that combines various security functionality into a single platform is imperative to improve customer experience. Effectively streamlining the security operation within a platform can simplify log monitoring and management.

3. To stay ahead in the competitive SIEM landscape, modern SIEM vendors should prioritize innovation and enhance differentiation to meet evolving customer needs, including pursuing strategic acquisitions to expand their product portfolios.

Source: Frost & Sullivan

Growth Opportunities

1. SIEM vendors should focus on the development of more comprehensive solutions that integrate various security tools, such as a threat intelligence platform, to enhance overall visibility and analysis capability. Scalable SIEM solutions that can adapt to growing data volumes and emerging technologies will be particularly attractive to organizations looking for resilient and future-proof options.

2. SIEM vendors can continue to leverage the demand for modern solutions by adopting a more proactive approach that further integrates AI and ML to enhance detection and automation and reduce investigation time. SIEM vendors can capture a larger market share, particularly among SMBs that have often been neglected, by offering comprehensive security analytics features and partnering with MSSPs to deliver managed SIEM services.

3. As demand for SIEM solutions grows in APAC and Latin America, vendors have significant opportunities to establish a foothold through local partnerships and tailoring solutions to address the unique cybersecurity challenges of these markets, such as regulatory compliance complexity, growing cyber attacks, and a shortage of skilled professionals.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Source: Frost & Sullivan

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

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

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

Frost Radar™ Empowers the CEOs 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**

Source: Frost & Sullivan

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

Source: Frost & Sullivan