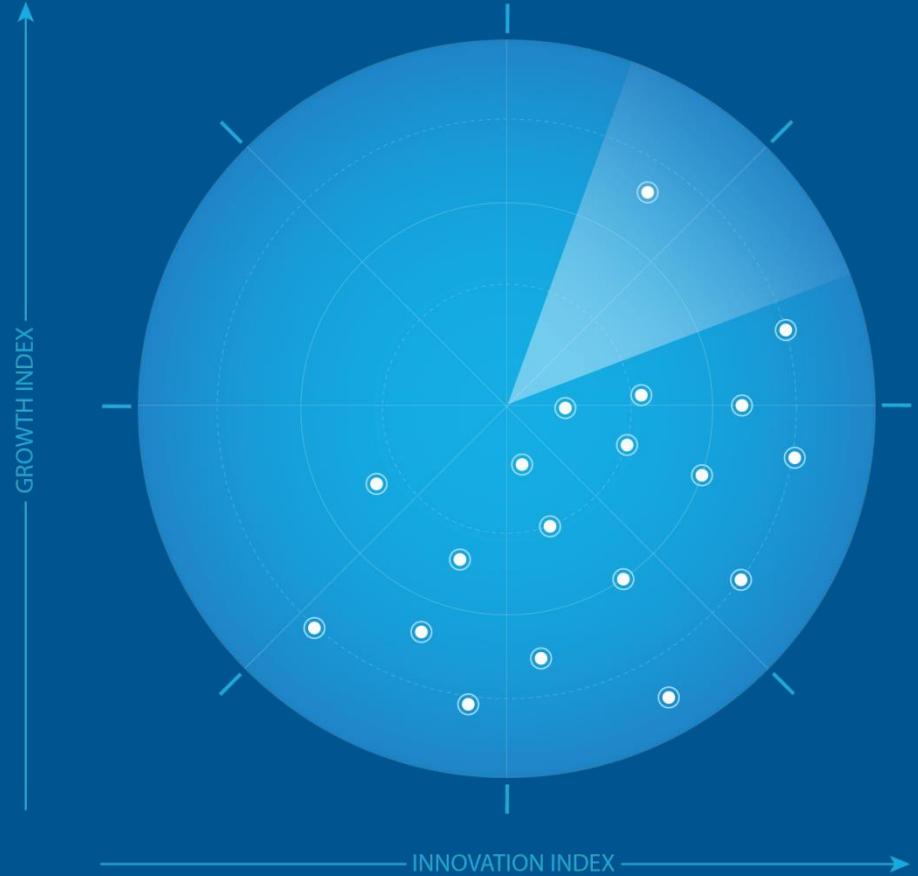


Frost Radar™: Threat Intelligence Platforms, 2024

Authored by: Martin Naydenov



FROST & SULLIVAN

Strategic Imperative and Growth Environment



Strategic Imperative

Factors Creating Pressure on Growth

- As the cybersecurity landscape evolves and threat intelligence (TI) vendors try to remain competitive, traditional TI point solutions are consolidated into integrated security platforms. The conventional TI ecosystem comprises four main areas: cyber threat intelligence (CTI), threat intelligence platform (TIP), external attack surface management (EASM), and digital risk protection (DRP), each serving distinct purposes. This convergence is giving rise to two main developments:
 - The emergence of unified external risk mitigation and management (ERMM) platforms, merging CTI, EASM, and DRP functionalities
 - The transition of TIPs into comprehensive security operations (SecOps) platforms, serving as centralized security control towers. SecOps platforms combine comprehensive TI with detection, response, and automation use cases, typically integrating security information and event management (SIEM), security, orchestration, automation, and response (SOAR), and generative AI capabilities.
- Amid these advancements, confusion persists within the market due to overlapping capabilities and varying vendor terminology.

Strategic Imperative

Factors Creating Pressure on Growth

- The TI market is experiencing steady growth, driven by factors such as the entry of new start-up participants supported by venture capital and the rising demand for proactive security. Advancements in data scraping and analytics engines have commoditized many TI capabilities, including threat intelligence aggregation and enrichment, enabling nearly all cybersecurity vendors to offer threat investigation and security operationalization solutions.
- However, traditional security operations centers (SOCs) remain primarily reactive and often operate in silos despite these advancements. Many TIP providers are now integrating basic SIEM, SOAR, and generative AI functionalities into comprehensive SecOps platforms to address these challenges and the increasing competitive intensity. This integration empowers organizations to transform their reactive, siloed SOCs into proactive, holistic cyber fusion centers with enhanced visibility and effectiveness.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- As TI capabilities become increasingly commoditized, vendors must invest in research and development (R&D) to expand their use cases and capabilities. Many TIP vendors have started integrating additional use cases, such as:
 - SIEM: Log collection, scalable data storage, and threat detection based on predefined rules
 - SOAR: Integrations across numerous security systems, workflow automation, and incident response
 - Generative AI: Natural language processing (NLP) queries, best practices recommendations, and internet browser and Microsoft Office extensions for data extraction and summarization
- By expanding these capabilities, TIP vendors can offer more comprehensive solutions to meet the evolving needs of modern cybersecurity operations and remain competitive.

Strategic Imperative

Factors Creating Pressure on Growth

- However, the rise of AI presents both opportunities and challenges. While AI empowers organizations to proactively enhance security, bridge talent gaps, and gain a strategic advantage in cybersecurity, it also enables threat actors to exploit vulnerabilities more efficiently. Integrating AI throughout the TI lifecycle enhances detection, response, productivity, and threat reporting, driving demand for AI-enabled TI solutions across industries and regions. This trend is expected to surge in the next five years, reshaping the TI landscape and compelling non-AI-enabled providers to adapt to avoid obsolescence.
- TI enhances security solutions by providing insights into emerging threats and attacker tactics, bolstering security ecosystems. However, practical implementation poses challenges, including quantifying TI's value and making compelling business cases. Therefore, vendors must focus on strategic marketing campaigns emphasizing outcomes and return on investment (ROI) rather than solely capabilities to navigate market confusion and drive adoption effectively.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Geopolitical tensions and conflicts, such as the Russo-Ukrainian War, have a dual impact on the TI industry. On the one hand, it increases demand for TI due to heightened threats from nation-state-sponsored hackers. On the other hand, sanctions and mistrust constrain the industry, hindering partnerships and global expansion for cybersecurity providers. This geopolitical turbulence affects the cybersecurity industry, shaping demand for TI and influencing vendors' go-to-market (GTM) strategies, especially for Eastern-based vendors from Russia and China operating in the West.

Source: Frost & Sullivan

Growth Environment

- The global TIP industry will increase at a CAGR of 28.6% from 2023 to 2028. Advancements in AI, platform consolidation, such as integrating TIP, SIEM, SOAR, and AI solutions, and increased emphasis on proactive security measures drive this growth. On average, TIP participants have seen a three-year CAGR of 19%, while marketing investments have averaged 20% of total revenue.
- Throughout the forecast period, North America (NA) will remain a focal point for vendors due to the prevalence of large enterprises with advanced security maturity and substantial IT/cybersecurity budgets. However, despite their smaller market sizes, Asia-Pacific (APAC), Europe, the Middle East and Africa (EMEA), and Latin America (LATAM) are expected to exhibit slightly higher growth rates, reflecting an overall upward trajectory in security maturity in these regions. Notably, APAC has surpassed EMEA to become the second-largest region, attributed to the presence of Chinese-based vendors such as ThreatBook, QAX, and NSFOCUS, whose customer base is highly concentrated in China, slightly skewing the revenue share of each region. Additionally, LATAM and APAC offer significant opportunities for Russian and Chinese-based vendors facing challenges expanding in NA and Western Europe.



Source: Frost & Sullivan

Growth Environment (continued)

- The technology, government, and financial sectors will continue to be the most profitable industry verticals, with the healthcare sector poised for significant expansion. This growth is driven by escalating threats from targeted phishing campaigns, supply chain attacks, and Internet of Things (IoT) vulnerabilities. Regulatory frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA), also indirectly drive CTI adoption in healthcare, with organizations increasingly focusing on continuous risk assessments across their supply chains.
- The TIP industry features fewer vendors compared to its CTI counterpart. CTI vendors offer versatile solutions accommodating many businesses, including smaller enterprises requiring only one CTI feed. Conversely, TIP solutions primarily serve large and mid-market enterprises that consume multiple CTI feeds and require contextualization and operationalization.
- This narrower industry segment results in a smaller total addressable market (TAM) for TIP vendors. However, as more organizations mature, Frost & Sullivan projects significant growth in these segments throughout the forecast period. As a result, Frost & Sullivan expects large and mid-market organizations to remain the most significant growth areas throughout the forecast period.



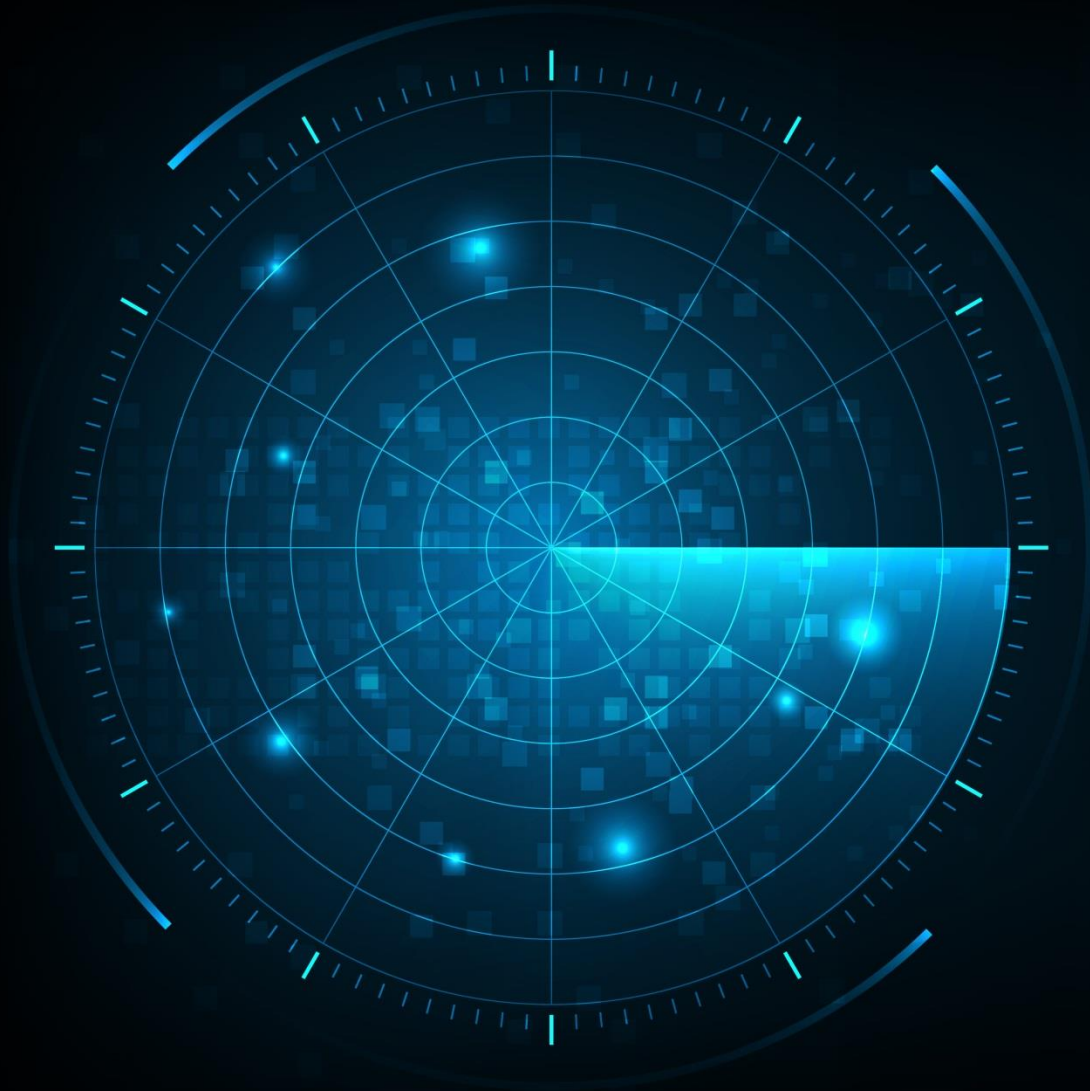
Source: Frost & Sullivan

Growth Environment (continued)

- However, small and medium-sized businesses (SMBs) are increasingly targeted by threat actors and need TI solutions. Through managed TI services and managed security service providers (MSSPs), TIP vendors can expand their growth pipeline and serve this traditionally underserved segment.



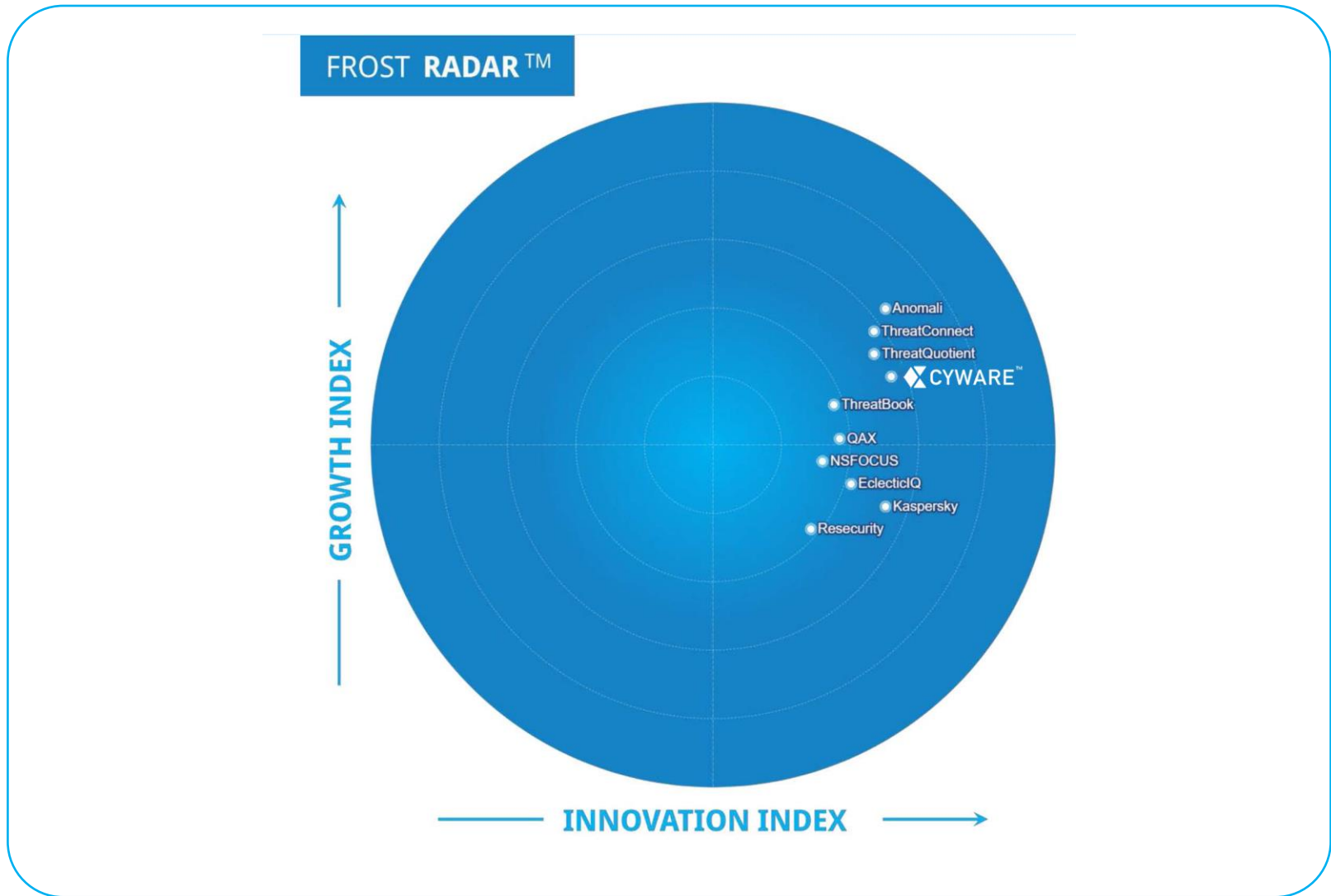
Source: Frost & Sullivan



Frost Radar™

**Threat
Intelligence
Platforms, 2024**

Frost Radar™: Threat Intelligence Platforms, 2024



Source: Frost & Sullivan

Frost Radar™

Competitive Environment

- The TIP industry encompasses over 20 vendors with different profiles, value propositions, and use cases. Frost & Sullivan selected the top 10 vendors with solid growth potential, displaying rapid growth rates and commitment to innovation. While many TIP providers are expanding their offerings to transform their platforms into more comprehensive SecOps solutions, their approaches vary. Some vendors prioritize integrating SOAR capabilities first, while others focus on SIEM functionalities.
- Meanwhile, several vendors remain pure-play TIP providers, enhancing their core threat intelligence capabilities without expanding into the SIEM and SOAR space. Others boast extensive security portfolios, achieving success through many distinct product lines beyond their TIP offerings. These may include SIEM, SOAR, network detection and response (NDR), endpoint detection and response (EDR), and firewalls. This diverse approach highlights the varying strategies within the TIP industry as vendors seek to meet the evolving needs of modern cybersecurity operations.



Source: Frost & Sullivan

Competitive Environment

- On average, vendors invest 41% of their total revenue in R&D. Anomali, Cyware, and Kaspersky lead the Innovation index due to their scalable innovations, thought leadership in the TIP space, and robust innovation roadmaps. Anomali leads the Growth index, holding a dominant global TIP revenue share, with steady growth rates and strong execution of its vision.
- Other key players, such as ThreatConnect and ThreatQuotient, hold significant market shares in the TIP space. They continue to invest in enhancing their value propositions and expanding their use cases. Chinese vendors, including ThreatBook, QAX, and NSFOCUS, boast extensive security portfolios and robust TIP offerings, though their growth is primarily concentrated in the APAC region.
- EclecticIQ stands out as one of the traditional TIP providers that has chosen to remain a pure-play provider, focusing on deepening its TIP capabilities. Meanwhile, niche player Resecurity has a robust product portfolio but limited global market share.



Source: Frost & Sullivan

Frost Radar™

Competitive Environment

- Notably, ThreatBook, NSFOCUS, QAX, Kaspersky, and Resecurity offer both CTI and TIP solutions that include proprietary CTI feeds and the capability to ingest third-party commercial CTI feeds from other vendors, further enhancing their threat intelligence offerings.



Source: Frost & Sullivan

Companies to Action:
Companies to Be Considered First for
Investment, Partnerships, or Benchmarking

Company to Action: Cyware

Innovation

- Cyware is one of the leaders on the Innovation Index, thanks to its comprehensive Cyber Fusion Center Platform that integrates TIP, SOAR, collaboration, threat detection, and generative AI capabilities called Quarterback AI. Cyware distinguishes itself with strong customer alignment, achieving 100% CSAT scores for three consecutive years and leading the industry with R&D investments, ranking in the 100th percentile.
- Intel Exchange, the vendor's TIP solution, offers many use cases and features, including ROI Feed dashboards, TI lifecycle automation, and bi-directional data sharing and actioning. Over the years, Cyware has continuously enhanced its TIP solution. In 2023, it introduced new collaboration capabilities, enabling threat detection and intel teams to join forces and share content, such as SIEM and YARA rules and automated playbooks. In 2024, the vendor added AI capabilities (Cyware Quarterback AI) designed to scale, optimize, and accelerate an organization's security team's effectiveness across their tech stack to up-level security teams.

Source: Frost & Sullivan

Company to Action: Cyware

Growth

- Cyware is one of the leading TIP providers, having rapidly progressed since 2021, reaching the top percentile in revenue growth rates. In addition, due to its significant marketing investments, ranking between the 60th and 80th percentiles, the vendor further amplified its growth potential.
- With a revenue share ranking between the 40th and 60th percentiles, Cyware primarily serves enterprise organizations of all sizes in NA and EMEA, with specific use case alignment within finance, energy, healthcare, manufacturing, government, and MSSP industries.
- In 2023, Cyware completed a Series C funding round, raising over \$30 million to support its global expansion efforts in collaboration with distribution channel partners and further amplify its growth potential.

Source: Frost & Sullivan

Company to Action: Cyware

Frost Perspective

- Cyware demonstrates a strong vision and execution in transforming the security landscape, underscored by its rapid growth rates and strong customer alignment. The vendor needs to increase its global market share to improve its positioning on the Growth Index. The recent \$30 million capital injection will enable Cyware to expand its distribution channels and enter new territories.
- Currently, most of Cyware's revenue comes from NA, and it has no presence in LATAM. To amplify its growth potential, Cyware should consider expanding into LATAM, which offers a low barrier to entry and limited competition. This strategic move will significantly enhance its global footprint and growth prospects.

Source: Frost & Sullivan



Key Takeaways

Key Takeaways

1

Cybersecurity vendors face significant challenges communicating their value propositions, especially for TI solutions. Many resort to fear-based marketing and gimmick capabilities, which lose effectiveness as organizations become desensitized to constant threats and dissatisfied with overpromises. Instead, vendors should highlight their TI solutions' unique benefits and positive ROI. Vendors can present a more compelling business case as these solutions evolve into comprehensive ERM and SecOps platforms.

2

Effective marketing campaigns should focus on tangible benefits, addressing critical pain points such as brand erosion, revenue loss, visibility constraints, and productivity limitations. Messaging must avoid overpromises and excessive buzzwords to prevent confusion. Implementing ROI metrics in product offerings, displayed in dashboards, is vital to conveying value. For instance, CTI providers can showcase cost savings from identifying leaked credit card data, while TIP providers can highlight how eliminating redundant data reduces costs.

3

While significant opportunities exist in NA, EMEA, and APAC, competition is fierce. Expanding into LATAM offers TI vendors a chance to establish a strong presence. Success in LATAM requires a well-balanced GTM strategy, including partnerships with local channels, customized pricing, regional offices, and local talent. Brazil, Mexico, Colombia, and Chile are particularly promising due to their large enterprises and unmet TI needs.

Source: Frost & Sullivan

Key Takeaways

4

Though the smallest TI market by revenue, LATAM holds substantial growth potential driven by economic, regulatory, and technological advancements. The region remains underserved, with countries such as Brazil and Ecuador experiencing high phishing attack rates. Frost & Sullivan reports that 50% of Brazilian organizations use DRP and EASM solutions, with 35% planning to implement them in 2024. This indicates the growing adoption of advanced security measures, presenting promising opportunities for TI vendors. In Brazil, over 50% of security products are acquired through resellers and more than 40% via direct channels.

5

Organizations struggle with visibility, limited resources, alert fatigue, and manual processes. AI technology complements TI solutions by enhancing security, visibility, and productivity. Full AI integration across TI ecosystems is ongoing, but current applications have already improved data analysis, providing historical context and identifying attack vectors. AI can also offer tailored reports, predictive risk analysis, workflow automation, and dynamic threat visualizations. To remain competitive, TI vendors must increase AI investment. Prioritizing R&D in AI empowers customers to leverage TI solutions fully. Partnering with AI providers to enhance and integrate AI capabilities is crucial, allowing vendors to address evolving customer challenges and boost growth prospects.

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

© 2024 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.