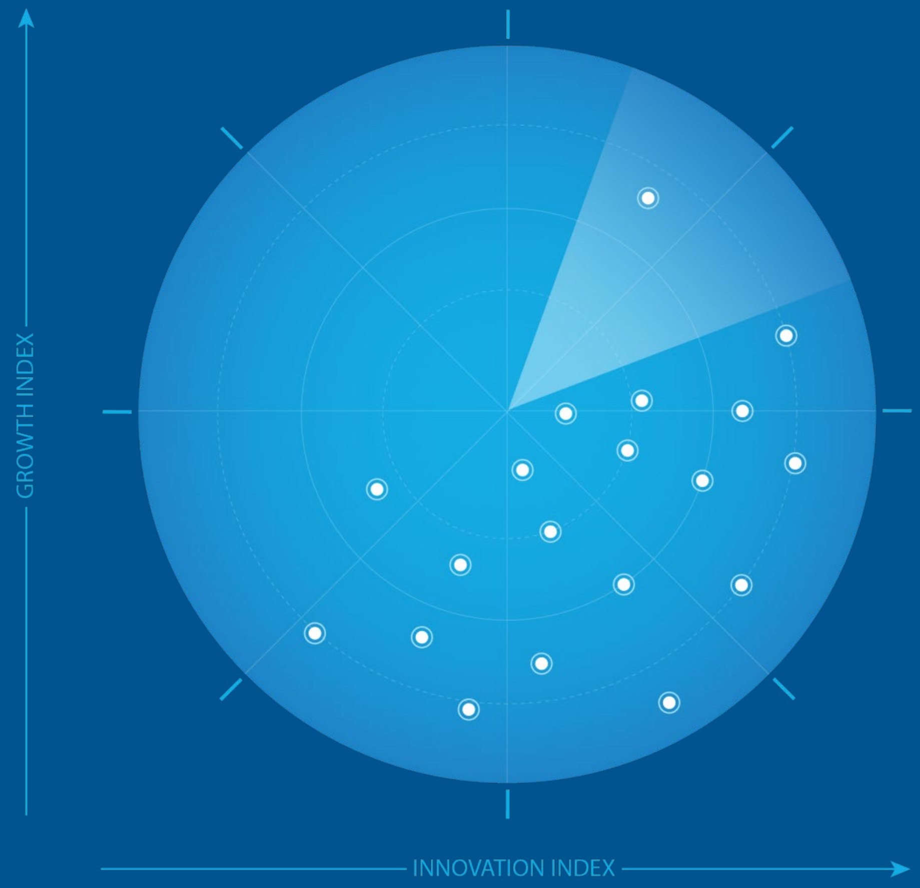
FROST & SULLIVAN

Frost Radar™: Managed Security Services in the Americas, 2024

Authored by: Lucas Ferreyra

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



July 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

Factors Creating Pressure on Growth

- Social and economic turmoil stemming from the COVID-19 pandemic resulted in budgetary constraints and a rethinking of priorities for enterprises of all sizes during the 2020–2022 period. Hybrid cloud and multi-cloud environments are increasingly the norm, even as enterprises are forcing their employees back into the office.
- Groups involved in the cyber warfare aspect of the Russo-Ukrainian War and the Israel-Palestine conflict are shifting focus to targets beyond those nations' borders. Organizations in the Americas will experience more state-sponsored cyberattacks targeting critical infrastructure.
- The threat landscape is rapidly evolving and increasingly sophisticated. Even minimal security breaches can lead to a security incident that compromises a company's entire value chain.
- Protecting such environments requires increasingly complex solutions that skilled cybersecurity professionals manage. The best option that allows enterprises to focus on their business without neglecting security is an MSSP that can provide and manage comprehensive ecosystems of cybersecurity solutions.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Over the last few years, vendors have improved the automation, machine learning, and AI capabilities of their security solutions and services. Comprehensive ecosystems spanning on-premises and cloud workloads generate hundreds of thousands of alerts daily. It is difficult to handle cybersecurity needs without automation: Even the reasoning and discerning capabilities of a skilled security professional cannot match AI.
- Accelerated digital transformation, strengthened by the push for automation, and the lack of security personnel have created the perfect conditions for MSSP success.
- Leading MSSPs have been developing their own XDR, managed XDR, or MDR platforms in the last three years. These solutions are increasingly harnessing the power of machine learning and AI, going as far as including generative AI security assistants that can help train new personnel and alleviate the workload of SOC veterans.
- In the next three years, MSSPs can take advantage of their broad portfolios to improve their managed XDR/MDR platforms and deliver additional services on top of them. This will provide an edge over security vendors that lack comprehensive coverage.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- The MSS industry is competitive and constantly changes to accommodate customer demands. The success of pure-play MDR, incident response, and other service companies puts more pressure on MSSPs.
- Competitors in North America must serve companies with the highest security maturity and the most complex use cases, and those that demand the most sophistication from security solutions.
- Conversely, staying competitive in Latin America involves flexible pricing, making the most of the existing security stack, and guiding companies on their maturity journey.
- MSSPs need to minimize confusion by showing the value that a broad portfolio supported by scalable managed security and professional services can bring to companies of all sizes and security needs.
- As differentiators such as integration with IT/IoT/OT environments and zero trust architecture become common, MSSPs will enhance their service integration. These will be platforms that deliver integration and leverage managed XDR and MDR to provide much-needed synergy and scalability to their offering.

Source: Frost & Sullivan

Growth Environment

- The Americas managed security services market is growing at a stable pace despite its maturity. Current strategic imperatives, global trends, organizational needs, and market drivers continue to provide excellent conditions for MSSPs to succeed, resulting in a 9.2% CAGR in the 2023–2026 period.

- These conditions include the already mentioned dearth of cybersecurity professionals, the rapid evolution of the threat landscape, and the need to handle complex solutions that require knowledge and expertise to master, but also many others: the need to secure hybrid environments (which are not going away even after some companies are forcing their employees back into the office); the growing threat of state-backed cyberattacks as the geopolitical conflict continues to rage on; and the increased money cost, reputation and brand equity loss, and regulatory oversight increase that comes as a consequence of a cybersecurity breach. These factors push organizations in the Americas to partner with MSSPs, who can provide visibility, integration, expertise, and top-tier security solutions at a fraction of the cost of an in-house SOC.

Source: Frost & Sullivan

Growth Environment (continued)

- Larger enterprises contribute the most to MSS revenue, but small businesses and the mid-market are quickly adopting managed security as a response to the higher amount and sophistication of threats. With the comprehensive portfolios and flexible pricing models offered by many MSSPs, companies with fewer employees are finding that their security budgets are better spent outsourcing security.

- The finance sector is the largest revenue contributor among industry verticals, but MSS adoption is growing in quite a few others too. Because of the geopolitical context coupled with the infamy and dire consequences of attacks on critical infrastructure, government organizations are more likely to partner with MSSPs that can manage or co-manage their environments, increasing their detection and response capabilities.

- Other sectors with heightened security awareness and expected increased adoption of managed security are utilities, health, manufacturing, and construction. Companies in all these industry verticals will dramatically benefit from MSSPs integrating OT and IoT Security into their offerings, and as more providers decide it's a worthwhile investment, enterprises in these sectors will flock toward the protection and efficiency of managed security.

Source: Frost & Sullivan

Growth Environment (continued)

- Education, professional services, and technology and telcos also see benefits in partnering with MSSPs thanks to the flexibility and variety of use cases that managed security can provide for their complex needs and environments.

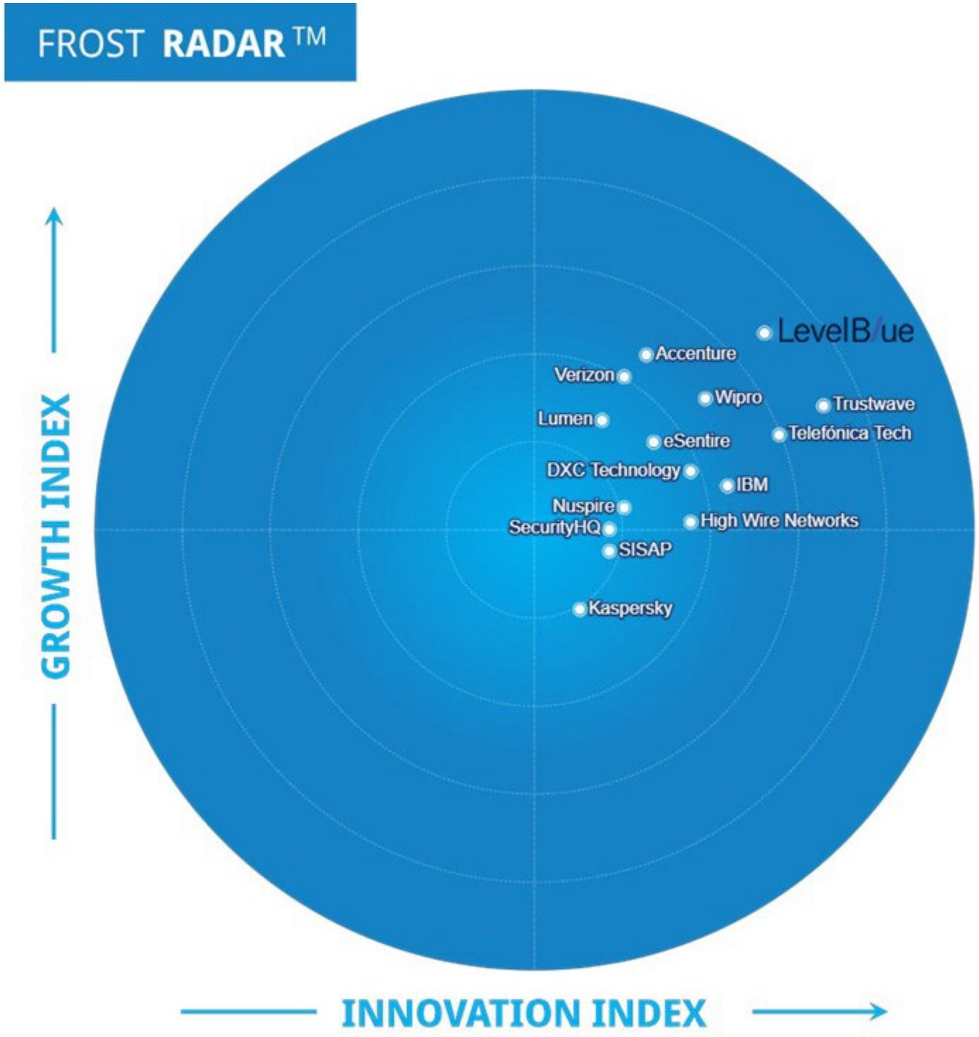
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™

Managed Security Services in the Americas, 2024

Frost Radar™: Managed Security Services in the Americas, 2024



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- In a rapidly growing field of more than 200 industry participants with revenue greater than $1 million, Frost & Sullivan independently plotted 15 of the growth and innovation leaders in the Americas MSS space in this Frost Radar™ analysis.

- MSSPs continue to develop their portfolios in line with the most required solutions and services by organizations. The sophistication of threats, the need to prevent them on top of just detecting and responding to threats, digital transformation, moving workloads to the cloud, and the dissolution of the security perimeter are some of the factors that contribute to this development. This means that standard offerings now include managed endpoint detection and response (EDR)/network detection and response (NDR), DDoS protection or mitigation, managed firewall, vulnerability management, risk assessments, and penetration testing. Additionally, a growing number of providers deliver managed SASE/SSE, managed SIEM, cloud security, managed identity security, and OT/IoT security, among other less traditional services.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- A broad portfolio continues to be incredibly important for MSSPs, particularly in delivering a combination of managed and professional services to multiply customer value. By including various assessments, consulting engagements, and prevention tools as part of their security suites, MSSPs create a positive feedback loop that can significantly increase the customers' security resilience. This is especially important for a market with a wide variety of security maturity levels such as the Americas – enterprises across the region require the most advanced security solutions as well as services aimed at fostering security maturity and increasing awareness. Additionally, these combined services are essential in building trust and improving customer relationships that are essential for MSSPs to succeed.

- However, MSSPs are no longer only competing against other MSSPs, but against MDR providers and even XDR vendors. These two solution categories address similar use cases as MSS, alleviating the cybersecurity workforce gap and enhancing detection and response against advanced threats. Customer organizations are not thinking about specific technologies or services, they are thinking about security outcomes and how to get them. Because of this, consolidating platforms should be an essential part of the strategy of market leaders in the MSS space.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- After seeing the success of pure-play MDR companies, leading MSSPs have developed their own security operations platforms. These platforms benefit from MSSPs providing threat hunting, incident response, CISO-as-a-service, cyber risk assessments, and other professional services or consulting engagements that increase synergy with the more traditional MSS portfolios.

- Security operations platforms are now an essential part of the expected portfolio of cutting-edge MSSPs. The inclusion of an ever-growing list of products and services will continue to promote growth in the MSS space – but MSSPs need to continue the integration of these services in single-pane-of-glass platforms and think about their overarching consolidation strategy.

- It is extremely difficult to rate the differences between MSSPs at the highest level. Frost & Sullivan considered a myriad of factors such as the depth and breadth of their portfolios, third-party integration to provide flexibility and visibility, coverage of diverse environments, interoperability of the tools, partner ecosystem, approach to generative AI, MDR/MXDR platform strategy, adequacy of strategy to target customers, R&D spending, revenue growth, and more. Ultimately, the differences between the top players in the market are relatively small, and any player on this Frost Radar™ would be the ideal fit for a particular type of customer.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- LevelBlue (formerly known as AT&T Cybersecurity) is the growth leader of the Frost Radar. The company leverages all the right megatrends to create an effective growth strategy, with significant R&D investment to capture a large share of the market and expand its footprint across the Americas. Additionally, its USM Anywhere platform integrates the entire security stack (including third-party tools and solutions) to provide flexibility and resilience for customers of all maturity levels, company sizes, and industries, contributing to its numerous growth opportunities.

- Trustwave is the innovation leader in the market. The company has a comprehensive portfolio of managed and professional security services, supported by excellent, value-multiplying tools such as Security Colony, and a roadmap that shows a keen understanding of where managed security is going in the future. Trustwave is growing rapidly, and its acquisition by the MC^2 Security Fund aligns the company for further growth opportunities in the mid and long-term.

- Telefónica Tech is close to both leaders. The company is the market leader for Latin America and is expanding its presence across North America, thanks to its broad and deep portfolio of tools and services consolidated as part of the NextDefense brand.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- Telefónica Tech's innovation and R&D efforts are excellent, and the company leverages its presence as a telecommunications provider to amplify its presence in the market.

- Accenture delivers a comprehensive offering with many varied consulting services supplementing its managed services, a synergistic strategy that results in excellent growth metrics in the sector. The company is keeping up with its investment in the most important Mega Trends and should continue expanding its OT/IoT security capabilities, as well as centralize its offering around a security operations platform to reach the level of innovation leaders.

- Verizon and Lumen leverage their extensive footprints as telecommunication services providers, which gives them a unique advantage in helping customers establish zero-trust security strategies and protecting their cloud workloads. Due to the size of their business, both firms have been slower in their transition to MDR/MXDR, and in leveraging the consolidation capabilities of such platforms. However, they are currently investing heavily in these tools, and are just a couple of steps away from the top of the innovation ladder.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- IBM, Wipro, and DXC Technology have extremely broad portfolios, covering most environments, and managing end-to-end security operations. These players have different market shares and growth rates, but their strategies, roadmaps, and innovation capabilities in the MSS space are similar. To continue on their way to the top-right of the Frost Radar, these companies need to continue investing in providing flexibility for customers, which will widen their reach across the market.

- eSentire is close to the previous group but has a different strategy and configuration of products and services. The firm has a more defined MDR strategy and is centering and uniting its offering around this platform, which leads to a more focused strategy that provides resilience and flexibility for customers across many industries and maturity levels. However, eSentire lacks the broad portfolios of some of its competitors, making it less ideal for organizations looking for specific tools and services.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- High Wire Networks, Nuspire, and SecurityHQ are all companies with faster-than-market-average revenue growths and smaller market shares. They have adopted MDR, MXDR, or security operations platforms very early, and while they do not have as wide portfolios as some of their competitors, compensate with more focused strategies. They will continue to expand their service offerings to move upwards and compete more directly with growth and innovation leaders.

- SISAP shares many of the same characteristics with the previously mentioned group, except its target market is in Latin America, and is currently expanding into North America. Its portfolio is ideal to accompany organizations in their digital transformation, but the company was an early adopter of MXDR, and can address advanced use cases for mature organizations as well. As SISAP continues its expansion across the Southern Cone and into North America, it could continue to climb in its positioning in future Frost Radars.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Kaspersky is focusing its MSS efforts in Latin America, as operating in North America is currently difficult for the company due to the ongoing geopolitical conflict. Kaspersky has a more defined MDR strategy than many of the players in the market but lacks deep visibility into some environments and the broad portfolios of MSSPs. However, its strategy centered around providing flexibility for Latin American customers and its significant R&D investments will offer Kaspersky growth opportunities in the long term.

- Overall, the market is highly competitive: the differences in service quality and effectiveness between the top 15 are incredibly small. Each one of these providers is idoneous for a particular customer, and the distinctions depend almost entirely on the approach and applicability to a specific region, company size, industry vertical, maturity level, or customer type.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

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

Company to Action: LevelBlue

Innovation

- LevelBlue offers a comprehensive suite of managed and professional security services supported by consulting engagements and additional tools. As the boundaries between consulting/professional services and MSS become increasingly blurred, LevelBlue has launched its cybersecurity-as-a-service, which provides clients with ongoing access to cybersecurity consultants in areas including virtual CISO support, continuous compliance, and on-demand advisory services.

- LevelBlue's MSS offering provides 24/7 continuous remote management of IT security functions from its eight global network operations centers (NOCs) and SOCs. These services include advanced network security, firewall management, access management, SSE, SASE solutions, DDoS mitigation, and web application and API protection. Specialized MSS are tailored for federal and state government entities, meeting specific compliance standards such as CISA TIC 3.0 and FedRAMP.

- As one of its flagship services, LevelBlue delivers advanced MDR capabilities through its open XDR platform, Unified Security Management (USM) Anywhere. The firm can provide this service either as part of its MSS offering or as a stand-alone offering that competes against pure-play providers.

Source: Frost & Sullivan

Company to Action: LevelBlue

Innovation

- LevelBlue’s MDR includes risk-based vulnerability management, incident readiness and response, and visibility across the endpoint, network, and cloud environments.
- While NOC services focus on device management, SOC services also manage data monitoring, threat detection, and incident response. LevelBlue can fully manage services or co-manage them with the customer. For MDR services, skilled security analysts monitor threats around the clock, leveraging LevelBlue's USM Anywhere platform and threat intelligence from LevelBlue Labs and other sources. API integrations enable enhanced telemetry, analytics, and automated response actions.
- Strong collaboration between LevelBlue and technology vendors including Palo Alto Networks, Cisco, and Fortinet allows LevelBlue to offer managed SASE solutions and build integrations into the USM Anywhere platform. USM Anywhere integrates over 600 LevelBlue Apps from multiple security and technology vendors via Syslog, API, and S3 connections to expand visibility. The platform enables MSSPs to respond rapidly to threats and deliver services efficiently. LevelBlue uses the feedback from its MDR operations team and network of MSSPs for platform development, constantly improving its alignment with service providers' needs.
-

Source: Frost & Sullivan

Company to Action: LevelBlue

Growth

- LevelBlue is the Growth Index leader on the Americas MSS Frost Radar. The company has a significant market share as well as a rapid revenue growth rate thanks to its ability to understand the megatrends in cybersecurity, invest in the right innovations, and address the most important issues in the industry.

- LevelBlue focuses its wider MSS offering on midsized and large enterprise customers in the banking, finance, manufacturing, healthcare, retail, and public sectors across North America. These industry verticals are often the ones with the highest security maturity and awareness and understand that cybersecurity is a business enabler. Their needs strongly align with LevelBlue's advanced portfolio of tools and services.

- LevelBlue's USM Anywhere platform consolidates the vendor's offering, significantly augmenting the third-party integration, data correlation, threat detection and response, and service and assessment capabilities of the entire security stack. This technology facilitates the convergence between LevelBlue's NOC and SOC capabilities and allows it to integrate professional services more directly into the managed offering. LevelBlue's ability to offer consulting engagements, a vulnerability assessment program, or digital forensics and incident response services creates growth opportunities for the provider while swiftly enhancing the customer's cyber resilience.

Source: Frost & Sullivan

Company to Action: LevelBlue

Growth

- Custom dashboarding, playbook automation, and expanded investigation features will empower SOC analysts, enabling quicker triage responses and scalability to meet customer needs. Integrations with compliance and risk-scoring platforms will be enhanced, improving customer access to specialty services.

Source: Frost & Sullivan

Company to Action: LevelBlue

Frost Perspective

- LevelBlue’s USM Anywhere platform is a differentiator in the MSS space. It provides customers with enhanced security, compliance, and reporting functionalities while ensuring ease of use and adoption through automation and integration with leading security vendors. It addresses key issues such as the need for consolidating security controls and management, protecting against sophisticated threats, and automating to multiply the value of analysts. On top of that, the platform doubles as the customer portal, offering direct access and serving as a communication channel for real-time data sharing between the SOC team and customers. The company should continue to heavily invest in USM Anywhere, expanding its capabilities to increase coverage, visibility, and integration with ML and generative AI.

- Thanks to a collaboration with AWS, LevelBlue will be able to develop new ML models and GenAI capabilities to improve reporting (operational, compliance, scheduled, and ML), providing SOC managers with comprehensive insights and enhancing customer experience. The company should continue to make these investments a priority because a clear AI strategy with concise investment and development goals will create growth opportunities.

Source: Frost & Sullivan

Key Takeaways

Key Takeaways

1

Frost & Sullivan’s 2023 Voice of the Enterprise Security Customer survey, a reference point for this Frost Radar, revealed a practical trend: a majority of respondents are adopting a combination of outsourced and in-house cybersecurity approaches—a choice driven by the reality that many enterprises lack the internal resources for a comprehensive in-house approach yet have reservations about complete reliance on external teams. This underscores the importance of flexible service providers offering solutions and services tailored to a client’s specific needs.

2

Many executives consider expanding their internal cybersecurity teams to bring certain functions in-house and reduce reliance on external teams. However, establishing effective synergies between internal cybersecurity specialists and service providers' analysts can be complex, especially when the provider's analysts are not exclusively dedicated to a specific client—a situation often associated with higher-priced service tiers.

3

MSSPs should not just consider but deeply understand their clients’ most effective approach to managed security. Organizations rarely fully outsource or keep all their cybersecurity in-house, often choosing a blend of the two. Best-in-class is not always needed; sometimes, “good enough” is the way to go, considering budgetary constraints and cybersecurity maturity levels. This client-centric approach is key to success in the industry.

Source: Frost & Sullivan

Key Takeaways

4

Organizations seeking to co-manage security with an MSSP partner need collaboration-oriented tools and guidance on their maturity journey. The MSSP's security team should be viewed as an extension of the internal one. The MSSP should be asked to provide information about turnover rates, as a higher rate will negatively impact the ongoing relationship between internal and external teams.

5

Conversely, MSSPs should be able to accommodate companies intending to outsource their security with broad, completely integrated portfolios. Periodic meetings, dashboards, and reports are essential to help clients understand the state of their security posture, risks, and challenges and allow the provider to demonstrate the ROI of dedicating money to cybersecurity.

Source: Frost & Sullivan

Key Takeaways

6

Other ways for MSSPs to diversify include:

- developing vertical-specific knowledge and portfolios;
- Having a portfolio that is flexible and able to keep improving the security posture as a client’s organization expands;
- Devising pricing models and SLAs that are clear and easy to understand to avoid the risk of budgetary challenges if they are not fully understood; and
- Being clear about data residency, especially in Europe, as clients might be wary of transferring their data outside the European Union in a region with different data privacy laws.

Source: Frost & Sullivan

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

VERTICAL AXIS

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GROWTH INDEX ELEMENTS

- **GI1: MARKET SHARE (PREVIOUS 3 YEARS)**
  This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.
- **GI2: REVENUE GROWTH (PREVIOUS 3 YEARS)**
  This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.
- **GI3: GROWTH PIPELINE**
  This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.
- **GI4: VISION AND STRATEGY**
  This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?
- **GI5: SALES AND MARKETING**
- This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

HORIZONTAL AXIS

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

INNOVATION INDEX ELEMENTS

- **II1: INNOVATION SCALABILITY**
  This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.
- **II2: RESEARCH AND DEVELOPMENT**
  This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.
- **II3: PRODUCT PORTFOLIO**
  This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.
- **II4: MEGA TRENDS LEVERAGE**
  This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.
- **II5: CUSTOMER ALIGNMENT**
  This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com