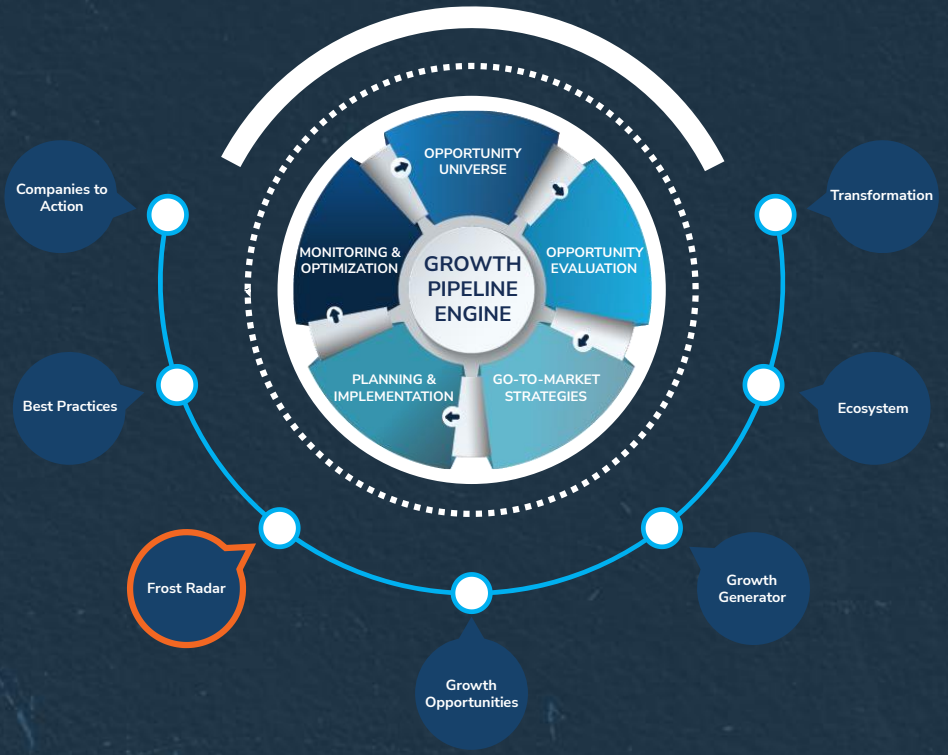
FROST & SULLIVAN

Frost Radar™: Managed Security Services in EMEA, 2026

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



MHFE-74
May 2026

FROST & SULLIVAN

Strategic Imperative and Growth Environment

List of Abbreviations

- **AI:** Artificial Intelligence
- **APAC:** Asia-Pacific
- **CISO:** Chief Information Security Officer
- **CNAPP:** Cloud-Native Application Protection Platform
- **CTEM:** Continuous Threat Exposure Management
- **CWPP:** Cloud Workload Protection Platform
- **DDoS:** Distributed Denial of Service
- **DevSecOps:** Development, Security, Operations
- **DFIR:** Digital Forensics and Incident Response
- **DPO:** Data Protection Officer
- **EDR:** Endpoint Detection and Response
- **EMEA:** Europe, the Middle East, and Africa
- **GenAI:** Generative AI
- **IAM:** Identity and Access Management
- **ICS:** Industrial Control Systems
- **IoT:** Internet of Things
- **IR:** Incident Response
- **ISV:** Independent Software Vendor
- **LATAM:** Latin America
- **LLM:** Large Language Model
- **MDR:** Managed Detection and Response
- **ML:** Machine Learning
- **MSP:** Managed Service Provider
- **MSS:** Managed Security Services
- **MSSP:** Managed Security Services Provider
- **MTTD:** Mean Time To Detect
- **MTTR:** Mean Time To Respond/Remediate
- **MxDR/MXDR:** Managed Extended Detection and Response
- **NDR: Network** Detection and Response
- **NG-SIEM:** Next-Generation Security Information Event Management
- **OT:** Operational Technology
- **SaaS:** Software as a Service
- **SASE:** Secure Access Service Edge
- **SD-WAN:** Software-Defined Wide Area Network
- **SIEM:** Security Information and Event Management
- **SOAR:** Security Orchestration, Automation, and Response
- **SOC:** Security Operations Center
- **SSE:** Security Service Edge
- **VAR:** Value-Added Reseller
- **vCISO:** Virtual CISO
- **WAAP:** Web Application Firewall and API Protection
- **WAF:** Web Application Firewall
- **XDR:** Extended Detection and Response
- **ZTNA:** Zero Trust Network Access

Strategic Imperative

- The MSS market in EMEA is being transformed by the combined effect of escalating cyber threats, rising operational complexity, and a policy environment that increasingly treats cybersecurity operations as a core pillar of business resilience rather than a discretionary IT function. As a result, managed security is becoming more strategically embedded in enterprise operating models.
- Regulatory frameworks, such as NIS2, DORA, and GDPR, are playing an outsized role in shaping MSS demand across the region, pushing organizations toward providers that can deliver continuous monitoring, auditable workflows, demonstrable risk reduction, and clear accountability in day-to-day operations and incident response scenarios.
- Sovereignty is emerging as one of the most important strategic differentiators in EMEA. Buyers increasingly expect locally anchored SOCs, jurisdiction-aware data processing, and sovereign options for analytics and AI inference, particularly in highly regulated sectors, such as financial services, healthcare, the public sector, and critical infrastructure.
- EMEA enterprises are also moving away from fragmented, tool-centric managed security arrangements and toward platformized MSS models that can unify telemetry, analytics, orchestration, and reporting across cloud, identity, endpoints, networks, OT, SaaS applications, and distributed user environments, simplifying operations while improving consistency and scalability.
- In this context, the most compelling MSS providers in EMEA will be those that can combine AI-augmented but human-supervised SOC operations, exposure-led security, and convergence with SASE/SSE and cloud-native architectures while reinforcing trust through transparency, governance, and measurable security outcomes rather than relying only on traditional monitoring-centric propositions.

Growth Environment

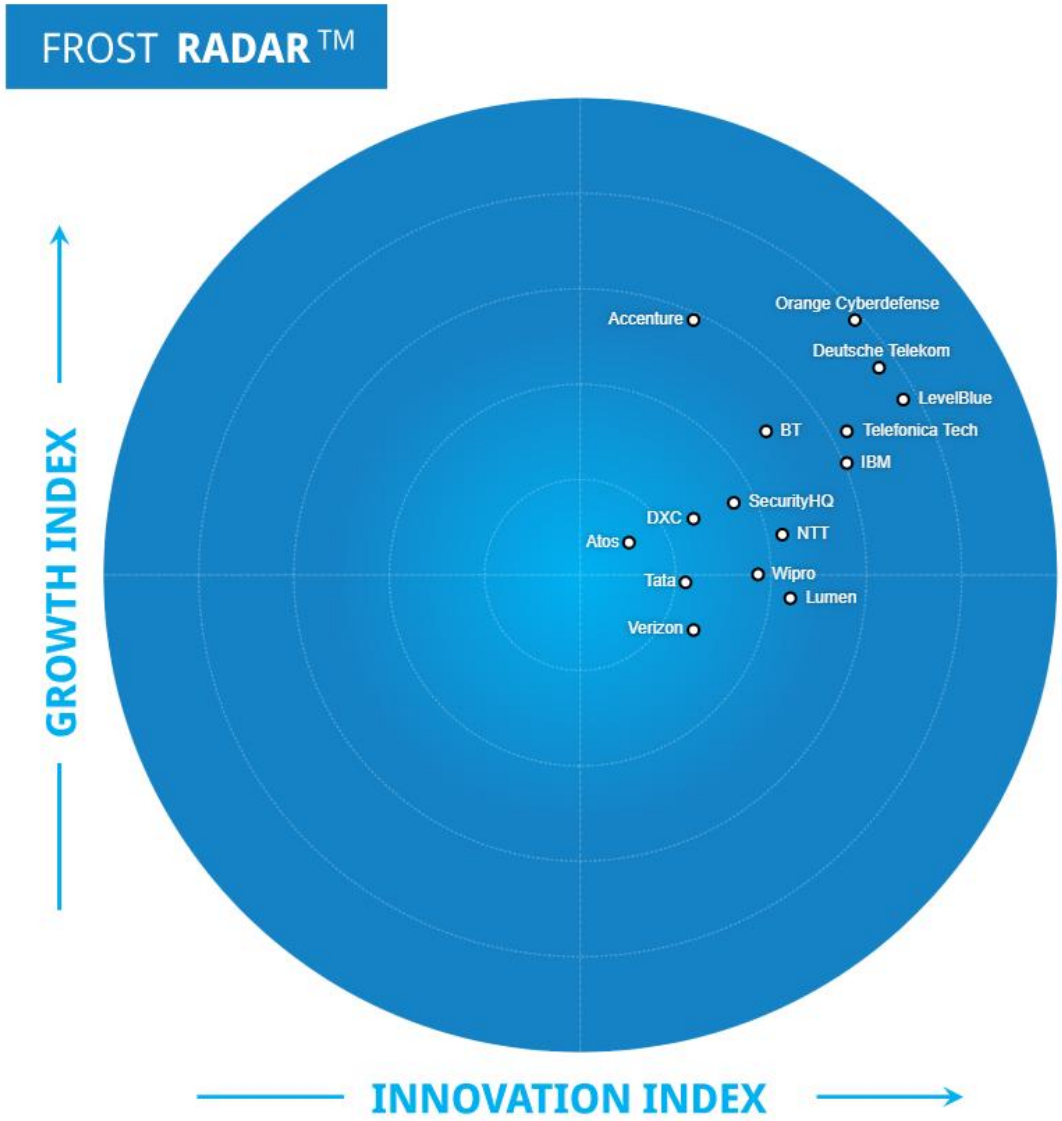
- EMEA is the second-largest MSS region and is forecast to grow from $10.9 billion in 2025 to $16.1 billion in 2028 at a 13.8% CAGR, which places it slightly above the global market growth rate and confirms it as one of the most important contributors to worldwide MSS expansion.
- What makes EMEA especially significant is its role in shaping how MSS is designed and delivered globally, particularly around sovereignty, governance, trust, and auditable security operations, which are becoming defining procurement criteria in many of the region's largest and most security-conscious organizations.
- Demand is particularly concentrated in sectors facing the highest operational and regulatory pressure, where organizations require managed security partners capable of supporting resilience objectives and formal compliance obligations over multiyear transformation cycles.
- EMEA growth is also being supported by the market's shift toward platformized, outcome-driven MSS, in which providers expand beyond traditional monitoring into managed detection and response, exposure management, cloud and identity security, and compliance-aligned operations that deliver broader scope and long-term customer stickiness.
- Although macroeconomic caution, energy costs, and geopolitical uncertainty may slow some modernization initiatives in the near term, MSS spending in EMEA remains resilient because enterprises increasingly view managed security as an operational necessity, especially when sovereign delivery, regulatory alignment, and AI-enabled efficiency improvements are part of the service proposition.

FROST & SULLIVAN

Frost Radar™

Managed Security Services in EMEA

Frost Radar™: Managed Security Services in EMEA



Frost Radar™ Competitive Environment

- LevelBlue combines an impressive mix of innovation and growth leadership in this Frost Radar™, pairing aggressive portfolio expansion with platform consolidation and AI-led service development. Its Trustwave acquisition, broad lifecycle coverage, and increasingly unified operating model position it as one of the most strategically complete MSS providers in Europe.
- Orange Cyberdefense stands out as a leading European innovator, with a cyber resilience model that goes well beyond conventional MDR. Its Core Fusion platform, intelligence-led operations, and growing sovereignty positioning support momentum, especially among organizations seeking a strategic security partner rather than a narrowly defined outsourced SOC.
- Deutsche Telekom / T Security is among the best performers on the Frost Radar™ thanks to its blend of telecom-native visibility, modular MDR, and AI-driven security operations. Its leadership is especially visible in regulated and sovereignty-sensitive environments, where network-embedded security, granular regional delivery, and automation combine to support innovation and sustained market traction.
- Telefónica Tech ranks among the innovation leaders through its highly cohesive NextDefense platform, broad managed and professional security portfolio, and increasingly AI-native SOC strategy. Its growth remains solid, and its sharpened focus on Europe should support its position as enterprises seek integrated, platform-led managed security outcomes.
- Accenture holds a good position through its large-scale managed services engine, broad cybersecurity portfolio, and ability to connect MSS with wider transformation programs. Recent investments in AI-enabled operations, secure AI, and packaged MxDR capabilities support solid innovation, while its scale and consulting reach continue to underpin growth.

Frost Radar™ Competitive Environment (continued)

- IBM remains one of the most advanced innovators in the market, particularly through its autonomous SOC strategy and agentic AI investments. While its broader services portfolio can sometimes dilute its MSS message, IBM's scale, consulting depth, and advanced automation roadmap keep it firmly in the upper tier of the Frost Radar™.
- BT's performance is rooted in its convergence of managed security, infrastructure, and sovereign platform strategy. Its position reflects a provider with meaningful innovation potential and improving growth prospects, particularly as it simplifies its portfolio and embeds security more deeply into broader digital transformation and regulated-industry service environments.
- SecurityHQ earned a solid position through its transparent, technology-agnostic MDR model and its distinctive emphasis on customer-centric, co-managed delivery. It is not the largest player in the field, but its service quality, platform modernization, and European focus give it credible innovation and healthy growth momentum.
- NTT is positioned as a scale player with broad lifecycle coverage, extensive global delivery capability, and a steadily improving MXDR story. Its innovation is less differentiated than that of the top cluster, but its operational reach, advisory depth, and ability to support multinational and regulated customers underpin a relevant market presence.
- Wipro shows balanced performance across innovation and growth, supported by consulting depth, proprietary IP, and growing investment in agentic AI for SOC operations. Its position suggests a provider with genuine upside, especially if it simplifies its market message and converts its technical breadth into clearer, high-impact customer propositions.

Frost Radar™ Competitive Environment (continued)

- Lumen brings credible innovation through its network security convergence strategy and the growing role of Black Lotus Labs intelligence across the portfolio. Its market position is more moderate than the leaders', but its Defender portfolio, connectivity-led differentiation, and bundling approach give it a meaningful role in complex, infrastructure-centric security environments.
- DXC occupies a more central position, reflecting a provider whose strengths lie in enterprise resilience, identity, and partner-enabled managed security rather than standout platform leadership. Its agentic SOC direction and modular delivery model are positive developments, but its differentiation is more evident when MSS is sold in broader transformation relationships.
- Tata Communications is positioned as an emerging converged services player, with managed security increasingly integrated into its broader Digital Fabric strategy. Its innovation is more architectural than category-leading, but its progress in SASE, zero trust, and hybrid visibility gives it relevance for enterprises seeking security embedded in network and cloud transformation.
- Verizon shows improving breadth and market potential, particularly through its MDR service and extensive adjacent portfolio. Its growth opportunity remains significant thanks to its reach and enterprise relationships, though it trails more advanced competitors in AI-led innovation and still has room to unify its broader managed security platform.
- Atos sits lower on the Frost Radar™ despite meaningful strengths in sovereignty, identity, and European delivery depth. Its portfolio is relevant and differentiated in regulated environments, but recent restructuring and uneven commercial momentum weigh on its positioning relative to higher-placed peers with clearer execution and better market visibility.

FROST & SULLIVAN

Frost Radar™

Companies to Action

Deutsche Telekom

INNOVATION

- Deutsche Telekom (T Security) differentiates itself in the European MSS market through a tightly integrated model that combines telecommunications infrastructure, large-scale SOC operations, and an increasingly AI-driven security stack. The company is positioning itself as a strategic enabler of digital sovereignty and cyber resilience in Europe. Unlike traditional MSSPs that rely primarily on third-party telemetry, DT leverages visibility into its own network backbone, which serves hundreds of millions of users, to enrich threat detection and improve response fidelity. This network-native advantage is operationalized through services such as Magenta Security OnNet, which embeds security controls directly into the connectivity layer, enabling immediate protection without requiring endpoint deployment.
- A central element of DT's innovation strategy is its evolution toward a modular, multi-domain MDR platform. MDR Pro integrates endpoint, identity, cloud, network, collaboration, and OT telemetry into a unified detection and response framework supported by 24/7 SOC operations, proactive threat hunting, and customizable playbooks. The platform is designed to operate across heterogeneous customer environments and supports leading technologies such as Microsoft, CrowdStrike, Palo Alto Networks, Cisco, and Fortinet. This vendor-agnostic approach allows customers to retain existing investments while consolidating detection and response workflows. DT is increasingly integrating exposure management capabilities into its MDR platform, reflecting a strategic shift from reactive detection and response toward continuous, risk-based security operations.

Deutsche Telekom (continued)

INNOVATION

- DT has also made significant investments in AI-driven security operations. Its Master SOC in Bonn centralizes large-scale analytics and automation, using AI to correlate signals, prioritize alerts, and provide analysts with contextual insights and recommended actions. Agentic automation capabilities enable semi- or fully automated response workflows, including account disablement, host isolation, and indicator blocking. In parallel, DT has developed a dedicated AI security portfolio, including automated LLM and chatbot pentesting (Deemster), runtime model protection, and AI governance advisory services. These capabilities reflect a shift toward securing both traditional environments and emerging AI-driven attack surfaces.
- The company has recently expanded this strategy through an enhanced partnership with Palo Alto Networks focused on sovereign AI security for Europe. The jointly developed "Sovereign Cortex with T Security offering combines Palo Alto Networks' Cortex platform with Deutsche Telekom's managed Security" operations and sovereign governance framework. The offering enables European organizations to retain control over telemetry data, encryption keys, identity management, and access governance while benefiting from AI-driven security operations. Initially targeting highly regulated sectors such as healthcare, financial services, public sector organizations, and critical infrastructure, the initiative strengthens DT's position at the intersection of AI-powered cybersecurity and European digital sovereignty.
- Additional innovation is evident in DT's identity and trust services, particularly its Zero Trust Identity Fabric and Magenta Security Sign, which provides eIDAS-compliant digital signatures within a sovereign European framework. The company's T-Pot honeypot network, comprising thousands of distributed sensors, further enhances its threat intelligence capabilities.

Deutsche Telekom (continued)

INNOVATION

- Recent developments, including the expansion of MDR Pro, the rollout of AI pentesting, the operationalization of network-embedded security, and the launch of sovereign AI-security initiatives, demonstrate DT's continued focus on integrating security across domains while increasing automation, strengthening data sovereignty, and reducing response times.

Deutsche Telekom (continued)

GROWTH

- Deutsche Telekom has established a strong position in the European managed security services market, supported by consistent growth and a broad customer base spanning midsize organizations, large enterprises, and regulated sectors. The company's growth trajectory has been driven by a combination of portfolio expansion, deeper integration of security into its telecommunications services, and increased demand for MDR and SOC-based offerings.
- A key contributor to growth has been the continued development and adoption of MDR Pro, which has enabled DT to transition customers from traditional, siloed security services to a more integrated, multi-domain detection-and-response model. Existing customers have expanded their engagements over time, moving from baseline managed services to more comprehensive MDR offerings that incorporate identity monitoring, automation, and advanced analytics. Client feedback indicates that this transition has been relatively smooth, with onboarding processes described as structured and efficient even in multi-entity environments, and service expansion occurring as new capabilities are introduced.
- DT has also benefited from its ability to address customer requirements around 24/7 availability, scale, and expertise, factors that continue to differentiate it from smaller regional providers. In competitive evaluations, customers have highlighted DT's combination of continuous service availability, depth of technical expertise, and cost-effectiveness as key decision drivers.

Deutsche Telekom (continued)

GROWTH

- The company's geographic footprint, anchored in DACH but extending across Europe and internationally through T-Systems, has supported expansion into new markets while maintaining a strong base in its core region. Growth has also been supported by increasing demand from regulated industries, including healthcare, manufacturing, and critical infrastructure, where DT's experience and sovereign delivery capabilities are particularly relevant.
- Operationally, DT has continued to invest in SOC infrastructure, including the establishment of its Master SOC, as well as in AI-driven automation and threat intelligence. These investments have improved service scalability and contributed to faster detection and response times, which in turn support customer retention and upsell opportunities.
- Looking ahead, DT's introduction of MDR Start is expected to broaden its addressable market by targeting smaller organizations, with a clear upgrade path into higher-tier MDR offerings as customer maturity increases. At the same time, continued expansion of network-embedded security and AI-driven services is likely to support further growth across both existing and new customer segments.

Deutsche Telekom (continued)

FROST PERSPECTIVE

- Deutsche Telekom /T Security's primary strength lies in its ability to combine network-native visibility, large-scale SOC operations, and a broad, modular MDR platform into a cohesive end-to-end service offering. This integrated approach provides a strong foundation for delivering end-to-end security across IT, cloud, and network environments. To further strengthen its position in future iterations of the MSS Radar, DT should focus on deepening automation outcomes, refining customer-facing value articulation, and extending its platform capabilities into adjacent areas.
- A key opportunity for DT is to build on its existing agentic automation capabilities by delivering more prescriptive, outcome-driven security services. While DT has already implemented automated response workflows, customer feedback indicates a growing expectation for faster, more deterministic responses, particularly in high-frequency attack scenarios such as phishing. DT should continue to refine its integration with upstream detection sources (e.g., identity systems and conditional access policies) to ensure that automated actions can be triggered consistently within minutes. By formalizing these capabilities into clearly defined “autonomous response tiers,” DT could further differentiate its MDR offering.
- DT’s network-native security capabilities represent another area of strategic advantage. The company is well-positioned to extend Magenta Security OnNet into a broader secure access and exposure management framework, leveraging its control of the connectivity layer to deliver continuous visibility and enforcement without reliance on endpoint agents. Expanding this model to include deeper integration with SASE and Secure Networking Platform initiatives would strengthen DT’s role as both a connectivity and security provider.

Deutsche Telekom (continued)

FROST PERSPECTIVE

- From a customer experience perspective, DT could enhance its value proposition by improving executive-level communication and reporting. While technical capabilities are well established, there is an opportunity to provide more structured, outcome-oriented reporting that clearly links security operations to business risk reduction. This would be particularly relevant for engagements involving senior stakeholders and board-level discussions.
- Finally, DT should continue to expand its AI-driven security capabilities beyond detection and response into proactive risk mitigation. By leveraging its extensive telemetry and data access, DT is well-positioned to deliver more predictive insights and automated remediation recommendations, moving closer to a continuous exposure management model. This would align with evolving customer expectations and reinforce DT's positioning as a forward-looking MSS provider.

FROST & SULLIVAN

Best Practices & Growth Opportunities

Best Practices

1. Prioritize platformized, outcome-driven service models. Leading providers are moving beyond fragmented, alert-centric delivery toward unified platforms that combine telemetry, analytics, orchestration, and reporting. A best practice is to show how the service reduces operational friction, improves consistency, and delivers measurable outcomes, such as faster response, lighter analyst workload, and risk reduction rather than simply providing nominal coverage.

2. Embed AI into workflows but keep governance and human supervision central. Best-in-class providers use AI across triage, investigation, prioritization, and response orchestration while maintaining explainability, override mechanisms, and clear accountability. The market is rewarding providers that can prove operational impact from AI in production, not just roadmap ambition, especially where customers demand transparency, auditability, and confidence in automated actions.

3. Align managed security with exposure reduction, trust, and operational clarity. Best practice increasingly means integrating exposure insights, identity, and SaaS posture, and remediation guidance into daily operations while also defining responsibilities, escalation authority, and data handling transparency up front. Providers that combine proactive risk reduction with auditable processes, sovereign options, and clear co-managed models are better positioned to build long-term customer confidence.

Growth Opportunities

1. AI-augmented, human-supervised SOC platforms are a major MSS growth opportunity as providers shift from labor-intensive, alert-centric delivery to scalable operating models centered on automation, consistency, and measurable outcomes. Vendors that embed AI across triage, investigation, and response while reinforcing explainability, governance, and human oversight will be better positioned to improve margins, differentiate services, and satisfy customer expectations.

2. Exposure-led MSS and continuous risk reduction services are expanding the market beyond reactive detection and response by aligning managed security with board-level priorities around resilience and measurable posture improvement. Providers that unify asset discovery, vulnerability intelligence, identity posture, SaaS risk, and configuration analysis into continuous remediation-focused workflows can increase customer stickiness, raise contract value, and differentiate from commoditizing MDR-centric competitors.

3. Sovereign, regulation-aligned MSS for high-assurance environments is becoming a high-value growth path as regulatory scrutiny, geopolitical uncertainty, and trust requirements reshape procurement criteria. Providers that combine local SOC presence, jurisdiction-aware data processing, auditable operations, and sovereign options for analytics and AI can command premium positioning in public sector, healthcare, financial services, and critical infrastructure accounts requiring modernization and compliance assurance.

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

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) 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

MEGATRENDS 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 megatrends 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