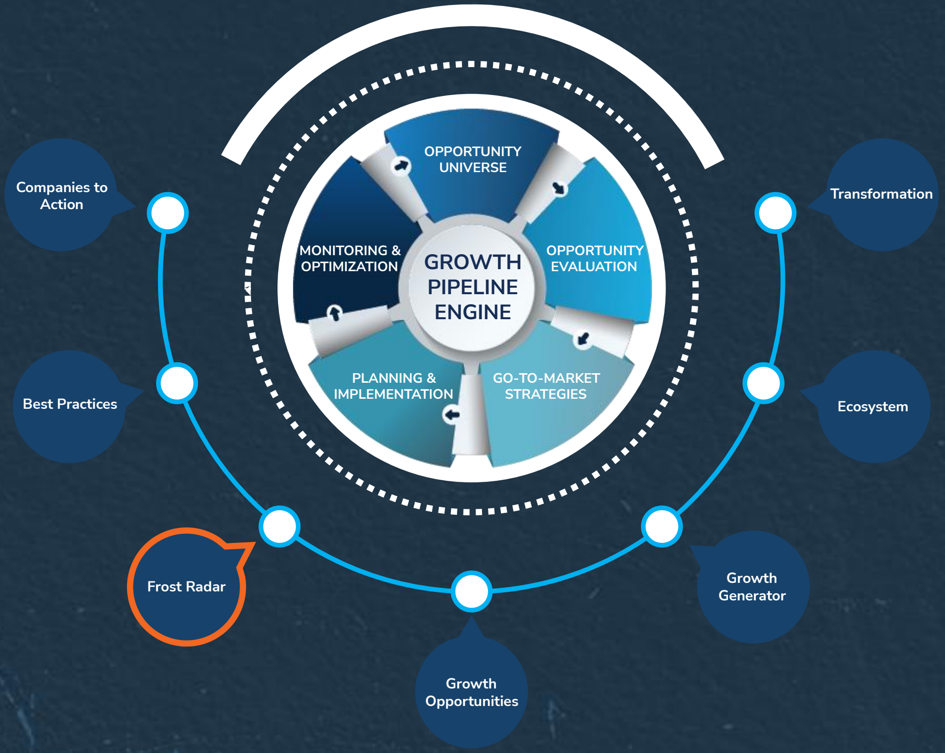
FROST & SULLIVAN

# Frost Radar™: OT Cybersecurity Solutions, 2025

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



Authored by: Tobias Folatelli
Contributor: Danielle VanZandt

KBF2-23
December 2025

# Strategic Imperative and Growth Environment

# Strategic Imperative

- OT cybersecurity has become a defining front in global stability and industrial resilience. The past two years have made it clear that cybersecurity risk is no longer confined to data theft or IT disruption; it can now inflict real-world harms, shape geopolitical leverage, and impact operational continuity and public safety. Attacks on Ukraine's power grid, breaches in Middle Eastern energy infrastructure, and the wave of ransomware incidents against European manufacturing plants have shown that adversaries are targeting the control systems that sustain national economies. The weaponization of cyber operations in regional conflicts and proxy campaigns has elevated OT cybersecurity from a technical concern to a strategic priority across governments and industry.
- The risk environment is intensified by structural change within critical infrastructure segments. Accelerated digitalization, remote operations, and the convergence of IT, OT, and IoT networks have dissolved the traditional isolation that once protected industrial systems. Real-time data integration, cloud-managed control platforms, and sensor-rich automation have expanded both efficiency and exposure. Attackers now exploit the same connectivity that operators rely on for optimization, using lateral movement from corporate IT into OT environments to trigger physical disruption.
- Governments are responding with regulation and enforcement in the European Union, the United States, Japan, Singapore, and Australia, among others. New regulatory standards are enforcing OT-specific risk management frameworks as part of national resilience strategies. Across the Middle East, sovereign wealth-funded energy operators are embedding cybersecurity into every new refinery, grid, and desalination project as state policy. These frameworks are closing the long-standing gap between awareness and enforcement, forcing operators to operationalize cybersecurity as an integral layer of safety and compliance.

Source: Frost & Sullivan

# Strategic Imperative (continued)

- At the same time, market awareness is advancing beyond regulatory compliance. Many organizations now view cybersecurity as a business continuity enabler rather than a mandated cost. Even in industries not yet covered by formal regulations, companies are voluntarily aligning with recognized standards to strengthen their digital resilience and maintain investor confidence. This shift is reinforced by supply chain requirements as large manufacturers, utilities, and energy providers demand verifiable OT security practices from their suppliers and service partners. Compliance frameworks have thus evolved into shared governance tools, guiding internal policies, procurement decisions, and vendor selection criteria across interconnected industrial ecosystems.
- The consequences of inaction are now immediate and quantifiable. A successful attack can suspend industrial production, compromise environmental controls, or cut power and water to millions. Beyond economic loss, such incidents erode public confidence, expose governments to political pressure, and delay national energy transitions. As AI-enabled attacks emerge and become increasingly capable of crafting adaptive payloads or mimicking normal process behavior, the modernization of defense architectures becomes more urgent.
- In this context, OT cybersecurity has become a strategic necessity. Organizations that once viewed security as a cost center are now integrating it into digital transformation and resilience planning. The focus has shifted from compliance to continuity and from awareness to action.

Source: Frost & Sullivan

# Growth Environment

- The OT cybersecurity market is expanding rapidly, with spending projected to rise from $4.37 billion globally in 2024 to $8.47 billion by 2030 at an 11.7% compound annual growth rate (CAGR). Growth is supported by converging drivers, including the modernization of industrial infrastructure, tightening regulatory frameworks, and rising threat activity targeting critical operations. Unlike IT security, where market maturity tempers expansion, OT cybersecurity remains in an acceleration stage as organizations move from awareness to implementation.

- Each major vertical contributes a distinct growth dynamic that shapes overall market performance. Manufacturing records the highest expansion at a 13.9% CAGR—a reflection of sustained investment in automation, asset modernization, and advanced threat detection across process and discrete environments. Industrial sectors follow at 11.9% as oil, gas, and mining operators accelerate visibility initiatives to reduce operational risk and comply with increasingly stringent security requirements. Growth in utilities and transport is steadier, influenced by maturing compliance standards, extended procurement cycles, and persistent budget constraints that moderate the pace of large-scale deployments.

- OT cybersecurity encompasses specialized technologies and services that secure control networks, industrial assets, and physical process environments. Core capabilities include asset inventory, network monitoring, intrusion detection, anomaly analytics, secure remote access, and incident response. The market increasingly favors integrated platforms that combine these functions under unified management, enabling operators to consolidate vendors and achieve cross-domain visibility between IT and OT environments. Vendors are advancing purpose-built solutions that emphasize scalability, ease of deployment, and interoperability with enterprise security tools.

Source: Frost & Sullivan

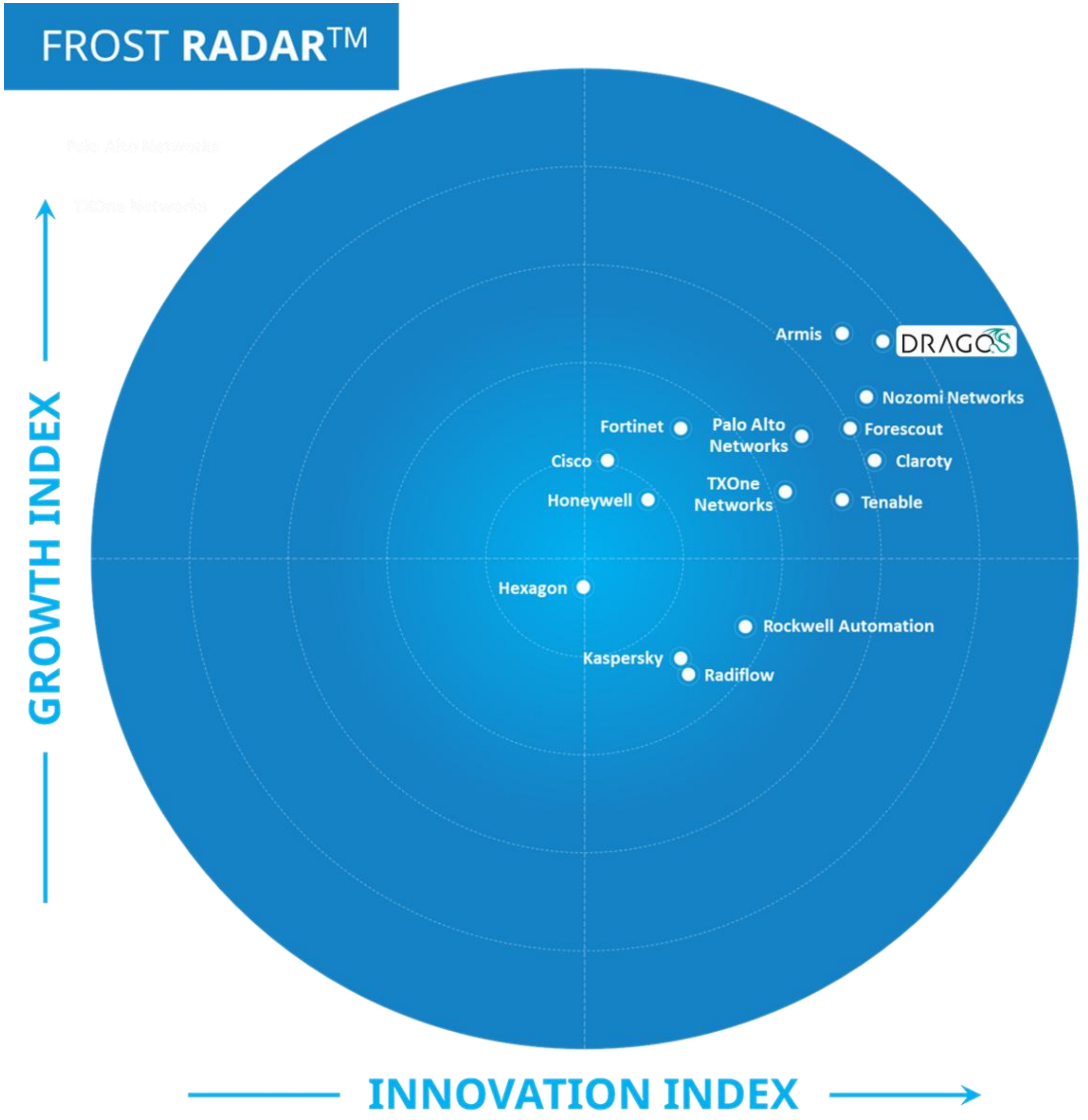
# Growth Environment (continued)

- Emerging trends are reshaping the technical scope of the market. AI has transitioned from experimental use to an operational foundation across OT cybersecurity solutions. These systems now enable near-real-time detection of emerging threats, configuration errors, and performance degradation, reducing response times from hours to minutes. Predictive analytics are increasingly used to anticipate asset failures and preempt downtime by combining security telemetry with operational data, turning cybersecurity monitoring into a contributor to overall reliability. At the same time, natural language processing and automated response orchestration are streamlining triage, allowing analysts to manage large alert volumes and standardize incident workflows.
- Despite strong momentum, barriers remain. Integration complexity, a shortage of skilled professionals, and operational resistance to downtime constrain the speed of deployment. Smaller operators face cost and training hurdles, while legacy infrastructure limits full adoption of advanced features. Nonetheless, the combination of regulatory certainty, sustained threat activity, and rising digital maturity ensures long-term structural growth. By 2030, OT cybersecurity will be deeply embedded into every major industrial modernization initiative, with platform consolidation, AI-driven analytics, and managed services defining the competitive frontier.

Source: Frost & Sullivan

# Frost Radar™: OT Cybersecurity Solutions

# Frost Radar™: OT Cybersecurity Solutions



Source: Frost & Sullivan

# Frost Radar™ Competitive Environment

- This Frost Radar<sup>TM</sup> benchmarking assesses vendors that deliver consolidated, product-based portfolios with measurable adoption across multiple critical infrastructure sectors. Eligible participants must actively develop and commercialize proprietary OT cybersecurity technologies designed specifically for industrial control environments. Inclusion requires multinational deployments and the ability to serve more than one vertical, reflecting the cross-sector demand for OT protection.
- The industries considered in this analysis are utilities (electric power and water), transportation and aviation, manufacturing (discrete and process), oil and gas, and mining. Vendors focused on bespoke solutions, consulting, or managed services without a stand-alone, customer-managed platform were excluded. Systems limited to proprietary ecosystems or tied exclusively to a single OEM architecture were not considered because the benchmark emphasizes open, vendor-agnostic platforms that integrate across diverse operational environments.
- For clarity of scope, this analysis evaluates OT cybersecurity as a distinct domain separate from IT and CPS security. OT encompasses the control systems, devices, and networks that manage physical processes and industrial operations. IT security focuses on data protection and information systems, while CPS security covers integrated computing-physical systems where digital and physical components are engineered together. This analysis concentrates solely on the OT layer—the operational infrastructure that enables continuous, safe, and reliable functioning of critical assets.
- The OT cybersecurity market continues to mature rapidly, with competition intensifying around platform consolidation, AI-driven analytics, and cross-sector scalability. Vendors are differentiating not only through technology innovation but also by demonstrating measurable operational impact, global reach, and integration maturity. The 2025 Frost Radar<sup>TM</sup> highlights a dynamic ecosystem balancing OT-native specialists with diversified cybersecurity and automation providers, each evolving their positioning as convergence deepens across industries.

Source: Frost & Sullivan

# Frost Radar™ Competitive Environment (continued)

- Dragos leads the competitive landscape with one of the most comprehensive and technically mature OT cybersecurity platforms. Its focus on threat intelligence, managed detection, and industrial incident response positions it as an innovation and execution benchmark. Continuous portfolio expansion, partnerships with global infrastructure operators, and the integration of advanced analytics have solidified Dragos as the reference point for industrial threat visibility and response maturity.
- Armis demonstrates exceptional growth momentum, driven by its unified approach to asset intelligence and cross-domain visibility across OT, IT, and IoT environments. Its rapid revenue expansion reflects market traction with large enterprises seeking centralized visibility and risk management. By expanding use cases into critical infrastructure and government, Armis is effectively bridging asset management and security analytics, reinforcing its leadership in scalable, data-driven protection strategies.
- Innovation Index leaders Claroty, Nozomi Networks, and Forescout continue to drive technical differentiation through visibility and AI-powered detection capabilities. Claroty's progress in integration breadth and data contextualization strengthens its standing among industrial operators, while Nozomi's sustained innovation in analytics and scalability reinforces its position as a trusted OT-native provider. Forescout has leveraged its enterprise heritage to deliver converged visibility across IT and OT, maintaining strong innovation performance with moderate but steady growth.
- Growth standouts Fortinet, Palo Alto Networks, and Tenable are leveraging their cybersecurity scale to capture OT opportunities through integration and compliance alignment. Fortinet and Palo Alto Networks are expanding through unified architectures that extend enterprise security into industrial domains, while Tenable's focused OT module and partnerships are translating its IT visibility expertise into operational environments. These vendors benefit from brand recognition and channel reach, balancing innovation with portfolio synergy.

Source: Frost & Sullivan

# Frost Radar™ Competitive Environment (continued)

- Diversified industrial conglomerates Honeywell and Hexagon, together with Rockwell Automation, continue to integrate automation and cybersecurity within broader industrial portfolios. Their embedded security offerings are gaining traction as industrial customers seek trusted ecosystem partners, though productization and scalability remain differentiating challenges. These companies play an important role in driving adoption among traditionally conservative operators by linking cybersecurity directly to operational reliability and safety.
- Emerging and regional specialists TXOne Networks, Kaspersky, and Radiflow contribute to the market's diversity through focused innovation in endpoint protection, industrial hardening, and network defense. Kaspersky and Radiflow maintain regional and vertical-specific relevance, with continued innovation in niche applications despite limited global scale.
- Overall, the competitive landscape reflects a market transitioning from fragmented point solutions toward integrated, analytics-driven platforms. The highest-performing companies combine technological depth with ecosystem openness, scalability, and measurable customer impact—traits that will define market leadership as OT cybersecurity becomes embedded in the operational fabric of industry.

Source: Frost & Sullivan

# Frost Radar™: Companies to Action

# Dragos

## INNOVATION

- Dragos delivers one of the most mature and specialized OT cybersecurity platforms in the market, purpose-built to protect ICS and critical infrastructure environments. The Dragos Platform unifies asset visibility, threat detection, vulnerability management, and incident response in a single architecture designed for the operational realities of industrial networks. It automatically inventories OT, IT, IoT, and IIoT assets south of the firewall using passive and selective active collection, enabling operators to achieve complete visibility without disrupting processes. With support for more than 2,500 protocols, the Platform provides the foundation for secure network monitoring across utilities, oil and gas, manufacturing, transportation, mining, and other industrial operations.
- A defining differentiator is Dragos's risk-based vulnerability management, which applies OT-specific context to prioritize the top vulnerabilities that demand immediate action. Instead of using generic IT scoring, Dragos introduces OT-corrected CVSS scores and its proprietary "Now, Next, Never" framework, allowing operators to focus remediation efforts where safety and uptime would be most affected. Threat detection is powered by WorldView, the industry's largest civilian OT threat intelligence database, which feeds weekly Knowledge Packs with new indicators, detection rules, and playbooks derived from real adversary tactics observed by Dragos's incident responders. These are complemented by Neighborhood Keeper, a collective defense network that anonymizes and shares insights across participating utilities and industrial firms to alert others of emerging threats.
- The Platform's Investigation and Response module translates this intelligence into operational guidance through expert-authored workflows and step-by-step remediation playbooks. In 2025, Dragos expanded the platform with AI-driven analytics, enhanced asset enrichment via project file ingestion, and new, lightweight collectors for edge environments.

Source: Frost & Sullivan

# Dragos (continued)

## GROWTH

- The acquisition of Network Perception (NP) in 2024 significantly advanced Dragos's visibility and compliance capabilities, integrating NP-View's network topology mapping and segmentation validation into the Dragos Platform. This addition provides dual-layer visibility across industrial networks, real connections, and potential access paths, enhancing defenses against lateral movement while automating compliance with regulations and standards.
- Public sector expansion has become a key growth engine. The launch of Dragos Public Sector LLC in 2024 formalized its US federal business, which has maintained a 67% CAGR since 2020, supporting defense and civilian agencies through DISA-validated implementations. Partnerships with Carahsoft streamlined procurement under GSA Schedule and SEWP V contracts, broadening the company's federal- and state-level adoption. Internationally, Dragos signed a memorandum of understanding with Singapore's Digital and Intelligence Service to jointly develop advanced cybersecurity capabilities, while the expansion of the Community Defense Program into Canada extended Dragos's collective defense model to utilities and water operators with limited cybersecurity resources, reinforcing its mission to safeguard critical infrastructure.
- Collaborations with industrial and technology leaders also accelerated commercial growth. The partnership with GE Vernova advanced OT protection for electric grids through combined monitoring and incident response capabilities, while the integration with CrowdStrike Falcon Next-Gen SIEM embedded OT threat intelligence into enterprise SOC operations. New alliances with insurance and legal partners, including Marsh, Axio and Pillsbury, aligned OT incident response with risk-management frameworks, improving customer readiness.

Source: Frost & Sullivan

# Dragos (continued)

## FROST PERSPECTIVE

- Dragos's continued success will depend on its ability to scale AI and automation while maintaining the operational integrity that defines its brand. The company's intelligence-driven detection and vulnerability models are an important step toward adaptive defense, but industrial operators will expect greater predictive and prescriptive capabilities, such as machine learning that correlates telemetry, maintenance, and process data to forecast disruptions before they occur. Investing further in explainable AI and cross-platform analytics would enhance operational trust and improve the platform's ability to deliver quantifiable business outcomes.
- To sustain growth, Dragos should continue strengthening its vertical-specific offerings. Its visibility and compliance features already align well with NERC-CIP and IEC standards in the power sector, but similar frameworks for oil and gas and mining present expansion opportunities. Extending partnerships with automation OEMs and regional managed security providers could accelerate adoption among midsize industrial operators, while continued integration with cloud ecosystems, such as AWS and Microsoft Azure, would appeal to hybrid OT/IT environments transitioning to edge computing.

Source: Frost & Sullivan

# Best Practices & Growth Opportunities

# Best Practices

1 Leading vendors are training AI engines with datasets that capture the unique behaviors of industrial assets, control systems, and sector-specific operations, such as energy distribution, manufacturing, or transport. Feeding OT and vertical-specific information into AI models enhances anomaly detection precision, reduces false positives, and contextualizes alerts in real process conditions. Continuous retraining with anonymized field data ensures ongoing relevance as new threat patterns emerge across critical sectors.

2 Providers are prioritizing open architectures that enable broad integration across legacy and modern operating systems. Through partnerships and multivendor compatibility, these systems can interface with diverse controllers, endpoint devices, and management tools. Support of hybrid deployments and older infrastructure allows vendors to deliver continuity with no need for replacement and ensure compatibility with non-Windows operating systems commonly used in industrial deployments outside the United States.

3 Vendors are strengthening ecosystem-wide resilience by facilitating secure data collaboration and threat intelligence exchange across customers, partners, and sectors. By anonymizing and aggregating telemetry from diverse OT environments, companies can identify cross-industry attack patterns and accelerate detection of emerging tactics. Integrating this intelligence directly into product updates and managed platforms creates adaptive defenses that evolve with the threat landscape while respecting data privacy.

Source: Frost & Sullivan

# Growth Opportunities

1 Vendors should leverage AI to offset the industry-wide shortage of skilled OT cybersecurity professionals. By automating detection, alert correlation, and response playbook generation, AI can significantly reduce analyst workload and improve mean time to response. Transparent, auditable AI features for continuous monitoring and incident triage will enable customers to secure broader environments without proportional headcount growth.

2 Vendors should embed performance analytics that link OT cybersecurity to measurable business outcomes. Demonstrations of quantifiable improvements in uptime, incident response efficiency, and cost avoidance strengthen executive-level justification for continued investment. Platforms that translate security performance into operational and financial metrics will position cybersecurity as a value-generating function rather than a compliance cost, increasing customer retention and strategic alignment.

3 Vendors should prioritize developing open, unified platforms that integrate core OT security functions through interoperable architectures. Consolidation of asset visibility, network detection, and access control into a single management interface reduces operational complexity and total cost of ownership. Solutions that interconnect IT and OT visibility via standardized APIs will gain a competitive advantage as customers seek scalable, enterprise-wide cybersecurity ecosystems.

Source: Frost & Sullivan

# Frost Radar™ Analytics

# Frost Radar$^{TM}$: 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$^{TM}$.

GI3

**GROWTH PIPELINE$^{TM}$**
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

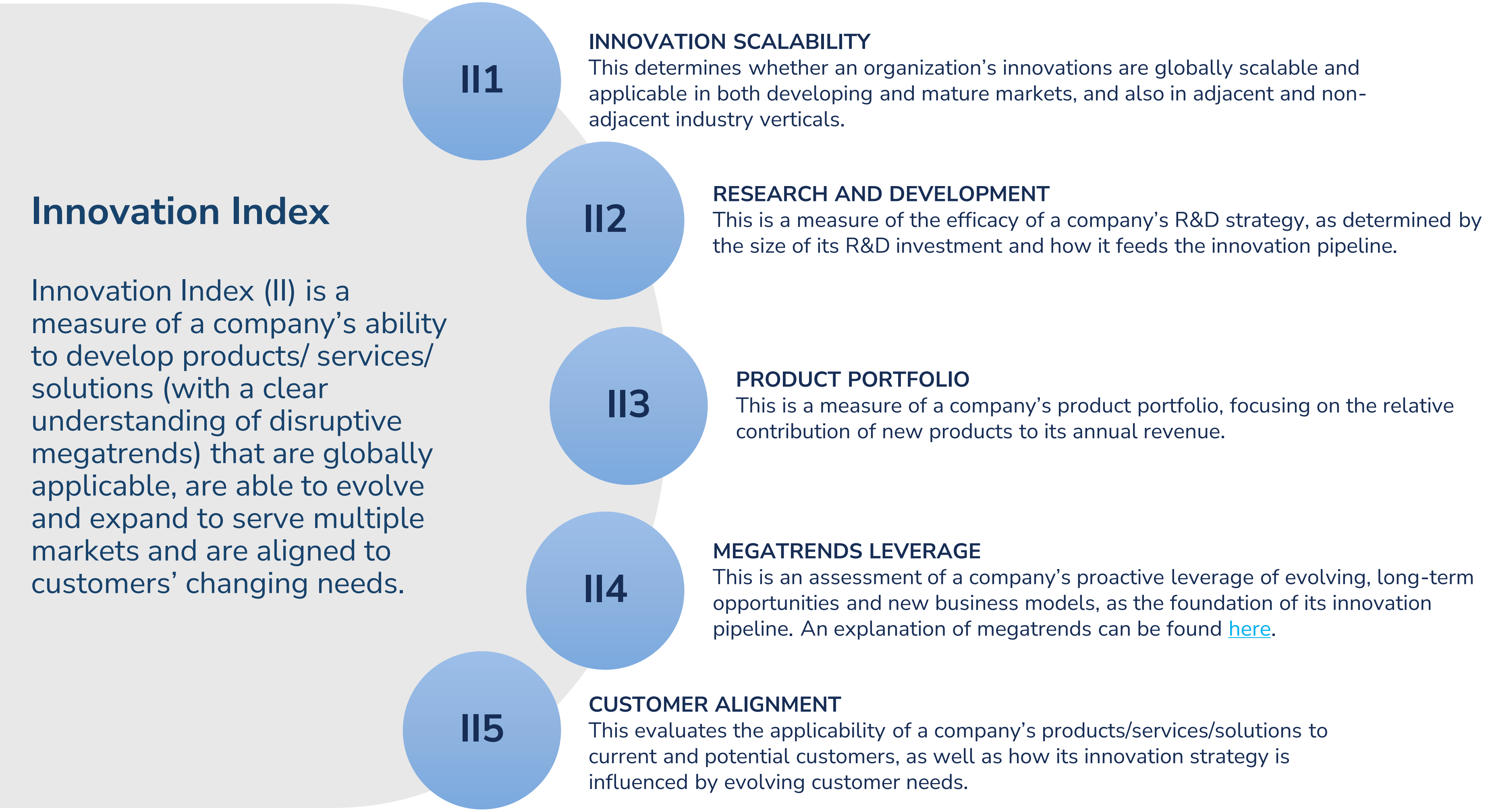
**VISION AND STRATEGY**
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

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$^{TM}$: 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 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.

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