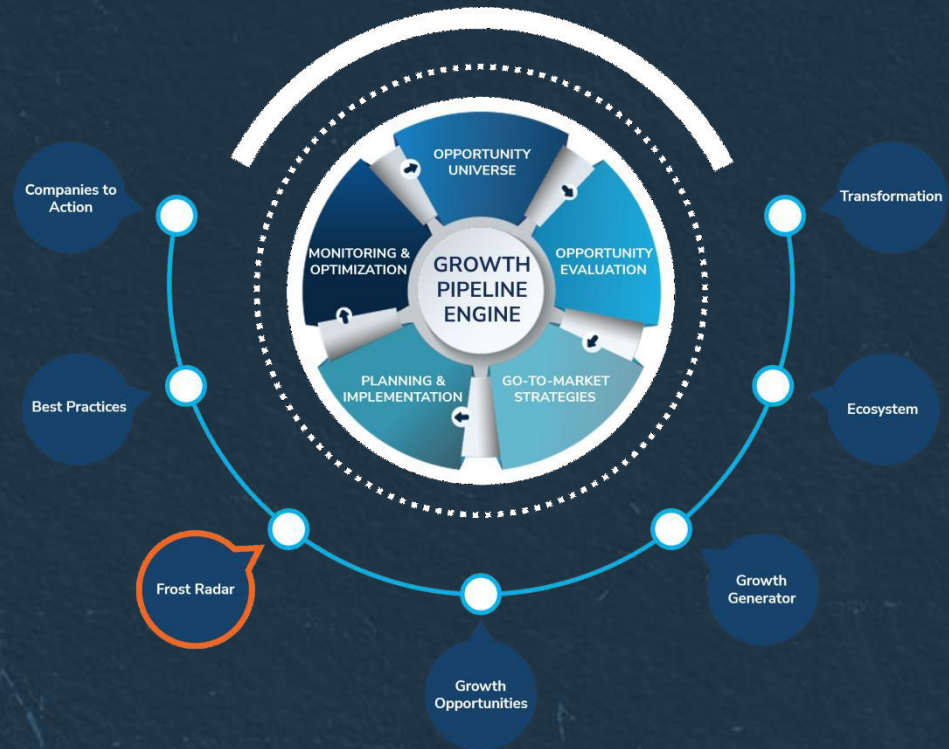


Frost Radar™: SaaS Security Posture Management, 2025

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

Authored by: Ying Ting Neoh
Contributor: Jarad Carleton



PG1W-74
October 2025

Strategic Imperative and Growth Environment



Strategic Imperative

- The rapid proliferation of SaaS applications has outpaced many organizations' ability to maintain visibility and control, exposing critical security gaps and increasing the likelihood of data breaches due to insufficient SaaS-specific protections. Compounding these risks, cybersecurity talent shortages and alert fatigue hinder effective prioritization and remediation. This drives demand for SaaS security posture management (SSPM) solutions that are scalable, intuitive, and require minimal specialized expertise to onboard and operate.
- SSPM offerings with broad pre-built integrations and low-code/no-code connectors enable organizations to secure their diverse SaaS portfolios while reducing operational complexity.
- Generative artificial intelligence (GenAI) is redefining the technology and cybersecurity market given that almost all sectors are taking advantage of its benefits, although GenAI embedded across SaaS applications introduces new attack surfaces ranging from misconfigurations to shadow AI usage. It is just as important for security providers and organizations to leverage AI tools to analyze, automate, and respond as to implement specialized AI security controls within SSPM to govern AI components and enforce data protection standards.
- As security needs evolve, there is an emphasis on SSPM platforms delivering actionable business intelligence (BI) over raw technical alerts, empowering security teams with contextual insights to make well-informed, effective risk management decisions.
- Demand for cross-domain and bidirectional orchestration between security tools through a single-pane-of-glass view contributes to the consolidation trend across the cybersecurity market including the SSPM space. Customer preference is shifting to unified, automation-driven SSPM platforms that cover the entire SaaS security lifecycle, providing visibility while minimizing manual effort and security inefficiencies.

Growth Environment

- The global SSPM market is growing steadily and moving quickly toward the mainstream. Frost & Sullivan expects its revenue growth rate for 2025 to be 71.2%, and its compound annual growth rate for the 2025–2030 period to be 48.7%.
- North America is the largest regional market, accounting for close to 74% of revenue, followed by the region encompassing Europe, the Middle East, and Africa (EMEA). Asia-Pacific (APAC) and Latin America trail. Very large and large organizations continue to be the top revenue contributors for SSPM, but small businesses are the fastest growing in 2025.
- SaaS applications fuel organizations' digital transformation and remote work, expanding the SaaS attack surface and increasing risks from misconfigurations, shadow SaaS, sophisticated breaches, and compliance challenges. The increasingly complex threat landscape drives demand for SSPM platforms that go beyond posture management, encouraging vendors to incorporate disruptive technologies into their SSPM portfolios. These include but are not limited to advanced threat detection, AI-powered analytics and assistant, identity governance including identity threat detection and response (ITDR), risk prioritization, shadow SaaS, shadow AI, SaaS-to-SaaS monitoring, browser extension control, agentic AI, granular control over remediation, context-aware threat correlation, and automated security operations (SecOps) workflows in a unified solution. Advanced and next-generation SSPM features can help organizations effectively monitor and manage their SaaS environment and improve security outcomes.
- Because of economic uncertainties and operational complexities, organizations are moving away from fragmented point solutions in favor of unified, single-pane-of-glass platforms that reduce total cost of ownership and simplify SaaS security management. This signals a shift from stand-alone SSPM tools to integrated, end-to-end, zero-trust SaaS security architectures that incorporate AI governance and streamline enterprise workflows.

Growth Environment (continued)

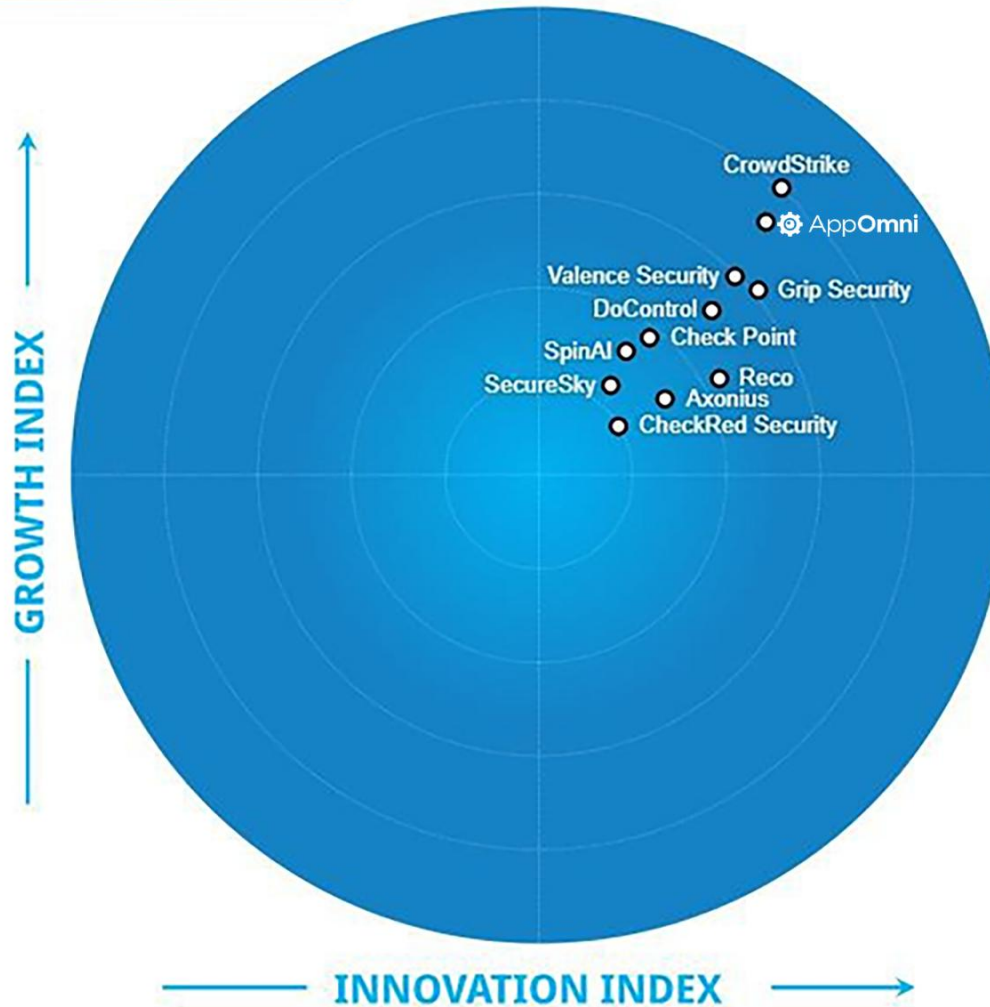
- The consolidation trend has also driven mergers and acquisitions (M&A). Vendors are embedding SaaS security capabilities into broader cloud and security portfolios.
- Frost & Sullivan considered the following factors as essential to a SSPM vendor when compiling this Frost Radar™ analysis:
 - New SSPM product launches and the scalability of SSPM product features or portfolio
 - The ability to leverage megatrends—including identity security (human identities [HI] and non-human identities [NHI]), shadow SaaS/IT/AI, AI-driven threat detection, automation, GenAI, and agentic AI—and offer or integrate with other technologies for enhanced security
 - The ability to deliver services and products tailored to local customer needs in North America, EMEA, Latin America, and APAC to strengthen regional presence
- Frost & Sullivan study related to this independent analysis:
 - SaaS Security Posture Management (SSPM) Market, Global, 2025–2030 (PG1V, to be published soon)
 - [SaaS Security Posture Management Market, Global, 2024–2029](#)
 - [Frost Radar™: SaaS Security Posture Management, 2024](#)
 - [SaaS Security Posture Management \(SSPM\) and Data Security Posture Management \(DSPM\)](#)

Frost Radar™: SaaS Security Posture Management



Frost Radar™: SaaS Security Posture Management

FROST RADAR™



Frost Radar™ Competitive Environment

- To maintain a competitive edge and stay relevant, SSPM vendors will need to continuously innovate and differentiate as customers' needs evolve from passive and static posture management to real-time, end-to-end proactive security with built-in runtime anomaly detection and context-aware correlation.
- As SSPM shifts from reactive to a proactive, vendors must prioritize flexible, scalable, and AI-enhanced solutions that integrate deeply with existing security ecosystems to maintain resiliency. In addition to meaningful automation, user-friendly features, such as an intuitive user interface and the ability to switch between tools, knowledge graphs, comprehensive attack path mappings, and collaboration tools will likely become competitive advantages over the next 3 to 5 years.
- Key aspects of SSPM include a unified platform approach, meaningful automation, and identity-centric security approach while factoring in various security vectors, such as enterprise-specific contextual data, real-life context, and runtime insights. Beyond configuration management, top competitors in the space satisfy these core aspects or exemplify clear innovation initiatives in this direction.
- With growing pressure to optimize security budgets and investment, organizations are seeking to consolidate their security. This platformization trend is fueling market consolidation through M&A, driving the integration of SSPM capabilities into broader cybersecurity platforms. Stand-alone SSPM vendors now are not only competing among themselves but also with extended detection and response (XDR), secure access service edge (SASE), and managed security service providers (MSSPs) that can deliver SSPM features in their comprehensive security portfolios.
- Frost & Sullivan research indicates that SSPM vendors will continue to complete their SaaS security portfolios through in-house development, technological partnerships, or M&A activity.

Frost Radar™ Competitive Environment (continued)

- In this Frost Radar™, Frost & Sullivan shortlisted and assessed the top 11 SSPM vendors from a pool of more than 20 global market players based on the following selection criteria:
 - Annual SSPM revenue of at least \$3 million in 2025
 - At least a 0.5% market share globally in 2025
 - A business presence in at least 2 regions (i.e., North America, EMEA, Latin America, and APAC)
- To ensure fair scoring and comparison, Frost & Sullivan excluded certain vendors that meet the inclusion criteria for this Frost Radar™ but were unable to share detailed insights into their business performance and SSPM solutions.
- The SSPM vendors selected for this analysis are AppOmni, Axonius, Check Point Software Technologies, CheckRed Security, CrowdStrike, DoControl, Grip Security, Reco, SecureSky, Spin.AI, and Valence Security.
- CrowdStrike, AppOmni, and Valence Security have topped the Frost Radar™ Growth Index because of their consistent and strong financial performance in terms of revenue or market share growth globally during the last 3 years. All three leverage broad partner ecosystems, including consulting firms, managed service providers (MSPs), MSSPs, technology alliances, and leading cybersecurity vendors, to expand reach across industries and geographies. Frost & Sullivan recognizes their active engagements in sales and marketing efforts as well as their established brand reputation in the cybersecurity space. The combination of scalable partnerships, technical integration, regulatory compliance, and strong market focus drives accelerated growth for all three vendors, maintaining robust growth pipelines in the next 2 to 3 years.

Frost Radar™ Competitive Environment (continued)

- AppOmni's achievement of Federal Risk and Authorization Management Program (FedRAMP®) Moderate Authorization to Operate (ATO) and Valence's close collaborations with Microsoft boost their credibility. CrowdStrike leverages its established Falcon platform customer base and incident response (IR)-led go-to-market strategy to accelerate adoption, reinforcing its leadership in the SSPM market.
- CrowdStrike, AppOmni, and Grip Security are the Frost Radar™ Innovation Index leaders. They offer comprehensive SSPM portfolios and demonstrate a commitment to technological innovations that align with customer needs and the latest market megatrends. What groups these vendors together on the Innovation Index is their incredibly robust R&D initiatives and their willingness to push the boundaries of SSPM to address the needs of customers. They are investing in advanced AI/machine learning (ML) and GenAI technologies in their offerings while offering seamless integrations. These vendors exemplify the industry's move toward unified, AI-enhanced, and operationally scalable platforms.
- The Innovation Index leaders share a common strength in delivering identity-centric SaaS security with deep visibility and contextual risk prioritization powered by AI and automation. Each brings unique differentiators to the table: CrowdStrike's advanced device-to-SaaS visibility and AI-powered assistants to manage emerging AI agent identities; AppOmni's deep application-level context, zero trust posture management (ZTPM), customizable policies and alerting features, and AI-assisted issue resolution, bolstered by partnerships such as Cisco's security service edge (SSE) suite, all while maintaining proactive security hygiene; and Grip Security's emphasis on multisource SaaS discovery with advanced ITDR.
- DoControl has a solid position on both Frost Radar™ indexes. The company stands out with low-code workflows that enable automated bulk remediation and multicontextual analysis, though it must broaden shadow SaaS visibility to cover shadow AI, enhance SecOps interoperability, and expand its global partner base beyond North America to strengthen its market share.

Frost Radar™ Competitive Environment (continued)

- Check Point, Spin.AI, Reco, SecureSky, Axonius, and CheckRed Security, may need to establish more strategic partnerships and aggressive SSPM-specific sales and marketing strategy to expand their geographic reach, maintain their innovation scalability, and sustain their growth pipeline for the next 3 years.
- Check Point and Spin.AI provide solid SSPM solutions with use case differentiators. Spin.AI differentiates itself through strong browser extension risk assessment, while Check Point's ability to cross-sell SSPM alongside its established security offerings, such as managed detection and response (MDR) and Infinity XDR, enhances its overall customer value proposition. Check Point's enhancement of its GenAI security capabilities and its increasing focus on proactive security highlight the alignment of its SSPM vision with broader market trends. To support continued growth, both vendors would benefit from deepening their industry-specific solutions and expanding their market presence in APAC and Latin America. Even though Check Point's SSPM innovation efforts and vision are in line with market direction, the pace of recent enhancements raises concerns about the company's long-term strategy for this product line. Spin.AI will need to strengthen its identity security capabilities with enhanced behavioral risk analysis. Both vendors are poised to improve their Frost Radar™ positions as they invest in additional SSPM innovations.
- Reco has scored competitively on the Innovation Index with DoControl because of its forward-thinking efforts in AI-driven dynamic SaaS security. Since its rebranding, Reco has differentiated itself from traditional SSPM providers, thanks to platform capabilities that align closely with emerging SSPM priorities. Despite holding a smaller share of the SSPM market, Reco is positioned alongside SecureSky, Axonius, and CheckRed Security on the Growth Index, with strong potential to accelerate revenue by expanding vertically and entering new regional markets.

Frost Radar™ Competitive Environment (continued)

- Compared to stand-alone SSPM vendors, SecureSky, Axonius, and CheckRed Security benefit from unified platform strategies and opportunities to upsell or cross-sell through their broader security portfolios: SecureSky's continuous threat exposure management (CTEM) platform, Axonius's asset inventory and attack surface management, and CheckRed Security's cloud-native application protection platform (CNAPP). As they continue to grow, there is potential to further boost advancements to their SSPM capabilities and adopt more SSPM-specific go-to-market strategies that highlight their value in the space, positioning them for greater differentiation and customer impact.
- Improving customization, expanding market differentiation, localizing offerings, and broadening geographic reach will be essential to strengthen SSPM vendors' positioning in the rapidly evolving SSPM landscape.

Frost Radar™: Companies to Action



AppOmni

INNOVATION

- AppOmni's SSPM platform delivers comprehensive SSPM by providing real-time visibility and risk assessment across SaaS applications. The solution integrates deeply with critical SaaS applications to continuously monitor configurations, user privileges, identities, permissions, regulatory requirements, and data exposure risks, helping organizations reduce false positives and proactively secure their SaaS environments at scale.
- The platform provides risk prioritization for organizations to focus on high-level risks and remediation guidance, coupled with customizable policy enforcement and reporting through a large number of out-of-the-box compliance frameworks. AppOmni distinguishes itself with dynamic integrations that enable unified management and compliance. It leverages contextual insights from advanced threat detection and intelligence services to support remediation. It also normalizes and sequences SaaS logs while integrating with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) to streamline SecOps workflows.
- In the last 2 years, AppOmni enhanced its SSPM capabilities by introducing ZTPM, an AI-powered SSPM assistant that streamlines issue resolution, and enhanced ITDR using Shared Signals Framework (SSF) for automated actions. Its recent integration with Cisco's SSE technology suite has expanded its zero-trust security to the endpoint, in line with the company's end-to-end SaaS security strategy.
- AppOmni's SSPM roadmap emphasizes further expansion of its next-generation SaaS discovery with dynamic risk classification models to map the entire SaaS estate, including AI agents. It also focuses on AI-powered security posture management, broader coverage across network and connectivity controls through a centralized firewall control plane, and a standardized ingress policy management, in addition to more seamless integrations with workflows and AI-native offerings.

AppOmni (continued)

GROWTH

- AppOmni is one of the Growth Index leaders on the Frost Radar™, thanks to its strong market presence and its consistent YoY growth performance in the last two years. Frost & Sullivan estimates that AppOmni registered YoY revenue growth of 41.9% in 2025, with North America contributing the most, followed by EMEA and APAC.
- Being a partner-first company, AppOmni partners with top-tier consulting firms such as Accenture, PwC, and KPMG, along with MSPs, MSSPs, and technology and reseller partners. This allows the vendor to expand its reach through channel partners and meet diverse customer needs across different regions and industries, particularly in banking, financial services, and insurance (BFSI) and healthcare and medical sectors.
- In July 2025, the company achieved the FedRAMP® Moderate ATO, besides being the first SaaS security platform to achieve the prestigious FedRAMP In-Process designation. Achieving FedRAMP Authorization signals AppOmni's commitment in meeting the stringent security standards, making it a trusted option for government and highly regulated enterprises.
- The company's partnership with Cisco in November 2024 enables AppOmni to be listed in the Cisco Global Price List with access to all Cisco sellers (with quota retirement), channel partners, and distributors, extending its market engagement through its now more extensive partner ecosystem.
- Its ability to seamlessly integrate with enterprise workflows and existing security tools, such as SIEM, SOAR, information technology service management (ITSM), identity and access management (IAM), and BI systems, is ideal for customers that are not willing to rip and replace their existing security solutions.

AppOmni (continued)

FROST PERSPECTIVE

- AppOmni is a Frost Radar™ leader. Through its recent enhancements and roadmap, the company demonstrates a clear innovation strategy in strengthening its SSPM portfolio. AppOmni's SSPM capabilities, which include the extension of zero-trust principles to SaaS applications, shadow IT discovery, ITDR, ML-based SaaS security analysis, AI-powered SSPM assistant, and agentic AI architecture for SaaS security, are in line with the SSPM market trends.
- AppOmni's strength lies in its in-depth posture checks, deep application-level context, and its ability to prioritize risks based on business impact, which empowers security teams to efficiently manage SaaS security posture. Its automated, customizable policies and alerting features reduce manual effort while delivering flexibility and maintaining proactive security hygiene. Its automated remediation guidance capabilities cater to security teams seeking comprehensive SaaS governance and emerging teams needing guided workflows and simplified risk management.
- Backed by AppOmni's prolific threat research team, AppOmni Labs, the platform also integrates with advanced threat detection and real-time threat intelligence services to provide actionable insights on emerging security threats, accelerate remediation efforts, and create integrated SecOps. These features show the company's alignment with the market direction of a seamless interoperability with SecOps and runtime correlation.
- AppOmni's ongoing investment in AI capabilities beyond automation to develop AI security posture management, which includes AI-driven threat detection and response (AITDR), context-aware threat correlation, AI-driven remediation, and workflow orchestrated with SecOps including endpoint and device telemetries, is essential for the company to maintain its position as an innovation leader and increase its growth opportunities.

AppOmni (continued)

FROST PERSPECTIVE

- AppOmni's solution is largely designed for large enterprises. Nevertheless, the recent introduction of simpler pricing and packaging options is expected to help the company increase its market presence among price-sensitive commercial and mid-market organizations. Flexible payment terms or financial programs would enable the company to better support smaller accounts and expand its customer base.

Best Practices & Growth Opportunities



Best Practices

1

Chief information security officers should prioritize SSPM solutions that comprehensively secure identity, data, and the broader SaaS ecosystem by continuously monitoring human, non-human, and third-party identities; enforcing least-privilege controls; providing granular visibility into data access; and mapping SaaS application relationships to detect risks stemming from third-party integrations and reduce the overall attack surface.

2

To address the prevalent challenge of alert fatigue, effective SSPM platforms must leverage contextual analysis that correlates alerts with deep runtime insights and BI, prioritizing only genuine, high-risk threats. This approach empowers security teams to efficiently focus their efforts, reducing false positives and improving IR timelines in increasingly complex SaaS environments.

3

Selecting the right SSPM vendor requires careful alignment with organizational needs, including scalability, easy integration with existing security infrastructure, compliance capabilities, and proactive vendor support for customer success. Vendors should demonstrate a clear roadmap and innovation strategy that evolves with emerging risks and regulatory requirements to ensure that their solutions remain effective and relevant in the long term.

Growth Opportunities

1

SSPM vendors should expand their portfolios by integrating SaaS lifecycle management capabilities and identity- and behavior-based security models, either into SaaS security platform or broader security portfolios, such as SASE or XDR. Whether through native integration, strategic partnerships, or M&A, a holistic SSPM strategy should focus on orchestrating insights through a single pane of glass; interoperability; coverage across cloud, endpoint, and SaaS; and a seamless user experience.

2

For SSPM vendors and market participants, investment in advanced AI, including GenAI, agentic AI, and ML capabilities, is imperative. Solutions that combine smart risk prioritization with automated workflows will empower customers to operationalize SaaS security at scale, reduce manual burden, and accelerate IR. Vendors should prioritize seamless interoperability with SecOps tools, ensuring that their platforms integrate well into automated SecOps pipelines.

3

Investment in identity-centric SSPM innovation is vital to enforce least privilege, maintain compliance, and proactively defend against identity-driven breaches. Given the explosive growth of NHI, SSPM vendors should emphasize managing NHI alongside human and third-party identities in SaaS environments. They should also expand ITDR functionality to detect abnormal behaviors and credential misuse, enabling automated or guided response workflows that ensure prompt remediation.

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.

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

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

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



Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Frost Radar™ Empowers the CEO's Growth Team

STRATEGIC IMPERATIVE

- Growth is increasingly difficult to achieve.
- Competitive intensity is high.
- More collaboration, teamwork, and focus are needed.
- The growth environment is complex.

LEVERAGING THE FROST RADAR™

- The Growth Team has the tools needed to foster a collaborative environment among the entire management team to drive best practices.
- The Growth Team has a measurement platform to assess future growth potential.
- The Growth Team has the ability to support the CEO with a powerful Growth Pipeline™.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

Frost Radar™ Empowers Investors

STRATEGIC IMPERATIVE

- Deal flow is low and competition is high.
- Due diligence is hampered by industry complexity.
- Portfolio management is not effective.

LEVERAGING THE FROST RADAR™

- Investors can focus on future growth potential by creating a powerful pipeline of Companies to Action for high-potential investments.
- Investors can perform due diligence that improves accuracy and accelerates the deal process.
- Investors can realize the maximum internal rate of return and ensure long-term success for shareholders
- Investors can continually benchmark performance with best practices for optimal portfolio management.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

Frost Radar™ Empowers Customers

STRATEGIC IMPERATIVE

- Solutions are increasingly complex and have long-term implications.
- Vendor solutions can be confusing.
- Vendor volatility adds to the uncertainty.

LEVERAGING THE FROST RADAR™

- Customers have an analytical framework to benchmark potential vendors and identify partners that will provide powerful, long-term solutions.
- Customers can evaluate the most innovative solutions and understand how different solutions would meet their needs.
- Customers gain a long-term perspective on vendor partnerships.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar™ Benchmarking System**

Frost Radar™ Empowers the Board of Directors

STRATEGIC IMPERATIVE

- Growth is increasingly difficult; CEOs require guidance.
- The Growth Environment requires complex navigational skills.
- The customer value chain is changing.

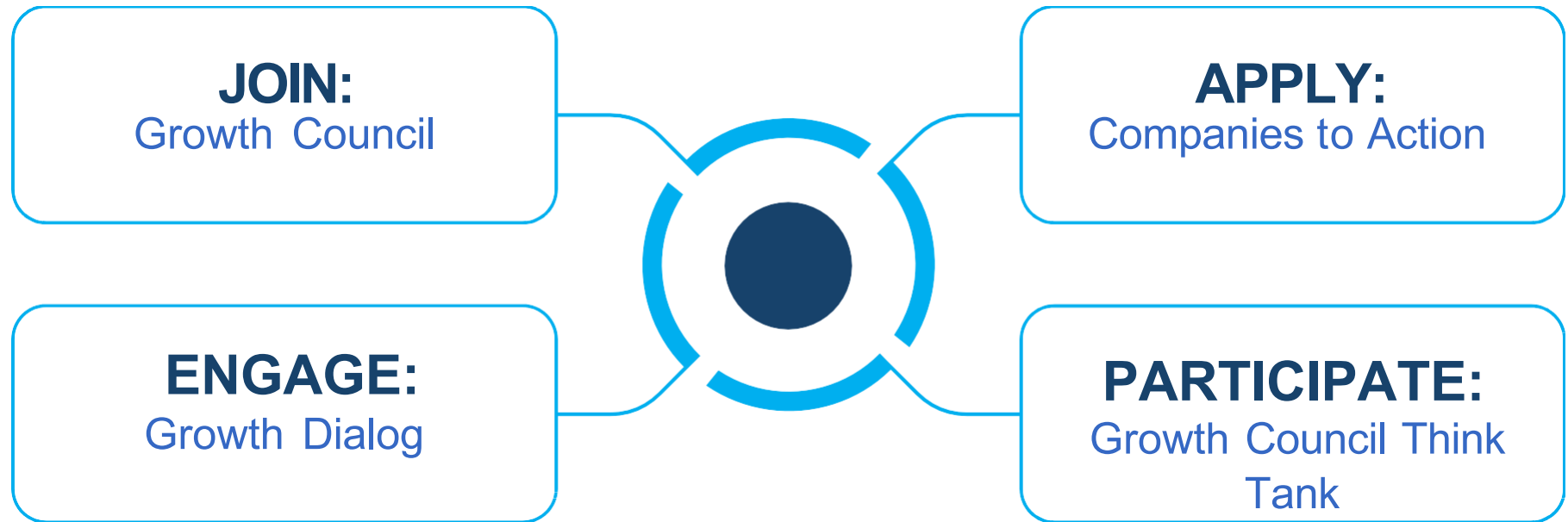
LEVERAGING THE FROST RADAR™

- The Board of Directors has a unique measurement system to ensure oversight of the company's long-term success.
- The Board of Directors has a discussion platform that centers on the driving issues, benchmarks, and best practices that will protect shareholder investment.
- The Board of Directors can ensure skillful mentoring, support, and governance of the CEO to maximize future growth potential.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Next Steps



Does your current system support rapid adaptation to emerging opportunities?

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

© 2025 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.