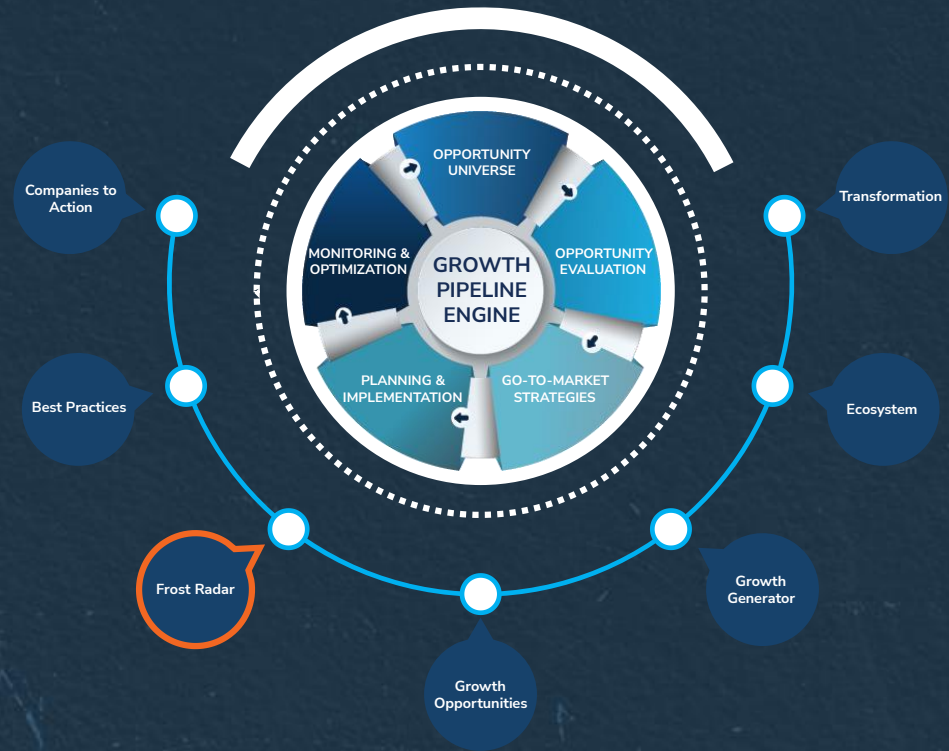


Frost Radar™: Zero Trust Browser Security, 2025

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

Authored by: Swetha Ramachandran Krishnamoorthi
Contributors: Jarad Carleton



PG4L-74
December 2025

Strategic Imperative and Growth Environment



List of Abbreviations

- **API:** Application Programming Interface
- **BDR:** Browser Detection and Response
- **BYOD:** Bring Your Own Device
- **CDR:** Content Disarm and Reconstruction
- **CISO:** Chief Information Security Officer
- **DDR:** Data Detection and Response
- **DLP:** Data Loss Prevention
- **DORA:** Digital Operational Resilience Act
- **EDR:** Endpoint Detection and Response
- **EMEA:** Europe, the Middle East, and Africa
- **FedRAMP:** Federal Risk and Authorization Management Program
- **GDPR:** General Data Protection Regulation
- **GenAI:** Generative AI
- **IdP:** Identity Provider
- **IDP:** Intrusion Detection and Prevention
- **MDM:** Mobile Device Management
- **MSSP:** Managed Security Service Provider
- **NIS2:** Network and Information Security Directive 2
- **PCI DSS:** Payment Card Industry Data Security Standard
- **PII:** Personally Identifiable Information
- **RBI:** Remote Browser Isolation
- **RDP:** Remote Desktop Protocol
- **SaaS:** Software-as-a-Service
- **SASE:** Secure Access Service Edge
- **SIEM:** Security Information and Event Management
- **SMB:** Small to Medium-Sized Business
- **SME:** Small and Medium-Sized Enterprise
- **SOAR:** Security, Orchestration, Automation, and Response
- **SSE:** Security Service Edge
- **SSH:** Secure Shell
- **SSO:** Single Sign-On
- **SSPM:** SaaS Security Posture Management
- **SWG:** Secure Web Gateway
- **UEBA:** User Entity and Behavior Analytics
- **VDI:** Virtual Desktop Infrastructure
- **VPN:** Virtual Private Network
- **XDR:** Extended Detection and Response
- **ZTBS:** Zero Trust Browser Security
- **ZTNA:** Zero Trust Network Access

Strategic Imperative

- The browser is rapidly becoming the hub of enterprise activity, evolving into the new endpoint for both productivity and threat risk. Enterprise browsers and browser extensions are eclipsing legacy tools, such as virtual private networks (VPNs), virtual desktop infrastructure (VDI), and proxy-based secure web gateways (SWGs), offering clientless and user-friendly secure application access. Enterprise customers demand lightweight, clientless, and browser-native security solutions that are easy to deploy and manage and offer high performance.
- GenAI integration in workflows is a major driver of innovation and a source of substantial compliance and security risk. There is strong demand for AI usage visibility, context-aware data loss prevention (DLP), and governance features integrated at the browser layer. The rise of agentic (AI-first) browsers requires new security guardrails, such as prompt filtering, AI response inspection, and model compliance hooks.
- Vendors must rapidly innovate to provide context-aware DLP, AI usage visibility, and governance features directly in the browser, increasing pressure to deliver secure, scalable, and user-friendly solutions. Security vendors are embedding AI-driven threat detection and precision controls to counter highly evasive threats and AI-powered attacks.
- Evolving data privacy laws and regulatory complexity (e.g., GDPR, PCI DSS, and FedRAMP) are driving new architectures that differentiate between work and personal activity, enforce granular audit controls, and ensure local data custody. These developments increase the complexity and cost of product development and support.

Growth Environment

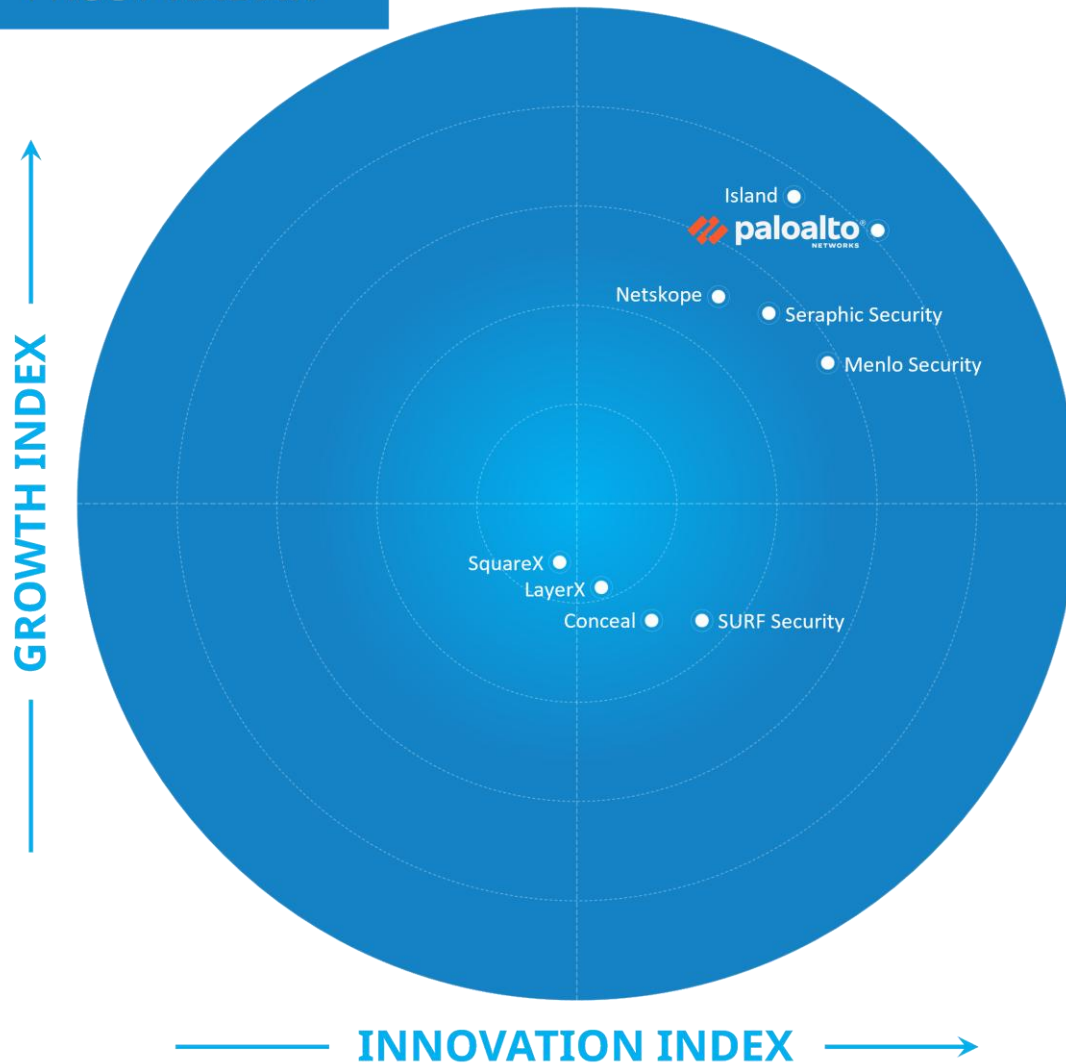
- The zero trust browser security (ZTBS) market is undergoing a profound transformation, driven by technological innovation, evolving threat landscapes, and changing enterprise needs. Over the next five years, the market is expected to shift from fragmented point solutions to integrated, browser-native platforms that serve as the central control plane for enterprise security and access.
- Frost & Sullivan expects double-digit or even triple-digit year-on-year growth rates in the emerging, start-up-dominated market. In 2025, the market generated aggregated revenue of \$622.0 million; a compound annual growth rate of 18.9% is anticipated from 2025 to 2030.
- The pace of mergers, acquisitions, and vendor consolidation is increasing as established players and start-ups seek to unify point solutions into broader enterprise platforms.
- There is a pronounced market movement toward identity-first, zero trust access models, moving access control and policy enforcement directly into the browser—especially as managed and unmanaged (BYOD) devices proliferate. Enterprise solutions are shifting away from heavy endpoint agents, focusing on lightweight, browser-native deployment models for rapid, seamless rollout.
- North America continues to dominate the ZTBS market, accounting for 73.2% of revenue in 2025. Asia-Pacific is emerging as a key region because of digital transformation initiatives and governments' data sovereignty requirements. EMEA, a compliance-driven region, is slow to ZTBS adoption and ranks third. Central and Latin America is slowly catching up with EMEA, especially in the enterprise browser and secure browser extension segments, because of the affordability and deployment simplicity of these solutions.
- Large and very large enterprises are the largest adopters of ZTBS solutions, while SMEs and medium-sized enterprises typically show high resistance to adoption due to cost considerations.

Frost Radar™: Zero Trust Browser Security



Frost Radar™: Zero Trust Browser Security

FROST RADAR™



Frost Radar™ Competitive Environment

- The ZTBS competitive landscape is rapidly evolving, shaped by shifting customer demands, strategic acquisitions, and new entrants. The market remains fragmented but is witnessing signs of consolidation and the emergence of clear market leaders that can provide comprehensive, browser-first security platforms.
- Larger vendors from adjacent markets are acquiring start-ups to fill capability gaps and deliver the breadth of features that customers demand. Vendors including Palo Alto Networks (Prisma) and Netskope are integrating or acquiring browser security solutions but often bundle them to protect core network revenue.
- Companies including Island, Palo Alto Networks, and Menlo Security are developing full browser solutions that offer enterprise-first security, but face adoption barriers due to user reluctance to abandon familiar browsers such as Chrome and Edge. At the same time, the market is witnessing the emergence of start-ups targeting narrow problems (e.g., DLP or GenAI risk in the browser), and adjacent browser security vendors. These entrants fall into two main categories:
 - Extension-based start-ups targeting SMBs and mid-market with lightweight solutions.
 - SASE/SSE vendors launching or acquiring browser security tools to complement their network-centric offerings.
- The technical complexity of building enterprise-grade browser extensions (e.g., anti-tampering and incognito mode support) and customer preference for consolidated platforms are among the challenges that new entrants face in this market.

Frost Radar™ Competitive Environment (continued)

- Island leads the ZTBS market in 2025 with a 25.7% share. The company provides an enterprise browser developed from the ground up to offer detailed security, policy management, and data protection during browsing. It stands out by incorporating DLP, activity monitoring, and seamless application access, appealing to organizations that want native endpoint security closely integrated with employee workflows.
- Menlo Security holds the second position with an 18.7% market share. It is recognized for its strong remote browser isolation platform that blocks web threats and prevents credential theft by keeping harmful content away from endpoints. Recently, the company shifted its focus from remote browser isolation to enterprise browsers, which has boosted revenue growth. Its scalable, cloud-native engine serves large enterprises prioritizing threat containment and zero trust browsing.
- Palo Alto Networks captured a 7.7% market share after entering the ZTBS market in 2024 through its acquisition of Talon and integration with the Prisma Access portfolio. The Prisma Browser leverages the vendor's security expertise to provide advanced browser protections within a broader zero trust framework, embedding threat detection, isolation, and policy enforcement into digital workflows.
- LayerX and Netskope each account for approximately 5% of the global ZTBS market. LayerX focuses on secure browser extensions that add runtime protection, visibility, and conditional access to standard browsers, while Netskope integrates enterprise browser features within its SASE portfolio, emphasizing inline threat protection, context-aware access controls, and advanced data security.
- Seraphic Security and SURF Security are emerging players in the enterprise browser space, demonstrating rapid and sustained growth through innovative technologies.

Frost Radar™ Competitive Environment (continued)

- Conceal and SquareX are emerging vendors in the secure browser extension space. While SquareX has pioneered the browser detection and response (BDR) capability, Conceal delivers agile browser isolation through its browser extension.
- Zscaler and Red Access were considered for inclusion on this Frost Radar™ but were omitted because of a lack of updated information relating to their solutions.

Frost Radar™: Companies to Action



Palo Alto Networks

INNOVATION

- Palo Alto Networks entered the enterprise browser market through the acquisition of Talon in 2024. The company has since integrated Talon's portfolio into its SASE portfolio and launched Prisma Browser.
- The company offers an expansive portfolio that spans a stand-alone Prisma Browser, a lightweight extension for managed endpoints, mobile clients, and an upcoming local application extender for desktop protocols (SSH, RDP, and SAP). Prisma Browser is also offered as a fully integrated solution in the Prisma Access platform, enabling customers to leverage a single policy framework across products.
- Prisma Browser operates as a stand-alone product that is tightly integrated with the larger Palo Alto Networks platform, enabling it to leverage best-in-class security services fed from 70,000 customers worldwide. This platform advantage translates into measurable threat detection superiority: it identifies and blocks up to 8.95 million new and unique attacks every day.
- Key differentiating capabilities include last-mile data leakage protection with browser-level visibility; AI-powered web attack detection and prevention with full page runtime visibility; detection and disabling of malicious extensions using behavioral monitoring; an advanced AI-powered DLP engine; in-browser anti-exploit protection; and a rich library of AI application and agents.
- The company's innovation is powered by significant R&D investment, which has enabled the Prisma Browser team to grow more than 8x in size since 2022.
- Palo Alto Networks proactively embraces megatrends, such as distributed work, last-mile attack sophistication, GenAI, and BYOD proliferation, by embedding controls directly in the browser. The company claims that 85% of new deployments in 2025 were driven by GenAI governance requirements and unmanaged device policies.

Palo Alto Networks (continued)

GROWTH

- Palo Alto Networks holds fourth place in the global ZTBS market with a 7.7% revenue share in 2025, according to Frost & Sullivan estimates.
- The company has demonstrated rapid growth, reaching 7 million secure browser licensed seats by the end of October 2025 (a 7x year-over-year increase).
- Palo Alto Networks has built a multitiered growth pipeline that begins with targeted use cases, such as securing contractor and unmanaged devices through full-browser deployments, and seamlessly expands into managed-device rollouts via lightweight browser extensions. The pipeline further extends into cross-sell motions in the broader Prisma SASE platform, leveraging shared policies to upsell DLP, zero trust access, and AI security modules.
- Palo Alto Networks offers 100% license portability across its Prisma Browser portfolio, which includes the full browser, the browser extension, a mobile solution, and firewall connectors. More than a third of 2024 bookings leveraged multiproduct bundles, demonstrating adoption across diverse cybersecurity segments. This breadth and depth across web, mobile, and desktop environments exemplify a portfolio leveraged for maximum cross-segment impact.
- The company employs a multichannel go-to-market model of direct sales and partnerships with value-added resellers, system integrators, and managed security service providers. This approach enables effective market coverage from the largest global enterprises to small businesses.

Palo Alto Networks (continued)

FROST PERSPECTIVE

- Palo Alto Networks, despite being one of the leaders in the SASE market, is still in its early growth stages with Prisma Browser. Sustaining efforts to raise awareness of the Prisma Browser product line will help the company capitalize on its initial growth momentum.
- Palo Alto Networks should continue to accelerate initiatives around BYOD proliferation, RBI replacement, GenAI usage controls, VDI reduction, and SWG replacement. The company has positioned itself advantageously in the VDI reduction space, offering 85% less total cost of ownership compared to shipping laptops or VDI, with 80% of VDI traffic being browser-based. The company should continue leveraging its native integration with Palo Alto Networks Cloud-Delivered Security Services and Enterprise DLP, which creates significant barriers for new entrants.
- The Prisma Browser product line is well positioned to utilize Palo Alto Networks' extensive partner network to drive rapid market penetration through system integrators and resellers. The company can develop partner certification programs and co-selling motions that position Prisma Browser as essential for modern zero trust implementations.
- Palo Alto Networks should focus on compliance-driven adoption across PCI DSS 4.0, FedRAMP, GDPR, DORA, and NIS2 frameworks. The company's ability to embed compliance into the browser itself, enforcing zero trust access, data controls, and logging all user actions, reduces reliance on bolt-on tools and accelerates certification readiness.

Best Practices & Growth Opportunities



Best Practices

1

Enterprises demand simplicity, seamless user experience, and rapid time to value from security solutions, rejecting complex, intrusive, or slow-to-deploy alternatives. Solutions that overlay onto existing workflows and browsers, minimizing user training and operational disruption, are more popular.

2

Despite strong investor interest, ZTBS market growth is restrained by limited awareness and end-user resistance. ZTBS vendors must improve brand awareness, highlight the critical need for their solutions through marketing campaigns, and improve user experience through seamless workflow integration.

3

Although ZTBS solutions are not mandated by regulation, compliance is a key factor driving growth in locations with data sovereignty requirements, such as EMEA and Asia-Pacific. Vendors considering international expansion must incorporate compliance-specific use cases to gain traction in these regions.

Growth Opportunities

1

Enterprises are demanding platforms that consolidate multiple security functions into a single, intuitive interface. The market will witness significant consolidation, with leading vendors acquiring smaller players to expand capabilities and address emerging use cases. Vendors that offer horizontal platforms with deep browser integration and AI-readiness will emerge as category leaders.

2

The proliferation of GenAI tools and agentic AI browsers will drive enterprise demand for robust, in-browser governance capabilities. Vendors that can deliver prompt inspection, model compliance, and real-time DLP enforcement directly in the browser will be in the best position to secure AI-driven workflows.

3

As hybrid work and BYOD adoption continue, organizations will prioritize browser-native security solutions that offer seamless protection across managed and unmanaged devices. Vendors that offer identity-aware policy enforcement without disrupting user experience will capture significant market share in this evolving landscape.

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.

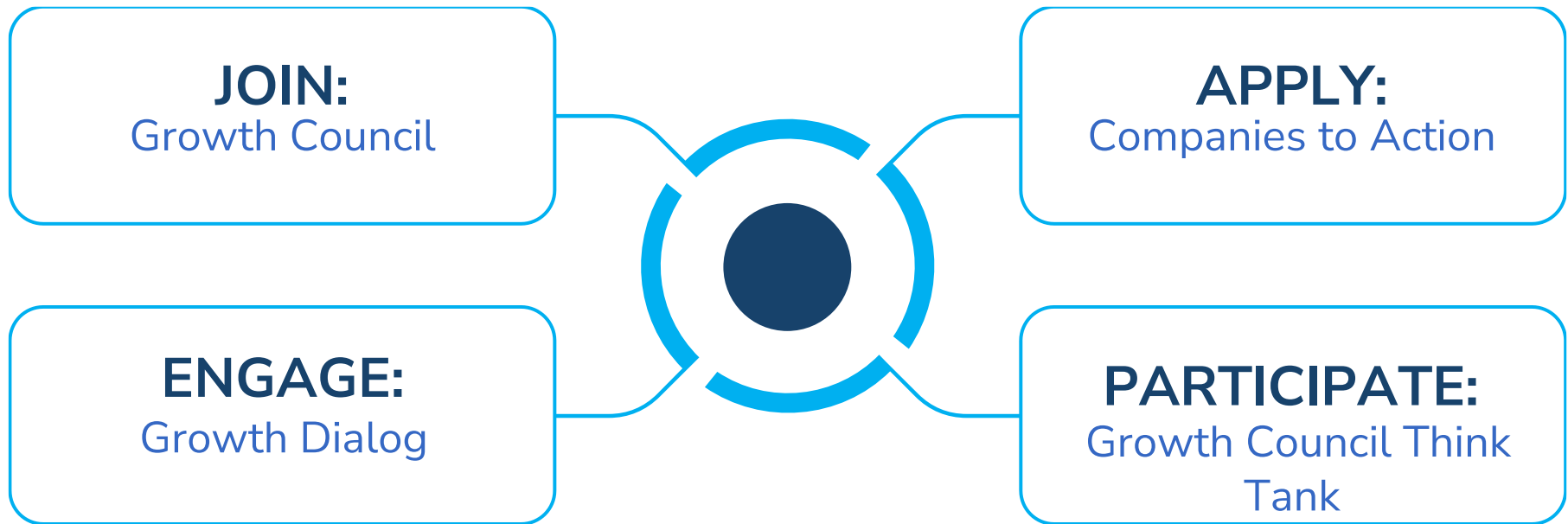
LEVERAGING THE FROST RADAR™

- 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.