

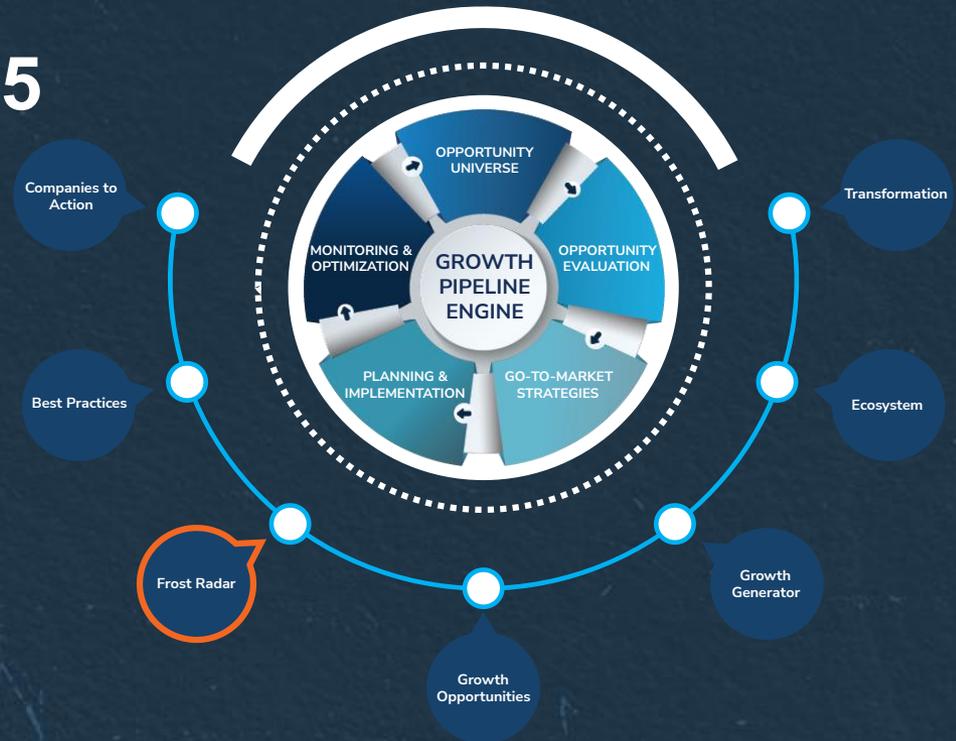
Frost Radar™: Secure Access Service Edge, 2025

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

Global Security Research Team at
Frost & Sullivan

Authored by: Claudio Stahnke

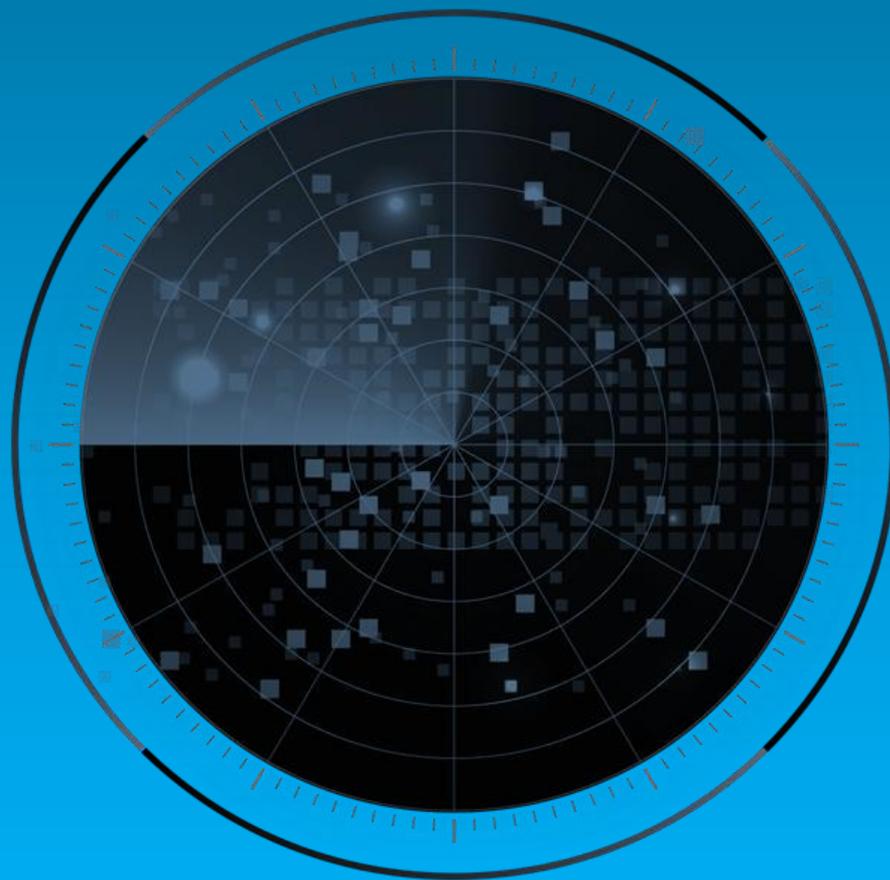
Contributor: Jarad Carleton



MH97-74

2025

Strategic Imperative and Growth Environment



Strategic Imperative

- The convergence of networking and security has become a business necessity. Organizations rapidly adopt cloud-first strategies, hybrid work models, and multicloud environments, making traditional perimeter-based security architectures obsolete. Secure access service edge (SASE) integrates networking and security into a unified, cloud-delivered framework, enabling secure, high-performance connectivity across distributed enterprises.
- The SASE industry is undergoing rapid transformation, driven by:
 - More than 80% of organizations now supporting remote or hybrid work models, creating new security and networking challenges.
 - Cloud migration and multicloud complexity, considering that 56% of enterprise applications are now cloud-native, requiring seamless, low-latency, identity-based security.
 - Legacy VPNs that are insufficient for modern cybersecurity threats, driving demand for zero trust network access (ZTNA) and dynamic identity-based security.
 - Regulatory compliance and data sovereignty, with stricter regulations influencing deployment models and forcing companies to balance security and compliance requirements.
 - Ransomware, AI-powered threats, and supply chain vulnerabilities that necessitate real-time threat prevention, automated security enforcement, and behavioral analytics.
- Successful SASE providers deliver fully converged networking and security through:
 - Cloud-native architecture, because multitenant, distributed SASE platforms with global points of presence (PoPs) ensure low-latency, secure access.

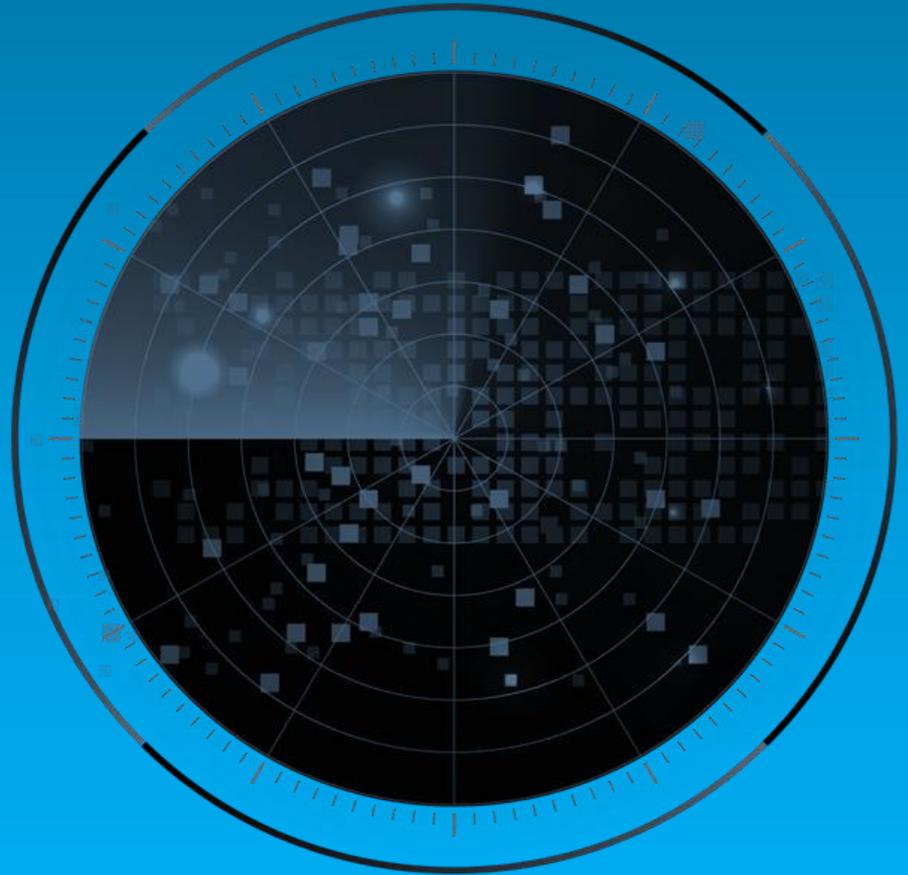
Strategic Imperative (continued)

- AI-driven security and automation, including predictive analytics, behavioral anomaly detection, and automated incident response that improve threat mitigation.
- Single-pass processing—optimized security enforcement that reduces latency and operational overhead.
- Zero trust enforcement—identity-based, least-privilege access across users, devices, and cloud applications.
- Localized SASE deployments to meet data sovereignty mandates.

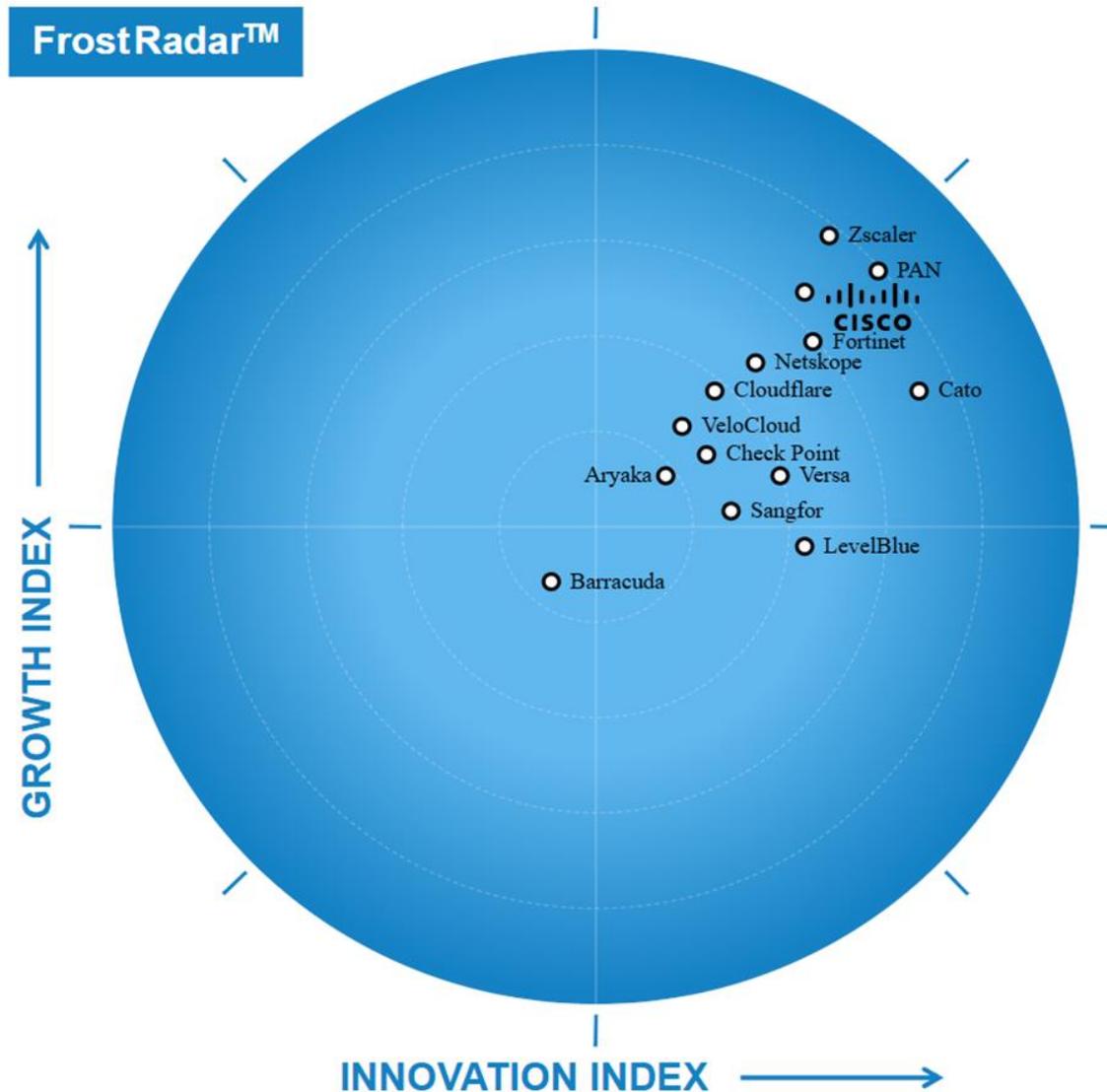
Growth Environment

- Frost & Sullivan expects global SASE market revenue to reach \$7.4 billion by 2029 (an increase from \$2.9 billion in 2024), driven by cloud migration, hybrid workforces, and regulatory mandates. The industry is in a high-growth phase, with a 2024–2029 compound annual growth rate exceeding 20%.
- North America is the leading market because of advanced cloud adoption, followed by the region encompassing Europe, the Middle East, and Africa (EMEA) and Asia-Pacific (APAC), where regulatory and data sovereignty concerns shape deployment models.
- Prominent market players are setting the standard by expanding AI-driven security automation to enhance real-time risk assessment; developing modular, cloud-agnostic solutions to support multicloud environments; strengthening compliance-driven architectures to support evolving regulatory frameworks; integrating secure web gateway (SWG), cloud access security broker (CASB), ZTNA, firewall as a service (FWaaS), and software-defined wide area networking (SD-WAN) under a single management console; and partnering with telcos and managed security service providers (MSSPs) to expand managed SASE offerings for small and medium-sized businesses (SMBs) and regulated industries.
- SASE adoption will accelerate as enterprises seek to reduce operational complexity, enhance security posture, and ensure compliance in a rapidly evolving digital landscape. Organizations must embrace converged, AI-enhanced SASE platforms to remain competitive in an increasingly borderless, cloud-first world.

Frost Radar™: Secure Access Service Edge



Frost Radar™: Secure Access Service Edge

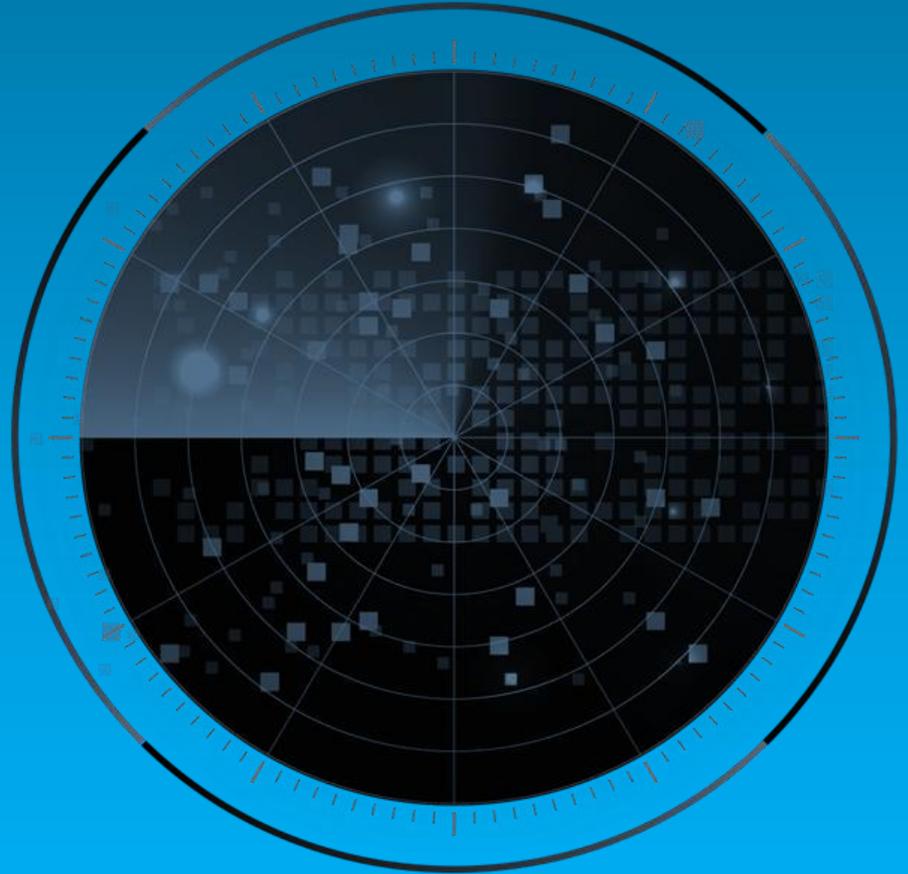


Note: All providers are pure-play SASE vendors except for LevelBlue, which offers managed services that integrate solutions from third-party vendors.

Frost Radar™ Competitive Environment

- The SASE market is highly fragmented, with a wide range of vendors approaching the convergence of networking and security from different angles. Network-first players enhance their security capabilities, security vendors add SD-WAN, cloud-native start-ups offer all-in-one platforms, and MSSPs repackage third-party technologies under managed services. As a result, the competitive landscape is diverse and dynamic, with no single blueprint for success.
- Frost & Sullivan selected 14 companies for deeper analysis based on their market relevance, innovation trajectory, global presence, and customer adoption trends. These vendors are either already shaping the enterprise SASE landscape or uniquely positioned to influence it soon. Many were included because of their convergence capabilities, strong enterprise adoption, and maturity of go-to-market strategies.
- What sets these companies apart from the broader pool of SASE providers is their demonstrated commitment to platform integration, cloud-native delivery, zero trust alignment, and operational simplicity—factors that enterprises increasingly prioritize in 2025.
- Notably, LevelBlue stands out as the only MSSP featured in this analysis. While some vendors may simultaneously partner and compete with MSSPs, LevelBlue's inclusion reflects the growing importance of service-centric delivery models in enterprise SASE adoption.
- Cisco along with others collectively hold more than 80% of the market share globally.
- Cisco combines world-class SD-WAN capabilities, extensive global reach, and AI-driven observability tools, such as ThousandEyes. Its Secure Access solution supports large-scale deployments with a flexible architecture and a robust zero trust framework, supported by a powerful partner ecosystem.

Frost Radar™: Companies to Action





INNOVATION

- Cisco stands out in the SASE market by providing a uniquely integrated platform that combines advanced networking, sophisticated cloud-based security, and comprehensive identity management into one cohesive solution. Cisco's SASE offering directly addresses the growing digital complexity faced by modern organizations, especially as they manage increasingly dispersed users, devices, and applications across heterogeneous environments.
- Cisco excels at delivering a flexible yet robust zero trust architecture (Zero Trust Access). Its unified Secure Access solution integrates Cisco SD-WAN, cloud security components, and continuous identity verification mechanisms. This approach stands apart because of its seamless coverage of on-premises and cloud-based environments, effectively streamlining the transition from traditional VPN security models to advanced ZTNA solutions. Cisco's Zero Trust Access ensures that secure access remains consistent, regardless of location or application type.
- Cisco significantly enhances network and application visibility through its integrated ThousandEyes technology. This allows for unparalleled, end-to-end performance analytics and proactive identification and mitigation of network issues via Predictive Path Recommendations. Cisco's AI-driven digital experience monitoring assures optimal end-user experiences and extends visibility and assurance to networks beyond direct ownership for comprehensive monitoring across the entire digital infrastructure.
- Cisco's cutting-edge AI Access technology is designed to detect and secure interactions with more than 1,200 GenAI applications. It provides essential safeguards against threats such as shadow AI, prompt injection attacks, and the potential distribution of toxic content. Cisco also utilizes advanced machine learning-based DLP controls, offering organizations thorough and proactive protection against data exfiltration and unauthorized information sharing.

Cisco (continued)

GROWTH

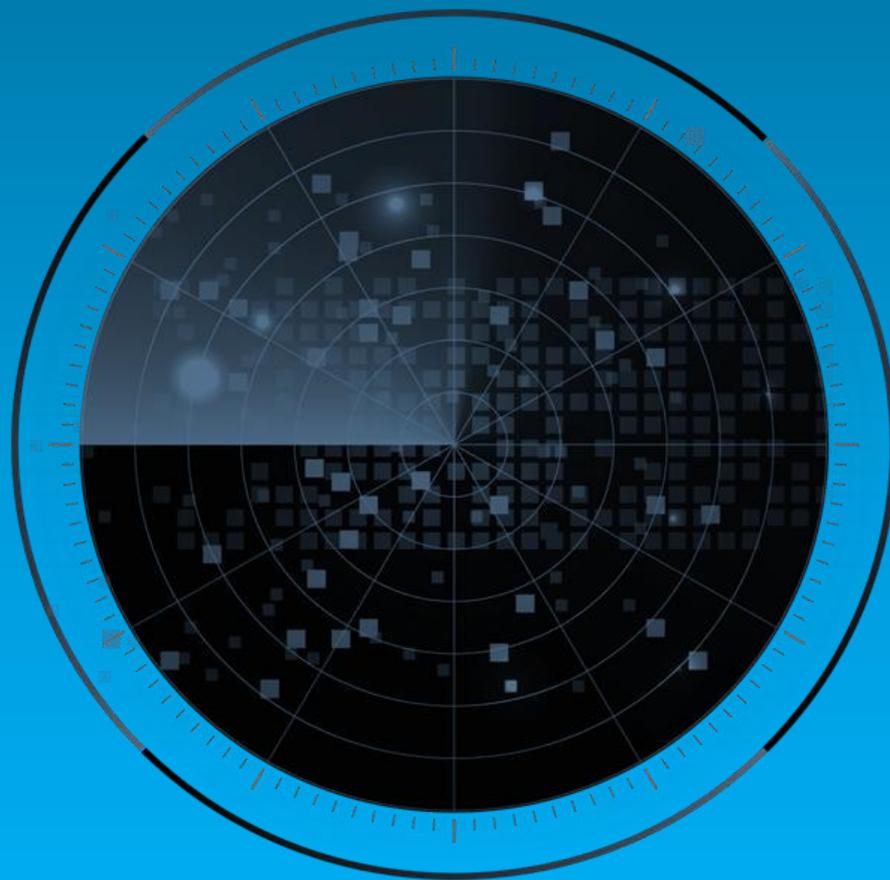
- Cisco maintains its strong position in the SASE market, bolstered by its strong foothold in SD-WAN and an expansive security portfolio.
- Cisco's dominance in the SD-WAN market enhances its visibility and customer adoption rates in the broader SASE framework, underscoring its credibility and stability as an industry leader.
- Cisco employs a hybrid POP strategy, blending proprietary data centers with AWS infrastructure to ensure global scalability, rapid deployment capabilities, and optimized infrastructure performance. This flexibility allows customers to select and customize infrastructure options based on latency and performance requirements.
- The company's extensive global partner network is a competitive asset, with approximately 90% of Cisco's security bookings facilitated through these partnerships. This ecosystem ensures wide-ranging market penetration, customer support, and comprehensive solutions tailored to diverse organizational needs.
- Cisco provides comprehensive coverage for traditional and modern applications, facilitating a smooth and controlled transition from VPN-based security models to zero trust frameworks. This capability ensures that Cisco can effectively support enterprises at different stages of digital maturity, simplifying the path toward robust security and optimized connectivity.

Cisco (continued)

FROST PERSPECTIVE

- Cisco's advanced SASE offering, characterized by AI-driven innovations, expansive visibility tools, and leadership in SD-WAN, places it in an enviable competitive position.
- Cisco's Predictive Path Recommendations already deliver reliable connectivity. By extending this technology to proactively anticipate and respond to emerging network threats and anomalous behaviors, Cisco can provide an additional layer of dynamic security, significantly enhancing customer defenses against evolving cyber threats.
- Cisco could further enhance its Cisco Security Cloud Control integration capabilities to manage and visualize third-party security tools effectively. This enhancement would solidify Cisco's role as the central security management platform in diverse, heterogeneous enterprise environments, maximizing the effectiveness of customers' security investments.

Best Practices & Growth Opportunities



Best Practices

1

Networking and security in a unified, cloud-native architecture is becoming the industry benchmark. Vendors that streamline management, policy enforcement, and analytics in a single platform are better positioned to deliver consistent performance, reduce operational overhead, and improve user experience.

2

Embedding AI-driven intelligence across security and performance layers is emerging as a key differentiator. Leaders are using AI not just for threat detection, but also for automated response, anomaly detection, digital experience monitoring, and real-time optimization, raising the standard for proactive, adaptive SASE environments.

3

Prioritizing platform simplicity, user-centric design, and managed service flexibility is essential. Companies that combine deep technical capabilities with intuitive interfaces, guided onboarding, and flexible delivery models (e.g., co-managed, service tiers) are succeeding in a fragmented market.

Growth Opportunities

1

AI-powered threat prevention and autonomous security operations are becoming essential for enterprises facing increasingly sophisticated cyber threats. Vendors that embed machine learning and behavioral analytics into their SASE platforms enable faster, more precise threat detection, reduce alert fatigue, and support self-healing, policy-driven security environments.

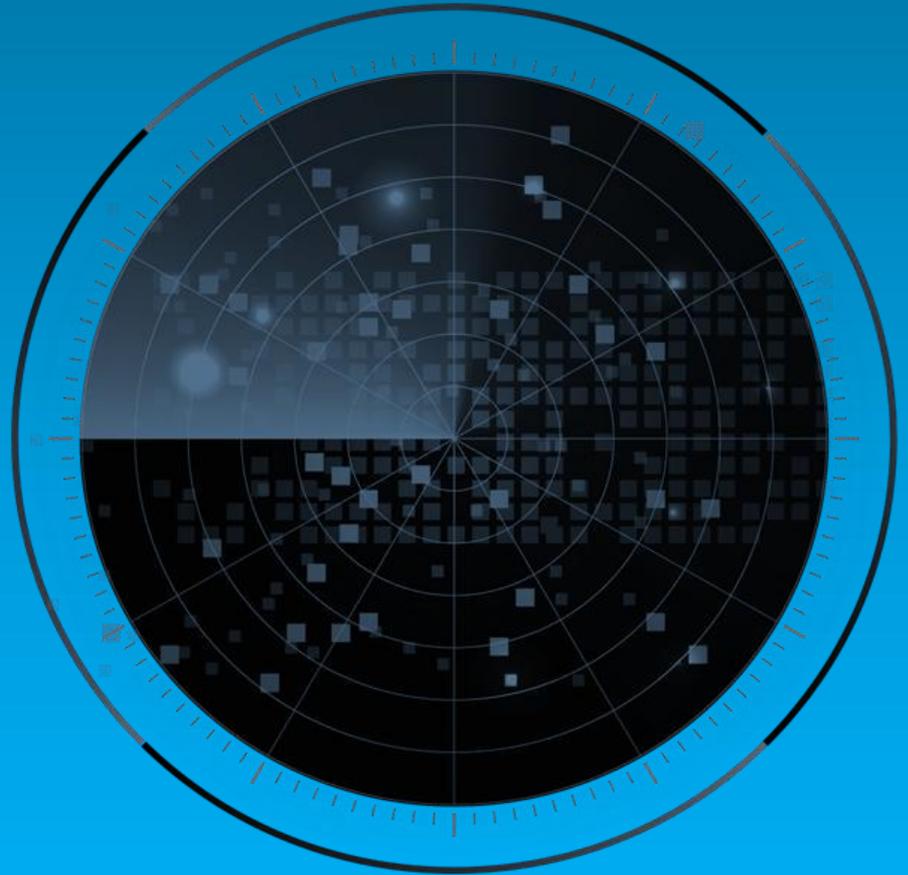
2

The popularity of managed and co-managed SASE services, often provided by MSSPs and telcos, is opening new avenues for adoption, particularly for organizations that lack in-house expertise. Vendors that offer flexible service delivery, support for industry-specific compliance, and integrated AI capabilities are well-positioned to satisfy the demand for scalable, ready-to-use solutions.

3

The expansion of edge computing, IoT, and private 5G drives demand for secure, low-latency SASE architectures capable of protecting data and devices across distributed environments. Vendors offering real-time threat prevention, granular zero trust access, and edge-native orchestration enable secure transformation in smart manufacturing, connected healthcare, and retail analytics.

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

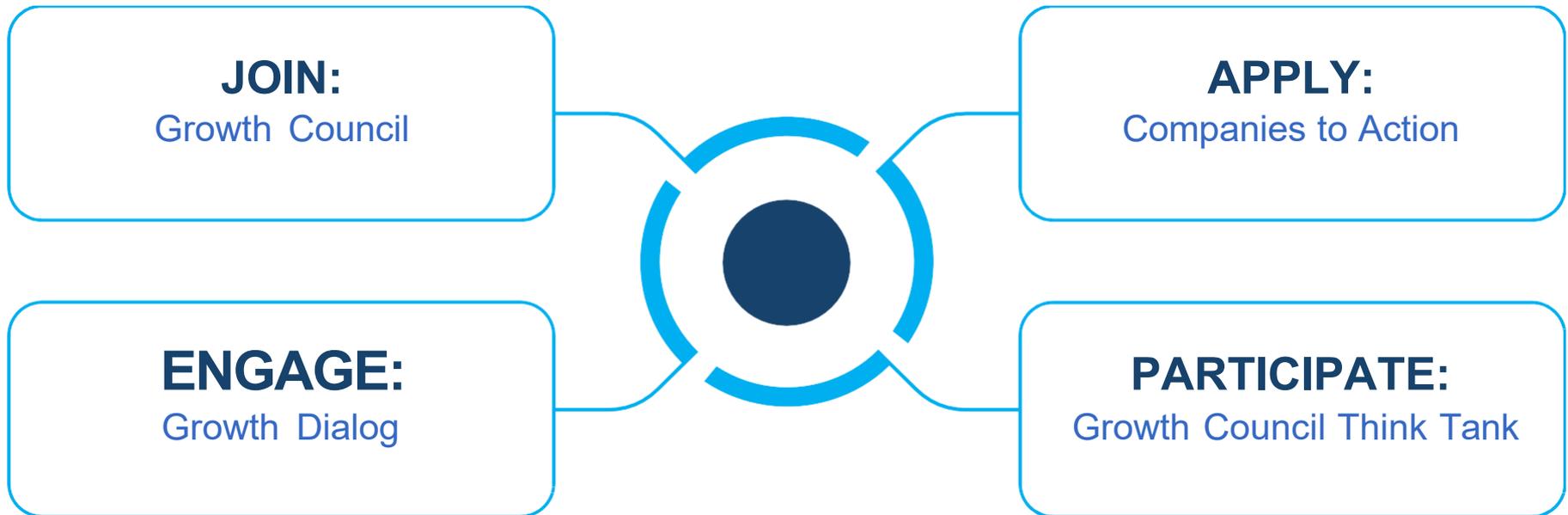
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of megatrends can be found [here](#).

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



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.