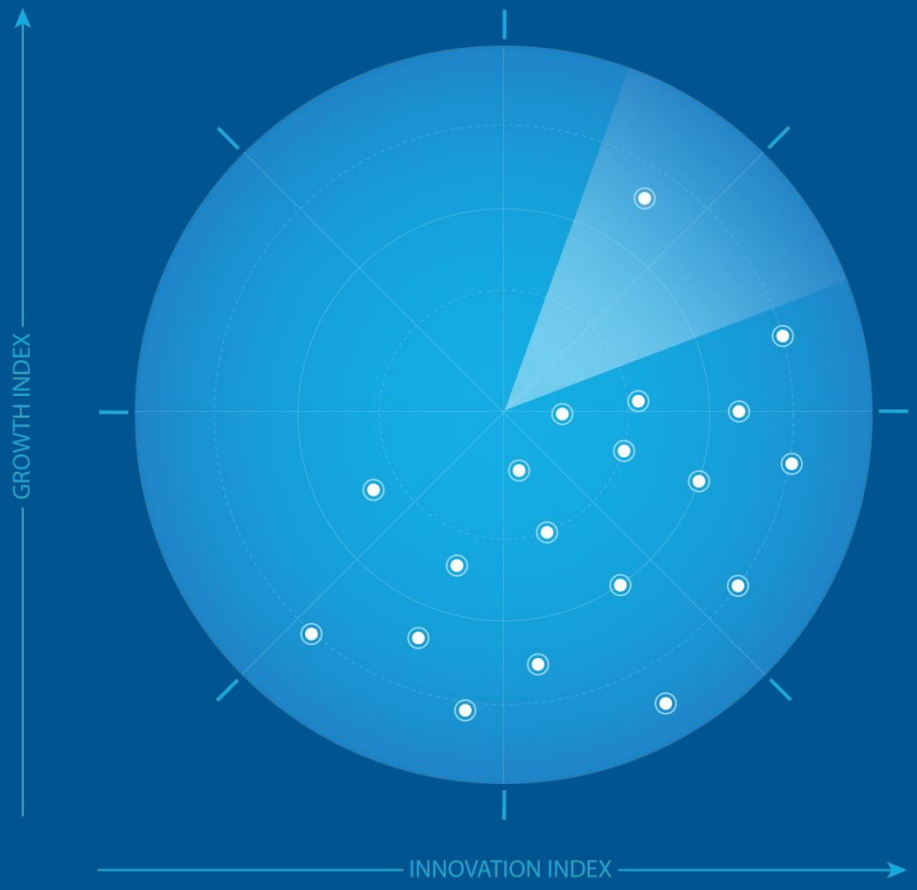
FROST & SULLIVAN

Frost Radar™: Email Security, 2024

Authored by: Sarah Pavlak

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



KA5F-74
July 2024

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

Factors Creating Pressure on Growth

- A major challenge for email security solution vendors is the continuous and rapid evolution of the threat landscape, as solutions must keep up with the increasingly sophisticated attacks to various vectors. Attackers target email but also breach organizational defenses via attack vectors such as web-based and other collaboration applications.
- Remote working has introduced new vulnerabilities for users and organizations. Threat actors have taken advantage with new, more sophisticated cyberattacks particularly targeting email.
- Many employees are using personal devices to conduct business. Employees accessing company email from a personal device continue to drive the need for cloud-based email security services.
- Organizations want advanced AI and ML security solutions to combat attacks. Many vendors are promoting API-based solutions as legacy secure email gateways (SEGs) cannot detect the advanced threats organizations are facing.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Attacks may combine web-based threats with specific email attack methods in multiple stages to try to evade security software solutions.
- AI has gained a tremendous foothold in various aspects of cybersecurity over the past year. Hackers are utilizing AI to launch sophisticated cyberattacks to quickly compromise email accounts to gain access to organizations' systems and exfiltrate data. AI adoption in email security solutions helps alleviate the ongoing challenge of staying a step ahead of the next attack vector.
- Security vendors increasingly leverage ML and AI, including generative AI, to strengthen organizations' security posture and reduce administrative overhead owing to a lack of security expertise to keep up with the fast-evolving security threats.

Source: Frost & Sullivan

Strategic Imperative

Factors Creating Pressure on Growth

- Organizations are outsourcing email security services because they do not have the security staff to do it themselves. This is especially true for small businesses. Many email security solution vendors are catering specifically to this customer group as a result.

Source: Frost & Sullivan

Growth Environment

- The global email security market is worth approximately $5,451.9 million, achieving a 22.9% YoY growth rate as of 2023. The market will grow to $9,577.8 million by 2027, indicating a double-digit compound annual growth rate (CAGR) from 2023 to 2027 of 15.1%.
- The email security market has seen strong double-digit growth for the last few years in response to increasingly severe and sophisticated email-borne cyberattacks.
- Organizations migrating to the cloud are transitioning from on-premises solutions to cloud-delivered solutions. Vendors within the space who are advancing and innovating their cloud-based email security solutions are experiencing continued revenue growth.
- Cloud migration has accelerated as organizations had to adapt to the security challenges of remote working and users had to work outside the traditional network security environment during the COVID-19 pandemic. This drove growth for email security in 2020 and 2021 and continued through 2023 as many organizations adopted remote working as their new norm.

Source: Frost & Sullivan

Growth Environment

- North America is the largest email security market. Because of its economy and security maturity, North America hosts most top email security vendors. North America's domestic requirements to comply with government and healthcare regulations and the many financial institutions contribute to business opportunities for email security vendors.

- EMEA is the second-largest market for email security. EU General Data Protection Regulation (GDPR) is a major driver for email security adoption. The increase in data protection and privacy regulations in this region drives customers to engage or upgrade email security to meet compliance requirements. Frost & Sullivan expects to see an increase in product demand because of concerns relating to cyberattacks, liabilities, and companies' reputations. Several email security vendors operate primarily in EMEA and are keen on the stringent compliance regulations within the region.

Source: Frost & Sullivan

Growth Environment

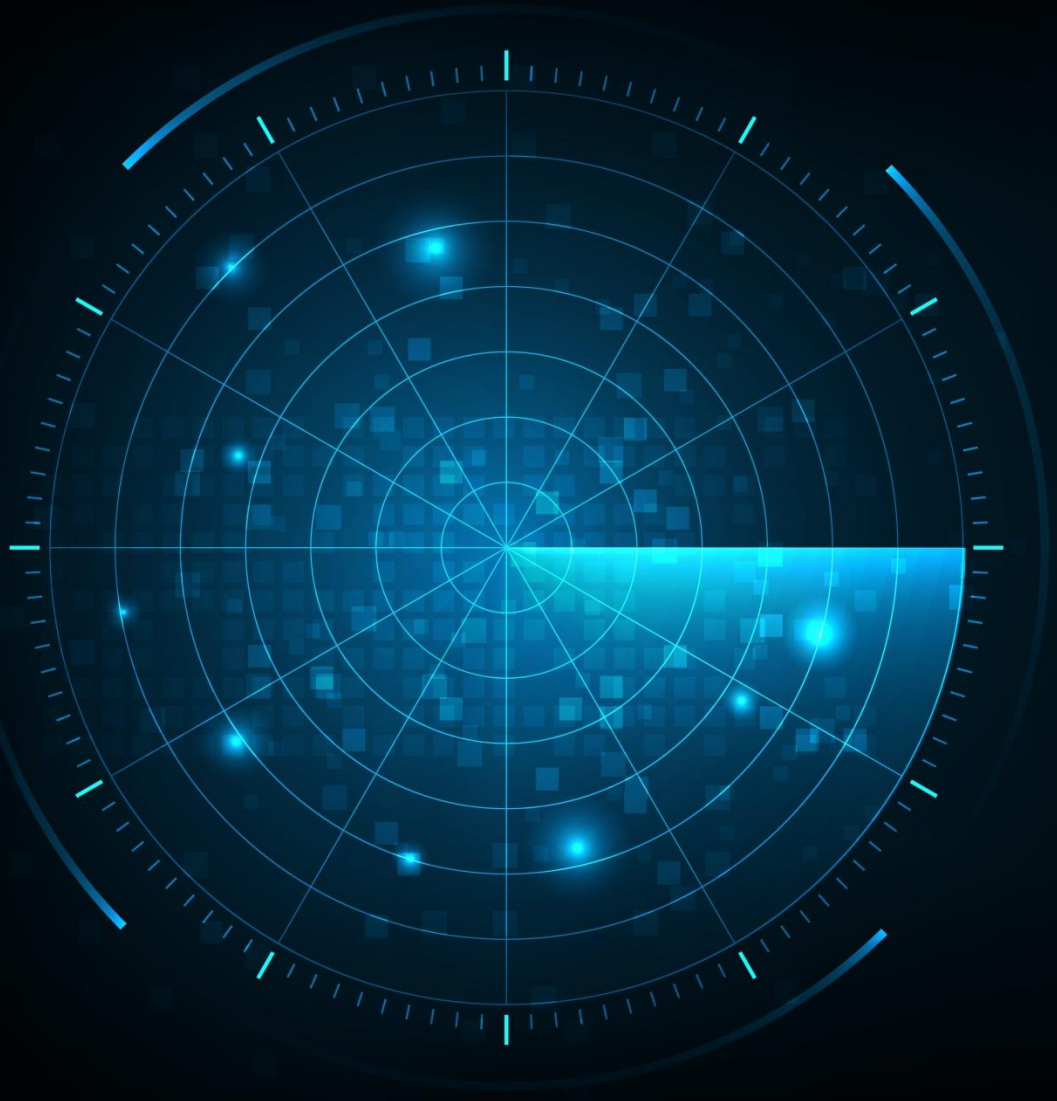
- APAC and LATAM are the smallest markets for email security but are seeing growth nonetheless. APAC has lagged North America and EMEA in cloud adoption, but this is changing despite supply chain disruptions in 2020 hampering vendors' ability to receive and ship hardware appliances. In contrast, greater demand for cloud-based security to safeguard the sudden increase in remote working buoyed email security market growth. LATAM has a promising market with modest activity. Many vendors are managing the region from their North American offices.

- The midsize business market accounts for the largest percentage of revenue for the email security sector. Midsize customers need security; however, they have limited security staff as compared to enterprise companies and depend mostly on managed service providers (MSPs) or managed security service providers (MSSPs) for support.

- The highest spending industries across the email security sector are banking and finance, healthcare, government, and education. These are the most widely targeted sectors by cyber criminals because of the types of sensitive data they deal with. But overall, adoption is high across every sector as email security is a critical need with some vendors addressing specific industries that require more advanced solutions.

Source: Frost & Sullivan

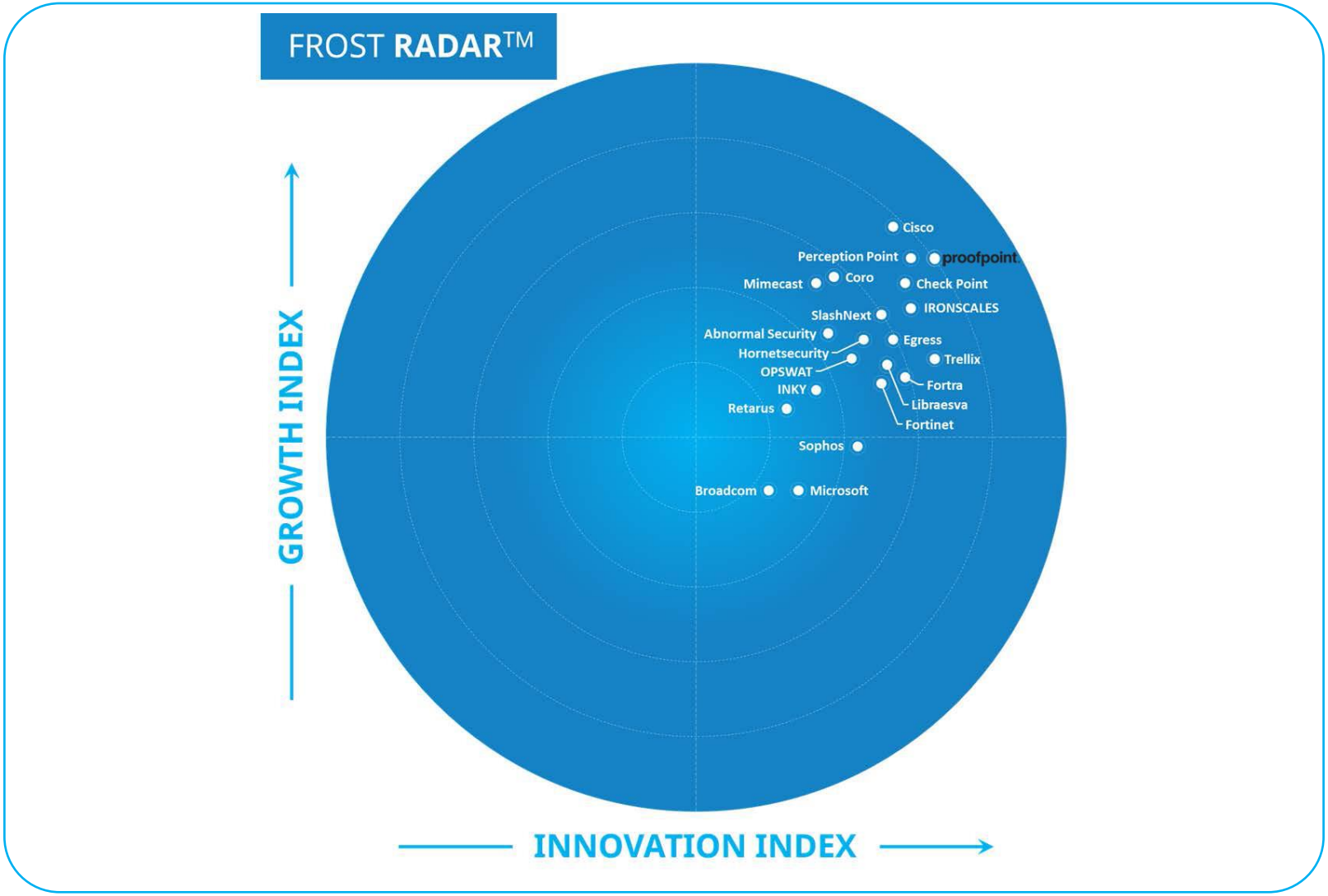
FROST & SULLIVAN



Frost Radar™

Email Security, 2024

Frost Radar™: Email Security, 2024



Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- The email security market is highly competitive and comprised of a plethora of vendors. There are a handful of large security companies, with the rest of the market comprised of email security start-ups.
- Email security start-up vendors have niche technology and frequently enter the market because they recognize a missing need and can provide a solution.
- Email security vendors must work diligently to continuously innovate. The market is quickly evolving due to the constantly changing threat landscape. The start-ups must keep pace with advanced technology.
- As organizations are increasingly aware that they must enhance their cybersecurity posture, vendors with innovative, advanced email security technologies will remain top of mind. As many email security vendors offer similar technologies because they are all trying to address the continuous threats facing email, competition is fierce to remain innovative.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Vendors are developing functions and features to counter advanced threats, adapt to the changing threat landscape, and help organizations transition from on-premises to cloud-based email solutions. Frost & Sullivan selected and plotted the top 21 out of more than 40 market participants in this Frost Radar™ analysis.
- In 2023, the top five vendors had a combined market share of 65.0%. This has been slowly declining since 2019, indicating inroads being made by other vendors.
- Proofpoint has been the market leader since 2015 and is an Innovation leader. It continues to invest heavily in research and development (R&D), and revenues from recent acquisitions and organic growth are resulting in leading market share gains. Proofpoint has a strong focus on innovation to remain a market leader with its technological advancements, in addition to its long-guiding people-centric approach. Proofpoint continues to solidify its market leader status with significant mergers and acquisitions (M&As) to enhance the security portfolio, striving for a holistic security approach that customers demand.

Source: Frost & Sullivan

FROST & SULLIVAN

Companies to Action:

Companies to Be Considered First for Investment, Partnerships, or Benchmarking

Company to Action: Proofpoint

Innovation

- Proofpoint continuously innovates and expands its integrated, multilayered threat protection solution. A key differentiator in its solution is the ability to continuously detect and stop threats throughout the email delivery flow (pre-delivery and post-delivery to click time). The detection technology stops known and emerging threats before entering the organization with behavioral AI analysis, sandboxing for links and attachments, QR code images, and message context, providing organizations with end-to-end people and business protection.

- With lateral movement being a key issue surrounding attacks, Proofpoint, in May 2024, announced new adaptive email capabilities integrating AI-based defense post-delivery to stop targeted threats. Protection for lateral internal phishing and advanced email fraud for at-risk employees are included in the new capabilities.

- Proofpoint further improved its detection efficacy with the following newly released innovations:

  - A new pre-delivery QR code detection technology that analyzes URL images and embedded URLs within QR codes and sandboxes them inline before message delivery. This is combined with post-delivery analysis and sandboxing of user-reported messages with QR codes.

  - The industry's first pre-delivery threat detection engine that uses semantic analysis to understand the meaning of words, phrases, and sentences to extract the underlying meaning and intent from text data. It is powered by a large language model engine to stop advanced email threats before they are delivered to users' inboxes in Microsoft 365 and Google Workspace.

Source: Frost & Sullivan

Company to Action: Proofpoint

Innovation

- Enhanced pre-delivery protection for URL threats, which allows organizations to hold suspicious messages with URLs for sandbox analysis, minimizing the risk of a user engaging with the malicious URL. Behavioral signals and threat intelligence determine whether a message should be held for a more thorough inspection. The sandbox technology analyzes URLs using static and dynamic analysis and analyst-assisted execution to maximize detection and intelligence extraction.

- Proofpoint's people-centric approach is universal but can be applied to the risks associated with specific people within an organization. Its global visibility and data correlation tools create a rich context for people's insights. Proofpoint has a unique process for identifying very attacked people (VAPs), giving security teams a better understanding of their organization's human attack surface.

- Proofpoint provides a thorough reporting suite for email security. Various reports, including Proofpoint Nexus People Risk Explorer, Business Email Compromise, and Executive Summary Reporting, can be PDF'd and exported for distribution to executive stakeholders to be informed of their organization's security posture. Its analytics dashboards include extensive filtering options so customers can customize their views and drill down into data for further insights.

Source: Frost & Sullivan

Company to Action: Proofpoint

Growth

- Proofpoint is the email security market leader. Its 24% market share is by far the highest of email security vendors.

- Proofpoint considers acquisitions a large part of its growth strategy to bring new data, developments, and innovations to its portfolio. Proofpoint's most recent addition was the acquisition of Tessian in December 2023, bringing Tessian's AI-powered behavioral and dynamic detection capabilities to complement Proofpoint's threat and data loss protection technology to offer organizations comprehensive defense against accidental and intentional data loss over email. This also boosts prevention effectiveness against inbound, human-targeted threats such as social engineering, malware, and credential phishing.

- In November 2023, Proofpoint appointed a new CEO. He quickly outlined strategic goals for the company aligning to specific primary growth engines. This includes providing a singular, targeted threat protection solution focusing on people, the most vulnerable aspect of the attack chain; expanding offerings by investing in international markets and underserved commercial segments, put into motion with a new global data center recently opened in Cork, Ireland; and

- Scaling information protection through shared visibility, using its people-centric approach to protect sensitive information across email, endpoints, cloud, and mobile devices.

Source: Frost & Sullivan

Company to Action: Proofpoint

Frost Perspective

- Proofpoint offers flexible deployment options and is available as a cloud service, dedicated appliance, or virtual appliance for its secure email gateway. Proofpoint also supports inline-plus-API and API-only deployment models. API-only deployments tightly integrate with Microsoft 365 and Google Workspace.

- Proofpoint provides a variety of APIs that enable organizations to feed data bidirectionally between its threat protection platform to endpoint protection, authentication, identity, and SIEM solutions such as CrowdStrike, Palo Alto, Splunk, CyberArk, SentinelOne, Microsoft Defender, Okta, and SailPoint. This demonstrates Proofpoint's ability to expand protection capabilities while considering that many customers likely use multiple security solutions and that integration is important.

- The vendors that Proofpoint has acquired over the past few years strengthen its security portfolio and reinforce that growth and innovation must be continuous to maintain market leader status and innovative competitiveness. The fact that Proofpoint has chosen vendors with a specialty shows the importance placed on enriching its portfolio.

Source: Frost & Sullivan

FROST & SULLIVAN

Key Takeaways

Key Takeaways

1

Email is the primary business communication method, making it a prime attack vector. Email-targeted attacks have skyrocketed over the past year, putting organizations at even greater breach risk and potential data loss.

2

Since the end of 2022, there has been a significant increase in malicious phishing emails. With limited visibility into an organization's digital footprint and the growing number of virtual interactions, the risk of successful phishing attacks and supply chain data breaches has increased significantly. AI exacerbates the situation and enables widespread, sophisticated phishing attacks, amplifying business risks.

3

AI is an emerging technology that allows attackers to deploy more types of attacks. Security vendors can also leverage the technology to combat the influx of attacks. AI plays a vital role in various aspects of cybersecurity, offering a multitude of impactful use cases. Among the most effective applications are threat detection & response, automated response, behavioral analysis, phishing detection, etc. The integration of AI into cybersecurity ecosystems is increasingly prevalent.

Source: Frost & Sullivan

Key Takeaways

4

Humans are the greatest cybersecurity threat to any organization. This holds especially true for email security because attackers rely on conning users into clicking on phishing links in emails to launch an attack. The prominence of targeted phishing, and ransomware, highlights the critical need for cybersecurity products and services that offer continuous network monitoring assisted by machine learning or AI to enhance automation and more effectively defend against cyber threats.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential

2 Major Indices, 10 Analytical Ingredients, 1 Platform

VERTICAL AXIS

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.

GROWTH INDEX ELEMENTS

- **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

HORIZONTAL AXIS

Innovation Index (II) is a measure of a company's ability to develop products/services/solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets, and are aligned to customers' changing needs.

INNOVATION INDEX ELEMENTS

- **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: MEGA TRENDS 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 Mega Trends can be found here.
- **II5: CUSTOMER ALIGNMENT**
  This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com