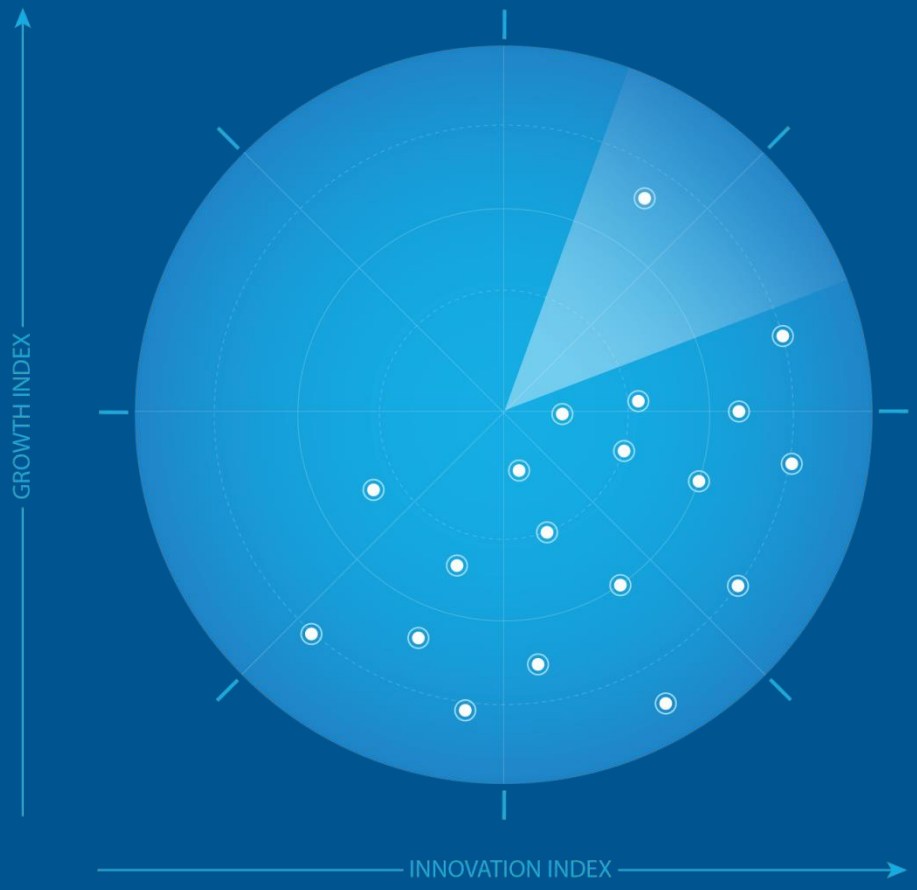
FROST & SULLIVAN

Frost Radar™: Email Security, 2022

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



Global Security Research Team at Frost & Sullivan

K80A-74
December 2022

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

- Email remains the center of modern cyberattacks. It is the primary communication method for business and is therefore a prime attack vector used as a gateway into complete takeover of an organization's networks.
- The threat landscape continues to change rapidly. Attackers target email but also breach organizational defenses via attack vectors such as web and other collaboration applications.
- The enterprise shift to remote work 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.
- With the evolution of remote and hybrid work environments, legacy secure email gateway security solutions are not equipped to manage the growing number of devices connected to cloud-based email services.
- Attacks may combine web-based threats with specific email attack methods in multiple stages to try to evade security software solutions.
- Integrating secure email solutions for devices and cloud-based environments will lead to growth over the next two to three years.

Source: Frost & Sullivan

Strategic Imperative (continued)

- Sophisticated cyberattacks are utilizing machine learning (ML) and artificial intelligence (AI) to quickly compromise cloud-based environments to gain access to organizations' systems and exfiltrate data.
- Ransomware attacks are increasing as hackers capitalize on multiple devices connected to business networks and remote working environments lacking proper security management methods.
- Utilizing application programming interfaces (APIs) with innovative ML algorithms allows for greater detection of sophisticated threats.
- Managing and integrating piecemeal solutions is expensive and complicated. The convergence of cloud security functions allows for a simplistic, highly effective solution to many cybersecurity concerns that organizations face.
- Mergers and acquisitions have taken place as vendors acquire technologies to enhance email security solutions. Those incorporated into a comprehensive security suite allow customers to invest in an entire digital platform protection solution.
- Holistic, integrated, and cloud-based security ecosystems will be the future of security portfolios. While some vendors already offer platform solutions, more will adopt this strategy in the next few years.

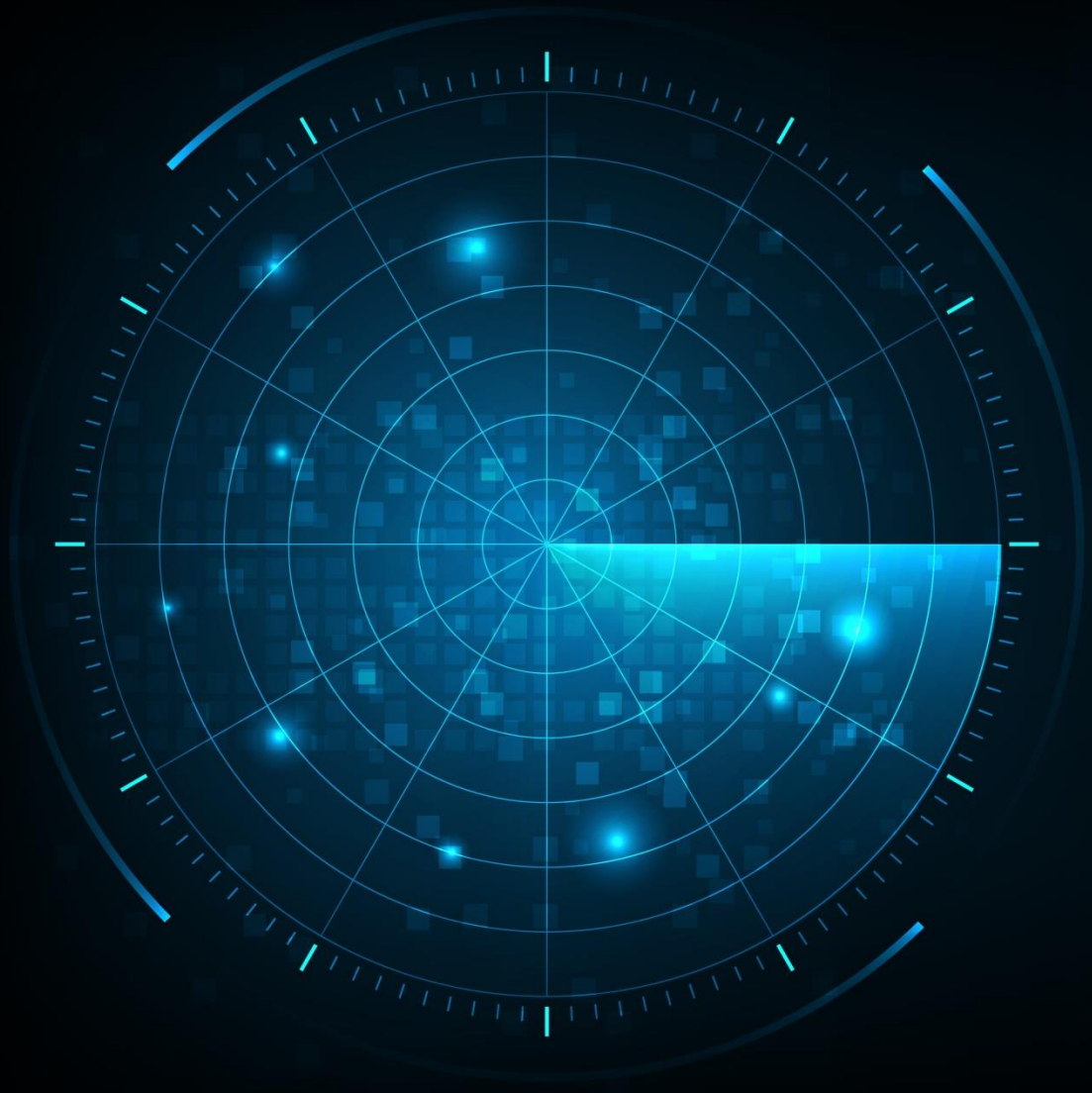
Source: Frost & Sullivan

Growth Environment

- The email security market has had strong double-digit growth for the last few years. This has been in response to the increasing severity and sophistication of cyberattacks.
- Organizations migrating to the cloud are transitioning from on-premises solutions to cloud-delivered solutions.
- The COVID-19 pandemic accelerated cloud migration as organizations had to quickly meet the security challenges of remote working. Users had to work remotely outside the traditional network security environment, which drove growth for email security in 2020 and 2021. This has continued throughout 2022 as many organizations have adapted to remote working as a new standard.
- The geopolitical effects of the Russo-Ukrainian War will compound the threat of cyberattacks as malware becomes weaponized for cyberwarfare. Organizations will want to strengthen their security solutions because of the increased uncertainty.

Source: Frost & Sullivan

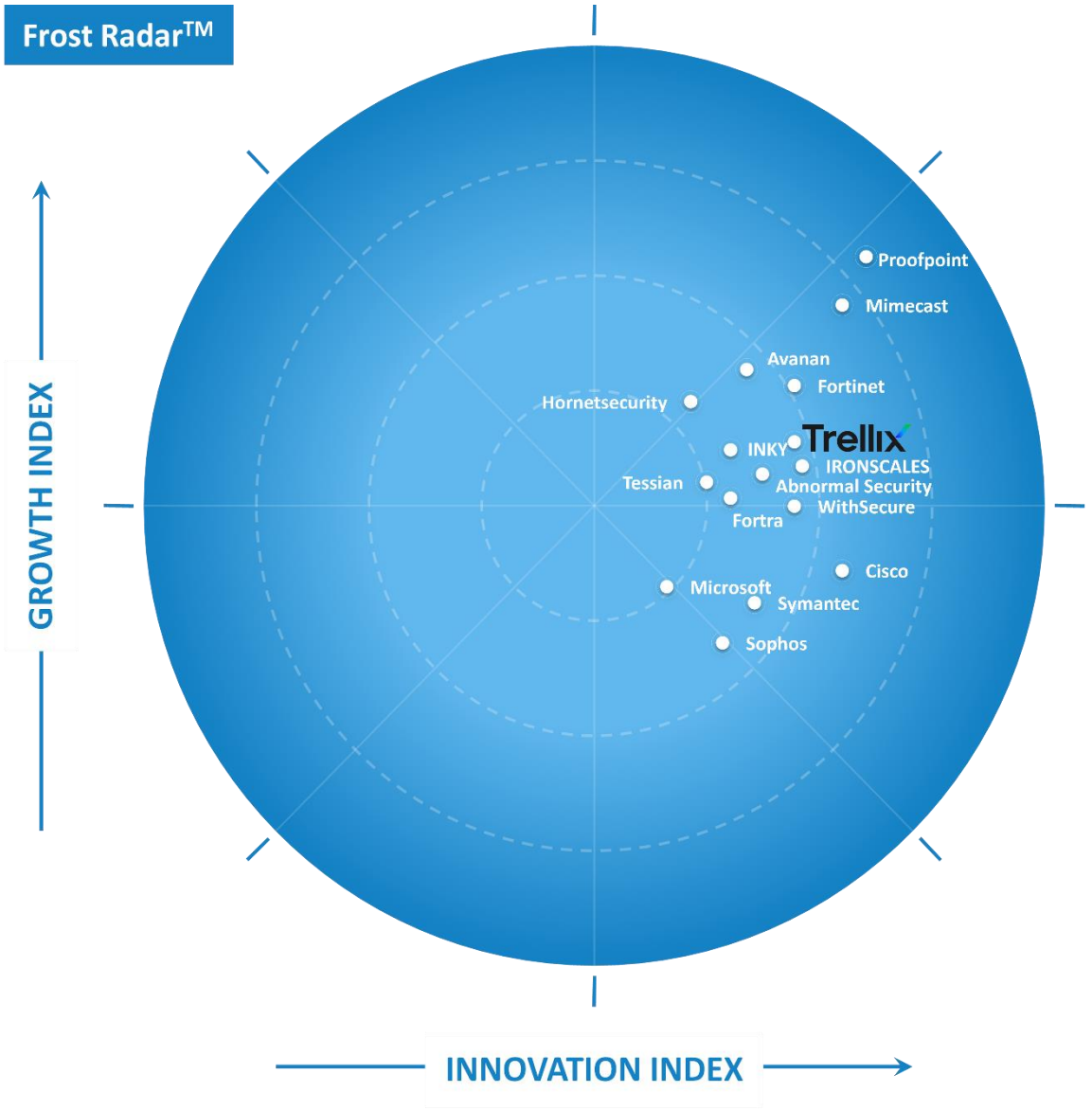
FROST & SULLIVAN



Frost Radar™

Email Security

Frost Radar™: Email Security



Source: Frost & Sullivan

Frost Radar™: Competitive Environment

- The email security market is saturated, mature, highly competitive, and crowded. Vendors are developing functions and features to counter new threats and adapt to the changing threat landscape, and must adapt protection technologies to help organizations transitioning from on-premises to cloud-based email solutions. Frost & Sullivan selected and plotted the top 16 out of more than 40 market participants in this Frost Radar™ analysis.
- In 2022, the top five vendors had a combined market share of 69.0%. This has been slowly declining since 2019, indicating inroads being made by other vendors.
- Trellix's main goal is integration throughout its line of products to provide a unified customer experience. This includes XDR. Email security is a key component of Trellix XDR and will drive growth strategies. With a concentration on R&D investments, Trellix is focused on growing its detection capabilities, operational efficiencies, and integrations to drive growth of its email security offerings.

Source: Frost & Sullivan

Trellix

INNOVATION

- Trellix's Multi-Vector Virtual Execution (MVX) engine detects, detonates, and reports on never-before-seen exploits and malware including zero-day, multi-flow, multi-stage, polymorphic, ransomware, and other evasive attacks. The ecosystem incorporates a suite of detection, protection, and investigation capabilities with email, network, data security, and endpoint, all feeding into Trellix Helix, which provides correlation, alerting, and automated response.
- Trellix provides a unique combination of adversary and victim intelligence. Victim intelligence provides information about how attackers gain access to target environments, as well as their intent and methods of operation. Adversarial intelligence provides in-depth knowledge of threat actor tactics, techniques, and procedures as well as an understanding of attacker motivations.

GROWTH

- Trellix's main goal is integration throughout its line of products to provide a unified customer experience. This includes XDR. Email security is a key component of Trellix XDR and will drive growth strategies.
- In line with market trends, Trellix aims to achieve additional growth by expanding current capabilities to provide internal email scanning, enhanced campaign detection, enhanced BEC and impersonation detection, native integration with Trellix DLP, encryption solutions, and anti-virus integrations.
- With a concentration on R&D investments, Trellix is focused on growing its detection capabilities, operational efficiencies, and integrations to drive growth of its email security offerings.

FROST PERSPECTIVE

- Trellix's threat intelligence capabilities being fed by email, endpoint, and network security allow the company to collect extensive information on adversaries. This is a differentiator that customers want to achieve security across many aspects of an organization and will drive growth for the company.
- Trellix's Email Security – Cloud with anti-virus and anti-spam meets FedRAMP security requirements for cloud services operated by government and public education entities. This will help drive Trellix's growth further into these market segments.
- Trellix puts heavy emphasis on customer support strategies. This includes customer success managers who can directly address customers' product-specific needs and relay them to the R&D team. This is unique to the market and shows Trellix's continued commitment to R&D and customer service.

Source: Frost & Sullivan

FROST & SULLIVAN

Strategic Insights

Strategic Insights

1

As the primary means of communication for business, email is a key gateway for cybercrime and the primary vector of phishing attacks. Cloud email security has become increasingly important as organizations continue to migrate to a cloud or hybrid email platform and need to address increasing cyberattack threats.

2

Experienced cybersecurity professionals coupled with advanced threat detection and prevention technology able to specify new rules and policies deliver high threat detection rates. Continual identification of new threats and implementation of optimizations create a multi-tiered email security solution defense strategy.

3

Organizations must ensure that existing security solutions are up to date and able to sustain in the constantly changing threat landscape. This includes boosting protection and prevention techniques for the increasing volume and successes of ransomware and phishing attacks.

Source: Frost & Sullivan

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

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, email permission@frost.com