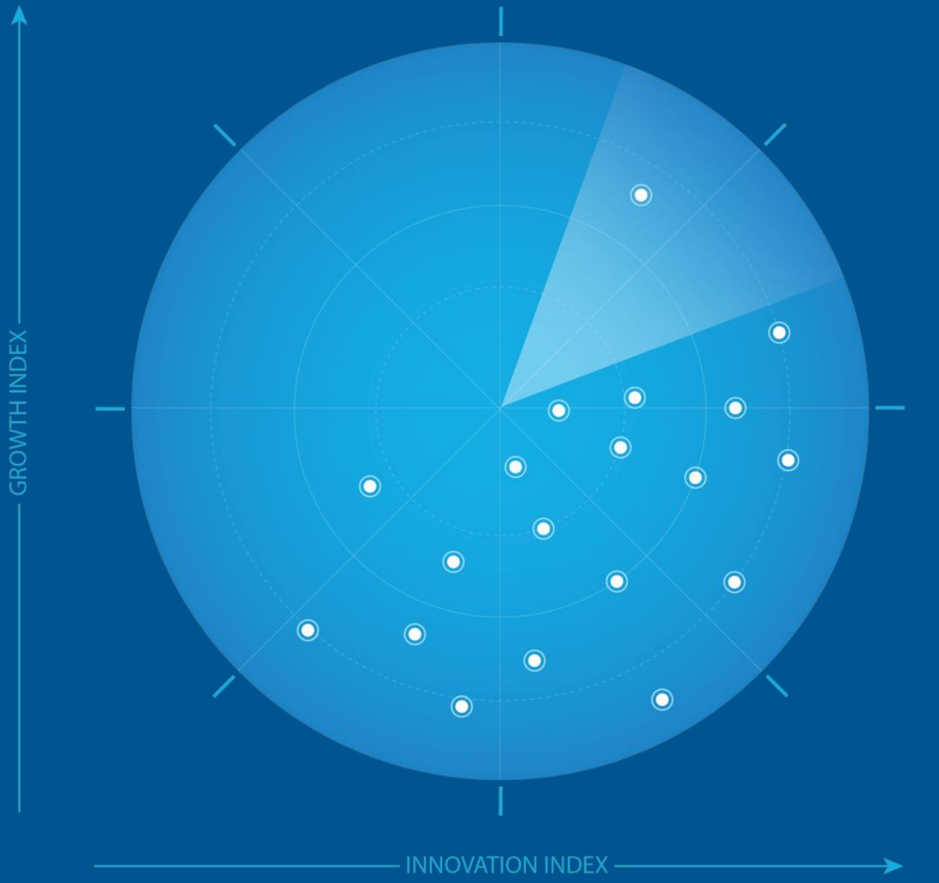
FROST & SULLIVAN

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

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.

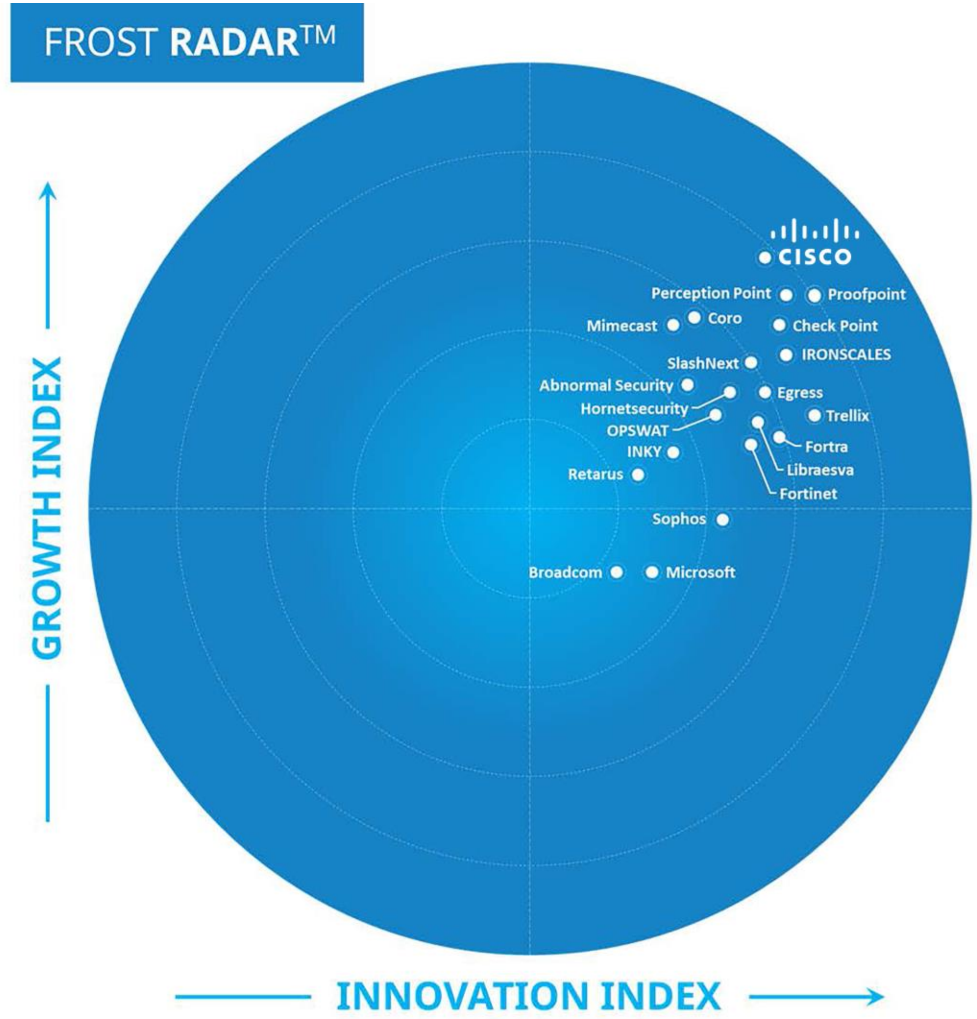
Source: Frost & Sullivan

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 Radar™
Competitive Environment

- Trellix is an Innovation leader. Trellix has a unique threat intelligence capability with its combination of both adversary and victim intelligence, as well as a growth strategy centered around integrating email security into its XDR capabilities. Email security is a key component of Trellix XDR and will drive growth strategies. Trellix's main goal is integration throughout its line of products to provide a unified customer experience. With a concentration on R&D investments, Trellix is focused on growing its detection capabilities, operational efficiencies, and integrations to drive the growth of its email security offerings.

- Cisco is the Growth leader on this Frost Radar. Cisco's Email Threat Defense solution has had remarkable growth with an astonishing 182.6% CAGR for 2020-2023. Cisco has made significant advancements in AI, global expansion efforts, and innovating its cloud email platform over the past three years. These aspects have all contributed significantly to its growth achievements.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Perception Point is a notable innovation and growth leader within the email security market. The company has introduced key innovative features over the past three years that set it apart from its competitors. Perception Point's email security offering encompasses next-generation detection with multiple layers of AI-powered protection to defend against many different types of threats. Perception Point also offers browser security – a keen extension to email security. Perception Point has shown very high growth rates over the past three years and continues to advance its growth strategy.

- Application Program Interface (API)-based email security is a significant trend within the email security industry. This is mainly because Secure Email Gateways (SEGs) are unable to detect social engineering attacks due to their design. Vendors including Check Point, Fortinet, and Mimecast all offer this capability but with varying factors to set themselves apart from their competitors.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Another key trend within the industry is that many vendors must keenly attune their solutions to compliance regulations. These vary greatly amongst regions and industries. With data protection being a key component of email security, organizations require security solutions that can meet these demands. Vendors that have a large presence in European regions, such as Hornetsecurity, Retarus, and Sophos, have strong data compliance capabilities within their email security offerings to cater to the needs of the organizations they serve. OPSWAT is also keen on customer regulation needs, but it is unique in that it caters to government and defense industries that require very specific data loss protection regulation capabilities.

- Human behavior analysis is a key component to effective email security as humans are the greatest cybersecurity threat. Vendors such as INKY, Egress, Coro, and Abnormal each take a unique approach to using AI to examine human behavior patterns and analyze anomalies to be proactive in detecting specific types of threats that target human behavior, such as phishing attacks.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- In February 2024, Google and Yahoo implemented mandatory Domain-based Message Authentication, Reporting, and Conformance (DMARC) email authentication requirements. DMARC prevents email spoofing. The requirement affects business-to-consumer (B2C) companies, specifically those sending bulk emails (more than 5,000 per day) to Gmail or Yahoo email addresses. Implementing DMARC is complicated and requires configuration and monitoring for system records, policy frameworks, and mail identifiers. Libraesva and Broadcom offer this solution to protect corporate brands through simplifying implementation and monitoring. This helps organizations identify and authenticate valid senders and block unauthorized users.

- Generative AI is a hot topic within cybersecurity, but few security vendors have effectively incorporated it into their solution offerings. Within the email security sector, the same holds. IRONSCALES and SlashNext are the only vendors featured in this research incorporating generative AI effectively into their solutions. These features have greatly contributed to each vendor's revenue growth rates, growth strategies, and innovative capabilities.

Source: Frost & Sullivan

Frost Radar™
Competitive Environment

- Fortra and Microsoft all have unique threat intelligence capabilities as well as extended detection and response (XDR) integration. These are important factors for email security because vendors that can ingest threat intelligence from a full ecosystem of security and technology capabilities can offer their customers a comprehensive view of the attack kill chain. Fortra recently launched its cybersecurity platform which offers a broad set of security products, including XDR, and combines its capabilities into a unified user experience with threat intelligence and analytic integration. Microsoft has incorporated a unified XDR-level investigation and response capability into its email security offering. Microsoft also has a large threat intelligence capability gathered from its wide breadth of security products and across its huge customer base.

Source: Frost & Sullivan

Companies to Action:

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

Company to Action: Cisco

Innovation

- Cisco's Email Threat Defense (ETD) offers multilayered protection through harnessing AI and ML capabilities to defend against threat factors most likely to affect organizations, including business email compromise, phishing, scams, and malicious and unwanted emails. Cisco's ML models target specific threat types, allowing for recognition and countering of sophisticated threat actor techniques.

- ETD creates user profiles in the organizational environment, allowing for relationship and pattern analysis. Potential threats can be identified by detecting anomalies in behaviors.

- Cisco has made significant investments in AI, both organically and through the acquisition of Armorblox in 2023 to further its use of generative and predictive AI. One advancement in this category is an ML concept known as Detectors. Through integrating individual detectors, a confidence level is generated for each email. These detectors function like signals, activating based on various aspects of the message such as tone, sentiment, and urgency to aid in understanding its intent. Cisco has more than 400 detectors working in tandem to safeguard customers from emerging threats.

Source: Frost & Sullivan

Company to Action: Cisco

Innovation

- Lateral email movement poses a significant challenge for gateway-based solutions and traditional threat detection engines, which often struggle to monitor internal emails. Cisco has dedicated substantial time and resources to address this issue effectively, utilizing innovative ML models and indexing all emails to evaluate them against these models. Consequently, ETD can trace the full trajectory of an email, pinpoint where it originated, and assess the potential impact.

- A differentiator is Cisco XDR, which integrates with numerous Cisco security products. The platform provides automation and orchestration that enhance response to high-severity threats on user accounts and endpoints. APIs allow customers to share data across platforms. All threat verdicts from ETD are part of Cisco XDR's incident attack chains.

Source: Frost & Sullivan

Company to Action: Cisco

Growth

- Cisco is the Growth Index leader on this Frost Radar. Its ETD solution is the second-fastest-growing email security solution profiled in this research, with an astonishing 182.6% revenue CAGR for 2020-2023.
- Cisco has two cloud email solutions: ETD and Cloud Email Security (CES). ETD is undergoing significant development to incorporate inline functionality to create a single platform for email that can be consumed based on customer needs. Existing customers will be able to migrate from CES to ETD to experience the new platform in mid-2025. The transition to a more streamlined platform will drive growth for Cisco for both new and existing customers.
- In FY2024 that began July 30, 2023, Cisco expanded its ETD locations to serving customers in Australia and India. The company plans to further expand into the United Arab Emirates and Canada by the end of 2025 and build out data privacy and sovereignty regulations as needed.
- ETD is an important component of the User Protection Suite and Breach Protection Suite that bring together the security tools organizations need to create comprehensive solutions whose parts work together to deliver better efficacy, better economics, and better experience.

Source: Frost & Sullivan

Company to Action: Cisco

Growth

- Cisco’s FedRAMP authorization is in progress. FedRAMP authorization is an important distinguished status, one that many cybersecurity companies seek to acquire. While Cisco is a leader in the federal government space already, this authorization will help it further expand its customer base. The coveted FedRAMP status demonstrates that Cisco is dedicated to securing data for its federal government clients by ensuring necessary controls and requirements are met for the agencies to use email security technology.

Source: Frost & Sullivan

Company to Action: Cisco

Frost Perspective

- Cisco can tailor its solutions to fit an organization's needs rather than forcing them to a single mode of deployment—a common practice for many new companies in the market today. Whether a customer requires a gateway in the cloud, a hybrid solution, or simply an add-on to an existing Office 365 service, Cisco can provide it.
- Cisco has a large customer base that has stayed with it for many years. Its threat intelligence capabilities are a large factor in this. ETD capitalizes on Cisco's Threat Intelligence organization, Talos. This enables merging signals from a diverse range of sources, including web proxies, endpoint, firewall, IDS/IPS, and network activity, giving customers the confidence that all necessary threat avenues are being addressed to keep their organization secure.
- Cisco has evaluated market trends and responded to its customers' needs by introducing email security integration with its XDR platform, furthering its holistic security resilience goal.
- Cisco must continue to invest in AI. Acquisitions of email security vendors that have significant generative AI capabilities would be a strategic growth move.

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