FROST & SULLIVAN

Hong Kong and Singapore

Email Security Market

Published January 2023

The role of email security practices is increasingly important to mitigate the risks from evolving phishing attacks in a world of shifting cybercrimes. In this research, Frost & Sullivan re-evaluates key players in this particular cybersecurity field in Hong Kong and Singapore.

Modern threats through emails include primarily ransomware, advanced malware, business email compromise (BEC), phishing, and spam. We would examine the evolution of these threats with respect to changing market conditions, policies, and business atmosphere as well as operational constraints. While preventative and reactive technologies have advanced considerably with many solution options, integration with locally adapted managed detection and response (MDR) services will also be examined, these services further increase the capture accuracy of adapted email threats so that companies only get legitimate messages, while lessening resource constraints in the respective constituencies.

This article seeks to analyze two significant, relatively established Asia-Pacific areas in greater depth, with the objective of identifying major regional trends and market-specific challenges in the field of email security.

Geographic Coverage	Hong Kong, Singapore
Study Period	2017-2021
Base Year	2022
Forecast Period	2023-2027
Monetary Unit	US Dollar

Definition of Email Security

- Email security is cybersecurity practices that protect users from receiving phishing, spam, malicious links, unsuitable images or content, and viruses. It can be referred to in various ways; for instance, some vendors refer to it as a secured email gateway etc.

- Email security solutions could be delivered as software, hardware, cloud-based services, and some integrated with manned operation support also known as Managed Detection and Response (MDR) services

Primary Functions of Email Security

- Preventing malware and targeted cyberattacks delivered via emails.

- Restricting access to inappropriate or ineffective content on the internet.

- Monitoring and tracking communications for compliance, regulatory issues, and corporate data theft.

Key Takeaway

- Advanced cyber threats necessitate intelligent email security services, especially managed detection and response services.

- Hong Kong and Singapore are experiencing an increase in socially engineered phishing emails; security suppliers with in-depth local knowledge are better able to tackle scams impersonating local brands.

- Due to the high value of user data and the sensitivity of the information, email security in the financial services, government, and manufacturing industries is receiving increased attention and investment.

- Shortage of local cybersecurity resources further compounds the challenge to strengthen necessary cyber defense measures.

Table of Content

1 The Importance of Email Security

Company perspective

Data Security Perspective

Security Features Required for Emails

As the world becomes more integrated and virtualized, email communication would naturally become the default channel of data exchange and will be relied upon to deliver an ever-increasing volume of commercial, business, and personal information. Cyber criminals will continue to ride on this evolution to carry out malevolent activities, exploiting vulnerabilities in the community in ever more creative and duplicitous ways. Email security practices protect the fringe of the organization, its people, against attacks initiated through the delivery of malicious emails. In an age where the hard perimeter has been crumbling fast and only to accelerate in the virtualized environment, hackers find attacking people is cheap and effective for their malicious purposes. Some organizations continue to believe that Internet threats only pose technological risks, ignoring the evolution of threats such as ransomware, phishing, and account abuse, which could significantly disrupt their business operations or result in significant monetary losses.

The importance of email security could be reviewed from the company and data security perspectives.

Company Perspective:

- According to Frost & Sullivan market research in 2022, more than 90% of cyberattacks used email to infiltrate businesses, and more than 95 % of organizations experienced breaches in Singapore and Hong Kong. Numerous phishing scams enter a business via emails with malware-hosting attachments and/or links to bogus sites that steal credentials, for example, for use in account takeover.

- With creative email frauds on the rise, fluidic understanding and approach to email security is required. Solutions based on static filtering techniques, malware sandboxing and reputational statistic policies fall short of the security measures necessary to keep up with the creativity and focus that hackers put in to phishing attack campaigns. The emergence of account compromise attempts is one such evolution that is affecting large number of organizations all over the world.

- Organizations experience challenges combating constantly evolving email threats while sustaining productivity and following regulatory standards. There is a persistent shortage of qualified cybersecurity professionals, and companies have limited financial resources.

- Cloud-based accounts are increasingly the focus of credential phishing attacks leading to account takeovers.

- Spear phishing is on the rise, with phishing campaigns that is customized to an organization and its management orientation, with different threats targeting different roles. Internal emails sent from compromised accounts can also be used to spread spam and malware, and more seriously to execute impactful financial frauds.

- Increasing staff security awareness and investing in employee email security education would reduce the likelihood of cybersecurity breaches and data breaches within a firm.

Data Security Perspective:

As systems and networks have become more secure, attackers no longer exploit their weaknesses; rather, they entice users to execute malware via email web/link/attachment.

Threats are becoming increasingly sophisticated:

- According to Frost & Sullivan, on a global scale, APTs, botnets, zero-day attacks, and other malware targeting commercial email systems have caused substantial financial harm, resulting in an average cost of $4.5 million USD per data breach in 2022.

- The rising popularity of social engineering threats such as spear phishing indicates a substantial shift away from unsolicited bulk email attacks and toward targeted email attacks. This is particularly evident in the Hong Kong and Singapore markets, where spear phishing emails, have resulted in huge corporate losses over the last couple of years.

- As part of impersonation attacks, such as Business Email Compromise (BEC)/Email Account Compromise (EAC), in which emails are sent to a specific recipient requesting immediate urgent actions. BEC / EAC have been seen to be focused, stealthy and patient to launder some of the most devastating monetary losses in the biggest enterprises over the last couple of years. These emails are usually simple text-based messages and appear as normal instructional communications, and are thus difficult for email security solutions to detect. To address this, refined security solutions are required.

- Attackers are discovering that intelligent automation is more effective than full automation, and worryingly staying ahead of enterprises. Traditional automated email defenses are being circumvented using human-augmented bots, multichannel phishing, and ransomware-as-a-service. For example, large transactional attacks involve email, cloud applications, and phone calls. Combining phishing emails with additional channels would increase the success rate of fraud and put personal data and corporate assets at risk.

- Account takeover poses a substantial danger for data breach within a company. According to cases submitted to the Privacy Commissioner of Personal Data (PCPD), for instance, Nikkei China had a compromised email account. This hacked account remained undetected within the IT security perimeter for five months. The hacker was able to forward approximately 16,860 emails, collecting the names, email addresses, company names, job titles, telephone numbers, and credit card information of 1,644 clients, 650 of whom are from Hong Kong and 994 from other countries.

Security Features Required for Emails:

-Security Operations Center (SOC): A centralized operation within an organization that monitors threats, manages vulnerabilities, and identifies incidents in order to maintain the security posture of the company.

-Managed Detection and Response (MDR): A cybersecurity solution that combines technology and human knowledge to detect, monitor, and respond to threats. The key benefit of MDR is that it promptly identifies and mitigates the impact of risks, requires no new enterprise staffing, and operates 24 hours a day, seven days a week. To fully utilize MDR and optimize the solution to handle increasingly sophisticated threats, however, service providers must commit substantial time and resources on adaption to keep pace with threat evolution.

-Data Loss Prevention (DLP): A technology that inspects and contextualizes data provided through messaging applications in order to prevent sensitive data leakage, misuse, or unwanted access. DLP software monitors and regulates endpoint activity to classify regulated sensitive and business-criticaldata flowing on corporate networks and is stored on-premises or in the cloud. When DLP detects violations of enterprise-defined or established policy, it responds with alarms, encryption, and other safeguards to prevent end users from disclosing data that could put the organization at danger, whether mistakenly or maliciously. As cybersecurity management has become more sophisticated, DLP approaches have developed in areas such as data inspection, discovery, leakage notification, enforcement, and so forth.

-Impersonation protection: It provides granular and customizable controls that enable businesses to identify, prevent, quarantine, and tag suspicious emails, thereby protecting users from targeted, socially engineered advanced email threats that are designed to circumvent traditional gateway security. In general, machine learning or AI-based engines will be used to discern distinct communication patterns and techniques to discover anomalies, then warn end-users and/or quarantine assaults in real-time.

-Advanced threat prevention (ATP) : A set of analysis techniques meant to protect against advanced threats employing both known and new attack vectors. In order to provide improved protection against spear phishing, ransomware, and other sophisticated assaults, malware samples are evaluated. The worldwide cloud malware database and the AM signature database would be utilized to identify emails containing known dangers. Sandboxing is a virtualized, separated, and secure network environment that executes unknown files for the purpose of analyzing their behavior, is frequently employed for unknown assaults. ATP complements conventional security measures designed to reject known entry techniques. Advanced threats are those that aim to acquire unobserved access to a network and remain there for months or even years, exfiltrating enormous quantities of data, conducting espionage, and/or causing substantial harm. Cybercriminals are continually refining their methods for acquiring network access. Typically well-funded, regularly targeted, and employing sophisticated malware designed to overcome standard security protections, these attacks are typically well-resourced. Countering advanced threats requires powerful analytic tools that can provide rapid visibility, analysis, context, and response into the contents and activities of hostile network traffic.

-Reputation filtering: This method of blocking unwanted email is typically based on a vendor's threat intelligence database. Each included hyperlink undergoes a reputation check to confirm the source's credibility. Websites and senders having a history of inappropriate behavior are prohibited automatically. Typically, reputation filtering avoids 90% of spam from entering a company's network, hence reducing the threat analytical burden.

-Graymail detection: Graymail includes marketing, social networking, and bulk messaging. By identifying and categorizing these emails, and so preventing their access into an organization, managers are able to take the proper action for each category. Typically, graymail would contain a link to unsubscribe, allowing recipients to inform the sender that they do not wish to receive similar emails in the future. However, because mimicking an unsubscribe mechanism is a typical phishing tactic, consumers should be aware of the risk associated with clicking on these links.

-Anti-virus: By providing a high-performance virus scanning solution, the majority of known viruses can be filtered and malicious content removed.

-Spam prevention: Spam is a complicated problem requiring a sophisticated solution. Advanced spam detection would consider a message's complete context, including its content, structure, sender, and destination of its call to action. By integrating these factors, the widest array of dangers might be effectively thwarted.

-Protection against phishing (Anti-Phishing): Traditional email security filtering engines utilize a global intelligence malware database to filter out dangerous links/attachments/emails.

-Orchestration and automation: To reduce threat response time by enhancing compatibility with other security solutions

-AI-based anomaly hunting: The ability for an email security solution to identify potential malevolent emails based on learning from good and bad emails. With the increased adaption of artificial intelligence, it is possible to learn the patterns of the email subject, content, URL, etc., and then to spot the smallest but potentially the most impactful attacks.

-Local Intelligence: Brands well-known to a locality (e.g. Hong Kong & Singapore) could be identified in the email solution and profiled, including its trusted domains or even marketing email sources for better refinement of protection

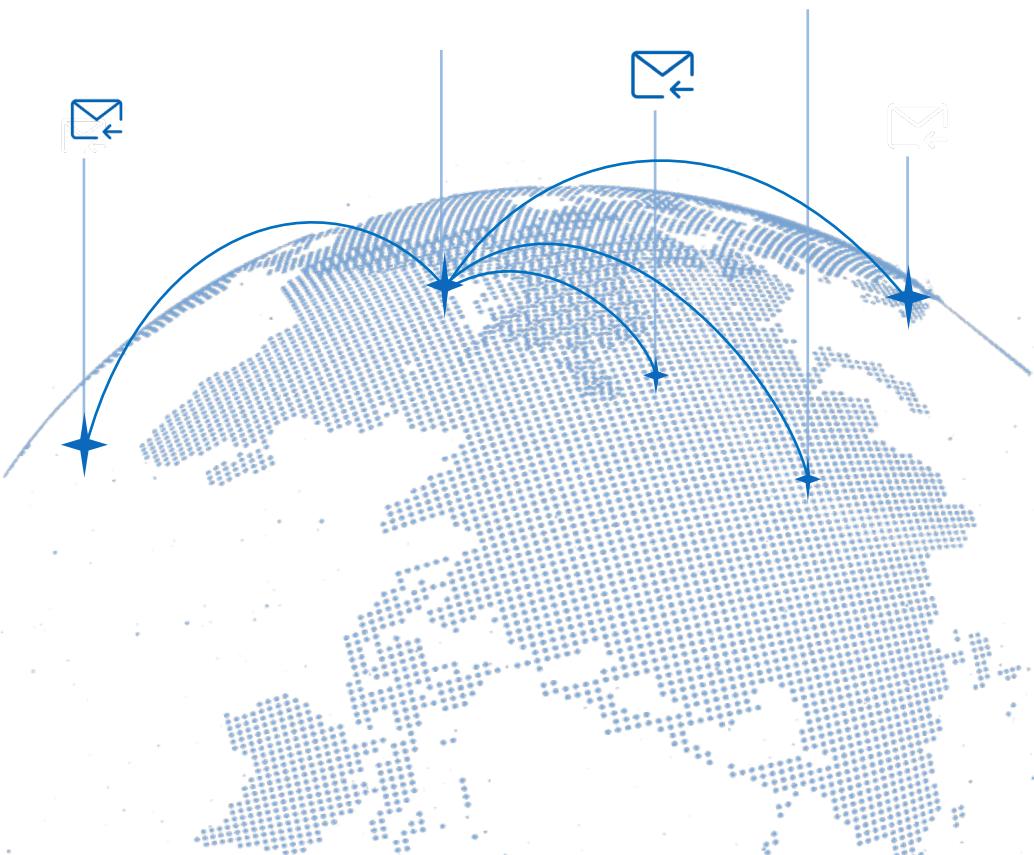
-Client Intelligence: A solution that profiles its client could further refine and identify emails sent against it, or imitated from its staff members, thus enabling more comprehensive BEC protection.

-Brand Indicators for Message Identification(BIMI): An emerging email specification that enables the usage of brand-controlled logos in email clients that support it. BIMI capitalizes on the effort an enterprise has invested in establishing DMARC security by delivering brand logos to the recipient's mailbox. In order to display the brand's logo, the email must pass DMARC authentication checks, guaranteeing that the domain has not been impersonated.

2 Market Trend of Email Security

Key Challenges

Market Trends



Key Challenges:

Sophisticated and localized threats with tailored updated content

Attackers are more intentional in industry selection, and localized content production, and are more capable of rapidly deploying relevant cloud computing servers. Phishing emails, for instance, pose as businesses that are highly relevant to local life, such as government bodies, courier companies, and major regional banks, and criminals employ local brand slogans and headlines as well as official images to deceive recipients. In addition to individuals, local companies are particularly susceptible to fraud. Since June 2021, approximately 65% of Hong Kong organizations have been subjected to a surge in malicious email attacks, with an average of two zero-day phishing attacks daily. Increasing localization and targeting poses a huge challenge to local businesses.

Increasing hybrid attacks in Microsoft 365

According to Frost & Sullivan, more than 78% of businesses have transitioned to cloud-based email by 2022, which gives hackers a vast database of high attack value targets. Enterprises enjoy the benefits of convenience and scalability, but they are also susceptible to account takeover attacks (ATO) and malware infections. Cybercriminals can employ numerous endpoints to launch hybrid attacks, by hosting harmful files on OneNote, OneDrive, and SharePoint. In the first quarter of 2022, Microsoft 365 was used to send over 8 million fraudulent emails, according to Frost & Sullivan. Even while Microsoft 365 provides certain security defenses for organizations, it is difficult for the natively-included SEGs to deliver more specific and targeted services in industries that are highly differentiated, given that Microsoft 365 has up to 300 million business active users.

Cloud dependency raises the bar for scalability and throughput

As a result of cloud migration and corporate expansion, vendors are compelled to pay strict attention to cloud resilience and enhance data throughput on demand. As a result, email security vendors need to continuously upgrade products and solutions to satisfy the requirements of various environments. In addition, several government agencies mandate that data centers be situated within their country or region for security and legal compliance reasons, requiring service providers to have globally dispersed data centers to comply with local data privacy rules. Companies must invest considerably in hardware, data centers, and networks to better compete in the market for cloud-based email security.

Lack of email threats awareness

Over 90% of data breaches are caused by phishing, which is becoming more prevalent due to the WFH model. Nevertheless, according to a Frost & Sullivan report, 83% of Hong Kong enterprises do not provide regular cybersecurity training for their employees, with the majority in the retail, housing, catering, and non-profit sectors due to a lack of training urgency and resources. When firms disregard cybersecurity, the result is a decrease in employees' phishing vigilance. They may even use their work email to create external accounts, raising the risk of exposure and loss for individuals and corporations. Meanwhile, it increases the difficulty of control for the service provider as well.

Attackers are concentrating their efforts on individuals

Currently, attackers target not just the system but also human psychology, typically employing BEC and EAC as attack methods. Generally, attackers know the victim's identity, position, subordinate relationship, etc. Then, they utilize EAC accounts, which are legal business email accounts that have been compromised by attackers, making it difficult for email security systems to capture and prohibit these properties. Meanwhile, they select industries with an abundance of vital data and a strong demand for data access, such as hospitals, universities, and banks. Because of the urgency and authority, numerous victims fall into the trap. In addition to the security system, the recipient's vigilance is crucial for detecting such sophisticated attacks, providing a higher security challenge for email security.

Professional shortages and high resource input requirements

According to a survey conducted by Frost & Sullivan in 2022, approximately 75% of of Hong Kong and Southeast Asia IT and cybersecurity organizations cited recruiting issues for cybersecurity personnel. It is challenging for enterprises to retain expertise of cyberthreats due to the severe shortage of skilled and professional security employees. Due to the fact that phishing assaults require human investigation and remediation, service providers confront a severe labor scarcity. This requirement will increase as the industry's scope broadens, as the management and upkeep of the relevant security solutions in numerous industries will incur greater expenses. Even if a large firm has the capacity to establish an in-house expert IT team, other business segments will be exhausted of energy and resources. Therefore, providers must have sufficient email security expertise and IT resource expertise to ensure their competitiveness with businesses that require additional email security services.

Market Trends:

-Constantly increasing demand for email usage. The migration to the cloud has led to rise in email utilization. In addition, cyber attackers continue to enhance their methods and establish cyber-attack business models, such as "ransomware-as-a-service," in order to capitalize on the rising trend in WFH under COVID-19. Microsoft 365's native secure email gateways (SEGs) address a small portion of email security problems as the leading enterprise communications threat vector. Nonetheless, enterprises committed to email security and confronted with a greater number of cloud-related threats require protection that is more robust. As cloud-based email usage increases, more companies will demand additional email security services.

-More concentrated competitive landscape. According to Frost & Sullivan, the APAC email security industry is ready for consolidation with more than 34 suppliers and channel partners, including several niche players. And as industry leaders continue to build integrated cloud-based solutions with high complexity and extensive coverage, such as convergent email and other security solutions (e.g., DLP, NGFW, SIEM, etc.), the demand for these solutions would only increase. With restricted enterprise resources, vendors can grab the market by providing organizations with additional value, such as better operational efficiency besides basic security. The atmosphere of intense competition will unavoidably lead to ASP (average selling price) reduction. In the future, the major players are likely to accelerate this trend by acquiring smaller competitors, resulting in a more consolidated email security industry.

-Raising cybersecurity awareness. According to a public study conducted by Frost & Sullivan in 2022, more than 90% of the 150 enterprise interviewees stated that they are making or intend to make email security policies, given that email scams can cause significant financial losses. Vendors have active strategies for creating and providing email security-related technologies, such as constantly improving threat detection and cloud-based email integration, in order to withstand the changing threat landscape. In the meantime, a number of suppliers began to offer training to raise security awareness targeting social engineering techniques, including BEC, ATO. Besides, they hone computer-based abilities in areas where attackers are concentrating their efforts.

-Rising demand for multi-layered security measures. To combat evolving cyber risks, service providers must regularly assess threats and monitor traffic trends through multi-layered security integration. Combining real-time system monitoring, maintenance, and a solution based on Machine Learning (ML) / Natural Language Profiling (NLP) and AI to detect phishing, malware, and sophisticated BEC assaults. The MDR integration solution is gaining in popularity because it provides 24x7 automated monitoring and rapid response, threat prioritization, comprehensive threat source analysis, as well as deep threat discovery, etc. Additionally, its automation monitoring enables enterprises to handle more crucial business and is anticipated to become more prevalent in the future.

-More granular business management for service providers. Generally, email security service providers simultaneously serve enterprises from a variety of industries, requiring a higher level of granularity as the organizations expand. In order to boost technology development and internal efficiency, more managed services will be necessary to increase standardization and visibility, such as clear email logs and threat report summaries, including detailed URL clicks and DLP violation logs, etc. Also, the expansion of a corporation into new countries or areas will demand policy and license management. The future growth and expansion of service providers will certainly necessitate more refined management to improve internal efficiency and service quality.

3 Hong Kong Email Security Market

In recent years, the rise in cyberattacks has posed substantial problems to the cyber security of the world's most vital infrastructures. Though Hong Kong currently lacks precise cyber security law requirements, the global trend of cyberattacks and security concerns is being constantly monitored by government officials. To maintain the security of government information systems, the Office of the Government Chief Information Officer (OGCIO) has produced a comprehensive set of routinely reviewed and updated Government Information Technology Security Policy and Guidelines. In addition, there are multiple security procedures in place to identify, intercept, and protect against a variety of security threats to government websites and systems. The OGCIO has also developed a Government Computer Emergency Response Team Coordination Centre to help and coordinate departments' responses to computer-related emergencies.

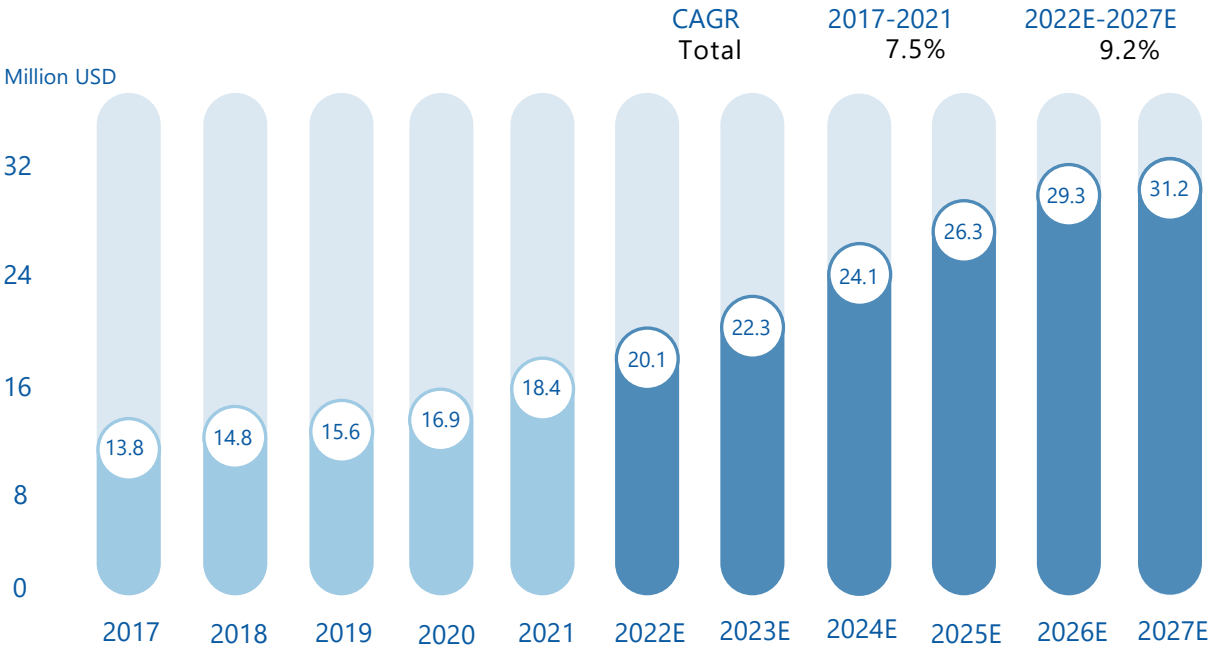
The Personal Data (Privacy) Ordinance (PDPO) is Hong Kong's fundamental data protection law and one of Asia's first comprehensive personal data privacy protection regulations. It safeguards commercial and public enterprises, including the government. Since its enactment in 1996, the Ordinance has been revised to safeguard the privacy of individual's personal data, now regulating the purpose, method, retention term, usage, access, and correction of acquired data to ensure its precision and security.

To further strengthen the cyber security of Hong Kong's vital infrastructures, the government is currently drafting laws that would outline the cyber security duties of operators of key infrastructures. This is expected to provide a more regulated business environment for the cybersecurity market in the future.

Year	Administration	Policy	Content
2021	Office of the Privacy Commissioner for Personal Data, Hong Kong	The Personal Data (Privacy) Ordinance (the "PDPO")	The second major amendment aims to combat "doxing" acts that infringe on personal data privacy by making "doxing" a criminal offense and strengthening enforcement.
2012			To make key amendments, including new requirements for using personal data in direct marketing, and to include additional safeguards in response to new challenges and public concerns about privacy protection.
1996			To ensure adequate protection of personal data and implementation the human rights treaties to maintain Hong Kong's status as an international business center.

Source: Frost & Sullivan

Hong Kong Email Security Market Size By Revenue(2017-2027E)



Source: Frost & Sullivan

Note:

2022 data is based on historical Q1,Q2,Q3 2022 data and Q4,2022 projection.

According to Frost & Sullivan, the Hong Kong email security market grew at a 7.5% CAGR from 13.8 million USD in 2021 to 18.4 million USD in 2022 and is expected to reach 20.1 million USD in 2022. It is expected to grow at a 9.2% CAGR to 31.2 million USD in 2027.

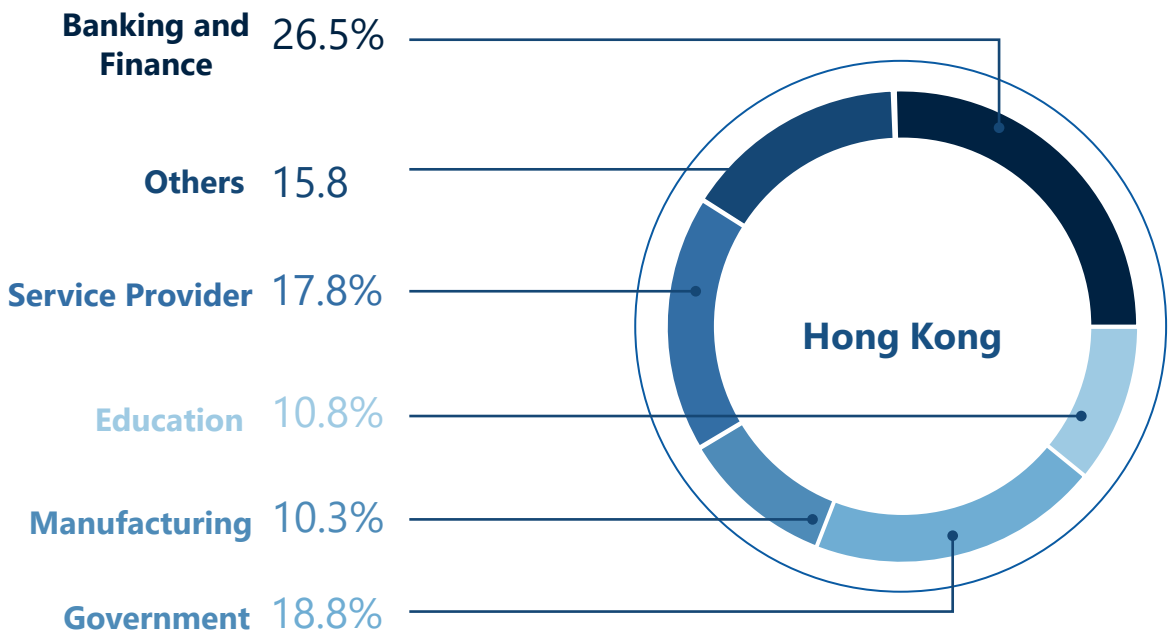
The key growth drivers for email security include:

-Localization and customization of email attacks. 90% of cyberattacks in Hong Kong infiltrate organizations via email in 2022. Meanwhile, Hong Kong was the initiation site of 9.4% of attacks staged against its inhabitants, ranking second only to the United States. In recent years, it has been seen that cybercriminals customize their attacks based on current events, such as attack themes riding on COVID lockdown-associated services, and even public service calendars such as tax collection dates. In each attack, hackers exerted additional effort to stay abreast of current trends, personalize their messaging, and reinvent their methods for optimal results. Although the Hong Kong government has cracked down on email fraud, it has yet to establish a clear cybersecurity law. Therefore, the relatively loose environment attracts more cybercriminals to join.

-Cybercrime scenarios expand as new industries emerge, e.g. metaverse. The rapid development of emerging fields such as metaverse, blockchain and crypto trading, which involve virtual reality, machine learning, and artificial intelligence technologies that require behavior learning based on an abundance of personal data. Additionally, the Hong Kong government is promoting the e-commerce industry, private address and payment information in cross-border transactions, and other privacy-threatening practices. These industries are in the early stages of development, providing cybercriminals with a large number of data collection channels and dimensions, where social engineering, fraud, and phishing attacks are anticipated to occur frequently.

-Digital transformation. Hong Kong is now committed to promoting the digitization of government and business, which is accelerated by the covid-19 pandemic. The Digital Economy Committee was formally established by the government in June 2022, promotes the adoption of digital strategies in various industries, and provides funding for small and medium-sized enterprises to conduct digital transformation pilots. However, the convergence of digital technology and trade will increase the risk of information leakage, security awareness and protection capabilities for SMEs are typically inferior, and large enterprises that place a high value on data sovereignty, especially in the financial sector, have a high demand for security services, particularly from vendors who can provide localized solutions.

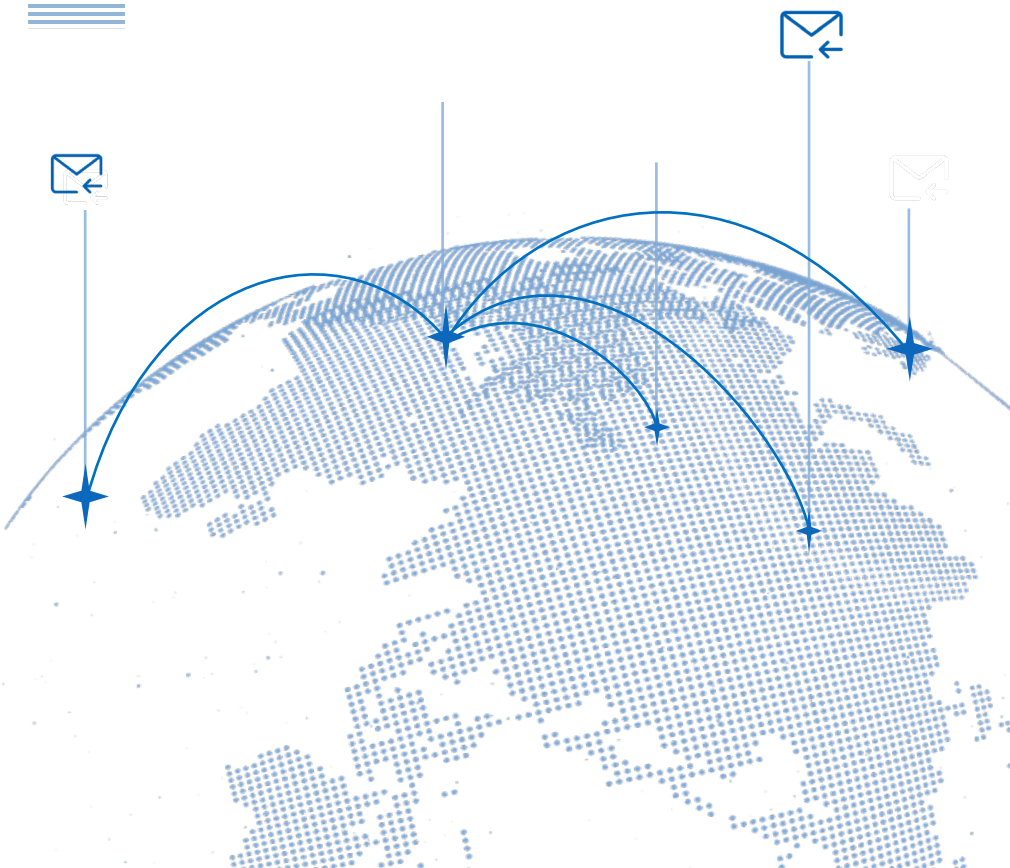
Hong Kong Email Security Vertical Segment Breakdown, By Revenue (2022)



Source: Frost & Sullivan

Being the financial gateway of Mainland China and western capital, banking and finance took up 26.5% of the email security market share in Hong Kong according to Frost & Sullivan.

Singapore Email Security Market



In response to the rise of the digital economy and the increasing significance of cyber hazards, the government of Singapore has established a series of cybersecurity support policies that have matured Singapore's institutional structure, national policy, and laws and regulations.

The publishing of Singapore's Cyber Security Strategy 2016 and 2021 is one of the most critical undertakings. Strategy 2021 outlines the key actions the Singaporean government intends to take in cybersecurity over the next five years. It establishes three strategic pillars in cybersecurity: building a resilient infrastructure, creating a secure cyberspace, and strengthening international cyber cooperation, with two fundamental underpinnings, building a vibrant cybersecurity ecology and developing a strong cybersecurity talent cultivation channel.

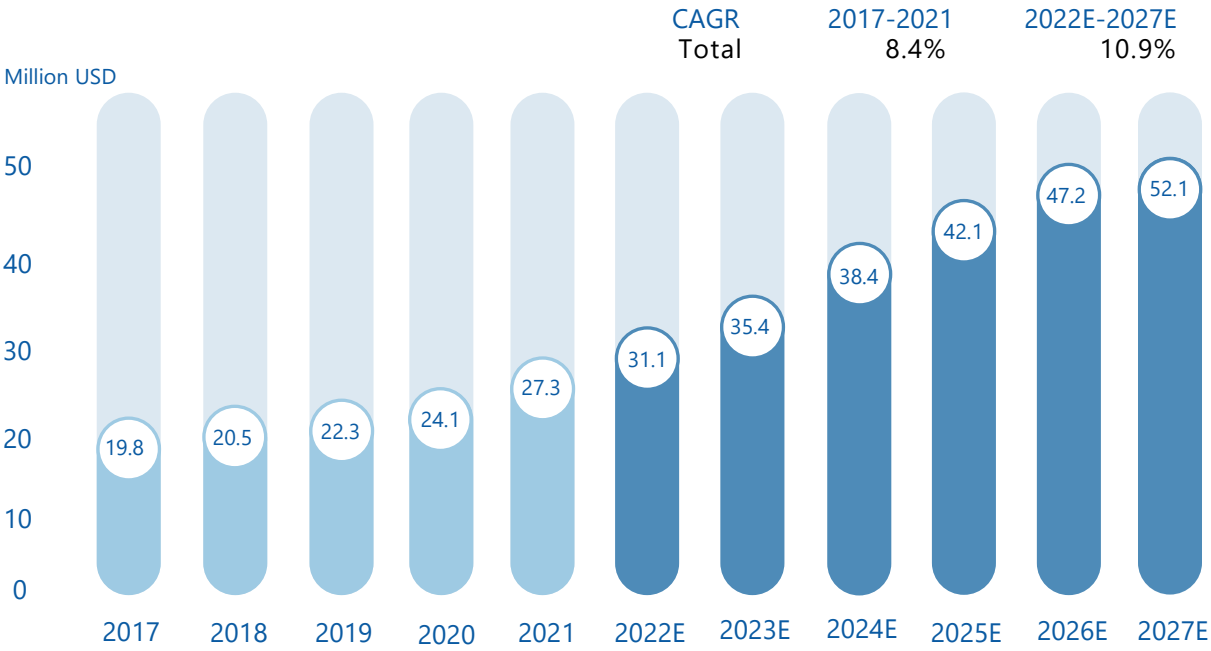
Compared to the 2016 strategy, the new strategy presents a series of adjustments and new trends, including three key focal points, taking a more proactive approach to strengthening infrastructure protection, providing simple solutions to improve cybersecurity, and promoting the exploration of international cyberspace norms and standards. In addition, the new approach would enhance investments in security skills and local production of cybersecurity solutions in Singapore.

With the support of Singapore's ongoing strengthening of cybersecurity, the increasing sophistication of regulatory authorities, and the refinement of legislative measures, the market will become more compliant and the industry's growth prospects will improve.

Year	Administration	Policy	Content
2022	The Cyber Security Agency of Singapore (CSA)	licensing framework for cybersecurity service providers under Part 5 of the Cybersecurity Act (CS Act)	To better protect the interests of customers and address the information imbalance between them and cybersecurity service providers. CSA first grants licenses to two categories of cybersecurity service providers, specifically those who offer penetration testing and managed security operations center monitoring services.
2021	The Cyber Security Agency of Singapore (CSA)	The Singapore Cybersecurity Strategy 2021	Introduced a number of modifications and new developments, such as enhancing infrastructure protection, providing simple solutions to improve cybersecurity, and supporting the investigation of international cyberspace rules and standards. Protecting essential digital technology infrastructure and operations, and assisting cyber-related individuals
2020	Singapore Government	Singapore's Safer Cyberspace Masterplan 2020	Protecting essential digital technology infrastructure and operations, and assisting cyber-related individuals
2018	The Cyber Security Agency of Singapore (CSA)	Cybersecurity Act	Established a legal framework for the supervision and maintenance of Singapore's national cybersecurity.
2016	The Cyber Security Agency of Singapore (CSA)	The Singapore Cybersecurity Strategy 2016	The institutional design has basically formed a four-pronged cybersecurity cooperation trend of "individual, private, public sector, and international cooperation".

Source: Frost & Sullivan

Singapore Email Security Market Size, By Revenue(2017-2027E)



Source: Frost & Sullivan

Note:

2022 data is based on historical Q1,Q2,Q3 2022 data and Q4,2022 projection.

According to Frost & Sullivan, the Singapore email security market grew at an 8.4% CAGR from 19.8 million USD in 2021 to 27.3 million USD in 2022 and is expected to reach 31.1 million USD in 2022. It is expected to grow at a CAGR of 10.9% to 52.1 million USD in 2027.

The key growth drivers for email security include:

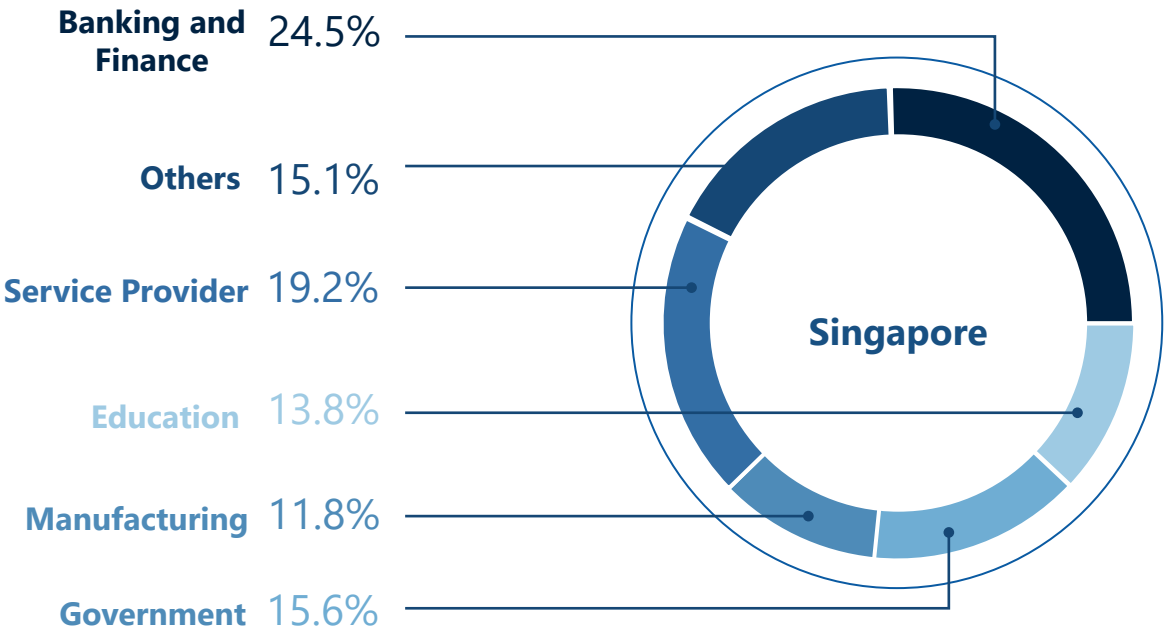
-Increase in phishing and BEC with evolving sophistication. According to the Singapore police force, in the first half of 2022, at least $70.8 million are lost from 149 organizations due to business email compromise scams, taking up more than 30% of the total top 10 scams of 227.8 million, where phishing cases reported doubled. The increasing tendency is mostly attributable to the increasing sophistication of scams. The persuasiveness of scams is growing as scammers are no longer limited to a single media, with email now being an integral component of the process. Scammers who conduct sophisticated schemes involving online conversations, emails, and phone calls utilize the entire workflow. For instance, bogus apps and email verification links leading to phished bank/payment websites are utilized to steal credentials. In addition, the use of QR codes by cyber criminals in lieu of URL links to circumvent victims' defenses is facilitated by the fact that awareness training has focused on URLs.

-Government business collaboration to advance industrial ecology. According to the Singapore Cyber Landscape 2020, ransomware assaults surged by 154% in Singapore's manufacturing, retail, and healthcare sectors between 2019 and 2020, with 47,000 malicious phishing links detected and that increased by 17% in 2021, reaching 55,000. In view of Singapore's strong emphasis on cybersecurity, the government is constantly developing its cybersecurity infrastructure and ecosystem by reducing cyber risks, including the email threat. In this process, the government will strengthen its cooperation with the private sector by, for instance, joining forces with industry leaders and chambers of commerce to provide awareness training, security products, and services in collaboration, thereby creating business opportunities for industry and contributing to the establishment of an Internet security ecosystem based on mature technology and the resources of large corporations.

-Rapid development of metaverse and digitalization. The metaverse is becoming an integral component of business and leisure, and an increasing number of enterprises are joining the realm. Singapore has a stable legal system, the rule of law, accessibility, connectivity, and legal infrastructure that fulfills most of the conditions for becoming the next major metaverse and cryptocurrency center. And, the impact of covid has hastened the development process, for instance, Singapore's legal procedure is already heavily digital, and courts are evaluating adopting meta-settlements. In addition, well-known cryptocurrency exchanges such as Binance, Gemini, Coinbase, and Crypto.com applied for licenses in Singapore in 2021 in an effort to boost the local market. It is anticipated that in the future, with Singapore's clear regulatory framework, there would be more innovations and an increase in cyber security threats.

-Favorable business environment. Singapore is ranked second on the Bloomberg Innovation Index for 2021 and eighth on the World Intellectual Property Organization Index Report (WIPO). As the government of Singapore places a high priority on innovation development, it provides a stable and legal business environment, including tax breaks and substantial subsidies. Therefore, it now hosts numerous APAC headquarters. In the email security aspect, in April 2022, the Singapore Cyber Security Agency (CSA) released a licensing framework in order to protect consumer rights and improve overall service quality, mainly for penetration testing and managed security operations center (SOC) monitoring services providers, which will continue to attract technology companies, especially for email security specialists.

Singapore Email Security Vertical Segment Breakdown, By Revenue (2022)



Source: Frost & Sullivan

Hosting numerous Fortune 500 headquarters, Singapore is gaining more weight in Asia given its stable and lawful business environment. According to Frost & Sullivan, banking and finance, manufacturing and education took up 24.5%, 15.6%, and 13.8% respectively in email security vertical segments.

Frost Radar on HK/SG Email Security Vendors

Introduction of HK/SG Email Security Vendors

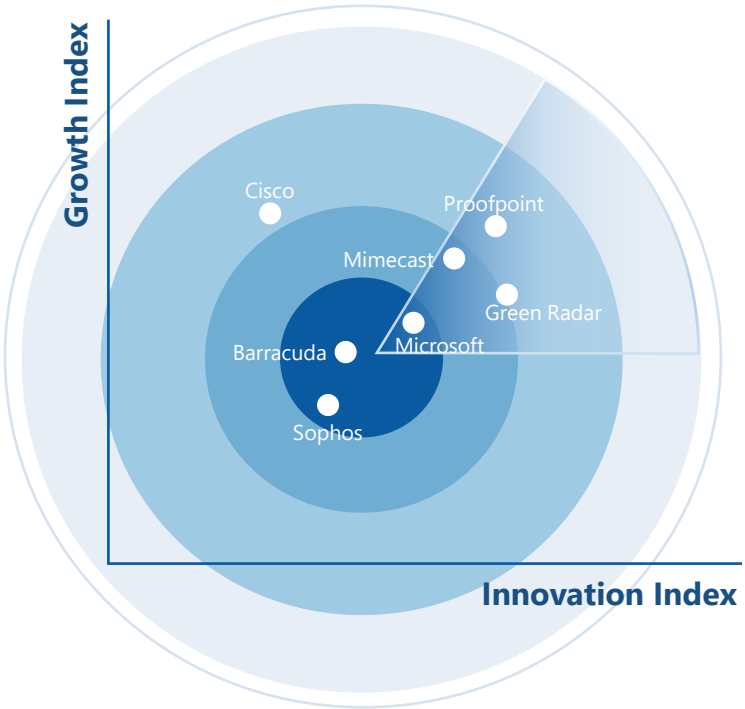
Frost Radar

Introduction of HK/SG Email Security Vendors

Vendor	Introduction	Key Products
Barracuda	Barracuda Networks is a solution provider for security, application, and data protection. It was established in 2003 in Campbell, California. It built its Asia Pacific headquarters in Hong Kong in 2019, which serves as a sales, marketing, and recruiting hub to supply consumers in the region with essential services. Barracuda Email Protection offers complete protection against the most prevalent email threats, from spam and ransomware to socially engineered threats including spear phishing, business email compromise, and account takeover.	Barracuda Email Protection
Cisco	Cisco was started in 1984 as a provider of networking and security solutions. Cisco has established offices in Hong Kong and Singapore to develop local businesses, offering the Cisco-IronPort, a cloud-based email security platform that provides protection against malicious threats such as spam, phishing, malware, and ransomware.	Cisco IronPort Cisco Secure Email
Green Radar	Green Radar is a Hong Kong and Singapore-based provider of email security MDR services, primarily filter out fraudulent e-mails and isolating users from internet activity risks. grMail is only available as a cloud-based MDR service augmented with focus on local threats. The platform combines big data, artificial intelligence, local and global threat information, and a team of cybersecurity professionals to secure and clean a cyber environment for its clients.	grMail
Microsoft	Microsoft is a technology firm headquartered in Redmond, Washington, founded in 1975. It maintains offices in numerous international locations, including Hong Kong and Singapore, providing series of email security solutions for Microsoft 365 subscriptions in terms of basic email protection such as anti-spam, anti-malware, and anti-phishing, and advanced solution including multi-layered security, and etc.	Exchange Online Protection Microsoft Defender for Office 365
Mimecast	In 2003, Mimecast was founded as a cloud-based email security and archiving provider. In the APAC region, it maintains offices in Singapore and Australia, with its headquarters in London, United Kingdom. On the Mimecast X1 integrated system platform, users have access to the Mimecast product suite, which provides email security and resilience, data retention and compliance, security awareness and user behavior assurance, covering the risks of human error and malicious actors such as phishing, impersonation, malware, and advanced persistent threats.	Email Security CI 365 Protect
Proofpoint	Proofpoint, founded in 2002 and headquartered in Sunnyvale, California, is a SaaS-based cybersecurity and compliance company with additional operations in Singapore and Japan in the APAC area. It offers a vast array of email security products and services, such as Targeted Attack Protection, Email Isolation, Threat Response, and Emerging Threats Intelligence, which are supported by real-time threat detection, advanced threat intelligence, user and content visibility, and DLP.	Proofpoint Threat Protection Bundles

Vendor	Introduction	Key Products
Sophos	Sophos is a provider of cybersecurity software and services founded in 1985 with headquarters in the United Kingdom and locations in Hong Kong and Singapore. Sophos Email & Cloud products offer protection against malware, phishing, and ransomware, in addition to security awareness training. Moreover, its Managed Detection & Response (MDR) solution offers real-time threat detection and enhanced threat intelligence.	Sophos Email

Frost Radar



Source: Frost & Sullivan

Quadrant Criteria Explanation

Growth Vector:

GI1: Market share in the last three years (Mkt share TTM, share growth)
GI2: Revenue growth in the last three years
GI3: Growth Pipeline: the strength and leverage of a company's growth pipeline system (corporate organization structure review for growth possibilities) to analyze, prioritize, and capture growth prospects.
GI4: Vision and Strategy: the extent to which a company's growth strategy is aligned with its vision, e.g., investment in new products/markets consistent with the stated vision.
GI5: Sales and Marketing: drive demand and meet growth targets **(Staff numbers, average revenue generated per sales, CPC, PPC, etc.)

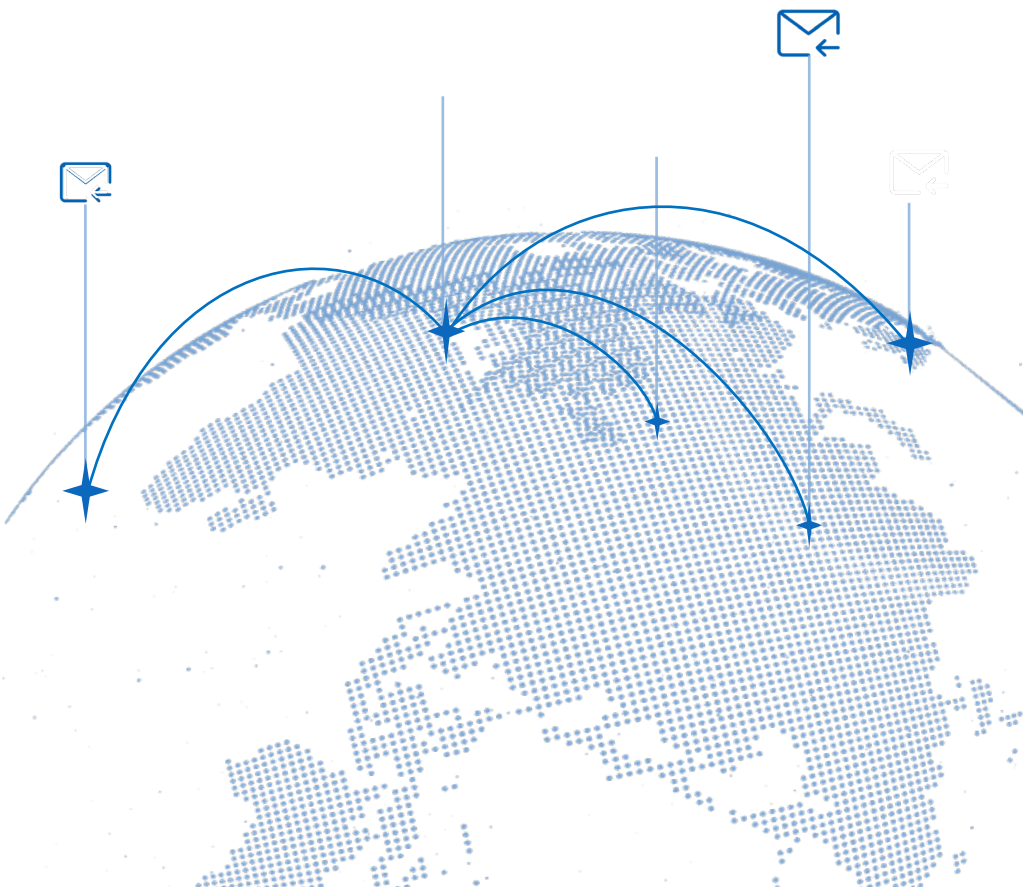
Innovation Vector:

I1: Innovation scalability: worldwide and applicable to both emerging and developed markets (percentage of revenue from different regions)
II2:R&D: R&D strategy effectiveness (R&D/Expense; Execution status; Result-based measures, such as patterns/paper)
II3: Product portfolio: concentration on the relative contribution of new goods to annual revenue
II4: Mega trend leverage: a company's proactive leverage of evolving long-term opportunities and business models.
II5: Customer Alignment: the applicability of the company's products/services to existing and potential consumers.

6 Vendors Capability Comparison

Capability Description

Capability Comparison Table



Capability Description

-Managed Detection and Response (MDR): MDR is a cybersecurity service that combines technical and human expertise to perform threat detection, monitoring, and response 24/7. It allows IT and security teams to spend more time focusing on strategic initiatives that support business objectives by saving organizations additional manpower and providing higher monitoring accuracy.

-Security Operations Center (SOC): SOC is a centralized department that monitors and improves the organization's security posture by preventing, detecting, analyzing, and responding to cybersecurity incidents.

-Location Intelligence (LI): LI is the collection and analysis of geospatial data from various sources, which results in strategic insights in capturing targeted impersonated phishing emails. SOC collects global and local threat intelligence to analyze and detect phishing incidents impersonating local brands in email security.

-Anti-Spam, Anti-Malware, and Anti-Phishing Filtering (known threats): They are cloud-based systems that filter spam and phishing emails while also blocking malware and DDoS attacks.

-Sandboxing: A cybersecurity sandbox provides a secure environment for opening suspicious files, running untrusted programs, or downloading URLs without affecting the devices on which they are running. It can be used at any time, in any situation, to safely examine a potentially malicious file or code before serving it to devices — all while keeping it isolated from a PC and the company network.

-Engines for AI/NLP/ML (Next Generation Engine): Using machine learning to determine which identities the recipient believes is sending the message, analyzing the expected sending behavior for anomalies relative to that identity; and employing predictive artificial intelligence to model trustworthy communications.

-Link/web isolation: It scans and analyzes emails when users click on malware URLs embedded in emails, and blocks users from visiting suspicious websites to prevent sensitive data leaks and zero-day attacks.

-Data Loss Prevention (DLP): It is a collection of processes and technologies designed to help organizations prevent data loss, misuse, or exposure to unauthorized users due to end-user errors or misconfigurations. The system will make remediation by monitoring endpoint activity and filtering the internal data flow at rest, in motion, and in use. It has now proven to be very effective in protecting data and privacy.

-Business Email Compromise (BEC): Attacks frequently rely on social engineering techniques rather than malicious payloads. Within a single attack, criminals behind email fraud frequently combine multiple tactics, such as impersonation via spoofing and compromised accounts via phishing.

-Account takeover (ATO): It is a cybercrime attack in which cybercriminals use stolen passwords and usernames to gain control of online accounts, which are often difficult to monitor and intercept because the accounts are legitimate.

-Cost-effectiveness: In terms of service subscription fees and maintenance costs.

Capability Comparison Table

	Barracuda	Cisco	Green Radar	Microsoft	Mimecast	Proofpoint	Sophos
Local Intelligence							
MDR							
SOC							
Anti-Spam, Malware							
Phishing Content Filtering							
Sandbox Integration							
Next Generation Engine							
Link/web Isolation							
DLP							
BEC							
ATO							
Cost-effectiveness							

Source: Frost & Sullivan

Impact Ratings:

The above are some key participants of email security solutions and services in Hong Kong and Singapore. We compare their relative technical capabilities and operational presence in these localities, rather than on a global scale. It should be noted that clients looking for potential email security vendors must always consider their organizational characteristics first and these vary with different business nature, geographical span, cybersecurity posture, size etc. As this evaluation is geographically focused on Hong Kong and Singapore, the strength of a players' local intelligence, threat understanding is also reviewed and contribute towards its overall score. Potential clients should also take into consideration its relevance.

Legal Disclaimer

All the information contained herein (including without limitation data, words, charts and pictures) is the sole property of Frost & Sullivan, treated as a highly confidential document, unless otherwise expressly indicated by the sources in the report. Should no one copy, reproduce, diffuse, publish, quote, adapt, or compile all or any part of the report without the written consent of Frost & Sullivan. In the event of the violation of the above stipulation, Frost & Sullivan reserves the right of lodging a claim against the relevant persons for all the losses and damages incurred.