Cloud-based Email Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Cloud-based Email Security Market size is estimated at USD 0.96 billion in 2024, and is expected to reach USD 1.52 billion by 2029, growing at a CAGR of 9.42% during the forecast period (2024-2029).

Key Highlights
-Cloud security software is one of the essential tools deployed by cloud service providers and users to protect the overall cloud infrastructure. Companies that rely on the Internet as a vital source of information exchange, such as e-commerce companies like Amazon, are more vulnerable to cyberattacks. Financial institutions and healthcare sectors are among the other businesses with high financial gains and lucrative targets for hackers. However, email security outsourcing has an inherent risk, as organizations must rely on and trust a third-party provider for service.
-Cloud-based email security software helps to prevent phishing and imposter threats, and it automatically identifies an organization's profile targets for malware-free impersonation and business email compromise attacks and blocks the attack with machine learning analysis of message content.
-According to 99 Firms, a prominent email market vendor in the global market, there were about 3.9 billion email users worldwide in 2019, which is expected to reach approximately 4.3 billion in 2023. According to the data port, 45% of emails are spam, which costs businesses about USD 20.5 billion annually. The growth of the cyber environment and related technologies paved the way for new threats. Cyberattacks are highly targeted, persistent, and technologically advanced.
-Moreover, technical issues or financial bankruptcy may interrupt email security outsourcing. A severe email failure of security providers can lower an organization's confidence in cloud-based security. According to IBM, 60% of emails are opened on mobile devices, depending on the industry, which increases the threat of spam mail, phishing mail, and other threats related to email. Factors such as a need for decreasing onsite datacentre footprints and cost savings, coupled with increasing incidences of spam, viruses, inappropriate content through email, and flexible deployment options, are spurring the market growth.

-Furthermore, with the widespread adoption of cloud email services, security vendors collaborate with cloud providers to offer faster and more seamless ways of rolling out security solutions. For instance, in June 2023, Cyware, a provider of threat intelligence management and cyber fusion solutions, announced a strategic partnership with Mimecast to extend cyber fusion with advanced email security. The joint solution will provide customers with proactive defense against ransomware, phishing, malware, and other evolving cyber threats.
-With the outbreak of COVID-19, the cloud-based email security market was expected to grow significantly as cloud-based services and tools were increasingly adopted due to organizations deploying remote work access amid lockdowns in various countries. Microsoft noticed an increase of 775% in Italy, calling and meeting monthly users for the Teams product in one month. According to data provided by Google, the company blocked about 18 million COVID-19 spamming emails daily. The increasing usage of cloud-based services during the pandemic is becoming a hotspot for cyberattacks, as millions work in unfamiliar and less secure circumstances.

Cloud-based Email Security Market Trends

Increasing use of cloud based email security in BFSI sector to drive the market.

- The financial sector generates a massive volume of data generated by its customers. Banks and financial organizations increasingly employ services to store and analyze complex data to use the collected data through various data points and improve customer satisfaction. Additionally, with higher customer expectations, growing technological capabilities, and regulatory requirements, banking institutions are pushed to adopt a proactive approach to security. This has resulted in the incorporation of cloud-based security platforms.
- Cybersecurity is even more important for BFSI companies, which need to ensure regulatory compliance and protect the sensitive financial information of their customers at all times. Large banks and capital markets increasingly recognize that the cloud-based security platform is more than just technology, further creating growth opportunities for the market.
- Cloud-based email solutions can help reduce implementation time and costs for banks trying to keep pace with regulations regarding administrative access control. The data is exponentially growing, with an increase in e-transactions. Email exchanges between employees and customers in the BFSI sector contain highly lucrative, important, and valuable information and can greatly benefit hackers. Additionally, organizations in the investment banking sector that use email as their primary means of communication internally and externally have encrypted their email accounts and taken steps to limit eavesdropping and hacking.

- To secure their IT processes and systems, secure customer critical data, and comply with government regulations, private and public banking institutions are focused on implementing the latest technology to prevent cyberattacks. Furthermore, with higher customer expectations, growing technological capabilities, and regulatory requirements, banking institutions are pushed to adopt a proactive approach to security. Cybercriminals are increasingly using a sophisticated range of tactics. Financial services firms' most expensive attack types are denial of services, phishing email attacks, and social engineering.
- Further, Machine learning and Artificial Intelligence (AI) are expected to emerge as the most sought-after solutions, as cybercriminals are also using similar capabilities to break in. It is expected to attract more investments in strengthening security capabilities by organizations to counter and mitigate such risks.

North America Accounts For the Largest Market Share

- North America is a primary hub for all the major organizations worldwide. The expansion of the various end-user industries and the growth of IoT drive the region's demand for smart devices and mobiles. The attacks' risks can impact the market varying from

individuals and government to corporates. Thus, securing the data has become a priority in the region.
- Email is one of the most popular tools and one that businesses use every day. According to the FBI's Internet Crime Report, the compromised business email and email accounts were part of malicious phishing campaigns, costing U.S. businesses about USD 2.4 billion.
- In addition, cyberattacks in North America, especially in the United States, are rapidly increasing. The number reached a record high, largely due to the rapid increase in the number of connected devices in the region. According to Microsoft, the United States remains the most highly targeted country, with 46% of global cyberattacks in the region.
- The United States is marked with increased investments in cybersecurity solutions and cyber threat-detecting software and platforms. With the increased awareness amongst companies from small to large enterprises, the U.S. government is taking several initiatives to prevent cyberattacks and deploy stricter solutions to protect data and install fraud and threat detection programs. For instance, in March 2023, the U.S. government announced the release of the National Cybersecurity Strategy to ensure that all Americans enjoy the full benefits of a secure digital ecosystem.
- Furthermore, several regional companies are focusing on offering new solutions to meet the growing demand. For instance, in November 2022, Barracuda Networks, Inc. announced it offered email security integrated with Amazon Security Lake to help customers reduce the complexity of email security data. The company's email protection solutions streamline access to customer security data through email security solutions, reduce costs, and cover a variety of security use cases such as investigation, threat detection, and incident response.

Cloud-based Email Security Industry Overview

The global cloud-based email security market is entirely consolidated due to fewer players occupying the larger market share. The new players are trying to penetrate the established market. Some key players in the market are Cisco Systems Inc., Proofpoint Inc., Trend Micro Inc., and Fortinet Inc. Some recent developments in the market include:

- In May 2023, LogRhythm announced a technology partnership with Mimecast to offer an advanced combination of email security, enterprise security, and threat management capabilities. The company will likely integrate Mimecast's email security capabilities with LogRhythm's enterprise threat management. Through this integration, both companies aim to help organizations around the globe protect against modern cyber-attacks.
- In October 2022, at the 2022 Microsoft Ignite Conference, the cybersecurity and compliance firm Proofpoint Inc. unveiled several innovations across its Threat Protection Platform, empowering organizations to counter the most advanced and pervasive threats like Business Email Compromise (BEC) and supply chain attacks. The improvements give businesses unparalleled insight into email fraud detection, defense against third-party and supplier compromise, machine learning (ML), and behavioral analytics, all made available via a new, simple-to-deploy inline API format.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Cloud-based Email Security - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-02-27
		Signature