WHITE PAPER

Trustifi

Overview of Gartner Market Guide for Email Security

Authored by **Mark Harris, Peter Firstbrook, Ravisha Chugh,** and **Mario de Boer**.

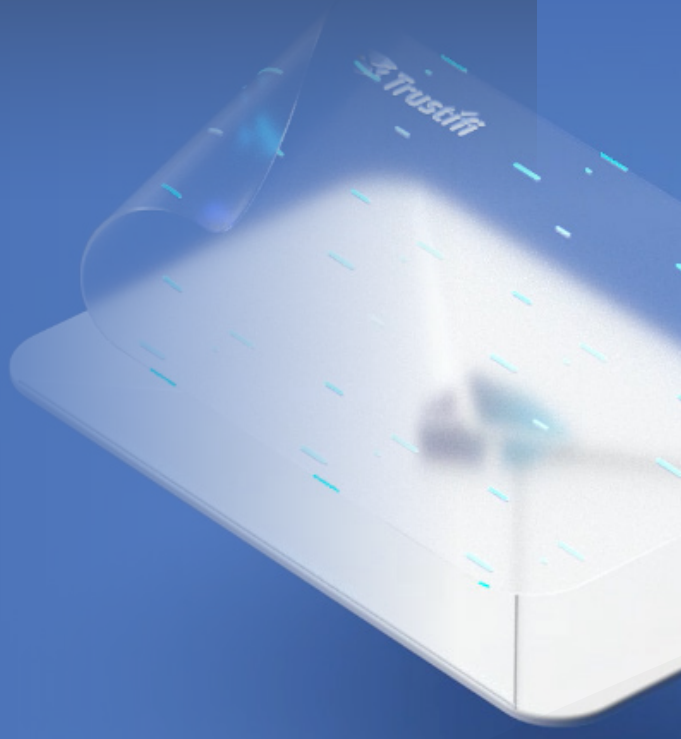
Gartner

Trustifi Recognized as a Representative Vendor in 2021 Gartner® Market Guide for Email Security

The guide details the market landscape and trends for email security solutions. The report's key takeaway identifies, "Solutions that integrate directly into cloud email via an API, rather than as a gateway, ease evaluation and deployment and improve detection accuracy, while still taking advantage of the integration of the bulk of phishing protection with the core platform."

Trustifi Named in Gartner Market Guide for Email Security

As cloud email security implementations become more popular, security and risk management professionals are taking an in-depth look at their capabilities. Cloud-based security solutions deployed through APIs instead of a gateway are easier to implement and provide more comprehensive protection. We believe that Gartner has published this Market Guide for Email Security at a timely moment. A growing number of frauds and deceptions are perpetrated through phishing, impersonation, ransomware, and business account compromises. These cybercrimes have direct financial consequences, and they are effective because users trust their email identities too much and are therefore vulnerable to fraud and deception.



Email Security Solutions Market

Email security is a process of predicting, preventing, detecting, and responding to attacks.

A comprehensive security approach to email encompasses firewalls, email systems, content protection, user behavior, and other related processes. In order to effectively secure emails, you must select products with the right capabilities and configurations, as well as ensure that your operational procedures are appropriate. A vast variety of solutions and capabilities for email security are available.

> ***"Integrated solutions go beyond simply blocking known bad content and provide in-line prompts to users that can help reinforce security awareness training, as well as providing detection of compromised internal accounts."***

Source: Gartner, "Market Guide to Email Security" , Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer, 7 October 2021.GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. [1]

Secure Email Gateway (SEG)

SEGs have traditionally protected incoming and outgoing emails for on-premise systems, whether they were local appliances, virtual appliances, or cloud solutions. A SEG's functions include filtering SMTP traffic and modifying the mail exchange record that points to the SEG.

Integrated Cloud Email Security (ICES)

Cloud email providers, such as Google and Microsoft, are becoming increasingly popular thanks to their built-in hygiene features. SEGs are less effective for cloud email systems. Therefore, the majority of advanced email security solutions today are ICESs.

ICES is more than just a malicious content filter. It offers in-line prompts that increase security awareness through training and detection of compromised internal accounts in addition to blocking malicious content.

Email Data Protection (EDP)

A standard EDP solution encrypts emails to detect and prevent unauthorized access to message content during or after dispatch. Further, if an email is sent to an incorrect recipient, the EDP prevents the information from being leaked.

[1] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Market Analysis

Email is the most popular means of conducting malware attacks and stealing credit card numbers and other sensitive information through phishing. An amazing 40% of attacks begin through email. With the threat landscape changing and accelerating, it's crucial to reassess the effectiveness and functionality of current security solutions in light of the latest products. This is especially true since the incumbent solution may not take advantage of the newest protection technologies.

Native Capabilities of Google and Microsoft

A number of email hygiene solutions are available from Google and Microsoft, such as:

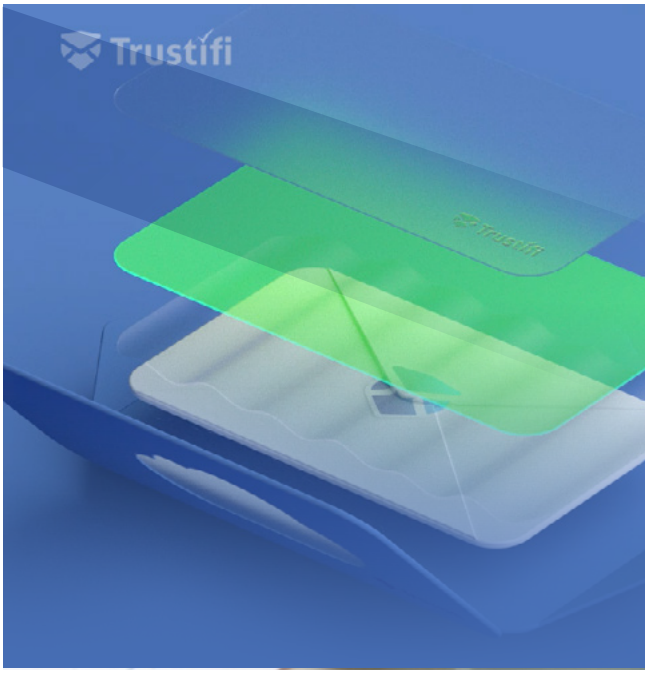
- Filtering out emails sent by known bad senders
- Filtering out emails sent with known bad links
- Using antivirus software to scan attachments
- Detecting spam by analyzing content

Despite the relatively few features it offers and the less sophisticated controls it provides, Google Workspace's simple—yet effective—three-tiered model is embraced by companies that use it for collaboration. The licensing process for Microsoft's E5 license package, which includes Microsoft Defender for Microsoft 365, can be complicated and expensive. A number of bundles and add-ons, however, are available to allow users to access advanced features. With all plans, Exchange Online Protection is included, as well as basic anti-phishing, anti-spam, and anti-malware protection.

Secure Email Gateways

The most common method of email security remains secure email gateways. Generally, SEGs are implemented as a physical or virtual appliance, but they can also be made available as a cloud service as well. In addition to basic hygiene solutions, SEG includes more advanced protection features, including:

- Multi-antivirus scanning
- URL rewriting
- Graymail handling
- Sandbox integration
- Post-delivery clawback
- Quarantine for spam with end-user digests
- Key individual protection from impersonation



Integrated Cloud Email Security

Email is usually the first point of entry for ransomware. Malware, however, is not the only threat. Business Email Compromise (BEC) and account hacking are also becoming more common. Because there is no attachment or link associated with these attacks, they are difficult to identify. They rely completely on social engineering to trap the recipient.

In previous studies: Gartner identified two categories of API products:

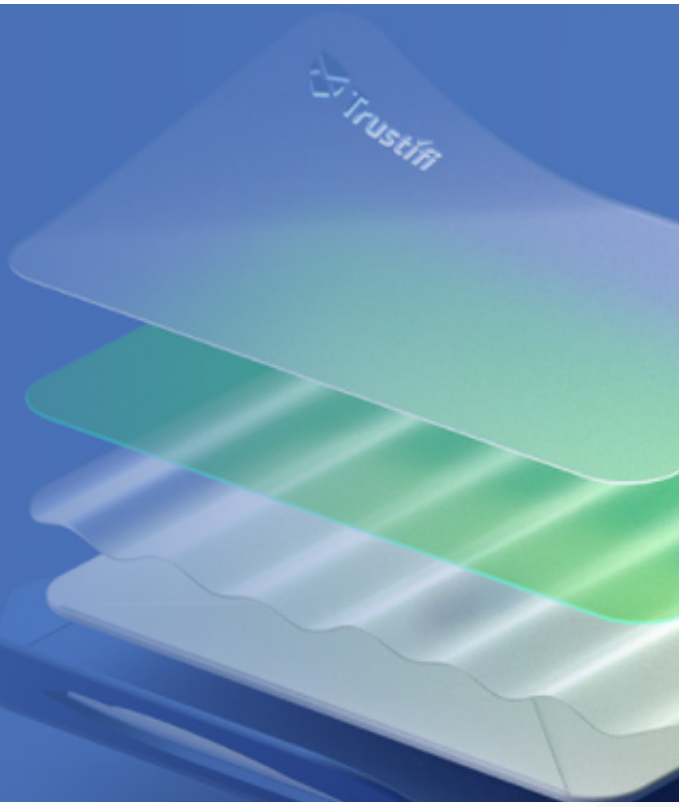
1. "Cloud email security supplements (CESSs) that focused on specific threats to enhance existing predelivery solutions."
2. "Integrated email security solutions (IESSs) that implemented more of the traditional controls found in an SEG."

The integration of Cloud Email Security can take place either pre- or post-delivery based on the APIs used. In the case of pre-delivery, the email is monitored before it gets into the user's inbox. In the case of post-delivery, the emails are intercepted once they reach the user's inbox. The best of these solutions employ AI and machine learning to engage advanced algorithms and natural language processing (NLP) to identify and block potential threats.

Data Protection

Aside from malware, phishing email is one of the most common ways to steal credentials from users. Due to the COVID-19 pandemic, more and more people are relying on emails for communication, leading to a need for data protection that goes beyond the standard gateway.

Misdirection of recipients is the main cause of data breaches in emails. In addition to a variety of solutions to counteract this problem, AI combined with machine learning models are increasingly being used to detect and warn users of misdirected emails. The alerts can appear either in the email client while composing the email or as bounce messages requesting confirmation that the specified recipient is legitimate.



Recommendations by Gartner

Gartner recommends that companies take the following actions when securing their email accounts.

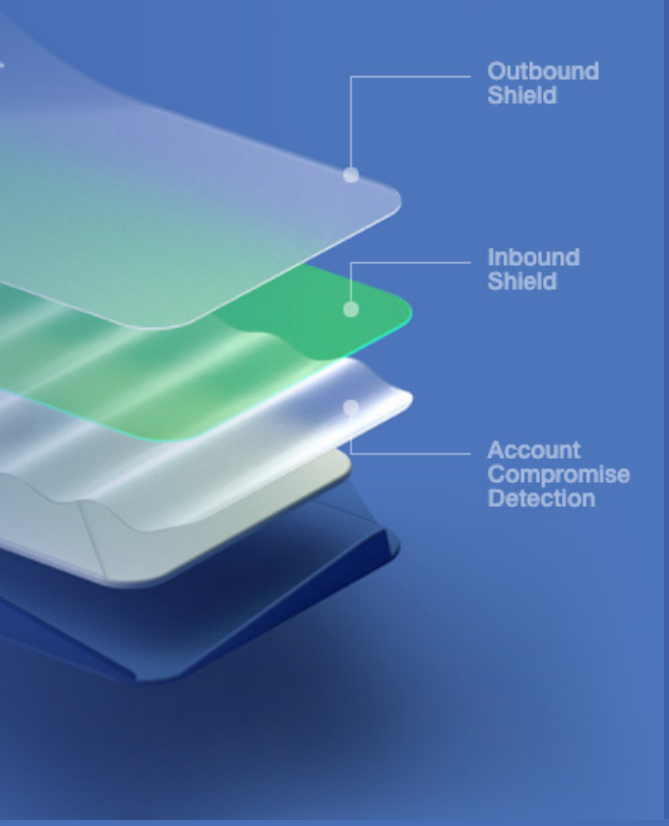
- "Use email security solutions that include anti-phishing technology for business email compromise (BEC) protection that use AI to detect communication patterns and conversation-style anomalies, as well as computer vision for inspecting suspect URLs."
- "Take advantage of emerging APIs to Integrate email events into a broader XDR or security information and event management (SIEM)/security orchestration, analytics and reporting (SOAR) strategy."
- "Invest in user education and implement standard operating procedures for handling financial and sensitive data transactions commonly targeted by impersonation attacks."
- "Ensure that email is included in your data protection strategy by examining the types or data shared externally via email and putting appropriate controls in place."
- "Implement DMARC for protection against domain spoofing attacks."
- "Don't rely on email as a way of carrying out secure transactions and sensitive data sharing by implementing data protection solutions."

"Use email security solutions that include anti-phishing technology for business email compromise (BEC) protection that use AI to detect communication patterns and conversation-style anomalies, as well as computer vision for inspecting suspect URLs. Consider products that also include context-aware banners to help reinforce security awareness training."

Source: Gartner, "Market Guide to Email Security", Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer 7 October 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. [2]

[2] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Trustifi: Cloud-based email security to keep your organization's data safe with complete protection from threats - all, while maintaining compliance



Outbound Shield™

Get peace of mind knowing that emails are automatically sent secured and compliant with easily enabled Data Classification and Data Loss Prevention Rules. Implementation takes minutes with Automated integrations for Microsoft Office 365, Exchange on-premise, and Google Workspace.

- EMAIL ENCRYPTION
- DATA LOSS PREVENTION
- MFA METHODS FOR RECIPIENT AUTHENTICATION
- COMPLIANCE MANAGEMENT WITH ONE-CLICK COMPLIANCE™
- TRACKING & POSTMARK PROOF
- SECURE STORAGE AND BACK-UP SYSTEM

Inbound Shield™

Keep your organization safe from targeted threats with powerful multi-layered scanning technology. Deeply analyze, detect, and classify the most advanced Phishing, Malicious, SPAM and even Gray emails.

Protection against:

- PHISHING
- SPOOFING
- IMPERSONATION
- BUSINESS EMAIL COMPROMISE
- MALWARE
- NEW THREATS, LIKE ZERO-DAY

Account Compromise Detection

AI Engines monitor user email behavior to detect anomalies in variables such as volume, context, devices, geo-location, type of sent emails, and more to detect, alert, and remediate when a user's mailbox has been compromised.

- ADVANCED MANAGEMENT PORTAL FOR TRACKING SUSPICIOUS ACTIVITY AND MANAGING USER PROFILES
- GEOLOCATION / NEW DEVICE DETECTION
- AUTOMATED ALERTS TO SYSTEM ADMINISTRATORS
- SUSPICIOUS ACTIVITY DETECTION

As a platform for advanced threat protection, Trustifi prevents data loss, adds encryption, and protects against sophisticated email threats. Other than the employees themselves, sensitive and proprietary data is the most valuable asset of any organization. Trustifi works hard to secure every organization's brand, reputation, and sensitive data. By encrypting email, providing an inbound shield that filters malicious email, and preventing data loss, Trustifi allows the clients to stay one step ahead of their attackers.

Overview of Gartner Market Guide for Email Security

Trustifi