



WHITE PAPER 2021

SEGS ARE DEAD

Secure Email Gateways (SEGs)
vs Cloud-based Email Security

Legacy on-premises SEG hardware
and software is giving way to cloud-
delivered email security solutions.



The email security industry is evolving away from SEGs. Get direct insight from Trustif's security experts and Forrester analysts, summarized from **The Forrester Now Tech and 2021 Wave: Enterprise Email Security Reports**

Forrester defines the enterprise email security market as –



Technologies that protect organizations' email communications in order to mitigate and lessen the impact of email-borne attacks. These consist of on-premises or cloud-based email gateways and solutions that integrate with cloud-based email infrastructure. Capabilities include antispam, antimalware, antiphishing, data loss prevention (DLP), encryption, phishing education, business email compromise (BEC) and spoofing protection, malicious URL detection and email authentication.

Forrester, Now Tech: Enterprise Email Providers, Q3 2020

FORRESTER®

On May 6, Forrester published its **The Forrester Wave™: Enterprise Email Security, Q2 2021 report** to help organizations and individuals understand the latest features and trends of the data security solutions out there.

In this report, Forrester says, “**Forrester’s 2021 Wave evaluation of the email security market revealed that**

Secure Email Gateways (SEGs) are slowly becoming dinosaurs

as customers turn to the native security capabilities of cloud email infrastructure providers like Google and Microsoft.

Security pros supplement these native capabilities with third-party solutions like cloud-native API-enabled email security (CAPES) solutions. Email security vendors ... respond by expanding API integrations **to integrate with email infrastructure vendors to deliver complementary capabilities and an additional layer of protection.”**


Forrester says that

“... hardware appliances are no longer recommended for anything but edge cases”.

Among the many reasons for this transitional trend towards cloud-delivered email security solutions is “the recent attacks targeting on-premises Microsoft Exchange Server vulnerabilities [which] are likely to drive more organizations to the cloud” and the fact that “vendors are now delivering [their cloud services directly from] customers’ geography of choice”.

Forrester suggests that, **“As a result of these trends, email content security customers should look for providers that ... Supplement their infrastructure provider’s capabilities with API integrations [and] ... Integrate with other security solutions in customer environments”.**





What are Secure Email Gateways?

Secure Email Gateways (SEGs) are the most common type of perimeter email security technology used to protect incoming and outgoing emails. They are widely used by enterprises to block BEC (Business Email Compromise) and cyber threats, such as phishing, ransomware, spam, trojan and other types of malware. According to Forrester in Now Tech: Enterprise Email Security Providers, Q3 2020, "Secure email gateways sit in front of an email infrastructure provider or in front of on-premises email infrastructure. They can deploy in the cloud or are delivered as on-premises hardware or software. SEGs deliver multiple inbound and outbound email security capabilities."

SEGs have gotten the job done for a long time, but are no longer able to keep up.

Inherently Designed to Protect Specific Perimeters

Secure Email Gateways (SEGs) are highly effective at securing on-premises email environments. **However, as email has moved to the cloud, these legacy dinosaurs have been no match for the virtuosity of nimble bad actors who use emails to continually setting traps for enterprises' employees, customers and business partners.**

SEGs are doing their utmost to adapt to this new ballgame to no avail. Because SEGs were inherently designed to protect a specifically defined perimeter, their ability to prevail against sophisticated, ever-changing multi-staged strategies and human manipulations has been insufficient and they have not been able to secure enterprises' most valuable resources – their people, funds and information.

SEGs are Looking for Traditional Threat Vectors

SEGs have been designed with two primary defense strategies – validation of an email's sender by authenticating its domain and the sender's reputation. SEGs also attempt to validate email content using content analysis tools, antiviruses threat intelligence and so on.

What has worked in the past (including signature and reputation-based defenses) is no longer a match for current threats.

With the increase of phishing attacks enterprises are re-examining their dependence on Secure Email Gateways (SEGs).

Email threats that did not exist before the prevalence of cloud email are not detected by these legacy solutions and a complete reinvention of email security strategy is necessary.



Lacking Sophisticated Detection Strategies

SEGs lack the sophisticated functionality required for detecting advanced threats.

Traditional gateways are only built to block malicious links and attachments. SEGs are able to verify whether the link to which an email connects or the file that is about to be downloaded doesn't contain viruses. Basically, a SEG acts like a firewall that scans content – it is very straightforward/binary.

SEGs lack the ability to examine emails at a granular level and investigate each individual user. For example, they lack the ability to recognize whether a specific contact or domain has been in touch previously or whether that contact is new. This lack of visibility contributes to significant increases in false positive and false negative detections.

Not Agile Enough

Threat actors can easily establish imposter or spoofed email accounts, domains and websites. Attacks spring up and shut down extremely quickly, making reputation-based detection ineffective.

Detecting modern phishing attacks requires computing intensive advanced email analysis and threat detection algorithms. These are tasks that appliance-based SEGs cannot handle due to their lack of the necessary processing horsepower.

SEGs move and react slowly. They only capture threat profiles and take action after identifying repeated threat samples from active, large-volume or high-impact attacks. This is in sharp contrast to phishing attacks that are typically specific, devious, low-volume, infrequent and targeted.

Not Detecting Imposter Emails

Phishing emails trick SEGs by spoofing trusted senders and websites. SEGs do not block or quarantine imposter emails that don't actually appear to be a threat.



Security pros know that despite best efforts, malicious emails will inevitably get through, so they need a layered approach that includes both prevention and response measures.”

Source: Forrester, “Now Tech: Enterprise Email Security Providers, Q3 2020”

In Summary

The fact is that emails are constantly getting by SEGs into enterprise inboxes –

No matter how much time, effort and technology an enterprise invests in its cybersecurity tools, phishing emails are still continuously landing in employees' inboxes, wreaking havoc on enterprise's finances, data and personnel resources.

The main reason that traditional email security is not able to defend against modern day phishing attacks is the nature of the beast that it is dealing with – phishing and their bad actors that are continually and quickly evolving.

Being dependent on yesterday's data, SEGs are only able to rally defenses after-the-fact.

These antiquated SEGs cannot compete with a solution that uses artificial intelligence and natural language processing to understand the context and the actual content of each email. Only these new sophisticated solutions will be able to detect when a person who seems to be the real-deal is asking for a wire transfer or some other suspicious request that they shouldn't be.



Trustifi's Email Relay

As more and more organizations make the transition from SEGs and on-premises hardware, the native security features of email infrastructure providers are being supplemented by Cloud-native API-enabled email security (CAPES) and cloud-based email security solutions.

Rapid adoption of cloud email infrastructure like Microsoft O365 and Google G Suite is forcing enterprises to move away from traditional secure email gateways and on-premises hardware. Organizations now often use the native capabilities of their email infrastructure provider, and then augment those protections with CAPES or cloud-based email filtering.

In Now Tech: Enterprise Email Security Providers, Q3 2020, Forrester identifies Trustifi's primary functionality segment as CAPES. Forrester considers CAPES to have high functionality in terms of email cloud integration and phishing protection -- with additional moderate functionalities, such as messaging cloud integration, malicious URL detection, incident response, and BEC and spoofing protection.



Trustifi's BEC – Three Step Protection

Trustifi provides end-to-end protection from BEC (Business Email Compromise) attacks.

Step 1

Protecting your outbound email is the first step in securing enterprise inboxes from BEC attack.



Hackers access unsecured outbound emails in order to learn how your users communicate and with whom. Cyber criminals watch your outbound email for the keys to the castle. They employ a variety of multi-stage email ploys containing sophisticated stories and buildups so that they can get their hands on the password credentials to log into enterprise accounts or to acquire unintended fund transfers. They often start with targeted phishing emails requesting that a victim protect their account by logging in to change their password or payment information.

Trustifi starts off its BEC protection by encrypting outbound emails, thus preventing hackers from accessing your organization's emails.

With Trustifi, automated DLP encryption uses a contextual framework to ensure confidential data is protected from the prying eyes of hackers.

Trustifi is the Simplest End-To-End Outbound Email Encryption Tool

Trustifi's outbound email features include –

1. Encryption

- NSA-grade end-to-end email encryption, with full inbound and outbound protection
- Secure mobile relay for full protection on any device
- Recall, block, modify, and set expirations for already sent and delivered emails

2. Data Loss Prevention

- 100% compliant with HIPAA/HITECH, PII, GDPR, FSA, FINRA, LGPD, CCPA, and more
- Know in real time when emails have been received, opened, and read with certified delivery and tracking
- Two-factor authentication on the recipient (even without registering)



Step 2

Inbound Phishing

Trustifi's Inbound Shield protects your inbox from malicious links, files, BEC attacks and spam by using dedicated AI and implementing a series of dynamic and comprehensive engines.

But real protection actually starts with a sophisticated email solution that can truly understand the content and context of each email and its user's behavior in order to detect sophisticated attacks.

Once hackers know with whom your users communicate, they will impersonate those known contacts with the intention to perform sensitive actions, such as money transfers and information exposures.

Watching multiple outbound emails enables them to identify the people in an organization who have the authority to request wire transfers and who has

the permissions to change credentials. Hackers can see who deals with credit cards, insurance and health information.

Having learned the terms and the style of language used by these people, as well as the appearance of their emails, bad actors become quite skilled at impersonating trusted organizations and executives, so that their email appear like they originated from these recognized trusted sources.

Trustifi uses its dedicated AI (Artificial Intelligence), ML (Machine Learning) and NLP (Natural Language Processing) to monitor emails in order to detect key phrases, such as requests for credentials, wire transfers, confidential information, Amazon gift cards and so on.

Upon detecting suspicious messages, Trustifi flags, warns and notifies relevant administrators regarding such emails.

3



Step 3

Email Account Compromise

After a user clicks on a malicious link or attachment, hackers can gain access to mailboxes in order to monitor, change and steal data and to secretly use this mailbox to generate more BEC attacks, while remaining undetected.

With Trustifi, machine learning technology creates baseline profiles of all users in order to detect an anomaly in user access or behavior. Trustifi gives administrators real-time notifications when an account has been compromised.

Advanced Threat Protection

- Malware and ransomware virus detection, prevention, protection, and alert
- Spoofing, phishing, and fraud detection
- Whitelisting and blacklisting options

Comparing SEGs vs Trustifi's Email-Relay

SEGs Introduce an Additional Point of Failure

The overall architectural structure of legacy SEG (Secure Email Gateway) inherently creates an additional point of failure. These gateways sit in between your organization and the outside world and basically serve as your firewall. This means that if this gateway goes offline, it becomes impossible for the organization using it to receive or send any email.



Trustifi is an email relay that sits on top of your mail exchange, so that email continues to flow no matter what. This architecture also enables Trustifi to leverage a wide variety of inherent benefits that enable it to enhance the security already provided by Microsoft, as opposed to moving all that to a third-party SEG.

Trustifi Ensures Email Continuity

An MX (Mail Exchange) record is an entry in your organization's DNS zone file that specifies the mail server to handle a domain's email. When an organization uses a SEG, in the event that the SEG goes down, the only way to restore email to the organization is for a skilled technician to go into the DNS management and to change all the MX records in order to alter the routes taken by emails.

Emails must first be rerouted away from the SEG. Configuring these changes may require some downtime. Later, after the SEG is back up again, these MX records must be changed back so that they point at the SEG. It may take 24 to 48 hours for all the email service providers to recognize that these records have been updated. Therefore, the organization's email may potentially be down for this entire period.



Trustifi ensures email continuity, because an email-relay inherently does not require any MX record changes since it sits directly on top of the Mail Exchange. Records are instead added and hosted under a subdomain, which is only used for Trustifi and does not affect the rest of the environment in any way. This architecture means that if Trustifi ever went off-line (which has never happened yet), enterprises will still be able to send and receive email.

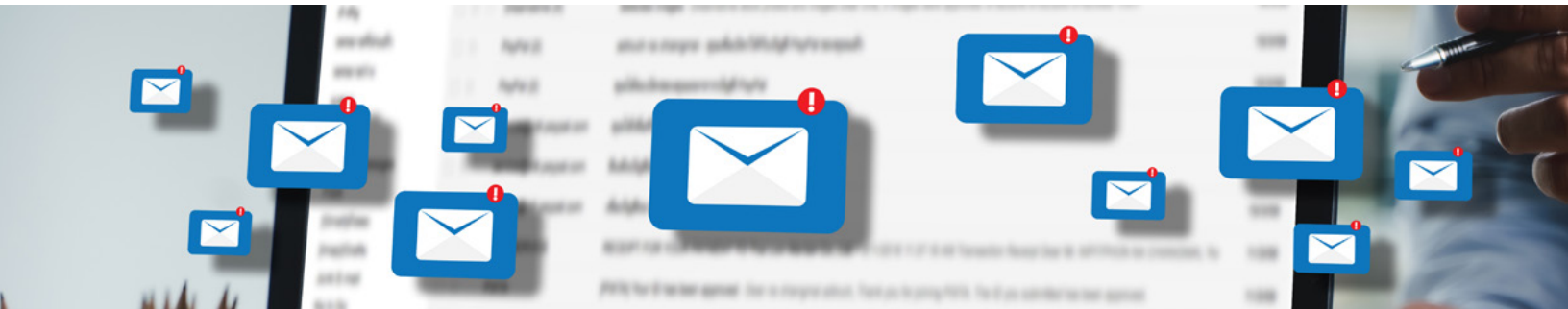
SEGs Require Highly Skilled Management Teams

SEGs require that the organization employ or have access to a highly skilled dedicated team that must perform a variety of management configuration tasks, such as log trace and so on. Such teams must invest many hours investigating incidents and then tuning the SEG's configuration in order to prevent follow-up attacks. Even the most dedicated team cannot configure away all the constantly evolving tactics that will be used in attacks that have not happened yet.



Trustifi was built with ease-of-use in mind for both end users and administrators. It is extremely user-friendly. Everything is based on simple If-Then statements that do not require set up by dedicated engineers, administrators or operators. Trustifi makes it easy for your IT security staff to get the security they need, while being straightforward, transparent and simple enough for end users to apply all this security at the click of a button.

Trustifi leads the market as the easiest to use and simplest deployment. All this while providing an extremely functionally-rich email security solution for both outbound and inbound email security.



SEG Visibility Enables Bad Actors to Easily Bypassing Known Vulnerabilities

Many SEGs have numerous vulnerabilities that are well known to hackers, and are used regularly to bypass SEGs. Malicious actors can easily detect which SEG brand an email recipient is using (for example, by examining the IP information of the destination to which they are sending). This gives bad actors a significant advantage because they can easily customize the attack to be used according to the specific vulnerabilities of the enterprise's SEG.



Attackers are Continually Outsmarting SEG Protection

SEGs lack advanced-threat detection features and the sophistication required to identify socially engineered attacks. Therefore, they miss a wide variety of information types, such as contacts, conversations and so on. Traditional gateways only block traditional payloads, such as links, files and attachments. They lack the ability to examine emails at a granular level and to investigate each individual user. For example, they lack the ability to recognize whether a specific contact or domain has been in touch previously or whether they are a new contact. This lack of visibility contributes to significant increases in false positive and false negative detections.

Malicious actors are continually changing tactics and adapting phishing attacks to SEG security advances.

SEGs rely heavily on weak and old-fashioned filters, such as IP reputations, global blacklists and signatures. They do not catch zero-day phishing sites.



Trustifi sophisticated array of artificial intelligence and natural language processing mechanisms proactively detect phishing strategies and provide early alerts regarding malicious campaigns in progress.

Overall Security

The authentication method used between a SEG and its mail server is typically quite weak and is often based on IP whitelisting. This requires detailed configuration setups in which mistakes can easily be made, thus leaving the organization exposed. Research shows that they can typically be easily bypassed by malicious actors (for example by sending a bypass message) in order to send emails directly to the mail server and release a business email compromise attack.



Trustifi scans 100% of emails and cannot be bypassed regardless of any configuration setups that are defined (mistaken or not).

Manual Updates

SEGs are usually deployed as an on-prem solution, which typically requires manual updates.



Trustifi is a SaaS (Software as a Service) solution that is frequently, constantly and automatically updated with the latest detection technology in real time, thus always providing your organization with real-time protection by the most advanced zero-day technology.

Mail Delivery Delays

The processing and analysis time required by many SEG tools and the extra hop through which these emails must traverse introduces delays into an organization's email flow. The introduction of this delivery lag time typically forces organizations to choose between security and speed. Users often report significant reductions in their ability to use email for realtime communications, even when their email security tools are not struggling with downtime or overload. In addition, SEGs tend to produce redundant functionalities with Exchange. Often times, this requires doing things twice.



Trustifi sits directly on the mail exchange and thus is able to receive emails almost instantaneously.



Limited Remediation Capabilities

Given the in-line nature of SEGs, once a message has moved into a user's inbox, there are typically no options for post-delivery modifications or remediation actions without employing expensive and poorly integrated add-on tools.



Trustifi's partnership with Microsoft enables its APIs to pull emails out of live inboxes – even after they have landed there. For example, emails that are already in enterprise inboxes can be pulled out of one or all of them after a zero-day attack has been detected (which may include pieces of malicious content). Organizations may also decide to use it upon detecting slanderous or confidential information in inboxes. Trustifi enables organizations to easily pull this harmful information out of inboxes without affecting any other aspect of the enterprise and without the employees even knowing.

About Trustifi

Trustifi is a cyber security firm featuring solutions delivered on a software as a service platform.

It's relay-based solutions use a proprietary cloud storage system that enables an extensive range of control over sent mail, thereby improving security. The solutions encrypt emails in the cloud, before those messages pass through the recipient's gateway. This gives users a considerable range of capabilities, allowing them to retract, change or block sent content, swap out attachments, set expiration rules or alter the recipient list within messages they've sent, according to the company.

Trustifi leads the market with the easiest to use and deploy email security products providing both inbound and outbound email security from a single vendor. The most valuable asset to any organization, other than its employees, is the data contained in its email, and Trustifi's key objective is keeping clients' data, reputation, and brand safe from all threats related to email. With Trustifi's Inbound Shield, Data Loss Prevention, and Email Encryption, clients are always one step ahead of attackers

For more information and to get a demo or pricing, contact:

844- 235-0084

Sales@trustificorp.com

www.Trustifi.com

We'd love to hear from you!

