White Paper by Expert Insights

Trustifi Email Security

A Comprehensive Deep Dive

Published
July 2021

Expert Insights

Sponsored by
Trustifi Security

01 Executive Summary

Introduction

Over the course of the past year, we've become more reliant on digital communications than ever before. As the pandemic pushed businesses out of the office and into a hybrid way of working, we've come to depend on technologies like email for critical business functions: signing contracts, sharing documents––even just chatting to our team about the game results.

But unfortunately, the more we rely on email, the more we put our data at risk. Email is a notoriously unsecure method of communication. When emails are sent from one person to another, they can bounce around multiple unsecured servers, where any malicious actors can intercept email data and attachments. In addition, sophisticated cyber-attacks like phishing, ransomware and business email compromise all exploit the email channel to steal and gain access to personal and private information.

For these reasons, and many more, email security should be a top priority for all organizations. Email security should comprise of two key aspects: protection against inbound malicious threats, like phishing, ransomware and account compromise, and encryption, which secures outbound email content by ensuring only the intended recipient can access sent messages.

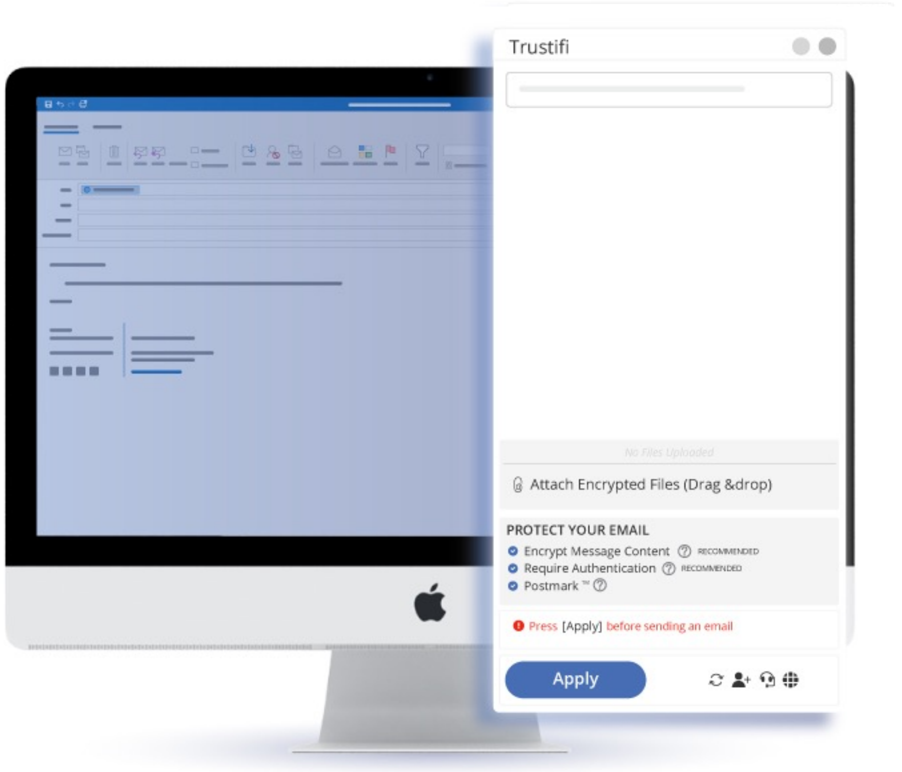
In this white paper, we'll take an in-depth look at one particular email security provider: Trustifi.

Trustifi offer a powerful suite of features that help organizations to defend themselves against incoming email threats, meet compliance needs and prevent data loss in the email channel. We will examine Trustifi's key features and benefits to help you decide if Trustifi is the right email security solution for your organization.

02 Who Are Trustifi?

Trustifi is a comprehensive, cloud-based email security solution that helps keep email data safe and secure. Founded in 2017, Trustifi has quickly gained recognition in the email space, being recently featured in Forrester’s 2020 Now Tech Enterprise Email Security Providers report. Trustifi provides highly secure email encryption that helps safeguard against data loss and protect outbound emails. It also features inbound threat protection tools to defend against spam, malware, phishing, account compromise, and other email threats.

Trustifi has focussed on simplicity and ease of use in their encryption platform, making it seamless for end users to send and receive emails, as well as for admins to easily onboard and manage users. Trustifi also provides comprehensive data loss prevention (DLP), with detailed reporting and control over inbound and outbound email. This means the solution is ideal for organizations looking to implement fully compliant email encryption. Trustifi is compliant with PCI, GPDPR, HIPAA, CCPA and more.


Trustifi
No Files Uploaded
Attach Encrypted Files (Drag &drop)
PROTECT YOUR EMAIL
Encrypt Message Content RECOMMENDED
Require Authentication RECOMMENDED
Postmark ™
Apply

Press [Apply] before sending an email

03 Why Use Trustifi?

There are a number of key use cases for partnering with Trustifi for both email encryption, and in-bound email protection.

Simplified Email Encryption

If your organization regularly uses email to send and receive personal information or sensitive data, it's critical you have a secure email encryption solution in place. Trustifi provides AES-256-bit encryption, providing end-to-end protection for email messages and ensuring all email data is totally protected from malicious third parties.

But simply having the ability to send emails securely is only half the battle—the other half is ensuring that people actually use encryption. Many large encryption providers use "secure web portals", which require recipients to log into an encrypted web portal to view, send and reply to encrypted email. While this is fine from a security point of view, it's cumbersome and time consuming, and can put people off sending encrypted emails in the first place.

Trustifi has an innovative approach to encryption, enabling the use of multi-factor authentication to ensure that emails are kept fully secure and can only be accessed by their intended recipients. Senders can encrypt emails just a simple click of a button. Recipients can securely and easily access encrypted emails in their inbox, after verifying their identity with an additional factor of authentication, such as an SMS passcode or a fingerprint scan, without having to make any new accounts or log into any third-party systems. This makes encryption much easier, so users are far more likely to use it.

> "Trustifi has an innovative approach to encryption, enabling the use of multi-factor authentication to ensure that emails are kept fully secure."

Mitigating Human Error

Human error accounts for about 60% of all cyberattacks. More often than not, data breaches are not caused by malicious cybercriminals working for nefarious nation states, or genius hackers looking to make a quick buck by breaking into your company systems. Instead, breaches happen because of everyday people making mistakes; small errors that can put personal information at risk and potentially incur hefty fines in the process.

Email in particular is a channel where mistakes can easily be made, with potentially harmful consequences for your business. Sending a sensitive attachment to the wrong recipient, sending financial information like credit card details over email, and falling for social engineering attempts via email are all common ways that mistakes can lead to data breaches and cyberattacks, potentially costing your organization thousands to fix.

Trustifi provides a comprehensive solution to the problem of human error in email with data loss protection. Trustifi's systems automatically scan and encrypt outgoing email messages according to admin policies, so any emails that contain sensitive information are automatically secured. This includes emails with sensitive attachments (such as those containing social security numbers), emails containing financial information or credit card numbers, and emails containing sensitive company intellectual property.

This process is completely automated and markedly reduces the likelihood of human error causing data breaches. In addition, Trustifi allows end users far more control over email than otherwise possible. End users can recall email messages, revoke access to attachments and prevent email forwarding—so if email messages are sent by mistake, they can quickly be retrieved. Trustifi also provides full reporting into encrypted emails, so you can identify people with risky email behaviours and mitigate against data loss in the future.

Protection Against Email Threats

Email threats continue to rise at an alarming rate. In fact, 94% of malware is delivered by email, and phishing attacks account for 80% of reported security breaches [1]. According to the FBI, email threats doubled over the course of the past year, with ransomware also up by 20% [2].

It can be a major challenge for organizations to protect themselves against advanced email threats. Secure email gateway technologies can be complex and expensive and will often struggle to block sophisticated malicious emails and social engineering attacks.

Trustifi's inbound email filtering provides powerful phishing protection and is well suited to Office 365 and Google Workspace. It provides comprehensive protection against inbound and outbound email threats, supporting DMARC analysis and sender domain reputation filtering.

Crucially, the service is easy to install and doesn't require any architecture changes, so you get peace of mind that your emails are protected, without any complex set up or concerns about missing email messages.

> "94% of malware is delivered by email, and phishing attacks account for 80% of reported security breaches."

Legal Compliance

Data privacy is a big deal, and governments around the world are increasingly recognizing the need for regulation to ensure that private companies are dealing with data responsibly and securely. In Europe, this has led to the passing of GDPR, replicated by many other governments around the world. In the United States, there are a number of state-specific data regulation bills being passed or debated —such as CCPA.

In addition to general data privacy acts, there are many specific industries that have legal regulations that must be followed. In healthcare, for example, HIPAA recommends encrypting the personal healthcare information (PHI) of patients, and similar regulations apply in both the legal and financial sectors when it comes to sending personally identifiable information, especially over unsecured channels like email.

04 Trustifi Features

Secure, End-To-End Encryption With MFA

Trustifi provides highly secure NIST-approved email encryption. Encrypted email messages and content are stored in secure databases in Trustifi's private cloud. Data is secured using an end-to-end AES 256-bit algorithm, which ensures that only the intended recipient can access encrypted email messages––even Trustifi can't view the content of encrypted email messages.

Enhancing the security of encrypted email messages is the use of multi-factor authentication (MFA), which makes accessing encrypted email more secure, as well as easier for the recipient, as there is no need to create a separate account or log in to a third-party web portal. Instead, users are asked to verify their identity with an additional factor of authentication. Trustifi offers a number of MFA options to choose from, including SMS pin-codes, automated phone calls, biometric scans, or a passcode agreed in a separate email.

It's extremely easy and simple to use Trustifi's email encryption platform—for both senders and recipients. Senders can encrypt emails directly from their email client with the click of a button, and recipients can access and reply to encrypted email directly from their inbox. Recipients can send encrypted email and attachments back to the sender, even if they don't have Trustifi installed. Trustifi provides end users and recipients with important information about encrypted email, including showing encrypted attachments without requiring a download, which can help to prevent phishing attacks.

> "It's extremely easy and simple to use Trustifi's email encryption platform—for both senders and recipients."

One-Click Legal Compliance

Trustifi provides One-Click Compliance for healthcare and financial services, removing liability and securing corporate data by using AI systems to automatically encrypt emails containing personal information and HIPAA sensitive information. This feature can be enabled with just the click of a button, ensuring that your organization remains legally compliant and preventing hefty fines against your organization, while taking pressure off your end users and reducing complexity for IT admins.

Trustifi helps customers become fully compliant with PII, HIPAA/HTECH, GDPR, FSA, FINRA, LGPD CCPA and more, with full tracking and auditing into email delivery. Trustifi simplifies the entire compliance process so your organization can meet all its compliance obligations, within your existing email infrastructure.

Data Loss Prevention

Trustifi helps organizations to meet legal compliance regulations and ensures that sensitive information is kept secure with comprehensive Data Loss Prevention (DLP).

> “If an email is sent without being encrypted, Trustifi will automatically encrypt the message.”

Trustifi’s powerful data sensitivity, detection classification and scoring algorithms scan outbound email content in real-time, looking for these types of sensitive information. When a user composes an email containing sensitive information, the system displays a pop-up, warning the user that information contained in the message should be encrypted. If the email is sent by the user without being encrypted, Trustifi will automatically encrypt the message, ensuring that no sensitive information will be sent without first being secured.

These rules can be configured from within the admin console, which is modern and easy to navigate. From this console, admins can also onboard users, configure polices, view and release quarantined emails, view reports and audits and raise support tickets if needed.

Advanced Threat Protection

Trustifi provides powerful inbound threat protection as part of its Inbound Shield platform. This involves comprehensives email scanning to identify and remove sophisticated email threats including phishing, spoofing and impersonation attempts, business email compromise, spam, malware, and more. The platform includes an admin dashboard, where you can see reports into email threats, and users can release quarantined emails when needed; these are held for 60 days before being deleted.

Admins can set allow and deny lists to prevent malicious email messages and reduce spam, and end users can report malicious messages from directly within their email inbox.

Trustifi's phishing protection includes URL scanning, business email compromise protection and impersonation protection for brands, user domains and contracts. All aspects of email messages, including headers, content, links and attachments are scanned, so emails can be assigned a safety score. If a malicious email sender or message is detected, a pop-up in the email inbox warns users against replying, clicking on links, or opening any attachments.

In addition, Trustifi provides outbound email protection and authentication. It supports DMARC, DKIM and SPF analysis to prevent brand spoofing, and provides sender domain reputation filtering. As we've already covered, emails containing any sensitive email data are automatically encrypted, helping to reduce the risk of successful spear-phishing and account compromise attacks.

Admins can manage user mailboxes and configure the system from the admin console. Admins can set policies on how to handle malicious emails and implement rules to automatically block certain email domains or file types. These rules can be applied to all users, or to certain groups.

Unlike traditional email gateways, Trustifi's email protection is easy to deploy and well suited to cloud-based email platforms like Office 365 and Google Workspace. There are no infrastructure changes needed or MX record redirects, the solution is deployed directly via API integration, so users can be onboarded in less than five minutes.

End-User Controls

As we've covered, it's easy for end users to send encrypted email with Trustifi. The service works natively within Office 365 and Google Workspace, and users can send encrypted email with just the click of a button. But alongside encryption, Trustifi also provides end users with a range of advanced email features that can be used from directly within the mail client.

End users can manage which method of authentication to use, including PIN codes or custom passwords. They can also set expiration dates and recalls for email messages, in case data was sent in error–– and they can even edit email content after it has been sent. To maximize security, end users can disable email printing, only allow emails to be opened once, and limit email forwarding. Users can also easily customize the look and feel of encrypted emails, so that email content always looks professional and correctly formatted.

In addition, Trustifi makes it much easier to track engagement with emails. Users can get notified when the recipient opens an encrypted email, can track when links have been clicked, and can be notified when recipients share or forward encrypted email content.

There's a huge amount of granularity in this data––users can track the exact times emails were opened, how many times the message was read, even what device was used to read the email.

Finally, Trustifi makes it far easier for users to send and digitally sign legal documents via email. Trustifi's Postmarked Email service is a federally accepted method of sending legal documents online. Users can easily digitally sign email content and attachments and get a timestamp of sending delivered straight to their inbox.

Auditing And Reporting

Trustifi allows enterprise administrators to generate detailed reports containing statistics over email usage and when encrypted emails are being sent. Trustifi also provides reporting into inbound email threats, and allows admins to monitor and investigate user-reported email threats. Within the admin console, Trustifi provides an email logging system which monitors and tracks every action performed by admins to meet compliance needs.

In addition, users can get real-time reports into when their encrypted emails have been received, opened and read.

Deployment

Trustifi is quick and easy to deploy in cloud-based email environments like Office 365 and Google Workspace. It does not require any MX record redirects or mailbox configurations. The service is deployed via API integration for cloud applications. This means that it can be rolled out organization-wide quickly (usually just a few minutes), with easy user onboarding with Azure Active Directory.

For end users, it's simple to get the service up and running. When users are enrolled, they will receive a verification email, which will give them access to the Trustifi portal and take them through the process of sending an encrypted email. No additional software is needed to send encrypted email, and Office 365 and Google Workspace users can send encrypted email directly from their inbox, using extensions that can be installed in seconds from the Outlook 365 and the Chrome stores respectively.

Support

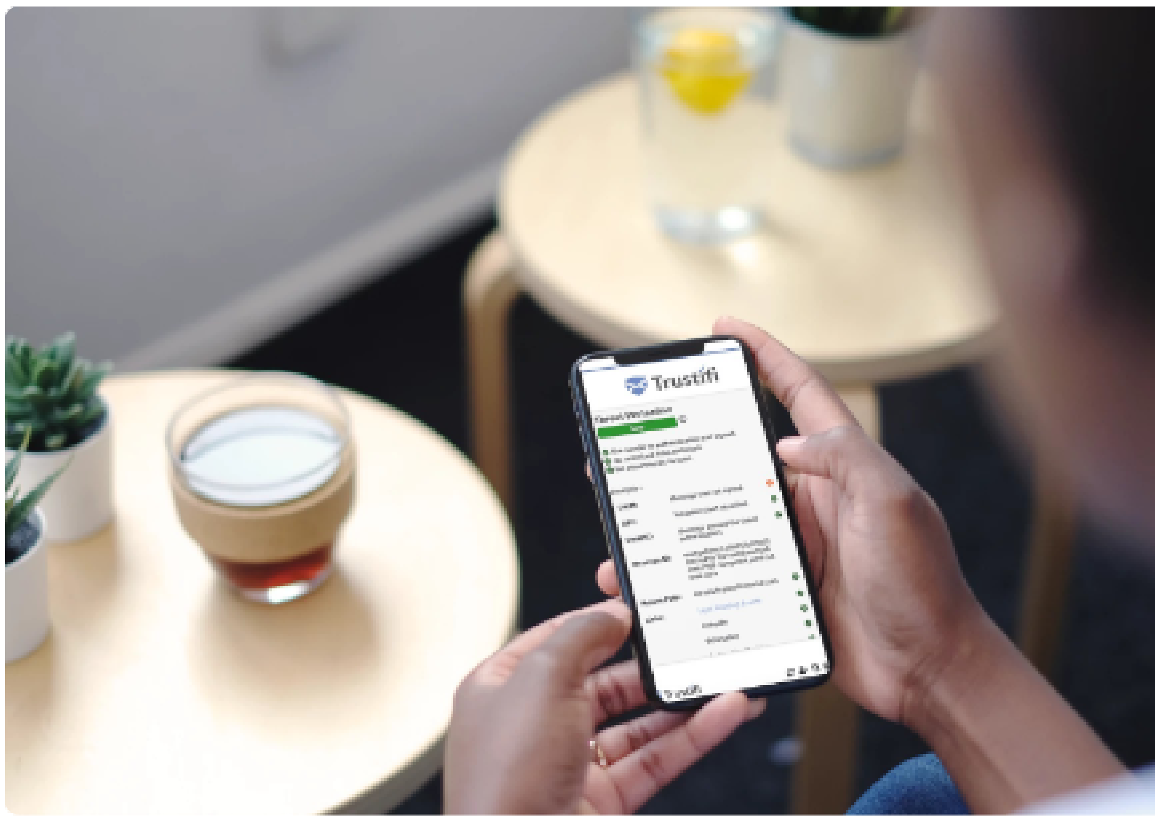
Trustifi provides comprehensive phone and email support. They also offer a detailed FAQ forum for users, including guides to API integrations, a technical resource centre, and a number of technical documents that detail how to configure and properly manage the service.

Trustifi provides technical support with the integration process and can also provide tailor-made security solutions upon request.

For MSPs and partners, Trustifi provides a number of key resources, including marketing materials, case studies and more to support your business growth.

> "When you send an email with Trustifi, you can easily encrypt using a plugin, you can see where and when that email was opened, you can go back and edit sent messages if you accidentally send the wrong attachment." [3]

Rom Hendler, CEO, Trustifi



05 Our Thoughts

Expert Insights:

One of the major benefits of Trustifi is the ease of accessing and replying to encrypted emails; the main weakness of many encryption solutions is that they often require users to manage over complex and cumbersome systems. Recipients often need to log into third party systems to access encrypted messages, and senders can get lost in settings menus just trying to send an email.

Trustifi provides an elegant solution to this with their multi-factor authentication technology, which ensures emails are kept secure at every state of email delivery, while also allowing recipients to easily access and reply to encrypted emails from directly within their email inbox. Users also get far more control over encrypted emails; they can see when emails have been opened, limit email forward, revoke access to email and even change the contents of emails after they have been sent.

Another benefit of Trustifi is their inbound email protection, designed to combat phishing, spear-phishing and business email compromise. Trustifi provides malicious content prevention, detection and protection, alongside end-user reporting and DMARC, so users can benefit from multi-layered email protection in the cloud. The whole platform can be very easily deployed and configured, with no changes needed to your email infrastructure.

Trustifi is an ideal solution for Office 365 and Google Workspace users looking for an all-in-one solution for email security and encryption. We'd recommend the solution in particular to SMBs and users in the healthcare, legal and financial sectors looking for a powerful, easy to use encryption solution.

06

Sponsor Of This White Paper

Trustifi

Trustifi is a leading encryption provider that enables organizations to leverage highly secure and hassle-free email encryption with all the key features we've just outlined. Their solution is a strong fit for those in the legal sector as it's extremely easy to use, both to send and receive encrypted emails, and is fully legally compliant.

Trustifi is fully compliant with HIPAA, GDPR, HITECH and automatically encrypts all private data, ensuring you can have peace-of-mind you are complying with all legal regulations when it comes to governing email data.

Trustifi

www.trustifi.com
6543 S Las Vegas Blvd,
Las Vegas, NV 89119
sales@trustificorp.com
info@trustificorp.com
+1-844-235-0084

07 About Expert Insights

About Expert Insights

Expert Insights is a global, independent resource for organizations around the world to research and compare business IT solutions and services. Our number one goal is to help businesses research and find the right solutions to solve their security problems. To help organizations achieve this, our independent editorial team have created buyers' guides, resources, vendor comparisons and interviewed industry leaders, so that our users can research and compare solutions on one technology-focussed platform.

References

1. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

2. https://www.digitaluppercut.com/2021/04/fbi-reports-cybercrime-was-up-in-2020/

3. https://expertinsights.com/insights/my-people-are-my-greatest-strength-how-empowering-users-can-improve-email-security/

Expert Insights Ltd. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any laws referenced herein. Expert Insights Ltd. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.