Trustifi

TRUSTIFI VS. ZIX

COMPETITIVE ANALYSIS 2020

www.**trustifi**.com

Trustifi vs. Zix

This competitive analysis compares Trustifi's email security solution (Trustifi.com) with the email security solution provided by Zix (zix.com).

Zix is a security technology company that provides email encryption services, email Data Loss Prevention (DLP), advanced threat protection, email archiving and email message privacy.

Zix provides many impressive email encryption and threat protection features that are on par with Trustifi. This paper describes multiple comparatively superior usability features and various unique functionalities provided by Trustifi's email security solution that Zix does not have.

WHY CHOOSE TRUSTIFI ?

COMPETITIVE ANALYSIS 2020

Trustifi

IT'S EASY FOR EMAIL USERS!

"With Trustifi, you don't have to choose between security and usability."

Mason Moore

IT Manager at Independent Financial Group, LLC based in Del Mar, San Diego, California

Trustifi is the easiest and most comprehensive email security solution on the market.

Sending and receiving secure emails is quick and simple enough to ensure employee compliance and efficiency.

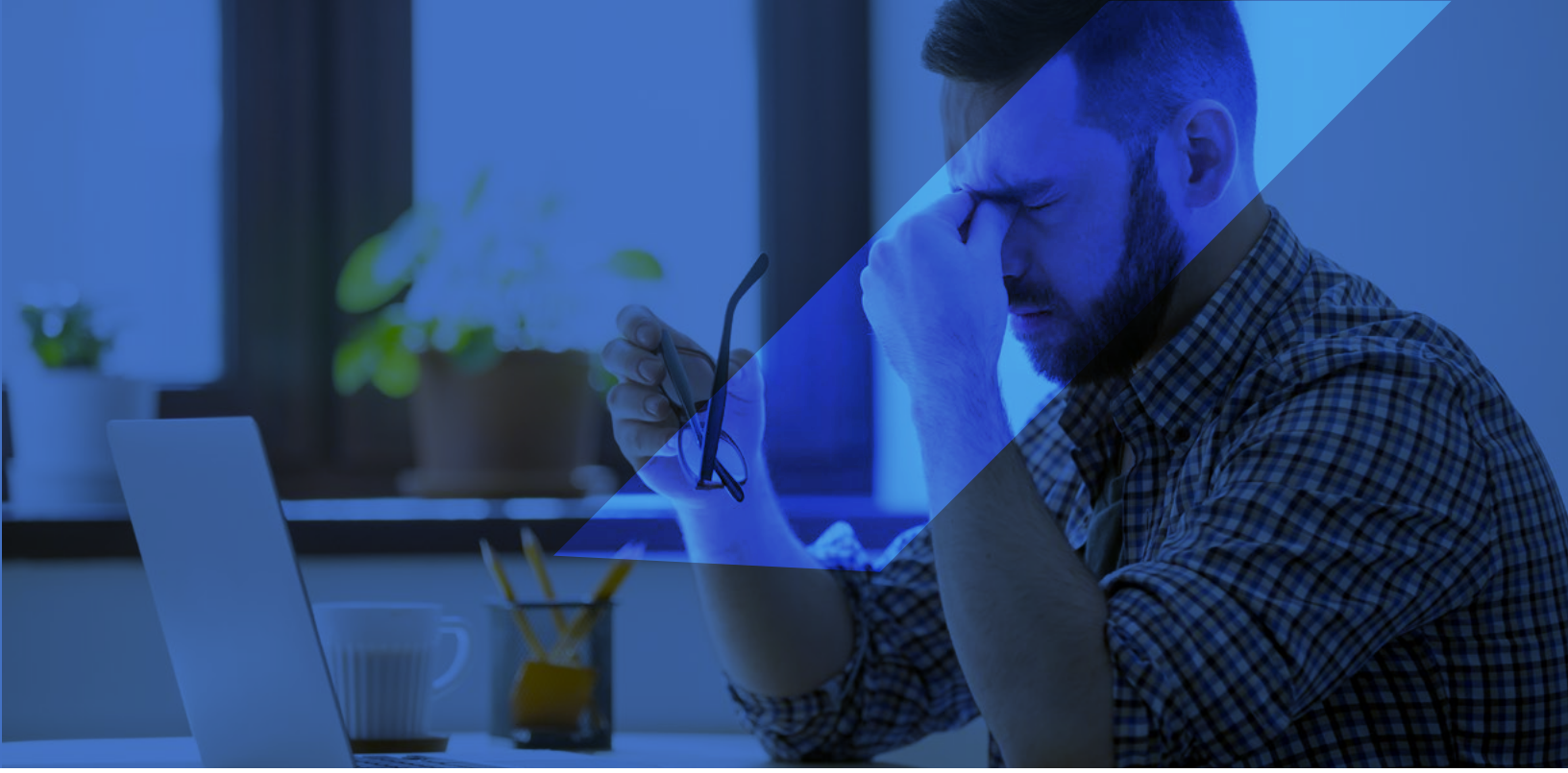
Trustifi automatically and transparently integrates into end users' standard email applications and workflows, while automating and hiding the corporate policies, protocols, guidelines, actions, alerts and other intricacies that it handles behind the scenes.

Sender and Recipient Security at the Click of a Button

Trustifi is unmatched in its simplicity. It provides a full-featured set of security features with unrivaled quick and easy usability.

- **Email senders can send fully secure encrypted emails** at the click of a button from their standard email application using a Trustifi add-on.
- **Email recipients can simply click a button to decrypt secure emails** and to send encrypted secure replies, even if they are not Trustifi users.

There is no need to sign up or register for anything or to create a special username and password. Even non-Trustifi email users can receive, decrypt, and resend secure encrypted emails without having to sign up or register for anything.



Zix – Requires Registration

Both Zix and Trustifi enable the transparent/automatic encryption of email messages and their attachments according to predefined security policies and/or the manual encryption of the email and its attachments.

However, there is a major difference for non-Zix email recipients. In order for a non-Zix email recipients to access a secure email sent by a Zix user, they must register their email address, create a new username and password for the Zix portal and then use their credentials in a separate login process each time they want to read a secure email.

> Mason Moore said about Trustifi that, "***One of the main features that our email users liked is not having to deal with a separate login. With Trustifi you simply open your email application and press a button to encrypt/decrypt email sending/receiving***."

Zix – Does Not Enable Non-Zix Recipients to Send Secure Email

In addition, Zix does not provide the option for non-Zix email recipients to send back a secure (encrypted) email.

UNIQUE EMAIL USER FEATURES

2

Trustifi provides an entire suite of additional features that do not exist in Zix, such as the ability to control and track email for each –

- Email recipient.
- Email-element, meaning message, attachment or link.
- Email action, such as opening the email and its attachments, reading/ decrypting, clicking links, printing and so on.

PRODUCTIVITY FOCUSED EMAIL SECURITY FEATURES

Recall and Email/Attachment Access Control

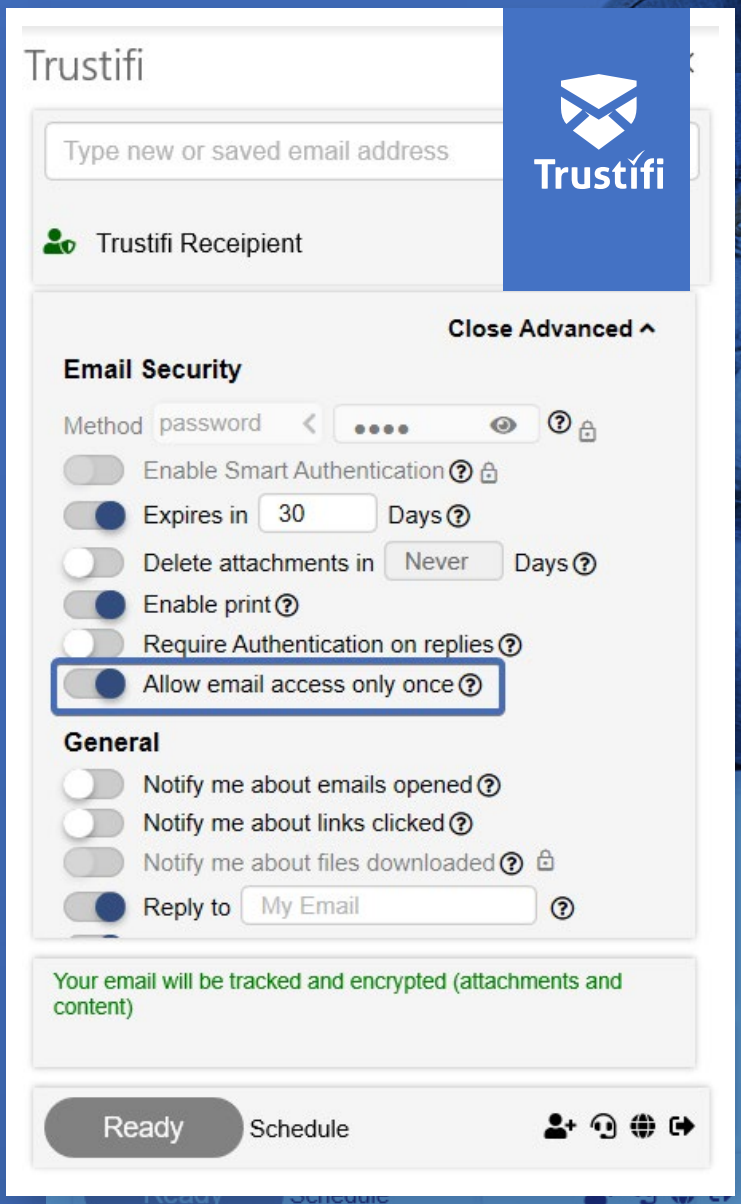
Trustifi provides a rich variety of recall and access control options even after an email has landed in a recipients' inbox.

Trustifi users do not have to block an entire email and then to create a new one. This saves the confusion created by sending multiple emails covering the same topic to the same recipient.

Trustifi provides granular options for recalling, blocking and modifying each component of a secure email sent from Trustifi, including blocking the message and each attachment separately per recipient. Trustifi users can also add, delete, and update attachments, at any time without affecting the actual message part of the email.

Trustifi not only enables a sender to block access to unopened email messages and attachments, Trustifi even controls access to messages and attachments that have already been read (decrypted) by the recipient and those that have been forwarded by recipients.

Trustifi also provides the option to specify how many times an email message and/or attachment can be viewed. For example, you can define that an attachment can only be viewed once and that after that, no access is allowed.

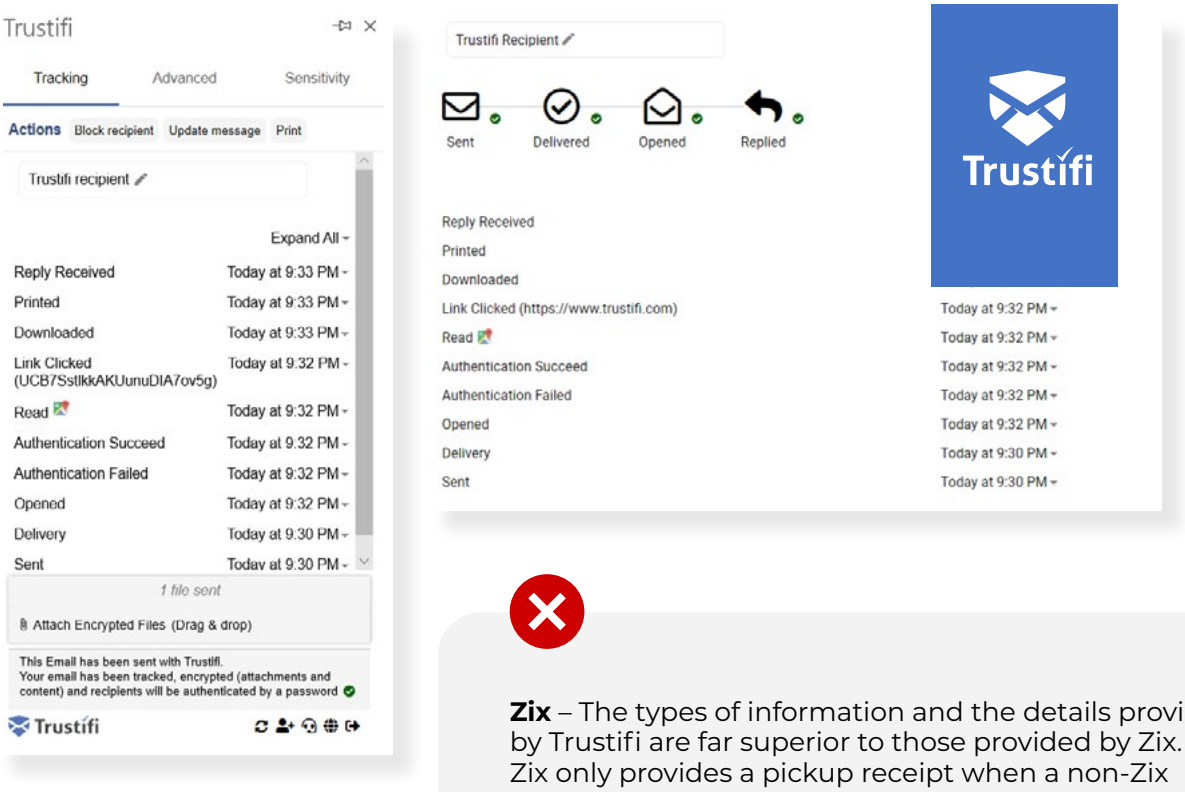


Zix – Only enables the blocking/ recall of an entire message, including all its attachments. Zix does not support granular blocking, per user, per attachment, per recipient or the deletion/ addition of attachments from/to an email. This forces Zix users to block/remove an entire email and then to send the entire email again with the corrected attachments, which is typically quite confusing for recipients.

TRACKING EMAIL ACCESS AND ACTIONS

Trustifi enables you to track a wide variety of email events.

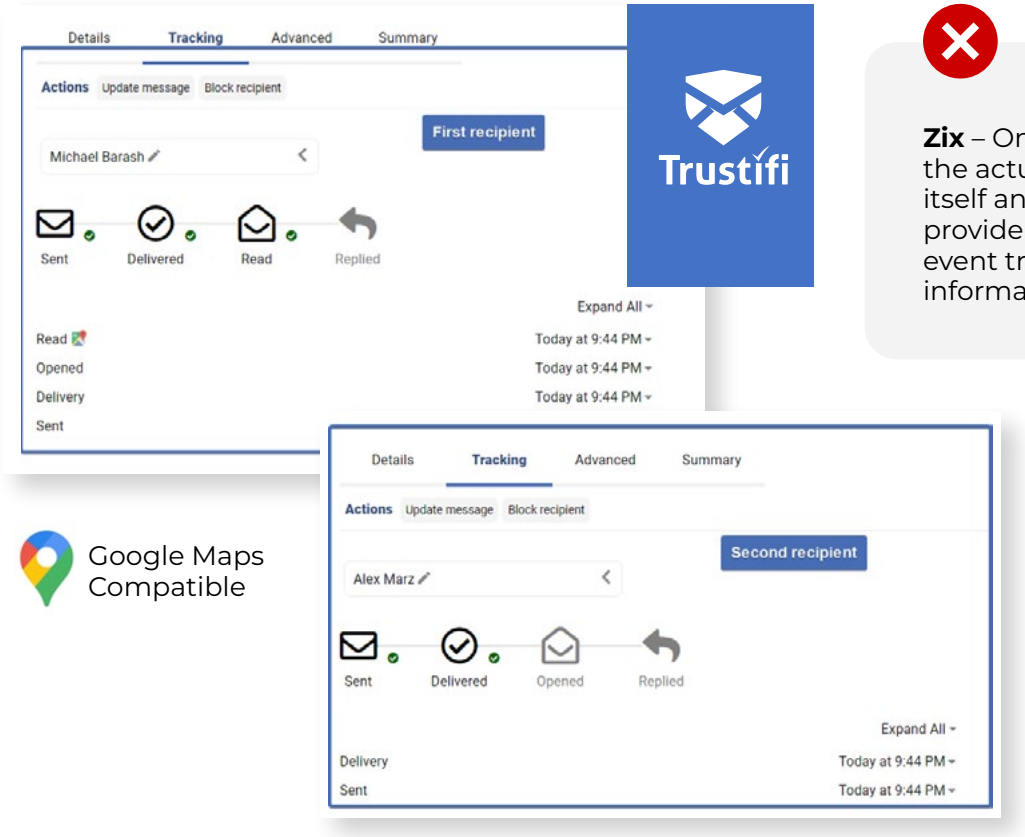
Trustifi provides a single easily accessible web interface that shows all email lifecycle events, per message, per attachment, per link and per recipient. These events indicate whether each element was opened, who opened it, when it was opened, whether the email/attachment was decrypted and by whom, who downloaded an attachment and when, which links were clicked and by whom, who printed the email and when, whether someone tried to authenticate or whether someone failed to decrypt and so on.



Zix – The types of information and the details provided by Trustifi are far superior to those provided by Zix. Zix only provides a pickup receipt when a non-Zix email recipient opens the email. The only information provided is the email subject, the sender and the recipient mail address. In addition, Zix does not provide any link between the pickup receipt and the email that was sent. Upon receiving a pickup receipt, in order for an email sender to see the original email, they must search their inbox for it themselves.

TRACKING PER RECIPIENT

Trustifi provides total awareness of all the email events described above per recipient! This goes for the message, for each of its attachments, its links and for every action performed by each recipient. Plus, users can see geographically exactly where their recipient has opened their email with Google Maps.



Google Maps Compatible

Zix – Only tracks the actual email itself and does not provide per recipient event tracking information.

EMAIL EXPIRATION DATE CONTROL

Trustifi enables users to define an expiration date for the content of any email and attachment and for any recipient action, such as reading, decrypting, clicking a link, printing and so on.

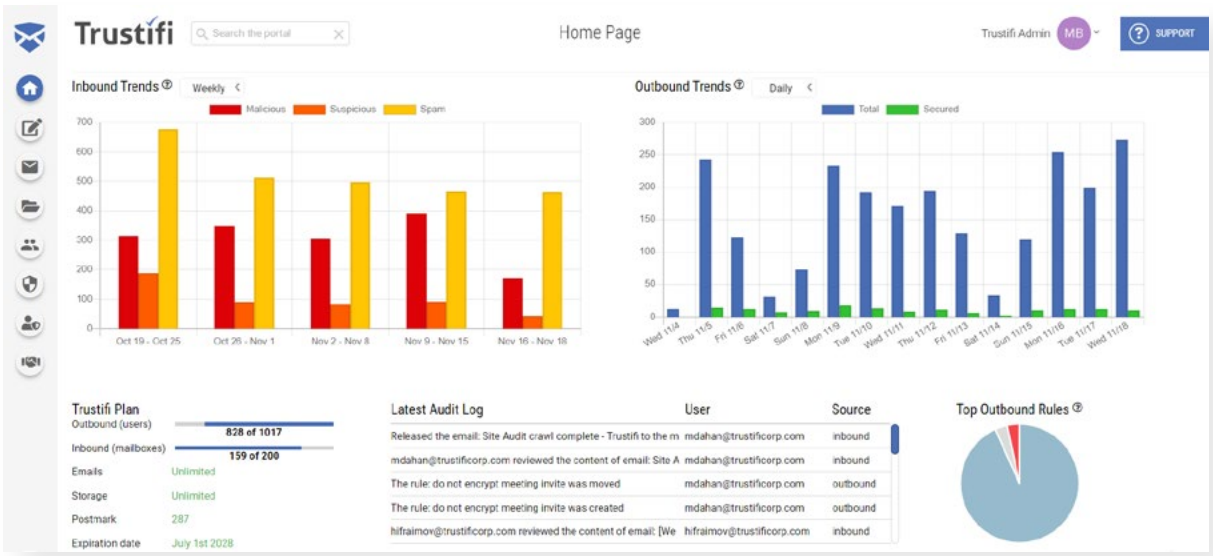
Zix – Does not provide this option.

UNIQUE EMAIL SECURITY ADMINISTRATION FEATURES

For security administrators, Trustifi makes it easy to get the security they need (including alerts, traceability, monitoring and awareness), while being both straightforward and transparent.

A SINGLE COMPREHENSIVE ADMINISTRATOR PORTAL

Trustifi provides all its services in a single holistic interface that simplifies management and use.



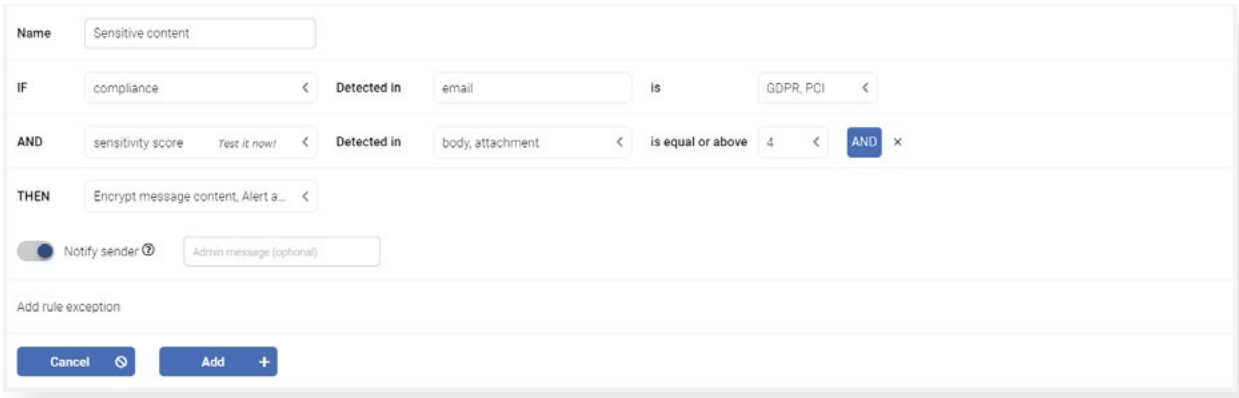
Zix – Has separate management portals for each of their services and features.

DEFINING EMAIL HANDLING

Trustifi provides administrators with a significantly superior array of rule and policy configuration options for automating and controlling the security of your inbound and outbound emails in a simple-to-use, but feature-rich web interface. Administrators can configure various types of rules and policies for specific actions based on domains, regulation/compliance, custom keywords, preset sensitive rules, email headers, get automated daily/weekly/monthly and real-time reports, and more.

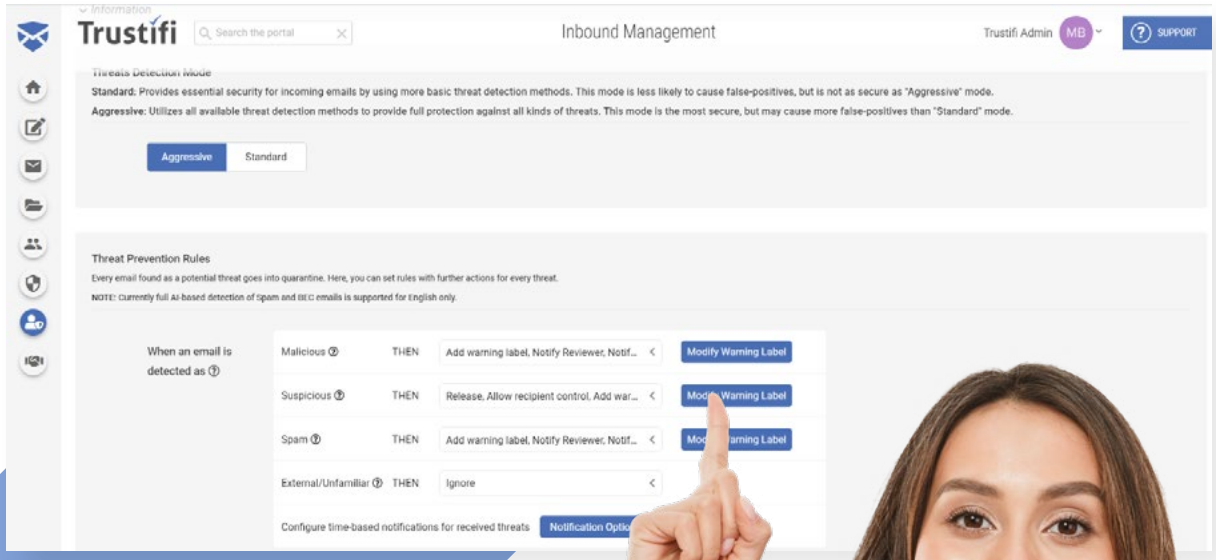
Defining Outbound Email Handling

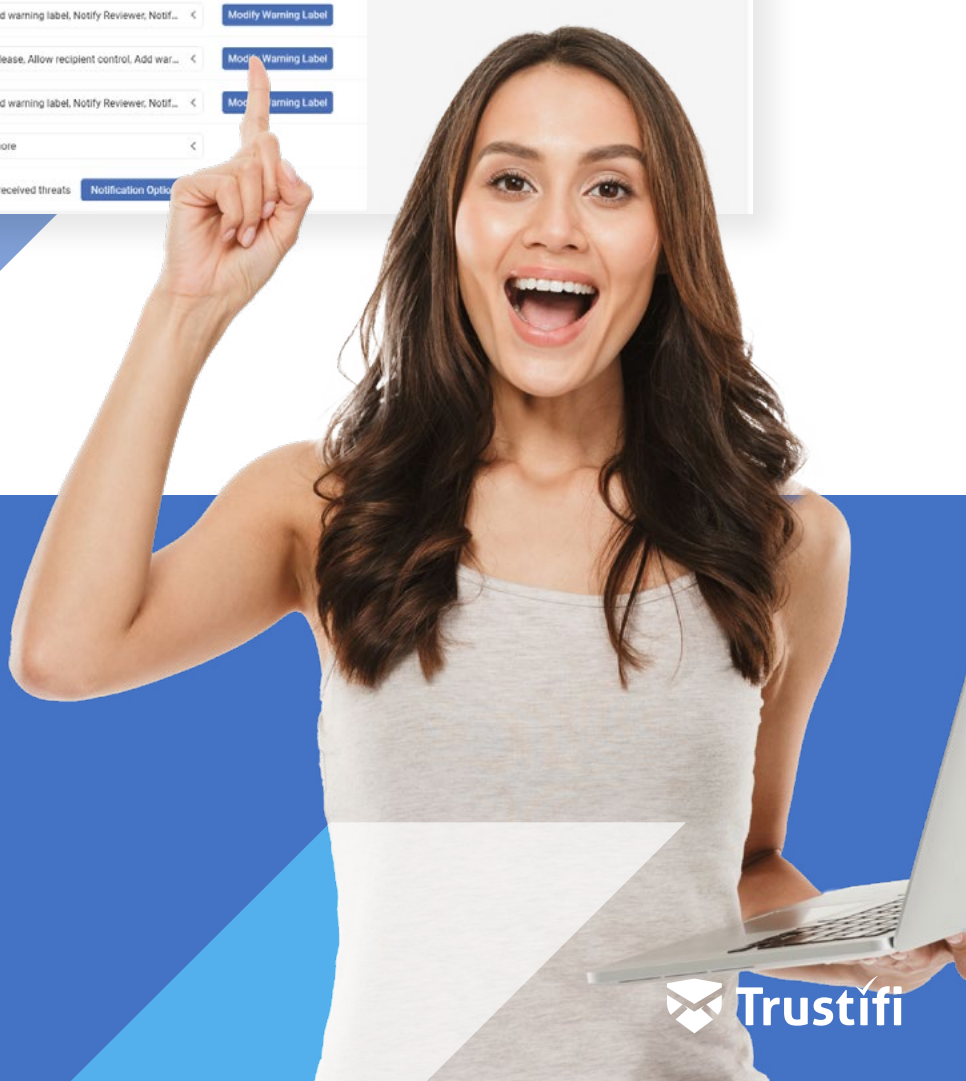
Trustifi makes it simple for administrators to set up automated handling of outbound email content so that Trustifi will automatically scrutinize email messages and their attachments and then take appropriate actions, such as encrypting, blocking and/or triggering security alerts to the relevant security administrators.



Defining Inbound Email Handling

Trustifi provides a comprehensive and simple administrator's interface for configuring how inbound emails should be handled. In Trustifi's portal, an administrator can define automated responses to different types of threats, configure detailed white and black lists, review and release quarantined emails, automatically block potentially malicious content and even configure auto-forwarding and automatic replies for incoming emails.





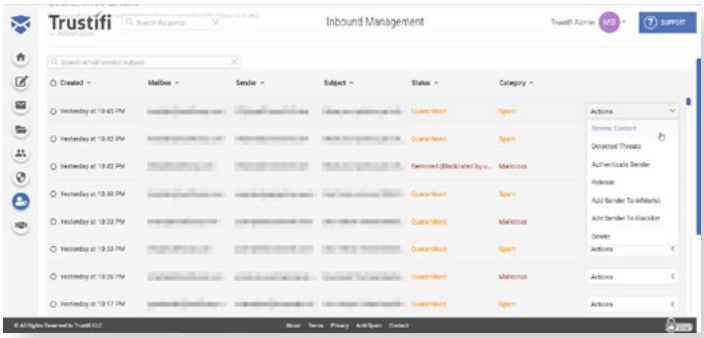
COMPETITIVE ANALYSIS 2020

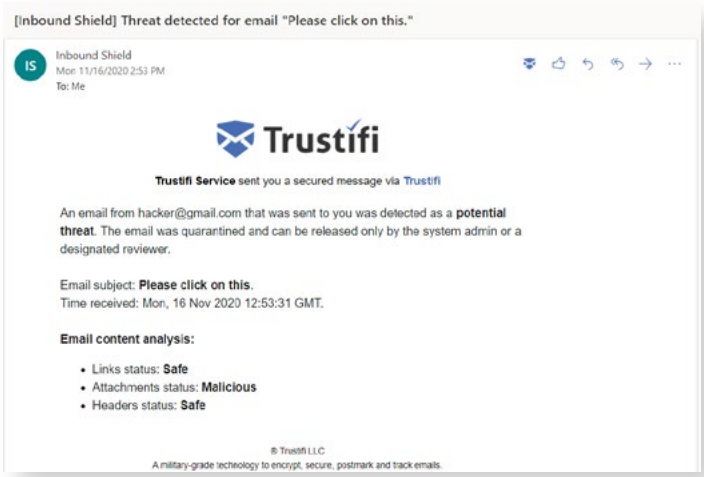
Trustifi

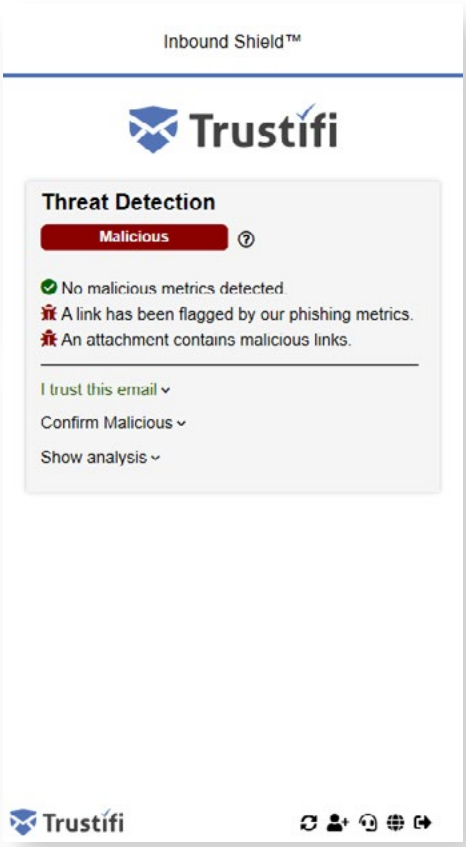
MONITORING

Trustifi allows designated admins and security staff to monitor and review all emails which have been detected as threats and quarantined. In a few simple actions using the Trustifi portal, an admin can safely review the content of a suspicious quarantined email and decide if it should be released.

On the individual user's level, users can manually scan emails in their inbox using the Trustifi add-in and see if the email is safe or potentially dangerous. Additionally, users are alerted if one of their emails has been found to be dangerous.







SEVERITY-BASED THREAT DETECTION

Trustifi enables you to define a wide variety of rule-based policies that automatically trigger actions upon detecting suspicious emails according to the severity of the detected threat, such as to quarantine, delete, release or to send an alert to the organization's security administrator.

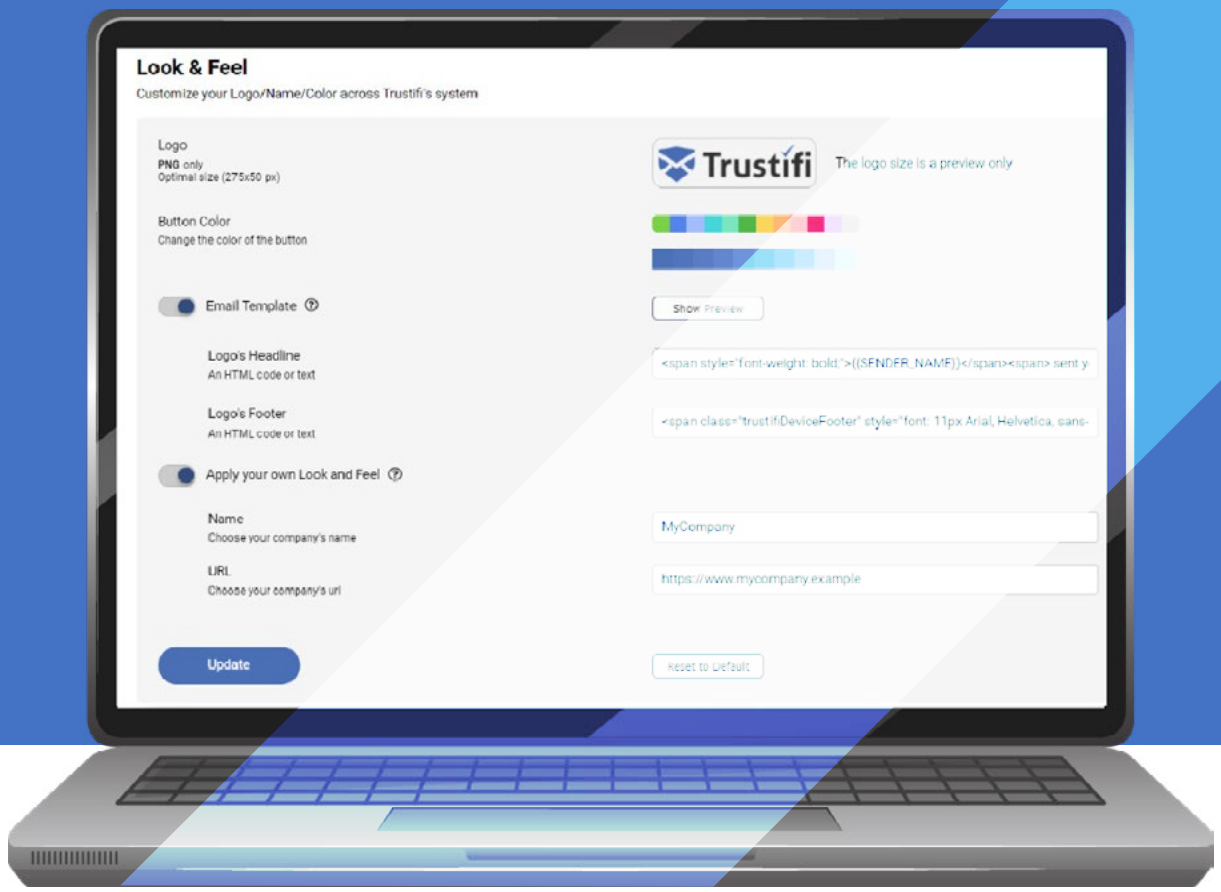
For example, different rules can be defined for handling harmless spam as opposed to the handling of malicious Trojan attachments.

Zix – Does not have this feature.

ADVANCED PHISHING DETECTION

Trustifi has its own proprietary phishing detection algorithms based on AI/machine learning analysis of the email message and attachment that can even detect zero day attacks. Trustifi's phishing detection algorithm recognizes and analyzes new threats, digests the new metrics and applies the insights to subsequent email analyses.

Zix – Only detects known phishing threats.



CUSTOMIZED/BRANDED EMAILS

Trustifi provides a simple user interface that enables the customization of the look and feel of the secure emails sent, including your own logo, headers, footers, colors, fonts, buttons and a variety of other design features.

RETROACTIVE EMAIL SCANNING

Trustifi enables administrators to retroactively scan all internal and inbound email at any time in order to detect malicious or abnormal activity. For example, after a new type of threat has been discovered.

Zix – Does not have this feature.

RETENTION POLICY CONTROL

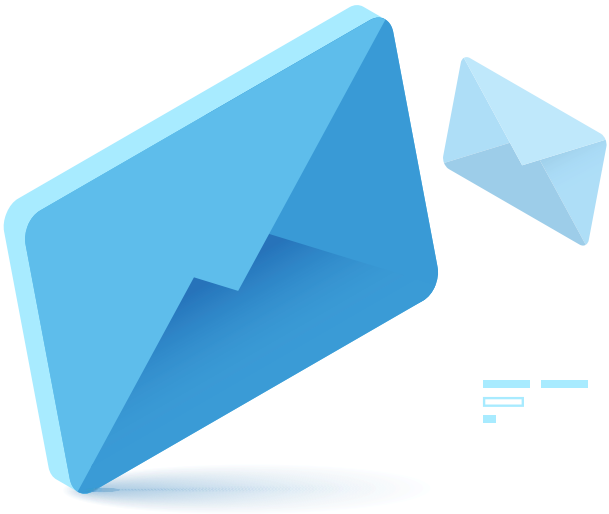
Trustifi enables you to control the retention of your data and to specify an expiration period, after which all emails and attachments are permanently deleted from Trustifi's databases.

Zix – Does not have this feature.

CUSTOMIZED SIGNATURE PROTECTION

Trustifi enables the addition of a customize signature to your apps, websites and login pages in order to protect against spoofing or the creation of phishing attacks. The validation of these signatures can ensure the authenticity of your pages.

Zix – Does not have this feature.



INTEGRATION WITH EXISTING EMAIL SOLUTIONS

Trustifi provides automated email encryption and data loss prevention that interfaces with enterprises' and employees' existing email applications.

Trustifi is easily deployed with

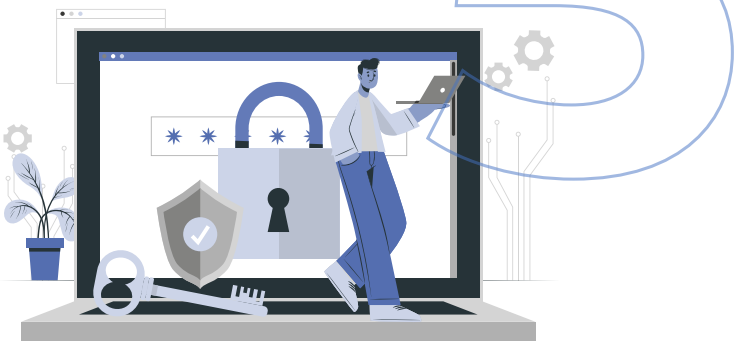
Gmail/G Suite – Add-in or Relay

Outlook/O365/OWA – Add-in or Relay

Any Email Server – Relay

Zix – Zix provides an add-in to Outlook and a hosted mailbox option.

SECURITY



OPTICAL CHARACTER RECOGNITION (OCR)

Trustifi provides classification and ruleset-based detection with AI capabilities in order to detect sensitive images attached to an email, such as passports, drivers licenses, hospitals records, IRS documents/reports and checks. Trustifi uses Optical Character Recognition (OCR) to extract the text in them and to detect sensitive data types or other restricted keywords.

Zix – Does not have this feature.

DATA LOSS PREVENTION (DLP)

Trustifi complies with GDPR, PCI, HIPAA, LGPD and CCPA predefined rulesets out of the box. It displays, reports, blocks, modifies and detects hundreds of sensitivity types by default (such as credit cards, social security numbers and so on).

Zix – Zix cannot scan PDFs or other image files for PCI/PHI or other targeted sensitive privacy data types and does not have OCR abilities.

PROTECTION

Trustifi uses machine learning to provide innovative contact history and sender behavior analysis in order to provide advanced protection against fraudulent contact attacks, such as spoofing, phishing or impersonation.

Zix – Does not provide the option to import contacts or monitor sender behavior in order to protect against fraudulent contact attacks, such as spoofing, phishing or impersonation.

AUTHENTICATION

Trustifi supports Multi-Factor Authentication (MFA) with automated SMS/phone call pin codes, passwords, email, and Single Sign-On (SSO) for both licensed users and/or administrators, in addition to unlicensed recipients as well. By extending MFA to the recipient, users and administrators can ensure that the secure email is only read by the desired recipient.

Zix – Provides Two-Factor-Authentication (2FA) for its licensed users and/or administrators in order to ensure access by authorized users only. But, the certified receipt provided by Zix only contains the time of delivery.

Smart Authentication

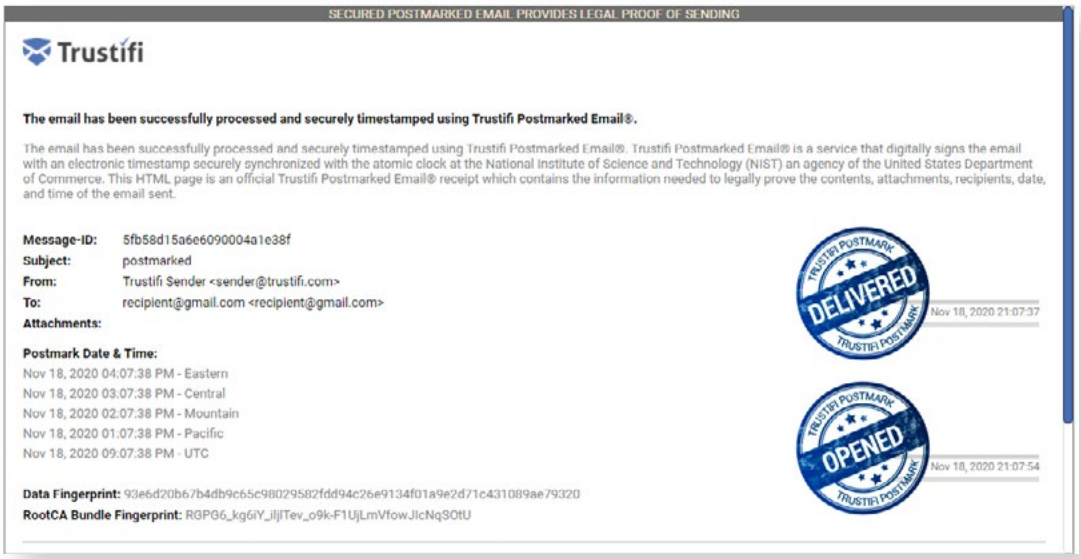
For the best combination of security and productivity, Trustifi enables a sender to apply its Smart Authentication feature to an email at the click of a button.

This feature enables a sender to authenticate a recipient using a variety of methods, such as pin via phone call, pin via SMS, pin via email, password entry or single-sign-on via Microsoft or Google in order to generate a unique fingerprint of the recipient. This unique fingerprint is used when subsequent emails and attachments are sent/shared to/with the same recipient who opens them on the same device (for example mobile device). Once a device has been authenticated, subsequent messages opened on the same device can be accessed by the recipient without the need to reauthenticate.

POSTMARKING

Trustifi enables the use of its patented **Postmark™** technology to apply a legally certified digital signature to emails, to provide legal proof of an email being sent and opened by a recipient.

Moreover, Trustifi patented Postmarked (Legal Proof) Proof & Tracking Encryption timestamps the email several times until it has been read.


SECURED POSTMARKED EMAIL PROVIDES LEGAL PROOF OF SENDING

Trustifi

The email has been successfully processed and securely timestamped using Trustifi Postmarked Email®.

The email has been successfully processed and securely timestamped using Trustifi Postmarked Email®. Trustifi Postmarked Email® is a service that digitally signs the email with an electronic timestamp securely synchronized with the atomic clock at the National Institute of Science and Technology (NIST) an agency of the United States Department of Commerce. This HTML page is an official Trustifi Postmarked Email® receipt which contains the information needed to legally prove the contents, attachments, recipients, date, and time of the email sent.

Message-ID: 5fb58d15a6e6090004a1e38f
Subject: postmarked
From: Trustifi Sender <sender@trustifi.com>
To: recipient@gmail.com <recipient@gmail.com>
Attachments:

Postmark Date & Time:
Nov 18, 2020 04:07:38 PM - Eastern
Nov 18, 2020 03:07:38 PM - Central
Nov 18, 2020 02:07:38 PM - Mountain
Nov 18, 2020 01:07:38 PM - Pacific
Nov 18, 2020 09:07:38 PM - UTC

TRUSTIFI POSTMARK DELIVERED TRUSTIFI POSTMARK Nov 18, 2020 21:07:37

TRUSTIFI POSTMARK OPENED TRUSTIFI POSTMARK Nov 18, 2020 21:07:54

Data Fingerprint: 93e6d20b67b4db9c65c98029582fdd94c26e9134f01a9e2d71c431089ae79320
RootCA Bundle Fingerprint: RGPG6_kg6iY_iljITev_o9k-F1UjLmVfowJlcNqSOtU

LARGE FILE TRANSFER

At no additional cost, Trustifi provides secure attachments of up to 1gb in size via Outlook, OWA, Chrome, the portal, and Trustifi plug-in.

For an additional cost, Zix provides secure attachments of up to 5gb in size via Outlook or its portal.

COMPETITIVE BATTLE CARD

COMPETITIVE ANALYSIS 2020

Trustifi

Trustifi

EMAIL SECURITY COMPARISON

Available | Limited | Not Available

	Trustifi	zix
Threat Intelligence and Response		
External threat feeds	✓	✓
Cross-enterprise threat investigation and response	✓	✓
Retroactive email rescanning	✓	✗
Severity based threat detection	✓	✗
Phishing Protection		
Advanced phishing protection	✓	~
Domain protection	✓	✓
Web interaction tracking	✓	✗
Scanning URLs in attachments	✓	✓
Shortened URL scanning	✓	✓
Anti-phishing, malicious URL detection, and AMP (in base offering)	✓	✓
Disposable Email Address (DEA) filtering (as part of spam/phishing filtering)	✓	✗
Business Email Compromise (BEC) protection	✓	✓
Advanced impersonation protection of brands, user domains, and contacts	✓	~
Custom made protection	✓	✗
Email Authentication		
DMARC, DKIM, and SPF analysis	✓	✓
Sender domain reputation filtering	✓	✗
DNS-based authentication of named entities (DANE)	✗	✗
Deep File Analysis		
File retrospection	✓	✓
Retrospective message remediation in a cloud-based service	✓	~
Macro and file-type filtering	✓	✓
Outbound Protection		
Data loss prevention policy solution integrated into email gateway	✓	✓
Sender control of encrypted envelopes via sender portal	✓	~
AI – OCR and sensitive image recognition capabilities	✓	✗
Cloud Infrastructure		
Dedicated cloud instance service per customer with dedicated IP addresses	✗	~
Redundant secure email gateways in different data centers for each customer	✗	✗
Enforce inbound protection on all or specific mailboxes	✓	✗

www.trustifi.com

John Doe
help@trustifi.com