

Inbound Comparison

 Available

 Limited

 Not Available

## Domain Protection

Custom Domain Monitoring



Sender Domain Reputation Filtering



Brand Domains Impersonation Protection



User Domain Protection



Internal Domains Sources Visibility and Control



Shadow IT Monitoring



## URL Analysis

Scanning URLs in Attachments



Shortened URL Scanning



On-Click Scan



URL Rewrite



URL Hunting



Numerous Redirect Link Detection



## File Analysis

Sandboxing



Static Analysis



Heuristic Analysis



Trojan/Viruses/Malware Protection



Macro and File-Type Filtering



ZIP and Archiving File Scanning



File Retrospection



Block File types, Easy Configuration



## Spam

AI



Internal metrics



Disposable Email Address Filtering



## Grey Mail

AI Classifications



Internal Metrics



Inbound Comparison

 Available

 Limited

 Not Available

## BEC

AI

Internal Metrics



## Text/Image-Based Attacks

Pre-phishing Attack Detection

Image-Based Attacks (Content & Attachments)



## Phishing

AI-Based Phishing Detection

Internal Metrics / Pattern Recognition

Proprietary Phishing Protection



## Email Account Compromise (EAC) Protection

AI Account Behavior Analysis

Internal Metrics

Credential Breach Alerts



## Email Authentication

DMARC, DKIM, and SPF Analysis



## Quarantined Management

Sender authentication

Review, release, and remove

Download email

Delete email from a mailbox

Reviewers' activity

Threat response

Advanced queries



## Blocklist/Allowlist

Advanced Blocklist/Allowlist

Global Blocklist/Allowlist

User Blocklist/Allowlist



## Cloud Email Archiving

Retention Management

eDiscovery

Restore Deleted Emails

Secure sharing

Specific query-sharing capabilities

Email status and tracking information display



Inbound Comparison

 Available

 Limited

 Not Available

## Add-in

Outlook Add-In



Gmail Add-In



## Other

Email communication patterns self-learning



False-Positive Reporting System



Security awareness (banner reporting mechanism)



Customizable Reports



Outbound Comparison

## Feature

Email Encryption Software



Data Loss Prevention (DLP) policy solution integrated



Optical Character Recognition (OCR)



Image Recognition



Admin notification for DLP-based rules/policies



Sender control of encrypted envelopes via sender portal



Inappropriate Content detection



Outbound Quarantine Management



Per-user quarantine



Compliance Management



Email Tracking



Recipient Authentication



Outbound rate limits



Advanced controls



Account Compromise detection



Add-ins (Outlook, Gmail, browser extensions)



API



Customizable Reports



MSP

 Available

 Limited

 Not Available

## MSP

Multi-tenant View to directly manage client plans



Client Management Portal with full user management and visibility



Fully Managed Client Plans with MSP Control and No Assigned Admin



Dedicated partner dashboard



Automated Policy and Configuration Copy Functionality for Clients



Advanced White Labeling Capabilities for Client



Customizable Reports for Client Emails (Inbound/Outbound)



## Other

A dedicated security team handling false-positive/negative incidents



Advanced easy-to-use management UI



DMARC analyzer tool



## Security Training

Launch phishing email simulation campaigns using realistic templates (credential theft, invoices, CEO fraud)



Rule-based policies with automatic training triggered on click, reply, or credential submission



Preconfigured automatic training scenarios (new employee onboarding, periodic refresh after 6-12 months, high-risk users, etc.)



Large training materials library including short, focused training lessons, quiz, option to upload user materials



Built-in Ability allows admins to create unique training videos using advanced AI techniques



Track click rate, report rate, repeat offenders, and improvement over time



Convert real blocked or quarantined emails into safe simulation templates for training



One-click AI training launched directly from quarantined emails



AI explains why the email is risky using the exact message the user interacted with



Trustifi makes it easy for your IT security staff to get the protection they need, including alerts, traceability, monitoring and awareness, while being straightforward, transparent and simple enough for your end users to apply all this security at the click of a button.

[trustifi.com](https://trustifi.com) | +1 844-249-6328 | [sales@trustifi.com](mailto:sales@trustifi.com)

Request a demo today

