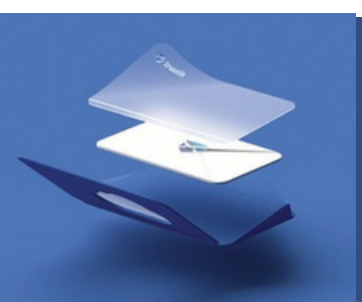
Trustifi

www.trustifi.com

	Inbound Shield Advanced	Trustifi Full Suite
Quick and easy integration No architecture changes. We carry out the process with you	✓	✓
Threat free mailboxes Full scan of all email's components (headers, links, attachments), using Trustifi's super sophisticated engines that are updated on a daily basis against all the latest email attacks	✓	✓
Email quarantine system Comprehensive and convenient system for quarantining Suspicious/Malicious emails. The admin and/or the reviewers receive all the information by email with a convenient and secure option to take immediate action (release/remove/whitelist/etc.) from anywhere and in real time - even from their mobile	✓	✓
Enhanced management system A web-based platform to manage users/mailboxes, configure preferences and tailor the system to your unique needs by choosing how to handle emails perceived as Suspicious/Malicious/other, by defining the security reviewers in your organization who will review and take action for quarantined emails, by deciding what file types automatically block, by defining the detection threshold of the scan engines, and many more	✓	✓
Personalization Set allowlist/blocklist for domains/addresses/links/files which affect all your users, while individual users can set those lists just for themselves (and you can review/edit those lists anytime)	✓	✓
Friendly reporting system Users can report on bad emails, directly to you or to us, using a banner on the email, or using our add-in. Admins and reviewers can also report potential false positives or false negatives directly from the management system	✓	✓
Audit logs Internal logging system for monitoring and tracking of every admin action performed in the system	✓	✓
Spam free mailboxes AI system to detect any spam/unwanted emails and prevent them from reaching your mailboxes	✓	✓
Eliminate the most advanced BEC attacks AI system that identifies texts urging recipients to do sensitive action (mostly finance) and avoid those from reaching your mailboxes	✓	✓
Sophisticated Inbound rules engine Improve security and efficiency by creating personalized inbound email rules tailored to meet any specific requirement.	✓	✓
Threat response tool Scan and identify potentially dangerous emails that have already been received by your users, and effectively eliminate these threats by removing the emails from their inboxes.	✓	✓
Retention period (quarantined/detected data) 1 year - we keep all your quarantined emails up to 1 year (it will then be deleted automatically but you have the option to save specific emails)	✓	✓
On-click-protection Perform links scans at the moment of clicking (not when the email is sent) And prevents entry to malicious pages that have changed after the initial scan or have not been detected	✓	✓
Trends & Insights graphs Easily monitor mailbox trends and potential threats with informative graphs and visualizations. Admins can quickly identify potential concerns and receive guidance on how to address them	✓	✓
Discovered services Automatically detect which web services are being used by your users to prevent cases of shadow IT and minimize exposure of sensitive data in your organization to 3rd parties.	✓	✓
Domain spoofing control Automatically create and manage unique digital signatures for your internal domains, and the domains of your partners and clients, to make sure no spoofing or impersonation attacks can get through even if standard authentication measures like SPF and DMARC fail.	✓	✓
Outbound Shield		
Inappropriate content control Detect and block any profanity, or content related to violence, drug use, nudity etc. sent by your users.		✓
Outbound quarantine management Admins and IT teams can set policies to automatically block and quarantine certain outbound emails from being sent.		✓
Encryption ▪ NSA-grade email encryption, plus full DLP with sophisticated rules engine to support any use case ▪ Secure mobile relay for full protection on any device ▪ Recall, block, modify and set expirations for already sent and delivered emails ▪ Tokenization - Instead of encrypting an entire email, only the sensitive information is replaced with a random string of characters, known as a token. This method improves productivity, open rates, and makes searching for emails from your inbox easier		✓
Permission management Set up highly specified reviewers for specific tasks like managing quarantined emails, archiving cases, or managing system users.		✓
Personalized Look & Feel Personalize every aspect of your Trustifi encrypted emails and web portal by adding your company logo, color scheme, disclaimers and more.		✓
Smart Indexing Cloud Archiving		
Retention management users can choose the amount of time an email can be retained before getting automatically deleted		✓
eDiscovery data will be preserved in its original state so it can be used as evidence for compliance regulators or legal teams		✓
Restore deleted emails restore emails after they were deleted and move them back to the user's inbox		✓
Secure sharing the ability to securely share it (MFA, tracking, etc.), even with an external recipient/identity, and for a limited time		✓
Specific query-sring capbilitis the ability to share just a specific subset of data with filtering options.		✓
Email status and tracking information display display the email status (quarantined, released, ext.), email tracking for outbound emails (if the recipient opened the email, ext.)		✓
Email Managed Detection and Response (EMDR) Ser vice		
Expertly-managed email security. Trustifi's team of cybersecurity experts can remove workload from your IT team by performing the necessary tasks to maintain your email security environment. Daily review of quarantined emails to identify potential false-positives or false-negatives Identifying potential weak points in your organization's security posture Updating and maintaining allowlists and blocklists Finding and fixing misconfigurations related to email security		✓



Protect Your Business Emails with AI-Powered Security

www.trustifi.com

info@ig.technology
www.ig.technology
1 786-712-5226

technologies