WHITEPAPER 2019



Traditional E-mail Is Not Safe

www.**trustifi**.com

Trustifi

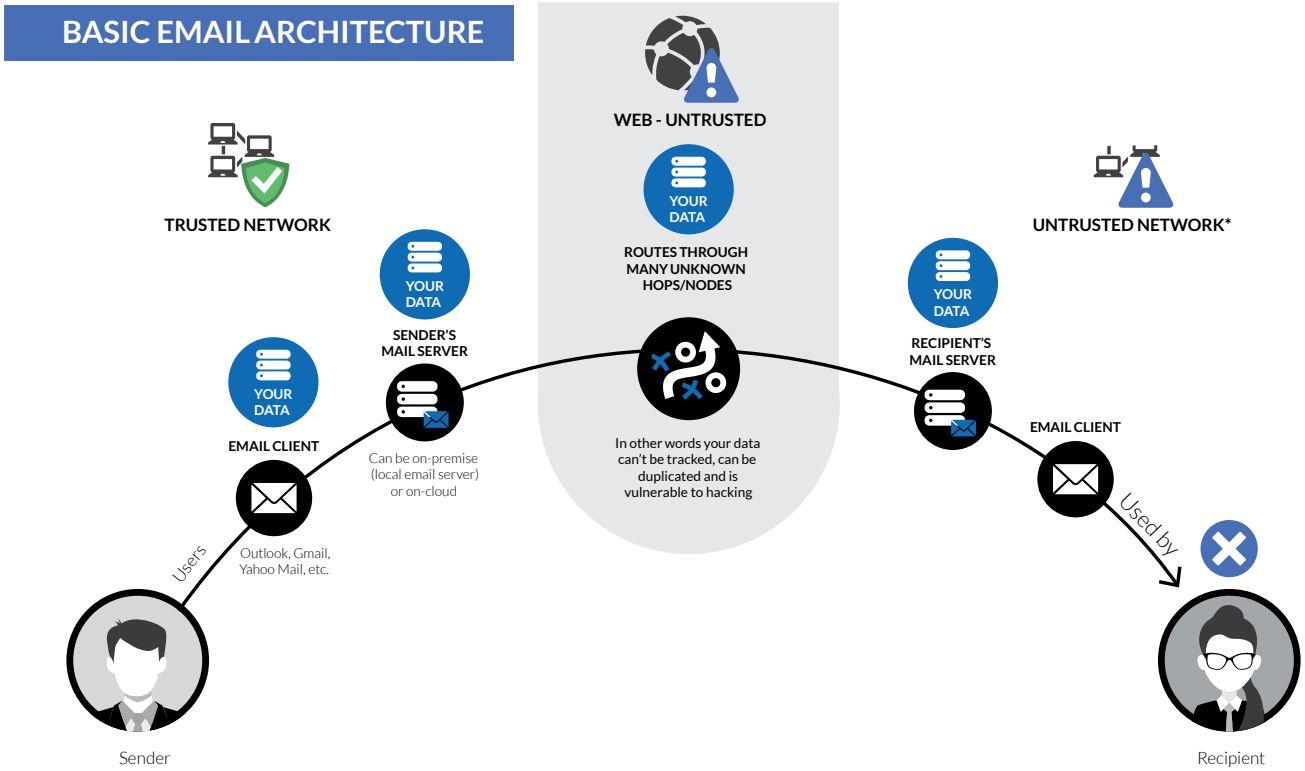
E-mail communication is the backbone of modern days business. Billion-dollar decisions are made based on information received via e-mails. It is critical that e-mail is arriving to the right person with the content the sender intended to send.

E-mails are not direct messages between the sender and the recipient. Traditional on-premise or cloud-based e-mail solutions are providing security and integrity of your message only to the point when the message leaves your email exchange.

After the e-mail has left your environment it passes through many other servers, nodes, and gateways on the way to the recipient. All these points are a potential threat to your e-mail content and integrity. Even a small vulnerability at the recipient's end or a misconfiguration at any of the hosts the message has passed through can expose the content of the e-mail, or give an opportunity to bad actors to modify the content, without you knowing about it.

You don't have control over what would happen with your message if it is copied, modified, printed or stored— it is all out of your control. You as a sender can't prevent recipients from further disseminating e-mail accesses on other devices, thus giving even more opportunity of exposure. The ability to authenticate the recipients to ensure the identity of the intended recipient is not available in a traditional e-mail environment, therefore necessary compliance requirements that are mandatory in many industries can't be fulfilled.

Traditional e-mail solutions are not compatible with recent changes in the privacy regulations (CCPA, LGPD) nor with other major compliance regulators (HIPAA, PII, GDPR).



There are two main problems today when trying to deliver private and sensitive emails:

Your information is sent and physically located in a lot of different servers where you have no control over them. A small vulnerability on the recipient's end can easily reveal all your information without you knowing about it.
You don't have the ability to authenticate the correct recipient(s) received your email, necessary for compliance reasons.

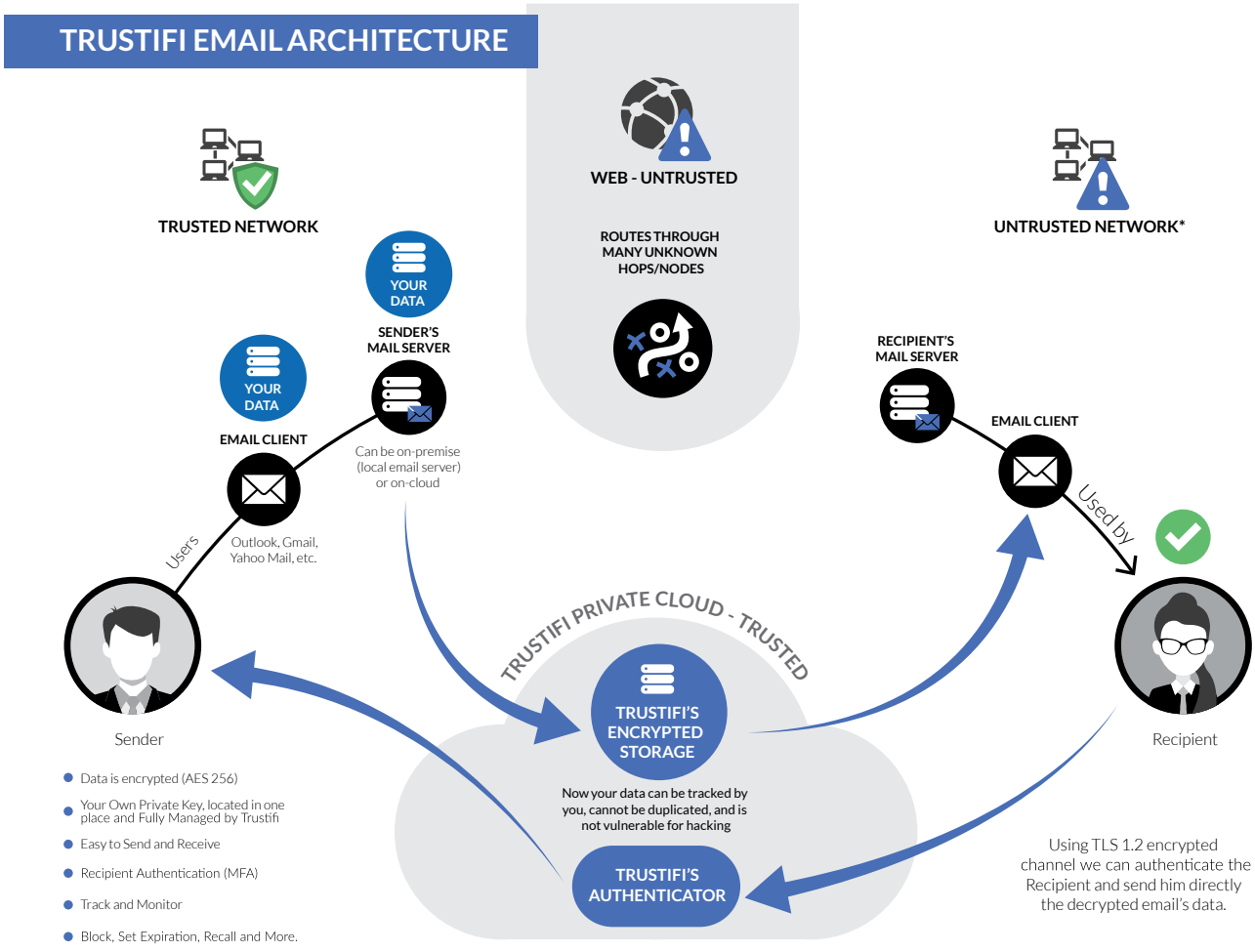
* It's an Untrusted Network environment because it is not yours

The Trustifi Solution

To provide trackability, encryption, and email security in a single platofrm is the kind of challenge that requires a tremendous amount of resources, knowledge, and time. Trustifi's secure e-mail architecture provides a simple yet very secure solution for all of the challenges explained above.

The e-mail message from your trusted network of on-premise or cloud-based e-mail servers travels to Trustifi's secure virtual private cloud storage which is fully encrypted with AES-256 encryption algorithm. The encryption key is your own private key which is stored and managed by Trustifi. Now your data can not be duplicated, hacked, or modified and you can track what is happening with your message.

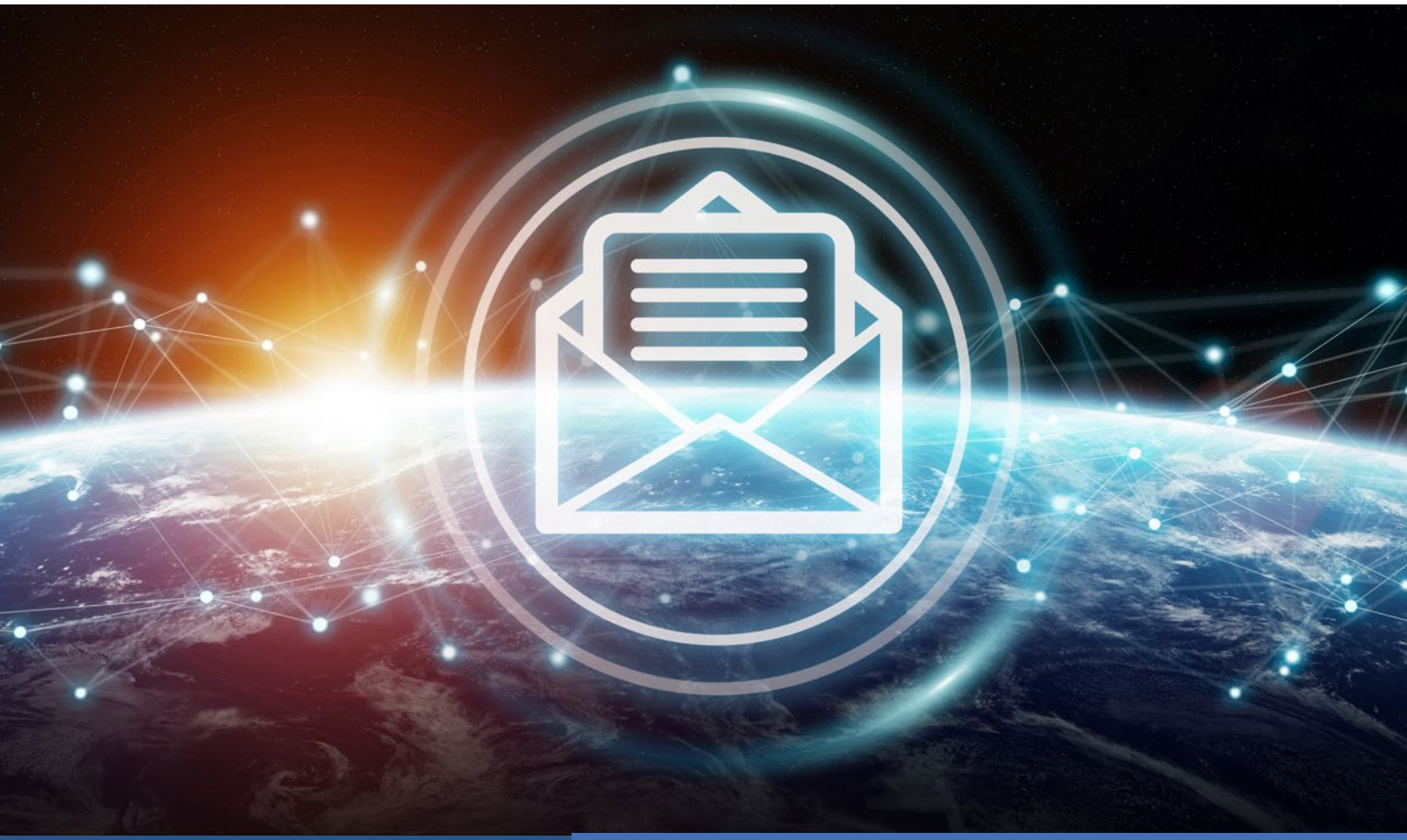
Trustifi sends a notification message to the recipient about the message you sent to the receiver. The recipient authenticates itself via a secure channel, encrypted by TLS 1.2 and after successful authentication, Trustifi sends your full decrypted message to the recipient. Secure, traceable, confirmed, compliant e-mail delivery: Done.



With Trustifi apps (for Outlook, Outlook 365, Gmail and Trustifi Web Portal) secure e-mail sending and receiving is the easiest to use and deploy email security platform on the market. You can track every step of your message life-cycle including, receive and read confirmation.

For increased security, you can set special attributes of your e-mails like blocking certain recipients to access, the message, set recall date and time, configure expiration date and time.

Recipients can be forced to use multifactor authentication when accessing the messages providing the highest level of confidentiality, security, and integrity of your message life-cycle.



For more information :

www.trustifi.com
1-844-235-0084
info@trustificorp.com