# Trustify eXperts

# Delivering Data Security for Investors

**Trustify**
Secure Everything. Always.

### Successful Malware attacks

Malware is a type of software specifically designed to disrupt, damage or gain unauthorised access to a system. With 94% of malware being delivered by email (Verizon 2019 report), attacks are an increasing threat for every business, especially in a highly competitive environment such as private investment.

### Examples of Data Loss / Theft in Investment Banks

1. A client receives an email requesting confirmation of their financial details, seemingly from their portfolio manager. The client replies with the required information, thus granting hackers access to their bank accounts.
2. An employee sends confidential information via email outside of the organisation about an upcoming investment opportunity, either by mistake or on purpose. As a consequence, the investment bank loses a deal.
3. Investment managers are corresponding regarding a major portfolio development. System login instructions are distributed via email and eventually fall into the wrong hands. This login is used to gain access to confidential information.

### What is the Cost of a Data Breach?

Not only can an email breach result in significant financial loss for the bank, the client or both parties, but it can cause detrimental reputational damage and loss of clients/contracts. Data loss and theft may also result in a breach of data protection laws like GDPR which could result in large fines from regulators.

### Common Examples of Cyberattacks in Investment Banks

### High value phishing attacks

CXO-level phishing attacks, referred to as 'whaling', are targeted attacks on high net worth individuals. A form of business email compromise, these attacks are designed to fraudulently gather information for other criminal activities, such as tricking a client into sending their bank account details. Phishing accounts for 32% of data breaches in 2019 according to Verizon.

### Accidental breach

In standard systems, there is relatively little control as to where your email goes once it has been sent. Employees may regularly use insecure email as a method of sensitive data exchange, not aware of the potential phishing and privacy risks. This can lead to confidential information or internal documents falling in to the wrong hands. According to IBM, over 95% of all incidents investigated recognize "human error" as a contributing factor.

### Email Security with TrustiMail

A good email security tool that can do both outbound email security through TLS and inbound email security through email scanning will ensure that any information being sent externally is encrypted and monitored.

With reliable email privacy and tracking, granular rule set-up and built-in compliance, risk of email breach can be eliminated – whether accidental or malicious.
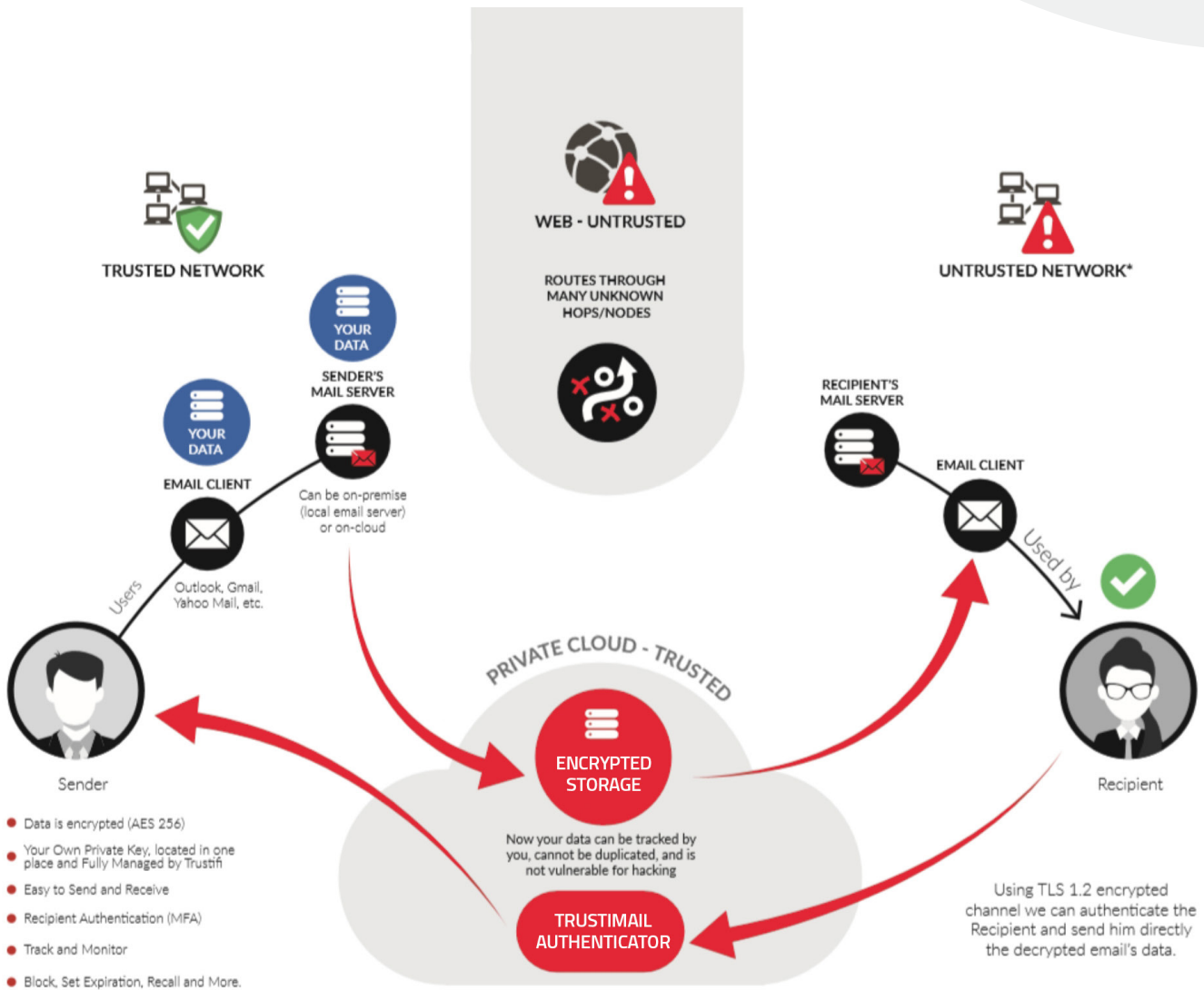
With personalised preferences, rules set-up and phishing awareness training to match, SMAIL can be a powerful tool to reduce the likelihood of email breach and business email compromise.

TrustiMail instantly integrates with Outlook and Gmail for military grade encryption on outbound emails and secure email management. Admins can set preferences to encrypt files and attachments, retract information after it is sent and see when, where and even which IP address your email has been opened from.

TrustiMail also boasts no set-up fees and an integration with existing email tools which means employees can enjoy instant access to TrustiMail features without having to be introduced to anything new.

1. Know who you are dealing with all the time, every time
2. Recall errant emails
3. See who has read what and prevent onward forwarding issues
4. Invite your clients into a circle of trust to avoid risk of scamming

# TrustiMail Architecture



**TRUSTED NETWORK**

**YOUR DATA**

**SENDER'S MAIL SERVER**
Can be on-premise (local email server) or on-cloud

**YOUR DATA**

**EMAIL CLIENT**
Outlook, Gmail, Yahoo Mail, etc.

Users

Sender

**WEB - UNTRUSTED**

ROUTES THROUGH MANY UNKNOWN HOPS/NODES

**UNTRUSTED NETWORK***

**RECIPIENT'S MAIL SERVER**

**EMAIL CLIENT**

Used by

Recipient

**PRIVATE CLOUD - TRUSTED**

**ENCRYPTED STORAGE**

Now your data can be tracked by you, cannot be duplicated, and is not vulnerable for hacking

**TRUSTIMAIL AUTHENTICATOR**

Using TLS 1.2 encrypted channel we can authenticate the Recipient and send him directly the decrypted email's data.

- Data is encrypted (AES 256)
- Your Own Private Key, located in one place and Fully Managed by Trustifi
- Easy to Send and Receive
- Recipient Authentication (MFA)
- Track and Monitor
- Block, Set Expiration, Recall and More.

# How can I find out more?

Let us find out how we can help you deliver real value from the investment you make in your people.

Visit us at **www.trustifyexperts.com**

Call us on **+44 (0) 808 196 4200**

**Trustify**
**eXperts**

The home of World Class cyber talent

**London**

**1 Ropemaker Street, London, EC2Y 9HT, United Kingdom**