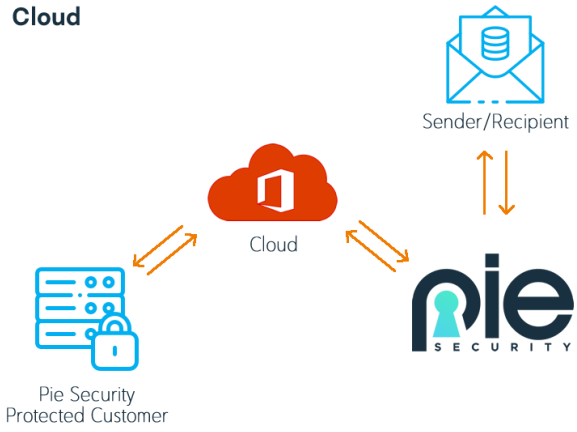
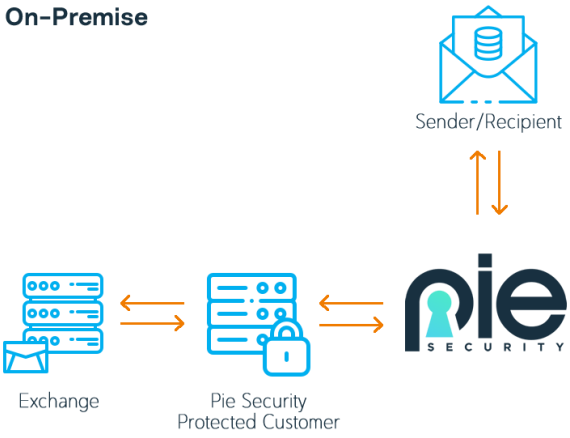
Email Security Service

Despite the prevalence of the internet and web-based communication platforms, email remains a primary communication mechanism for organisations today. The security threats and risks, such as ransomware, malware, phishing attempts, spoofing and data theft, as well as compliance regulations for email, are forever evolving.

Organisations are expected to have a strong and compliant email security posture, with email expertise on hand to mitigate the threats to operations and business, but having these solutions and resources in place can become expensive and time-consuming, especially for SMBs with limited budget dedicated to cyber security.

In an everchanging landscape of both threats and regulatory requirements, Pie Security simplifies email security, providing assurance of compliance with regulations around data transfer and access to both personal and financial information, while offering additional levels of security through encryption.
Pie Security, experts in email security for over 30 years, are here to help take the pressure away from managing email security regardless of your existing infrastructure.





It is essential to filter threats from entering your organisation's network, sensitive information must also not leave the network. Implementing a multitude of encryption mechanisms ensures that only pre-validated data is securely leaving your network.

With GDPR on everyone's mind, an exact simple mechanism of proving that sensitive data is only to be shared with valid recipients, using encryption can be the cornerstone of the GDPR policy. You, in turn, give your clients, suppliers and partners a level of assurance that sensitive data is the number one priority.

Email Hygiene

- We are using industry best practice filtering for Spam looking at the **sending connection host** and the **content of the email** based checking
- Self-service release and management function
- Multiple **Anti Virus engine** checking both inbound & outbound
- **File content** checking
- Message tracking

Encryption Services

- Certificate / key management.
- Automated email signing
- On-premise implementation services (remote)
- Client integration training
- Engage with customers, suppliers, vendors, partners to enable email encryption

On-Premise Email Encryption

- Portal based encryption
- PDF encryption
- PGP encryption
- S/MIME encryption
- Email Signing

Hosted Email Encryption

- Portal based encryption
- PDF encryption
- PGP encryption
- S/MIME encryption
- Email Signing
- Auto encryption for sensitive data such as Personal Identifiable Information (PII)

Security & Privacy By Design

At Pie Security, we understand that email security is more than just scanning/filtering your inbound email for known spam and malware. Data laws currently demand the stringent safeguarding of financial, personal and confidential information, and while many organisations implement data security policies and awareness campaigns, it is also essential to ensure that data is processed using appropriate technical measures in a manner that ensures privacy and demonstrable compliance with security principles.

Pie Security will engage with your organisation to understand what email communication and associated data is confidential or sensitive or restricted due to data law, and design a solution to meet your security, privacy and compliance needs. This should be part of your Data Privacy Impact Assessment (DPIA) when reviewing all data acquisition and data departure on the network. This creates higher data visibility as well as improved data management, creating privacy by design.

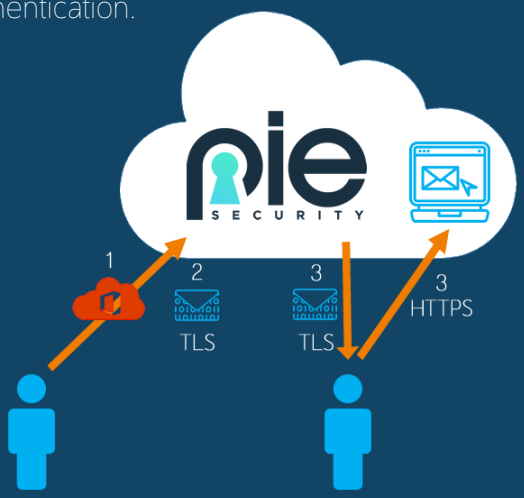
Leaks of sensitive data and subsequent regulatory penalties represent a real business risk. This risk can easily be mitigated by ensuring that all relevant communications containing protected or confidential information are encrypted and fully secured in transit.

Deploying an encryption solution using the best mechanism for the sender/recipient pair, is the foundation of a solid secure communication/data protection policy.

When communicating to a web-based email platforms such as Hotmail or Gmail (B2C), it is advised to use web-based portal or PDF encryption solutions.

The examples are:

1. An employee sends an outbound email to a customer, partner or supplier through the normal internal channel such as Microsoft Exchange or O365.
2. The email is then routed via the Pie Security web portal, where the original message is held for collection.
3. Pie Security sends a notification to the recipient that they have a new email to be accessed securely.
4. The recipient logs into the portal to review the email using options such as two factor authentication.



Learn more about becoming a reseller

Email: info@piesecurity.com

Phone: 020 4519 2702