



Mailock & Microsoft 365 For Secure Customer Communications

Mailock empowers businesses and customers to exchange sensitive information using email with the confidence that only the right people can gain access.



Crown
Commercial
Service
Supplier



MAILOCK OVERVIEW

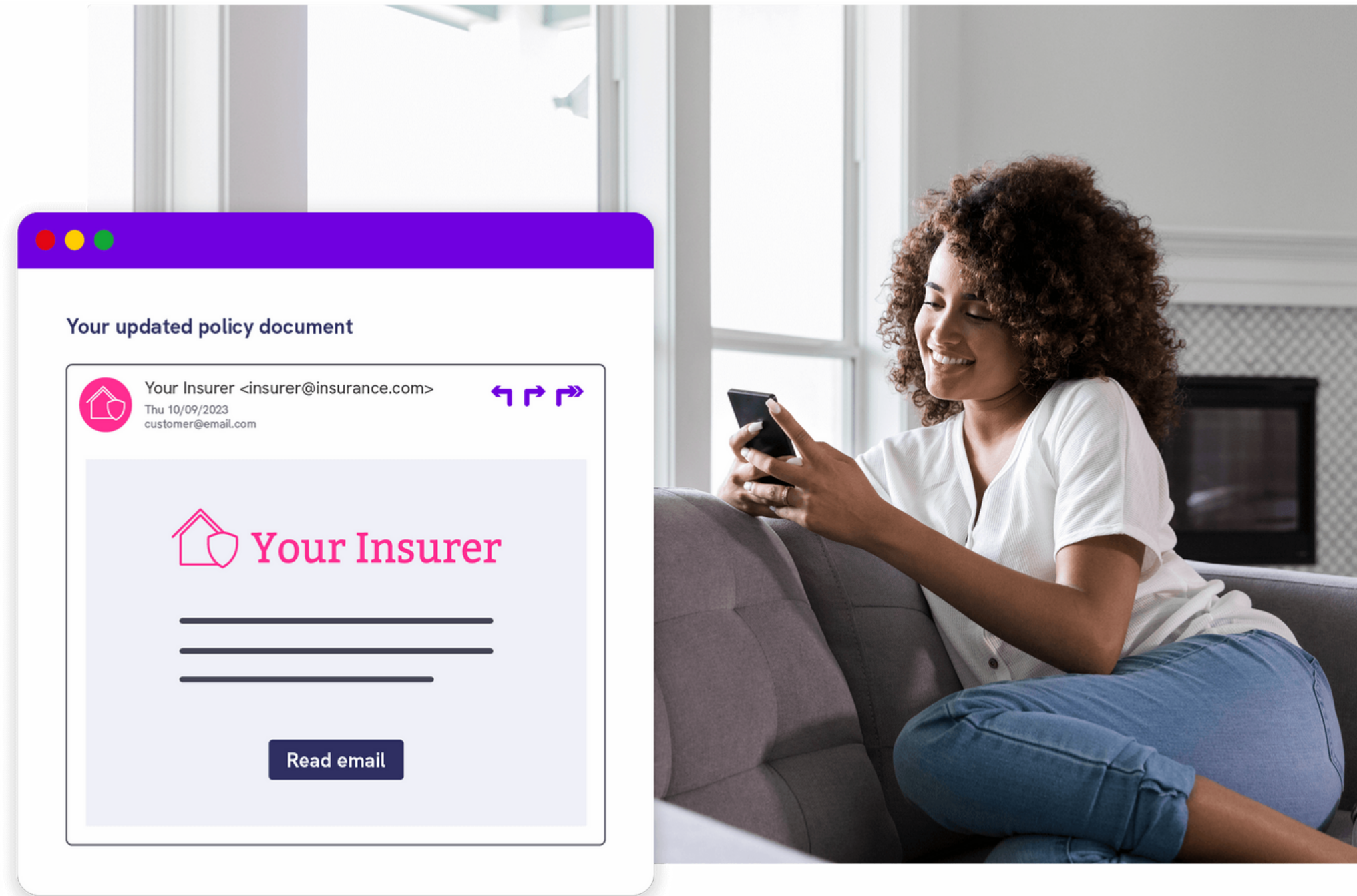
What is Mailock?

Mailock secure email uses military-grade encryption and multi-factor authentication to deliver confidential information by email to the right person - only.

It integrates tightly with Microsoft 365 and Windows Outlook helping organisations to remain compliant with regulation, protect their communications, and deliver sensitive messages and documents at high volumes.

Key features:

- End-to-end encryption
- Recipient authentication
- Unilateral revoke function
- Audit trails (proof-of-delivery)
- Engagement data and analytics
- Automation for delivery at scale





M365 ENCRYPTION

What is Microsoft's encryption?

Top tier Microsoft 365 plans (e.g., E5) offer customers access to **Microsoft Purview Message Encryption (MPME)**, part of the Azure Information Protection suite.

MPME uses email encryption and inbox access verification to increase the chance of an email reaching the right person without it being intercepted.

Key features:

- End-to-end encryption
- Inbox access verification
- Email recall (recipient infrastructure dependent)

"The rights management suite is designed to be used to prevent accidental misuse and is not a security boundary."

— Microsoft Spokesperson, 2022

Purview Message Encryption offers an additional layer of protection for everyday business emails, however Microsoft discourages the use of its encryption for secure delivery at high volumes.

MAILLOCK AND MICROSOFT PURVIEW ENCRYPTION: FACT SHEET

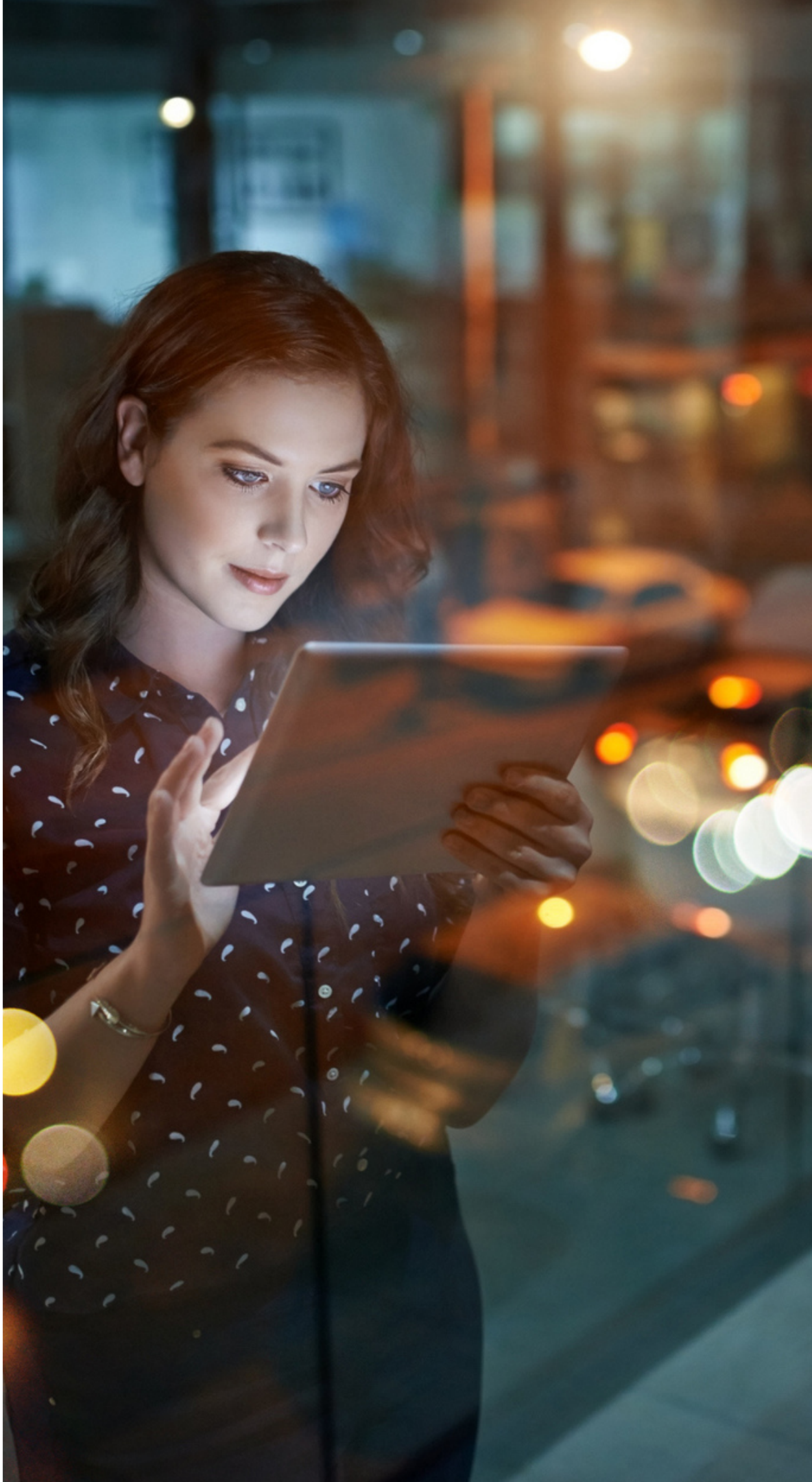
	What is it?	What does it do?	Microsoft Purview Message Encryption	 maillock
End-to-end encryption	AES-256 end-to-end encryption obscures message data using military-strength algorithms	Encryption protects emails from interception in transit	✓	✓
Custom branding	Customisable templates allow you to brand secure emails sent out from your organisation	Branding creates a consistent experience for your customers	✓	✓
Scaled delivery	Support for high-volume delivery means no hard ceiling on message volume or message throughput	Scaled delivery capabilities enable you to switch from confidential print and post to digital recorded delivery		✓
Multi-tenancy/brand	Add multiple brand instances to a single appliance for the delivery of secure email using multiple, separate brands	Enable multiple brands, sub-brands, or clients to send secure emails using shared infrastructure		✓
Recipient authentication	Require recipients to authenticate their identity to open a message (e.g., SMS, Q&A, Unipass ID)	Authentication protects emails against inbox attacks and ensures compliance with ESMA/FCA/MIFID II proof-of-delivery obligations		✓
Message revoke	Administrators and senders can revoke access to secure emails regardless of recipient infrastructure	Unilateral revoke helps organisations to comply with ICO guidelines on responding to an email breach		✓
Audit trails	Senders and administrators can view audit trails displaying timestamps of send and read access for their sent messages	Audit trails help with litigation and ensure compliance with ESMA/FCA/MIFID II proof-of-delivery obligations		✓
Trigger words	Set custom keywords that trigger a warning if they appear in an email that could be sent unsecured	Trigger words prevent sensitive data from being sent unsecured by company employees		✓
Read notifications	Read notifications tell senders when secure emails are opened regardless of recipient infrastructure	Read notifications empower senders of secure emails to follow up with recipients at the right time		✓
Engagement analytics	Administrators can access accurate open rate and attachment download analytics for reporting	Open/download analytics show you how your secure emails are driving recipient engagement		✓

BENEFITS

Mailock & 365

Mailock integrates with Microsoft 365 enabling organisations to exchange confidential information with their customers at scale, securely and with full compliance.

Compliance	Comply with regulations that require organisations to maintain audit trails, prove delivery to the right person, and protect sensitive data.
Security	Deliver confidential information and documents using advanced security and provide your recipients with the tools to do the same in reply.
Engagement	Empower your recipients to read and respond easily to secure emails regardless of their email provider, device, or experience.
Efficiency	Arm your organisation to send sensitive information at scale and support its journey from paper-first to digital-first communications.



COMPLIANCE

Ensure regulatory compliance

Comply with guidelines that require organisations to maintain audit trails, prove delivery to the right person, and protect sensitive data.

Prevent FCA - SM&CR	"If a firm breaches one of our requirements, the Senior Manager responsible for that area could be held accountable if they didn't take reasonable steps to prevent or stop the breach."
Encrypt ICO - GDPR	"Have a policy governing encrypted email, including guidelines that enable staff to understand when they should or should not use it. For example, there may be a guideline stating that any email containing sensitive personal data (either in the body or as an unencrypted attachment) should be sent encrypted."
Audit FCA - COBS	"Keep a copy of relevant electronic communications, made with, sent from or received on equipment: (1) provided by the firm to an employee or contractor; or (2) the use of which by an employee or contractor has been sanctioned or permitted by the firm."
Authenticate ESMA - MIFID II	"Have sound security mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information leakage maintaining the confidentiality of the data at all times."
Revoke ICO - GDPR	"[in the event of a data breach] act quickly. Try to recall the email as soon as possible. If you can't recall it, contact the person who received it and ask them to delete it. In the future, consider turning off the Autofill tool when sending work emails. The 72 hours following a personal data breach are particularly critical."
Reply FCA - Consumer Duty	"Ensure consumers receive communications they can understand, products and services meet their needs and offer fair value, and the support they need."



SECURITY

Make sure only the right people can gain access

Maillock extends Microsoft's native capability to verify that recipients have access to their inbox with more secure modes of authentication that prove they 'are who they say they are'.

Inbox access verification protects against a number of the most common email attacks. However, recipient authentication is a multi-factor solution that extends this protection against:

- Inbox takeover
- Stolen credentials

Maillock offers the ability to authenticate recipient identity using Unipass ID (for financial services professionals), an SMS code sent to their mobile device, or a custom question and answer. Recipients are guided through the process easily and securely.



ENGAGEMENT

Drive engagement, communicate freely

Mailock is designed for customer communications, so the recipient experience is a top priority. We're proud to be able to say our open rates are over 80%. Receiving a message is easy.

A notification email lets your recipients know they have a message to be opened. This message can be customised with your company branding or use the familiar Mailock template.

Recipients click 'Open' on the notification delivered to their inbox. They'll answer any challenges that have been set, if they're trusted, they can open and read right away.

If recipients need to reply to a secure message, they can use Mailock to compose, attach, and send using their existing email address and account. They'll even get a limited number of secure emails to send to other people if they need.



mailock



YOUR
LOGO HERE

Reply

Save

Subject: Your secure message

From: sender@company.co.uk

To: recipient@company.co.uk



Your-secure-document (105 KB)



EFFICIENCY

"We've already saved 270 tonnes of CO2!"

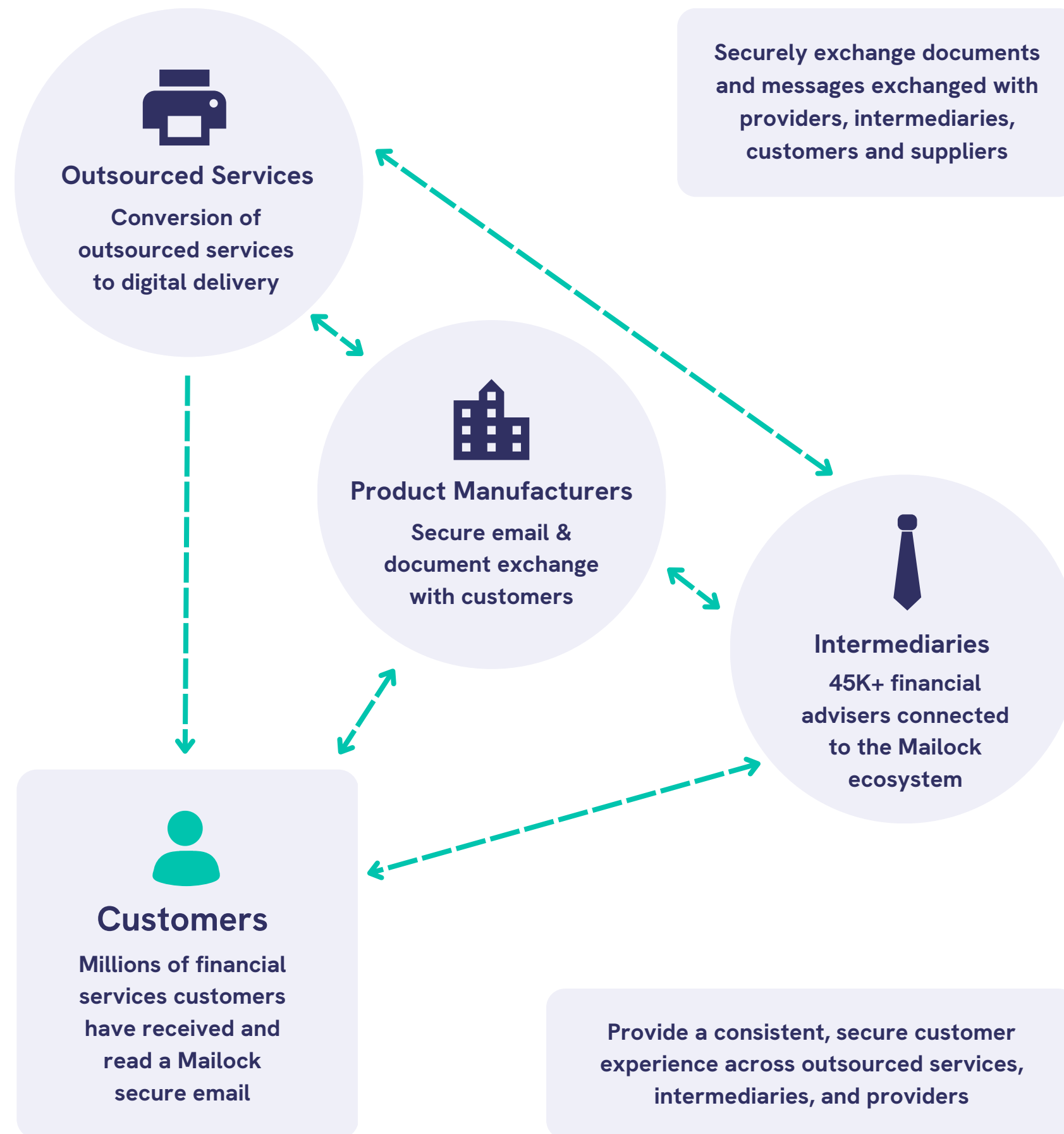
— Ronnie Taylor, CDO, Aegon

Empower your organisation to transform its confidential communications by converting print-and-post to digital.

Our network is designed to withstand high volume, batched and automated sending. This means organisations delivering high numbers of printed and posted documents can benefit from the carbon and cost savings that come from reducing their paper-based output.

Research conducted by sustainability consultants Project Rome estimates that switching post to secure email could result in up to 95% cost savings, not to mention the sustainability benefits.





ECOSYSTEM

The secure communication network of choice for the financial services

Mailock is the network of choice for financial services professionals, organisations, and their customers.

Designed with the information security and compliance requirements of the financial services in mind, Mailock enables connection - between advisers, product manufacturers, outsourced services, and consumers.

- Unipass ID authentication eases adviser communications.
- Network verification for trusted organisations eases communication with financial providers/platforms
- Read-without-registration and encrypted replies ease communication with clients and customers



FACT SHEET

Maillock For Microsoft 365: Securing Your Communications