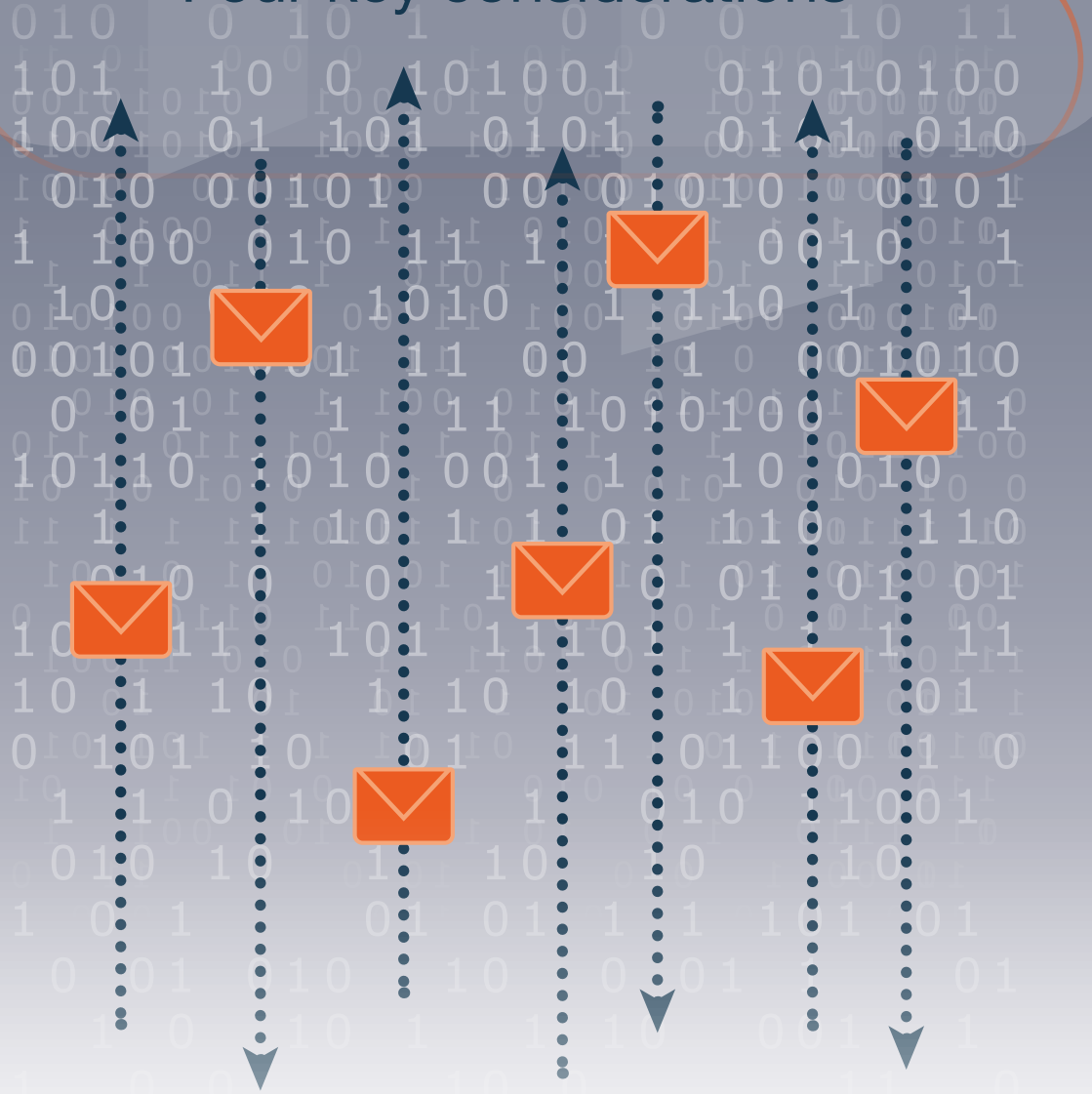
TECHNICAL WHITE PAPER

Secure email messaging in Office 365: Four key considerations



egress®

Organisations worldwide are moving to Microsoft Office 365 for hosted email services, and for good reason. The benefits that Office 365 brings are numerous; from reduced costs and infrastructure requirements to practically limitless scalability and storage. These benefits add up to an outsourced mail service that is more flexible, powerful and productive than ever.

This uptake in use of hosted mailboxes is occurring alongside a greater decentralisation of working practices, with the rise of remote working, long distance collaboration, and cloud-based software and services.

Unfortunately, with these revolutions in mail hosting and working practices, comes greater information security risk than ever before. Attacks are getting more sophisticated, and data breaches linked to user error are becoming ever more frequent.

Taken together, these three trends create an information security atmosphere that urges the use of encrypted email security processes.

"Office 365 (O365) provides its own message encryption functionality, but it's important to consider a business' requirements before relying on it wholesale for encrypting email."

Office 365 (O365) provides its own message encryption functionality, but it's important to consider a business' requirements before relying on it wholesale for encrypting email. Is it effective? Is it appropriate for your business? What can it do? What can't it do? This white paper discusses four issues that are highly important when considering email security functionality in O365.

The key point is that while the risks have never been greater, with the right systems and solutions in place, our ability to mitigate these risks has never been stronger.

Why secure messaging?

Sending messages over the Standard Mail Transfer Protocol (SMTP) is notoriously insecure. It wasn't designed with security as the guiding principle, and indeed is now causing email to suffer from technological lock-in: a dependency on these old systems and ways of sending and processing email has hindered development of more secure alternatives.

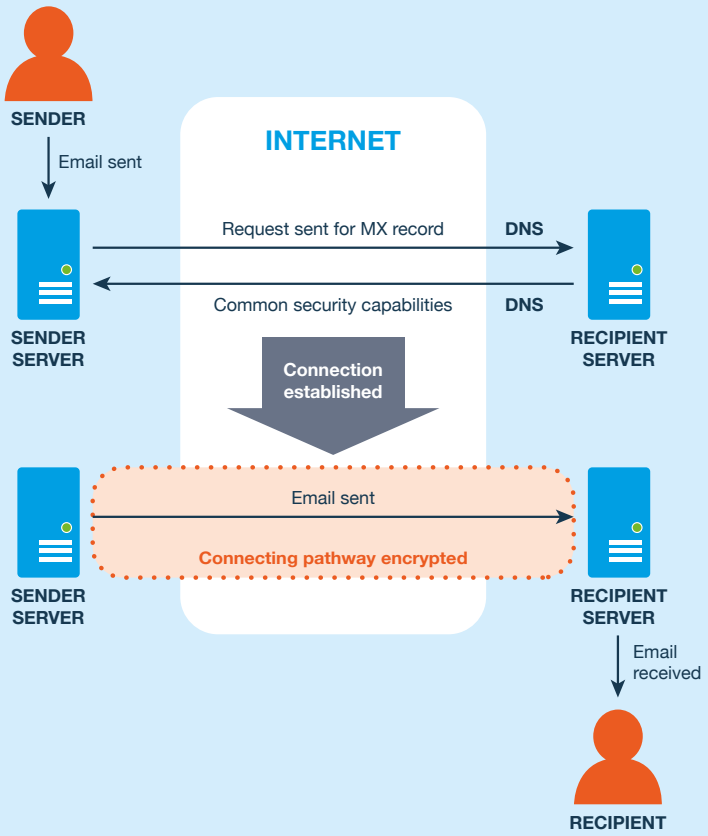
The goal now is to work within this traditional mail infrastructure, whilst also providing the security and usability required by today's workforces, dealing as they do with highly sensitive customer and corporate data every single day.

There are many ways to encrypt an email. These methods can differ widely, with some designed for technologically advanced users (e.g. PGP), and others that essentially require no end-user involvement (e.g. TLS).

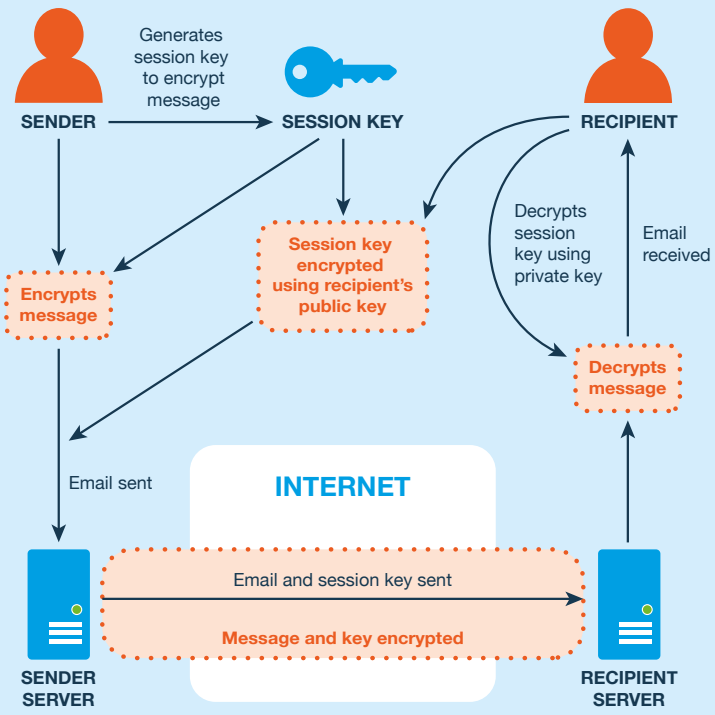
With all of the different options available, it's no surprise that when migrating to O365 for mail hosting, organisations choose to rely on O365 message encryption for their email security needs.

But evaluating O365 message encryption, or any other email encryption solution, is critically important, since data breaches of sensitive information can be devastating for not only the individuals involved, but also the reputation and finances of a business. It's therefore crucial to not only be informed about the email security solutions available, but also knowledgeable about the most appropriate ways in which to evaluate these solutions.

Sending an email via TLS



Sending an email via PGP



Four things to consider

ONE: USABILITY

How will we secure our emails and file attachments to protect sensitive data?

The best email encryption solution is one that integrates seamlessly with existing workflows and has enough features to achieve everything that users need to do with sensitive data, but isn't overcomplicated and bloated with irrelevant functionality.

In the O365 method of encrypting an email, the sender puts specific text in the subject line, e.g. '**encrypt**'. The message is then sent encrypted. While this sender experience is straightforward, and integrated within the Outlook client, recipients face more of a task to access secured email.

Emails do not decrypt into the mail client, so recipients are required to open the HTML attachment in the secure email, access a secure portal, and sign in or create a Microsoft account to access decrypted content. Of course, any replies to the original sender happen in the same way. So O365 message encryption is not fully integrated into a user's email workflow, always relying on the external online portal.

In addition, some useful, perhaps crucial, features are currently missing from O365:

- Message revocation
- File encryption and the ability to send files securely without size restrictions
- Sending to shared mailboxes
- Recipient's ability to request access to encrypted email
- Client-side DLP checking
- Customisable end-user messaging and alerts
- Client-side encryption at rest
- Internal encryption

> "Without end-to-end encryption there will always be places within the network where data is sent unencrypted."

These features add up to the ability for senders to retain control of their sensitive data even after they have sent it - and are therefore potentially critical in the event of user error. The lack of support for sending large files securely also leaves open the risk for users to revert to using free, insecure web services to accomplish this task. The lack of internal encryption is also potentially detrimental to an organisation's data security. Without end-to-end encryption there will always be places within the network where data is sent unencrypted.

There are also additional limitations in the way O365 message encryption functions:

- Replies are received encrypted in a user's mailbox, compromising mail scanning and archiving activity
- No apps are available for third parties
- The full encryption feature suite is dependent on the O365 plan

So although O365 does provide a variety of message encryption features that can secure email, the limited feature set presents the question of whether it is truly effective and comprehensive enough for the modern organisation looking to send and receive sensitive emails and data in and out of their domain. There is also no flexibility to manage sensitive data wherever its location.

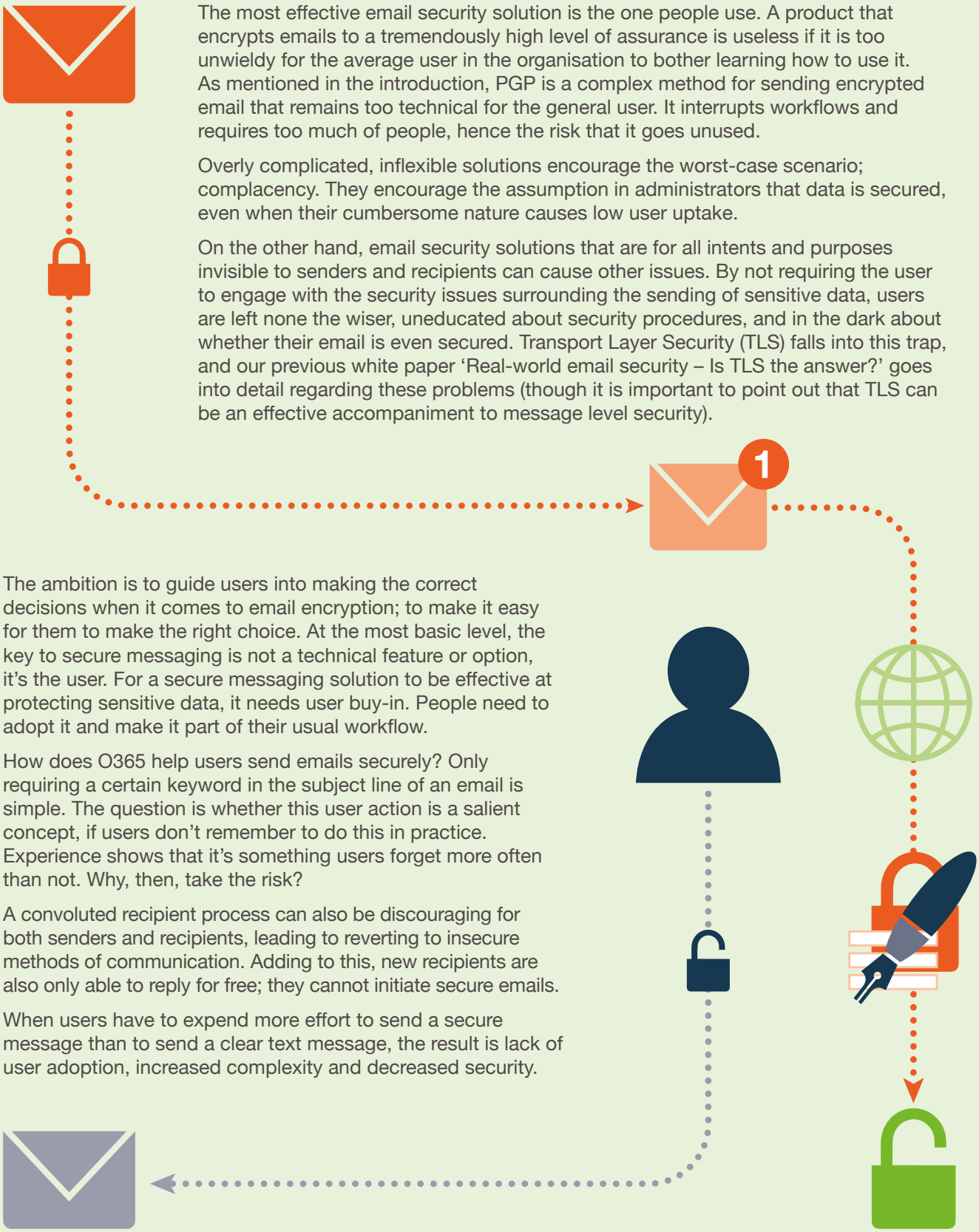
TWO: USER ADOPTION

How can we make sure our staff are sending emails securely when sharing sensitive information?

The most effective email security solution is the one people use. A product that encrypts emails to a tremendously high level of assurance is useless if it is too unwieldy for the average user in the organisation to bother learning how to use it. As mentioned in the introduction, PGP is a complex method for sending encrypted email that remains too technical for the general user. It interrupts workflows and requires too much of people, hence the risk that it goes unused.

Overly complicated, inflexible solutions encourage the worst-case scenario; complacency. They encourage the assumption in administrators that data is secured, even when their cumbersome nature causes low user uptake.

On the other hand, email security solutions that are for all intents and purposes invisible to senders and recipients can cause other issues. By not requiring the user to engage with the security issues surrounding the sending of sensitive data, users are left none the wiser, uneducated about security procedures, and in the dark about whether their email is even secured. Transport Layer Security (TLS) falls into this trap, and our previous white paper 'Real-world email security – Is TLS the answer?' goes into detail regarding these problems (though it is important to point out that TLS can be an effective accompaniment to message level security).



The ambition is to guide users into making the correct decisions when it comes to email encryption; to make it easy for them to make the right choice. At the most basic level, the key to secure messaging is not a technical feature or option, it's the user. For a secure messaging solution to be effective at protecting sensitive data, it needs user buy-in. People need to adopt it and make it part of their usual workflow.

How does O365 help users send emails securely? Only requiring a certain keyword in the subject line of an email is simple. The question is whether this user action is a salient concept, if users don't remember to do this in practice. Experience shows that it's something users forget more often than not. Why, then, take the risk?

A convoluted recipient process can also be discouraging for both senders and recipients, leading to reverting to insecure methods of communication. Adding to this, new recipients are also only able to reply for free; they cannot initiate secure emails.

When users have to expend more effort to send a secure message than to send a clear text message, the result is lack of user adoption, increased complexity and decreased security.

THREE: AUDITING

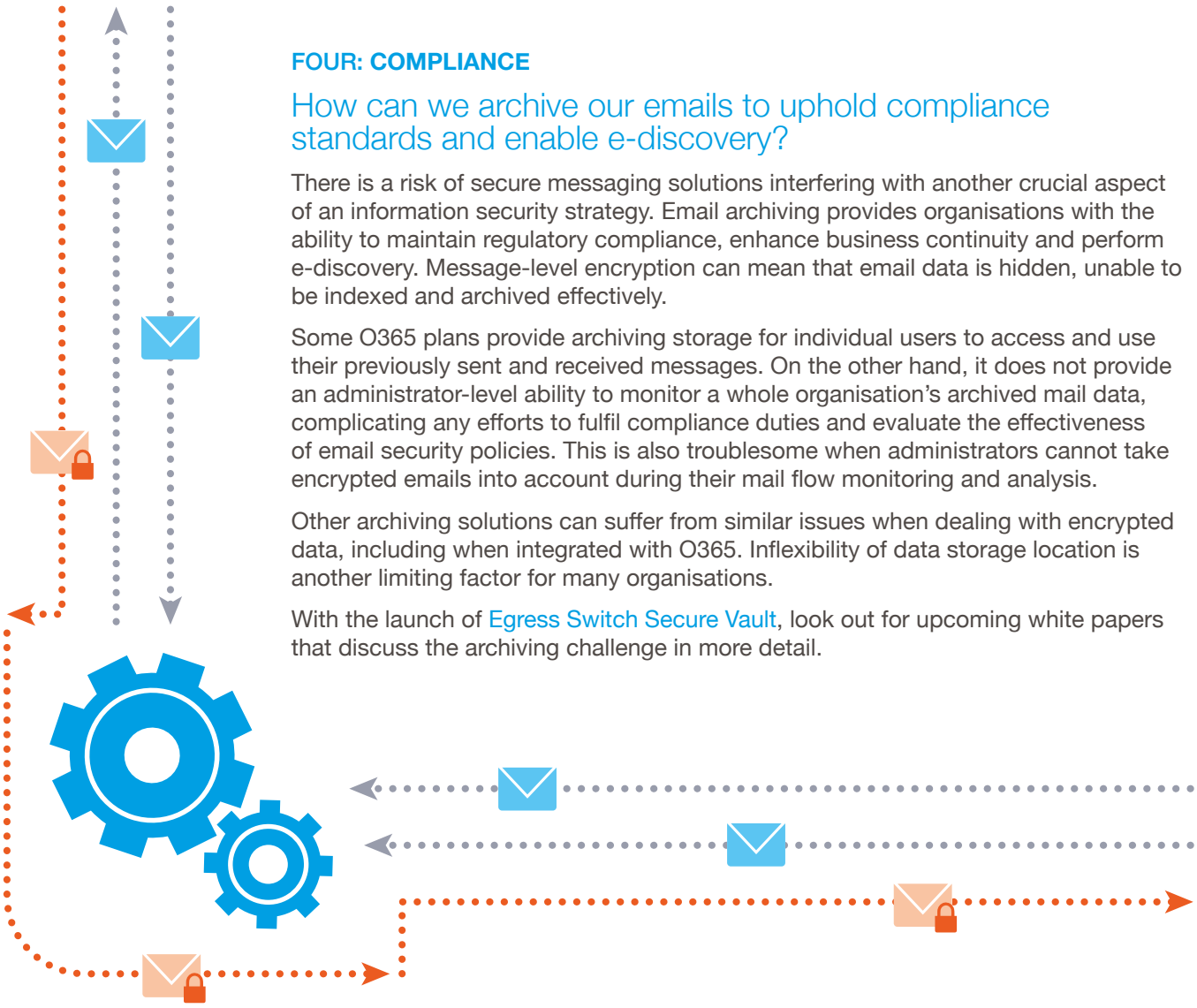
How can we keep track of the flow of sensitive data in and out of our organisation?

We have previously mentioned the importance of user buy-in when considering email encryption software. This is half the battle. While users need to easily send their secure email, administrators need to be able to check that this is happening. They need the tools to monitor the flow of sensitive data in and out of their organisation.

This is crucial for compliance and control. Being kept in the dark, not being able to see the types of sensitive data being sent and the level of protection applied, leaves businesses especially vulnerable to data breaches.

A lack of auditing functionality, similarly a drawback in TLS, is a critical barrier to adoption of O365 in the enterprise space. There is no auditing of sent encrypted messages, including access reports and forwarding. There is no revocation feature, so senders cannot prevent access to secure messages after sending.

Detailed auditing is essential to confirm secure receipt of sensitive information, as well as monitor which domains are being sent this data, and this can be a crucial feature of many organisations' compliance requirements.



FOUR: COMPLIANCE

How can we archive our emails to uphold compliance standards and enable e-discovery?

There is a risk of secure messaging solutions interfering with another crucial aspect of an information security strategy. Email archiving provides organisations with the ability to maintain regulatory compliance, enhance business continuity and perform e-discovery. Message-level encryption can mean that email data is hidden, unable to be indexed and archived effectively.

Some O365 plans provide archiving storage for individual users to access and use their previously sent and received messages. On the other hand, it does not provide an administrator-level ability to monitor a whole organisation's archived mail data, complicating any efforts to fulfil compliance duties and evaluate the effectiveness of email security policies. This is also troublesome when administrators cannot take encrypted emails into account during their mail flow monitoring and analysis.

Other archiving solutions can suffer from similar issues when dealing with encrypted data, including when integrated with O365. Inflexibility of data storage location is another limiting factor for many organisations.

With the launch of Egress Switch Secure Vault, look out for upcoming white papers that discuss the archiving challenge in more detail.

Conclusion

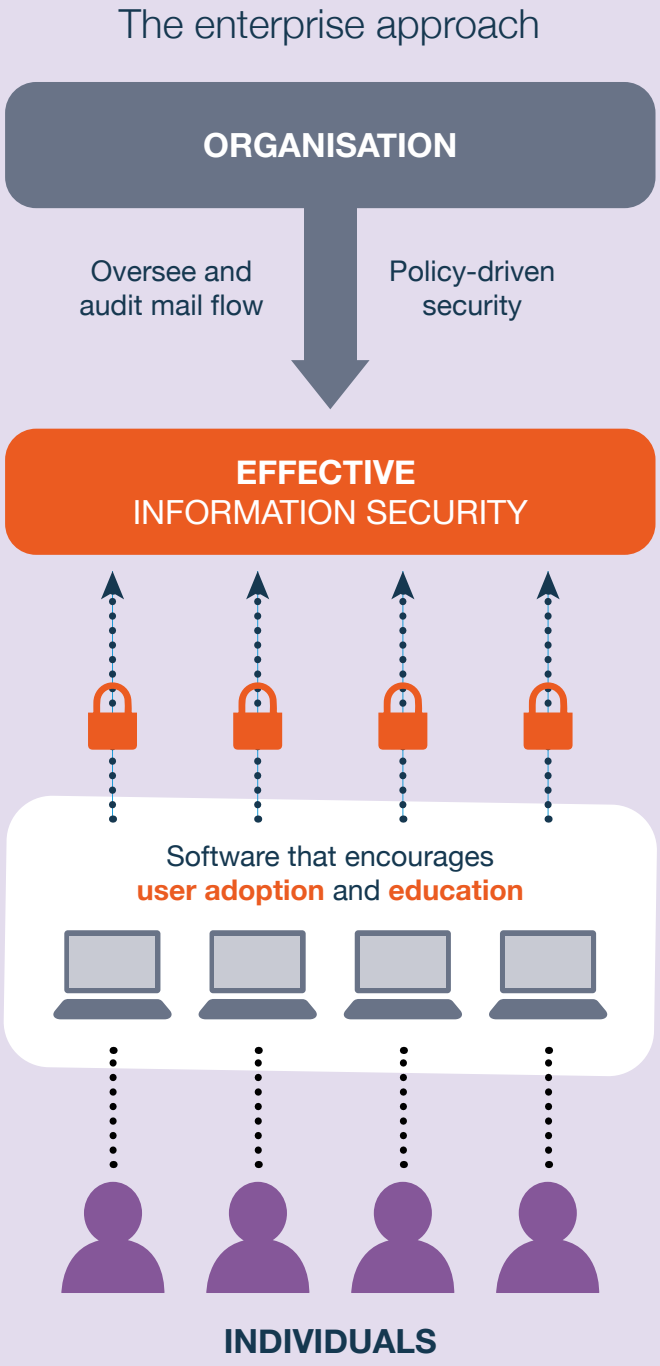
Choosing an email security solution is not a decision to take lightly. In the modern world, where data loss is an increasing risk, efforts to steal data are becoming ever more sophisticated and users are complacent, there has never been a more important time to choose an email encryption solution, and choose wisely.

O365 brings so many benefits to email, it's not hard to explain the attraction of O365 message encryption. The four considerations raised in this white paper should therefore hopefully highlight some of the practicalities and pitfalls of adopting O365 message encryption. Sometimes it is a question of finding out what else is available, discovering features that you require that you didn't even realise existed.

One idea that presented itself in the white paper is the difference between email security for the individual user and email security for the organisational as a whole.

A combined top-down and bottom-up approach is required: individuals need to adopt the solution, and they can do so via software that is easy to use and provides the features they require in their day-to-day work. Every individual's email activity, when taken as a whole, leaves organisations with the requirement to oversee mail flow and conform to compliance standards, whilst maintaining business continuity and analysing the success of their email security strategy.

This enterprise approach to email security seems lacking in O365 as it stands: the lack of auditing, lack of organisation-level compliance-based search, and lack of e-discovery leaves administrators in the dark. At the same time, individual users are not provided with the features and functionality that allow them to securely maintain current working practices, such as sending encrypted files, revoking access to previously sent emails, and sending to shared mailboxes.



Egress Switch and Office 365

About Egress Switch

Egress Software Technologies is the leading provider of security services that protect shared information throughout its lifecycle, delivered using a single platform: Egress Switch.

The Switch platform enables end-users to share and collaborate securely, whilst maintaining compliance and reducing the risk of data loss. These award-winning integrated services include email and document classification, email and file encryption, secure managed file transfer, secure online collaboration, and secure email and file archiving. Certified by UK Government, Switch offers a seamless user experience, powerful real-time auditing and patented information rights management, all accessible using a single global identity.

Office 365 integration

The Switch platform integrates fully with O365, allowing users to send encrypted emails directly from MS Outlook and benefit from the comprehensive Switch security feature set. Users can revoke messages after sending, send to shared mailboxes and send encrypted files without size restrictions, as well as track and control access and use of their sensitive shared data in real-time. Administrators can monitor mail flow in and out of their organisation, and have greater confidence in their network security via client-side encryption at rest and internal encryption.

Switch can aide adoption of O365. It can encourage enterprise organisations to move to a hosted mail service with the reassurance that data security and compliance is maintained. Since Switch integrates perfectly into their existing workflows, organisations can be confident that their users will buy into the secure messaging strategy. Even when communicating with people outside the organisation, data exchange is kept secure and simple, thanks to the recipient's ability to sign up and communicate securely for free, using their existing email address, without even having to download any software.

Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of security services that protect shared information throughout its lifecycle, delivered using a single platform: Egress Switch.

The award-winning Switch Platform includes email and document classification, email and file encryption, secure managed file transfer, secure online collaboration, and secure email and file archiving.

www.egress.com

info@egress.com
0844 800 0172
@EgressSwitch