EMAIL PROTECTION

sealpath™

SealPath enables you to protect attachments easily and conveniently for both the sender and the receiver. The attachments and the body of the message are sent with lasting protection that enables remote control of what others can do with them.

- Keep your attachments and messages under control at all times, even although it has already been sent.
- It prevents information leaks by third parties, limiting what others can do with your messages (read only, edit, etc.).
- It deletes attachments that have been sent erroneously to third parties.
- It monitors who accesses, when they do so, and whether anybody tries to access without permission.
- Complies with the data protection regulations by keeping the information encrypted.
- Very simple to use for both senders and recipients.

DO YOU CONTROL YOUR ATTACHMENTS SENT BY

According to data from the ICO in UK (Information Commissioner's Office: https://ico.org.uk) a significant part of information leaks reported in the past year were caused by sending emails to the wrong recipient.

Some interesting statistics about email:

- Worldwide more than 140 billion emails are sent every day.
- We dedicate 2 hours a week collaborating using attachments.
- We send and receive an average of 15 attachments/day. 5000/year.
- An average of 6 copies per document are generated.
- 73% of the documents are modified after being sent.

This data shows that our documentation travels without restriction via attachments and copies. Multiple copies of corporate documents can end up in different email inboxes of recipients, on PCs and even personal devices.

DLP AND ENCRYPTION TO PREVENT DATA LEAKS BY EMAIL

A DLP system for email is on the perimeter of the network and scans emails sent outside of the organisation. Problems considered:

- Blocking confidential documentation from being sent, but it is sometimes necessary to let it through to share it externally.
- It is difficult to determine what is confidential and what is not.
- It is not possible to revoke access once the email has been sent.

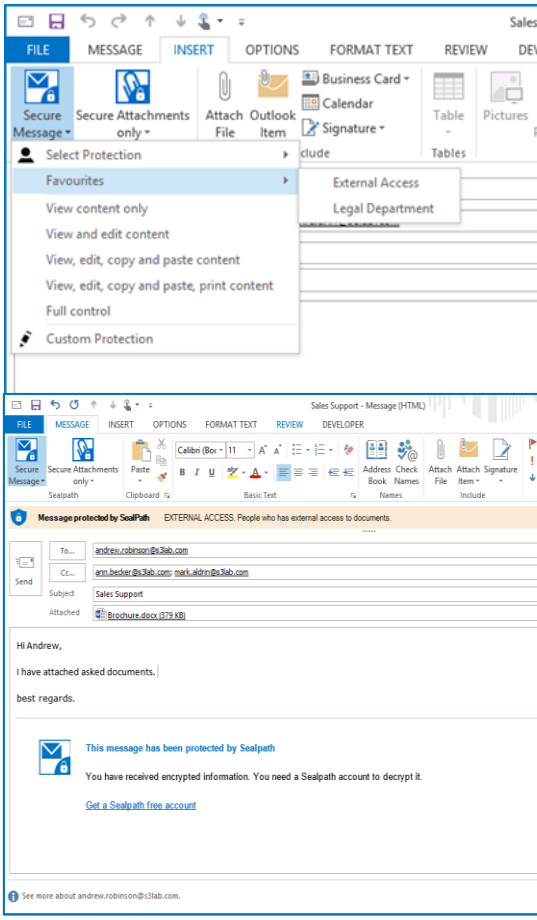
Another method used to minimise data leaks via email is PGP or S/MIME type encryption. The problems with this technique are:

- It is necessary to understand how public/private key technology works, generating a few keys, providing the public key to the person who wants to send information and receiving theirs.
- The receiver must also understand how this technology works.
- Plugins are needed for the encryption/decryption.
- Once the email or attachment has been decrypted by the recipient, it is not possible to prevent it being forwarded, printed, saved, etc.
- It is not possible to revoke access to the email or document.

EMAIL PROTECTION

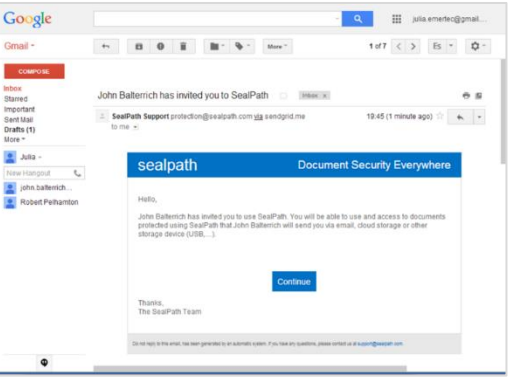
SEALPATH: SIMPLICITY AND FLEXIBILITY IN EMAIL PROTECTION

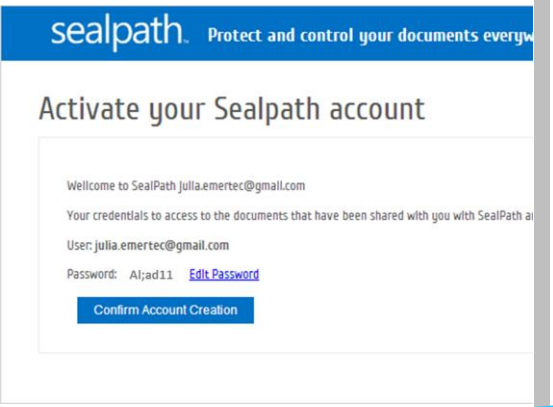
SealPath for Outlook (2003, 2007, 2010, 2013, 2016) enables you to protect emails and attachments easily and conveniently, simply by following these steps:



AS THE SENDER OF THE MESSAGE

- Include in Outlook the recipients to whom you wish to send it.
- Select the attachment(s) you wish to send.
- Use the option “Secure attachments only” to protect only the attachments or “Secure message" to protect the message and the attachments.
- You can chose to protect the message or attachments for the recipients or protect through a specific protection policy that has already been defined (e.g. Messages to lawyers XYZ, Protection for project XYZ, etc.).
- If it is protected for the recipients, you decide what level of access control they will be permitted: Read only, Read and Edit, etc.





AS THE MESSAGE RECIPIENT

- If you have not yet registered at SealPath you will receive an invitation automatically to do so. This step only needs to be completed once.
- Moreover, in the footer of the message received you will see the registration instructions, if you have not done so previously.
- When you receive the message or Office attachments, simply include the credentials with which you have registered and you will be able to open the document with the permission you have been given.
- After you have registered and opened the first file, simply open the documents or emails when you receive them; it will not be necessary to enter your password again.
- The receiver can use any email client; it is not necessary to have Outlook or to install any type of plugin, you just need to have Microsoft Office on the computer.

EMAIL PROTECTION

sealpath™

ADDITIONAL CONTROL REGARDING ATTACHMENTS

Although the message and attachments have already been sent, you may:

- Destroy them remotely or revoke access, preventing anyone accessing a certain attachment again, or anyone accessing a certain set of documents again.
- Know if anyone has opened the attachments, when they did so, whether anyone has tried to open them without permission, etc.
- Activate more permission for the attached documents or limit them without the need to re-send them. E.g. give permission to edit when before they only had permission to read, or the other way round, making it read-only when before it could be edited and printed for example.

INSTALLATION AND IMPLEMENTATION

SealPath for Outlook is available within the SealPath Enterprise SaaS and On-Premise solutions.

- Both are integrated within Active Directory or LDAP with which the internal users can use their domain credentials for SealPath.
- It is not necessary to manage the external users. They register themselves on their own and no additional action by IT is needed.
- The Outlook plugin is integrated in the SealPath client that may be installed individually or by policies of AD group, System Centre, etc.
- The "*look and feel*" of the invitations that the external users receive can be configured to include the company logo or specific text.
- The signature of the protected emails can be configured to inform the receiver that the content is encrypted by the issuing company.

Moreover the administrators of the solution may at any time:

- Revoke access to any attachment sent in the organisation.
- Fully track the access to the protected documentation and attachments.
- Recover an encrypted message or document leaving an audit log.
- Transfer ownership of the documents and attachments among users.
- Prevent ex-employees accessing attachments previously protected.
- Have statistics on blocked access attempts, more active users with protected documentation, etc.