sealpath™

THE MOST FLEXIBLE IRM PROTECTION FOR OFFICE 365 USERS

Thousands of businesses collaborate daily using the Microsoft Office 365 cloud. They upload their documents to OneDrive, manage critical documents with SharePoint Online or send emails with attachments that may contain confidential information.

SealPath allows Office 365 users to easily and flexibly manage their most critical information. Simply dragging or uploading documents to a file, which completely protects them. Users can control who accesses their documents, when and with which permissions, as well as remotely deleting documents, even those in the hands of external users.

AUTOMATED PROTECTION FOR SHAREPOINT AND ONE DRIVE

With SealPath you can automatically secure the documentation stored on Share-Point or OneDrive without requiring user intervention. It is not necessary to trust the user to perform manual protection. Thus when users download the documentation from a certain library it travels with SealPath protection and you can control who opens it and when or revoke the permission remotely.

A business user may manage a server's file permissions at any time using the Seal-Path automated protection. They can forget having to make requests to TIC and the associated waiting time involved. The administrator initially applies a generic policy for said file with the business user adding and removing permissions where necessary.

NATIVE INTEGRATION WITH OFFICE

When you protect an Office document and send it to your collaborators, the latter do not need to install any special software, plugin or complement to access said document. Depending on the authorisation they have, users can open the document, edit it, create comments, etc. You will have full control of the document and can see who accesses it and when. You can also remotely delete the document.
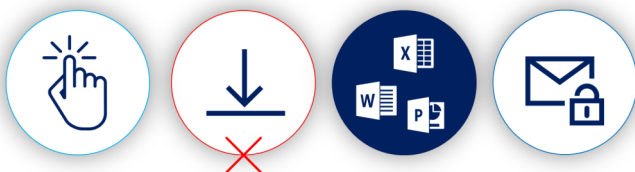
This can be easily protected via a Office or Outlook plug-in. Either using the mouse via the right click function over the documents or with a simple drag & drop to the SealPath Desktop.

Protects the body of the message and attachments with a single click from Outlook. You can protect for all addressees or according to specific protection policies. Addressees do not need to have Microsoft Outlook to open the protected document.

WORK WITH STANDARD TOOLS

In contrast to other solutions you can protect PDFs without having to use inconvenient, limited viewers. Use your favourite PDF reader or editor (Adobe Reader, Foxit, Nuance, Nitro, etc.). Not only does it enable display of protected PDFs but, if the user has the required permission level, also editing of the same.

This also includes other types of applications such as Visio, Access, Project, etc. SealPath also integrates with CAD (AutoCAD, SolidWorks, Siemens) native tools without the need to use viewers, as well as having the most complete support for file formats available on the market.
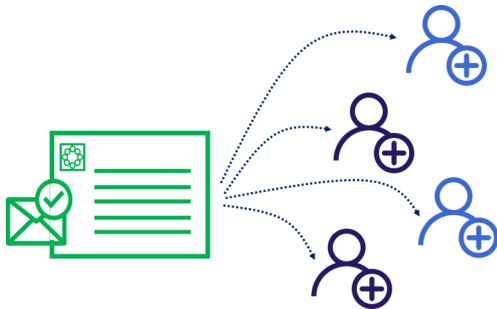
EXTREMELY SIMPLE SHARING

Collaboration with external users is extremely simple. External users will also have the option of self-invitation to access the protected documents. Approved users do not need to request the administrators to register them as third party users. Neither do the administrators have to manage who has access to the platform. Invitations and self- registration portals may be tailored with your look and feel, in order for when the user receives them they will know they originate from a collaborator with whom they have been working.

FLEXIBLE POLICY MANAGEMENT. ADAPTED TO YOUR USAGE REQUIREMENTS

Having flexible management of protection policies is vital in an IRM application so that users do not have to contact IT to protect information or repeat tedious operations every time they wish to protect a document.

With SealPath both users and administrators can create specific protection policies for their needs and the cases they deal with. Users can create policies to share with external users without having to depend on IT. Moreover, administrators can create protection policies (e.g. COMPANY CONFIDENTIAL, COMPANY INTERNAL, LEGAL DEPARTMENT, etc.) and assign them to individual or group users so that said users have policies ready to use by right-clicking on the document (from Office, etc.).

With SealPath you don't need to assign users to each protection policy one by one. You can assign AD or LDAP groups or include whole domains or subdomains (e.g. *@company.com). You can also provide access to all users while retaining the full access tracking option over a document by adding anyone@any.com.
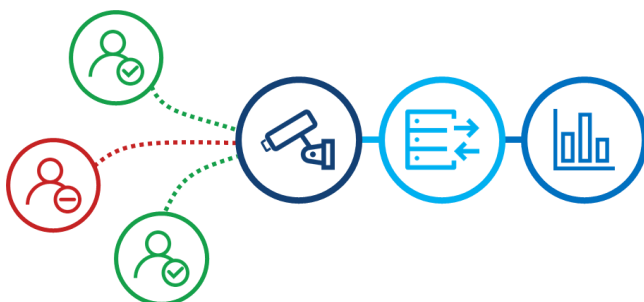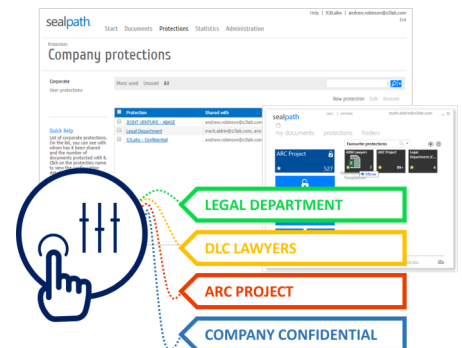
MONITORING, REMOTE DELETION AND MORE

Both users and administrators can see who has accessed their documents, when, or if somebody has tried to access them without necessary permissions.

Remote denial of access to a specific person is possible, as well as the deletion of a specific document, the transfer of documents between users automatically, as well as off-line access permission to documents without having opened them previously etc.

The administrator has at their disposal powerful centralised monitoring, policy settings and auditing tools, that allows the company's most critical information to remain safe and sound.