sealpath

# KEEP YOUR DATA PROTECTED AND UNDER CONTROL IN G-SUITE

Google G-Suite enables companies to collaborate conveniently without needing to manage internal infrastructures or servers. Thanks to G-Suite's cloud computing capability, users conveniently manage their email, schedule and documents in the cloud from the browser and administrators have tools to manage privacy and control access to corporate data in the G-Suite environment.

However, once your documents leave this environment and are downloaded from Drive, sent by email, etc. the users and the administrators themselves lose control of them. Would you like to be able to control access to your documents even when they have exited Drive? Now you can. With SealPath.

## YOUR FILES AUTOMATICALLY PROTECTED IN DRIVE

SealPath can be used to automatically securitise the content that you upload to Google Drive, adding a protection layer to documents that enables you to send them encrypted and restrict the right of use over the same. SealPath removes the need to trust users to manually protect the information before uploading to Drive.

With the automatic protection for Google Drive:

- Automatically protect content uploaded to Drive, transparently for users, without requiring them to perform additional actions.
- Avoid unauthorised accesses to confidential information stored on Drive.
- Comply with the regulations on protection of data by keeping your sensitive data in the cloud.



## DYNAMICALLY CONTROL THE ACCESS PERMISSIONS TO THE DOCUMENTS

You decide what permission level users need to access the documents. You can grant some users *read only* permission, others *read and edit* but not *cut and paste* or *print out* content, depending on the sensitivity of the documents involved.

You can grant permission to 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.

Place dynamic watermarks so that if the user makes a screenshot it will be saved with the user's email address. SealPath enables granular access control that can be configured by users and administrators to act on the document regardless of its location.

## DELETE DOCUMENTS BY REMOTE CONTROL AS REQUIRED

Both users and administrators can revoke access to the documents or delete them from a remote workstation. The revocation may apply to an individual document or to a group of documents. Furthermore, the user will lose access to all the protected corporate documents without the need to modify the SealPath policies by simply deleting said user from the active directory.

Link expiry dates to documents so that the users with whom you have shared a document no longer have access rights to the same after a specific date. Edit the expiry date of market files in real time.

## MONITORING AND TRACKING ACCESSES

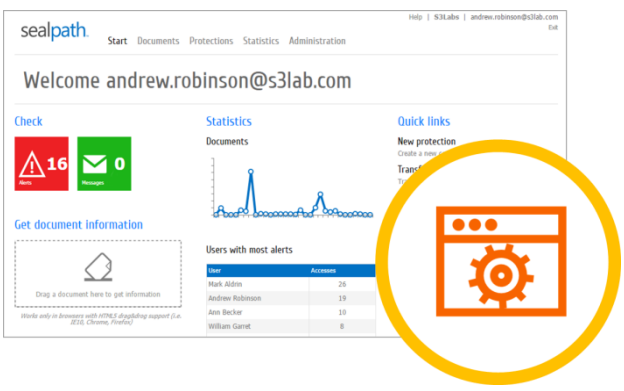
Users can see in real time if other users for whom they have protected the documents have opened them, if anyone has removed the protection because they have sufficient rights or if anyone is attempting to access the protected documentation without permission.

SealPath provides centralised monitoring for the administrator with risk control reports on the documentation including the Top 10 blocked access attempts, which documents they attempted to access plus those accessed without permission, most active internal and external users, most and least used policies, etc. This will give you and instant overview of the situation of the company's protected documentation.

## SO SIMPLE TO SHARE WITH EXTERNAL PARTNERS

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.

The administrator may initially provide permission to the company's users from the website administrator's dashboard. He/she can also register external users automatically. Administrators can control whether or not to provide the option of self-invitation/self-registration to external users or if they prefer to manage it without sending automatic invitations.




## POWERFUL ADMINISTRATOR CONTROLS

The administrator is provided with various controls to easily manage the company's protected documentation and to audit use of the same at any time.

- The administrator can transfer ownership of the protected documents among users. This can be done for all the documents or by protection policy.
- The administrator can create protection policies and assign them to users or groups of users, departments, etc. so that the users can then employ these policies to protect documents with the desired protection level without having to create them themselves.
- It has a super-user mode that enables the holder to de-protect any file, leaving a record in the audit log, powerful audit controls to know who has accesses a file and when, etc.