AUTOMATIC PROTECTION FOR FILE SERVERS AND DOCUMENT MANAGEMENT SYSTEMS

One of the most common forms of internal collaboration in business is managing files or documents via shared network folders stored on internal file servers. Each department and user in the company has different network folders for exchanging and storing documents.

On the other hand, it is also common to store internal documents in document management systems such as SharePoint, Alfresco, etc. Documents are sometimes stored in internal access libraries, and other times stored and then shared with users outside the company by providing them access to the document manager.

INFORMATION CONTROL BEYOND THE REPOSITORY

While the documents are in the folders in the file server folder or document management system, the users who can access them and their permissions (read, write, etc.) can be restricted. However, once the documents leave this environment, and are downloaded to the user's desktop, control over their access is completely lost. That is, the user can copy the information, send it by email, leave it in other folders or even save it to a USB device.

Would you like to be able to control access to your documents even when they have exited these repositories? With SealPath you can, so that documents travel with persistent protection to accompany them wherever they go, even outside of the corporate network.

AUTOMATIC TRANSPARENT PROTECTION FOR THE USER

SealPath can be used to automatically secure the content uploaded to a folder on a file server or document management system, adding a protection layer to documents that enables them to be sent encrypted and restrictions placed on their rights of use. SealPath removes the need to trust users to manually protect the information:

With automatic protection for information repositories:

- Automatically protect content saved transparently for users, without requiring them to take additional actions.
- Avoid unauthorised accesses to confidential information removed from the repository.
- Comply with data protection regulations by keeping your sensitive data encrypted and audited.

DYNAMIC CONTROL OF ACCESS TO 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. These permissions can be changed dynamically even if the documents have been downloaded from the repository.

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.

REVOCATION OF ACCESS TO DOCUMENTS IN REMOTE

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, simply deleting a user from the active directory will restrict his or her access to all the protected corporate documents without the need to modify the SealPath policies.

Set the expiry date on documents so that they are inaccessible to users after this date.

MONITORING AND FULL AUDIT OF ACCESS TO DOCUMENTS

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 provide an instant overview of the situation of the company's protected documentation.

This monitoring is available whether the document is stored on the file server or document management system or if the documents have been downloaded and sent to third parties, etc.

INTEGRATION WITH AD/LDAP AND ADMINISTRATION CONTROLS

The administrator is provided with various controls to easily manage the company's protected documentation and to audit its use at any time. The administrator can transfer ownership documents among users, create corporate protection policies, etc. It also has a super-user mode that enables super users to de-protect any file, leaving a record in the audit log, etc.

SealPath also integrates with Active Directory and LDAP, so that groups defined in it can be protected, the domain credentials used to access documents, etc.