sealpath

DATA-CENTRIC SECURITY FOR THE ENTERPRISE

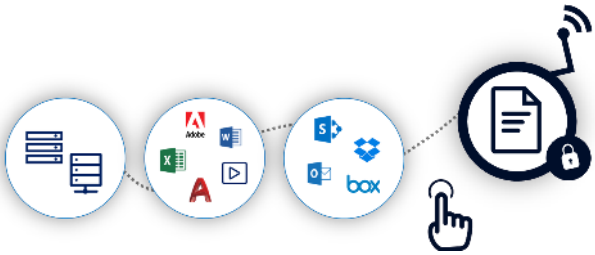
SEALPATH PROTECTS AND CONTROLS CORPORATE DATA. WHEREVER THEY TRAVEL

Don't leave your data security to chance. It's your data and belongs only to you. Every day, important business data is stored in documents, PDF, Excel worksheets, CAD designs etc. that are exposed to internal threats, human error, extraction by external attacks and the non-compliance of regulations.

By using a security approach which is based on data, SealPath allows organizations to continuously protect their sensitive data in any location throughout its lifecycle. The security travels with the file, allowing the company to keep it under control even when it is in other networks or on other devices. It offers full visibility regarding who accesses, when they do so, and whether anybody tries to access without permission. With one click, SealPath allows data access to be restricted, in real time, even if this data is in the hands of other users.

DYNAMIC DATA PROTECTION

- Granular access rights for data (view only, edit, plot/print, etc.).
- Set expiry dates, watermarks, off-line access, etc.
- Delete documents remotely even if they have already been sent.
- Control the subnets or IPs from which the information can be accessed.
- Data is encrypted, safe from improper access.



MAXIMUM EASE OF USE

- Unhindered access to standard tools: Office, Adobe, AutoCAD, etc.
- Intuitive and easy-to-manage interface.
- Protect by simply dragging the document to a folder, from Office, etc.
- Integrated authentication: AD, LDAP, SSO, Identity federation.
- Facilitate secure file sharing via email, Office 365, G-Suite, Box, etc.

COLLABORATION WITHOUT AGENTS OR INSTALLATIONS

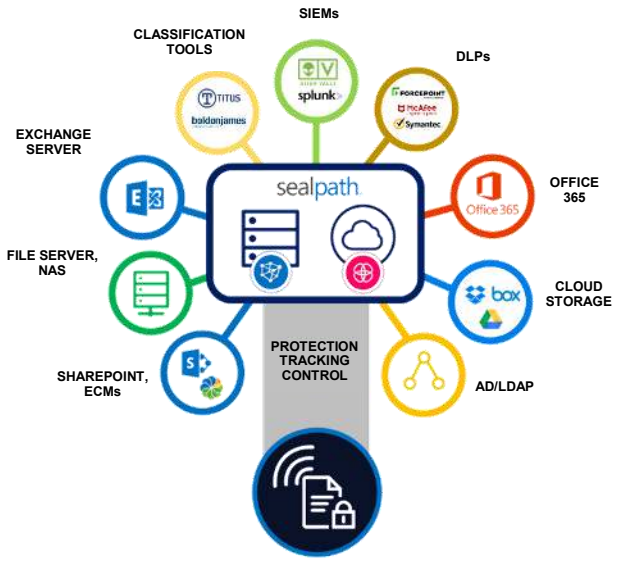
- Access protected documents from the browser.
- Cross-platform compatibility.
- Simple and secure collaboration directly in cloud repositories.
- Protect, manage policies and monitor access without agents.
- Automatic sending of invitations to external users.

EXHAUSTIVE AUDITING AND ACCESS CONTROL

- Audits of accesses and use of protected documentation.
- Available to the user it protects and to administrators.
- Alerts for attempts to access by blocked users, breached protection, etc.
- Risk control reports on the documentation.
- Powerful Top10 graphics, filterable lists, exportable, etc.

AUTOMATION OF THE PROTECTION

- Automatic protection for file servers, NAS, etc..
- Automatic protection of SharePoint libraries and Office 365.
- Automatic protection in Box, Dropbox and G-Suite.
- Automatic protection in the email through Outlook and Exchange.
- Integrated automatic protection with classification systems and DLPs.



INTEGRATION WITH CORPORATE SYSTEMS

- Seamless integration with Active Directory and LDAP.
- Option of working with groups and domain credentials.
- Integration with SIEM tools.
- Integration with DLP solutions (Symantec, ForcePoint, McAfee)
- Specific integration with simple, flexible SDK.

USE YOUR USUAL TOOLS

- Native integration with Office without requiring installed agents.
- Open protected PDFs with Adobe, Foxit, Nitro, Nuance, etc.
- Native integration with AutoCAD... No viewers required.
- Supported on Windows, Mac OSX, iOS and Android.
- Use Microsoft Outlook to send protected emails.

FLEXIBLE DEPLOYMENT OPTIONS

- Possibility of 100% On-Premise deployment.
- SaaS Model without requiring the installation of server components.
- Model for Managed Service Providers (MSPs).
- Can be integrated with SOCs adding data protection services.
- About physical, virtual infrastructure. Multi-tenant.

OPERATIONAL EFFICIENCY AND FAST START-UP

- Easy implementation both in SaaS/Cloud and On-Premise.
- Autonomous user management without depending on the administrator.
- Option of corporate and departmental policy creation.
- Possibility of having delegated file administrators.
- Protection from the outset, without the need to establish complex processes.

RISK REDUCTION AND LEGAL RESPONSIBILITY

- Facilitates compliance with regulations and standards (e.g. GDPR).
- Controlled access to files with regulated information (PCI, etc.).
- Full audit that registers attempts to access by blocked users.
- Option to reverse accesses remotely to avoid data leaks.
- Audit logging of the administrator that registers any operation.