DATASHEET

sealpath
SMART PROTECTION FOR SENSITIVE DATA

AUTODESK® AUTOCAD®

# IRM/E-DRM PROTECTION FOR AUTOCAD

## THE CHALLENGE

An important part of the most sensitive information of a company in the industrial and manufacturing field is its designs in CAD format. They contain competitive information about the company, specifications and details which, if they get into the hands of those who should not, can be of significant detriment to the company.

In manufacturing, engineering and industrial companies these types of files are shared throughout the supply chain with internal users, subcontractors and external partners, customers, etc. It is difficult to maintain transparency over sensitive information in the design and manufacturing process, which increases the risk of leakage of intellectual property and trade secrets.

Companies working in this sector with AutoCAD require the ability to protect and control their designs with product details, parts, etc. when shared internally and with other partners in the supply chain. Auditing access, controlling what they can and cannot do and being able to revoke access to designs when they stop working with a certain partner or when an employee leaves the organization.

## THE SOLUTION

SealPath protection for AutoCAD, through its SealPath Security Sandbox technology, adds persistent Information Rights Management (IRM) / Enterprise Digital Rights Management (E-DRM) protection to CAD designs no matter how they are shared within or outside the organization. The platform allows companies and engineering or design personnel to establish usage controls over designs (e.g., view only, edit, print, copy and paste, etc.), and monitor file usage.

Even though they are shared, the company protecting them will retain ownership of these designs so that if there is a potential risk of data leakage they can remotely delete these files or see who has attempted to access them without authorization. When you no longer wish to collaborate with these designs, the owner of the design can destroy it with a simple "click" of the mouse.

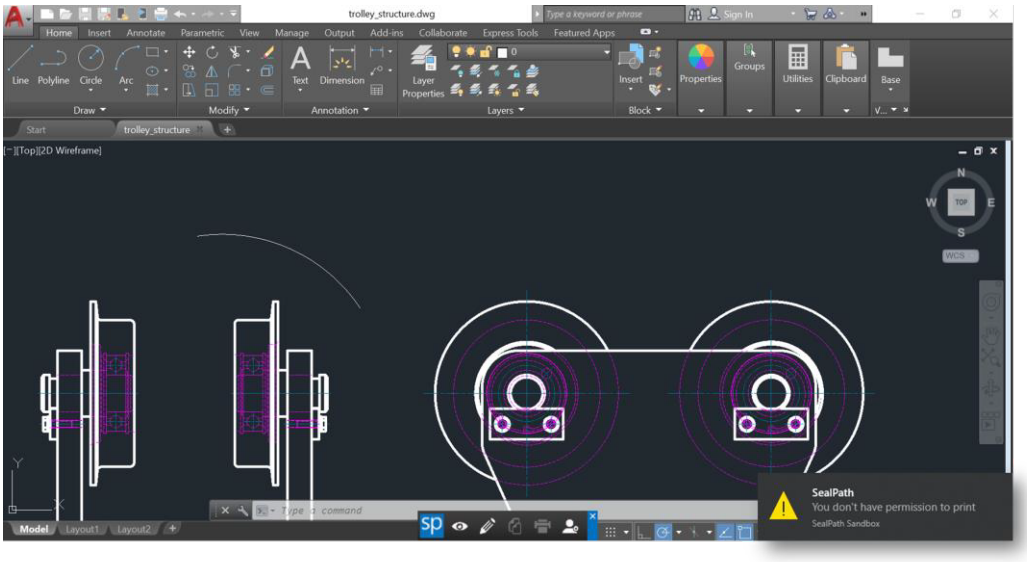

© SEALPATH TECHNOLOGIES S.L. – ALL RIGHTS RESERVED.

## HOW IT WORKS

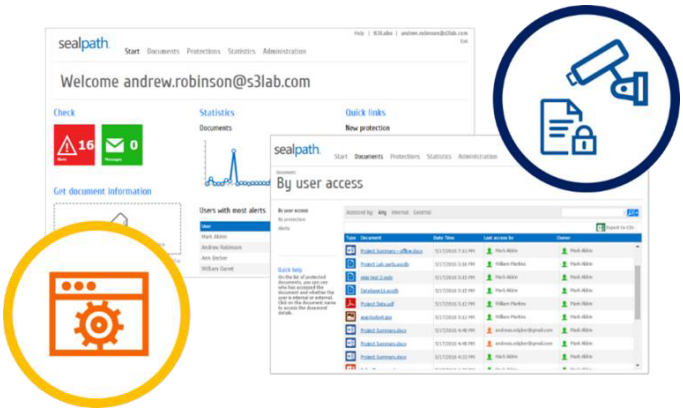
SealPath for AutoCAD is a solution that integrates with SealPath Enterprise SaaS and SealPath Enterprise On-Premise solutions. Users protect designs through the SealPath client by indicating the users, groups or domains with access to the information and their permissions (e.g. view only, edit, print, etc.). They can add expiration dates, and other controls such as offline access capability.

Protection can be manual or automatic, integrated with different information repositories: File servers, SharePoint, O365, G-Suite, Box, etc. In this case, just by storing or copying the designs in the repository they will be protected with the selected protection policy.

Once shared internally or with external partners, users can access the designs protected with AutoCAD, without external viewers. The user must first install the SealPath thin client with SealPath Security Sandbox technology, which will validate the user, control the user's permissions and only allow the user to perform the actions permitted by the information owner. For example, you will not be able to export content, copy, or print it.




User permissions are displayed in a floating bar above the design. In case the user tries to perform an action that is not allowed he/she will receive a notification on screen indicating that the action is not allowed.




On the other hand, the owner of the designs, will be able to see who is accessing, when, if someone tries to access without permissions, ultimately having full control of their files regardless of where they are.

sealpath
© SEALPATH TECHNOLOGIES S.L. – ALL RIGHTS RESERVED.

## AUTODESK AUTOCAD COMPATIBILITY CHART

| | |
|---|---|
| Supported Suites | AutoCAD, AutoCAD LT, AutoCAD Civil, AutoCAD Map 3D, AutoCAD Mechanical, AutoCAD Electrical, TrueDWG, DesignReview. |
| Versions | 2018, 2019, 2020, 2021. 32 y 64 bits. |
| Client platform | Windows 7 to Windows 10. |
| Supported formats | .DWG, .DWF, .DWS, .DWF, DWT |
| Available permits | View, Edit, Export (STEP, PDF, Save As, etc.), Copy & Paste, Print (Plot, Batch Plot, 3D Print), Add Users |
| Others | • Support of CAD drawings with references to other parts or files.<br>• Ability to import files with external extensions: e.g. CATIA, Pro/Engineer, SolidWorks, etc.<br>• Possibility to export files to other formats (if you have permissions): .DGN, .EPS, .IGS, etc.<br>• Limitations: Import of protected files is not supported. |
| Additional controls | Expiration by date, offline access to the design. |

## FEATURES

SealPath for CAD in conjunction with SealPath Enterprise On-Premise or SealPath Enterprise SaaS offers the following features:

| |
|---|
| ✓ Protection of CAD designs by controlling the identity of the user with access to the document and their permissions. |
| ✓ Assigning permissions to individual users, AD groups, domains (e.g. *@company.com) or sub-domains. |
| ✓ Application of time controls, offline access, etc. to designs. |
| ✓ Facilities for sharing with external users: self-provisioning, sending personalized access invitations, etc. |
| ✓ Automatic protection of designs stored in repositories such as file servers, SharePoint, O365, G-Suite, Box, etc. |
| ✓ Manual protection by the user or in batch mode |
| ✓ Monitoring of file access, blocked access attempts, statistics, risk levels on protected documentation. |
| ✓ Real-time remote file access revocation by file or policy. |
| ✓ Integration and automation with other systems through SDK .Net and REST. |
| ✓ 100% On-Premise or SaaS/Cloud deployment possible. |
| ✓ Support of additional CAD formats such as Office, PDFs (including 3D PDF), images, etc. through the SealPath Enterprise On-Premise or SaaS solution. |
| ✓ Integration with DLP tools (Symantec, ForcePoint, McAfee), SIEM, information classification, identity management, MDMs, etc. |


© SEALPATH TECHNOLOGIES S.L. – ALL RIGHTS RESERVED.

## USE CASES

SealPath enables the protection of designs and sensitive information in multiple use cases for engineering, manufacturing companies, etc. Some of them are:

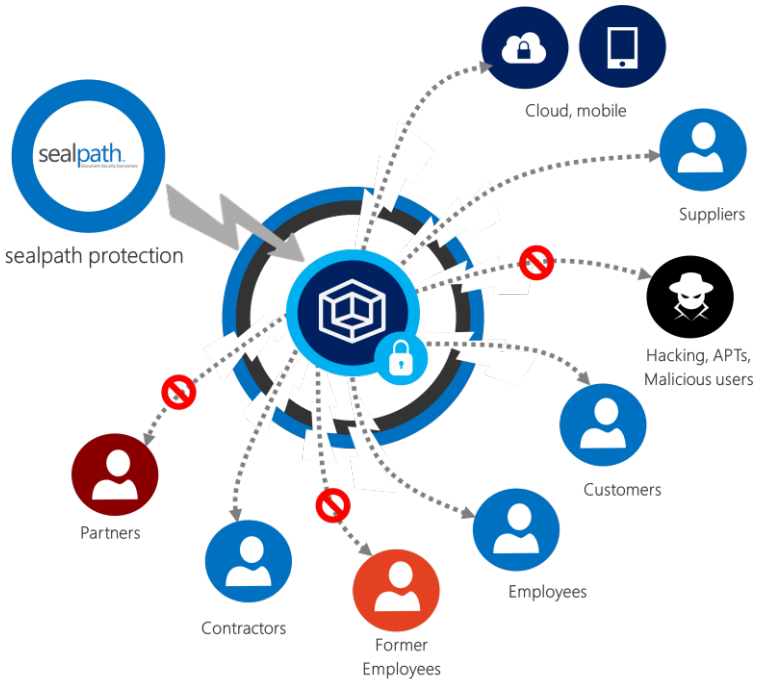
| | |
|---|---|
| Supply Chain Collaboration | CAD drawings and sensitive information are shared with suppliers who collaborate on design, testing, production, trials, etc. These suppliers can in turn work with others and you want to have traceability and control of who accesses the sensitive information avoiding possible leaks in the process. |
| Collaboration with partners in alliances | The organization collaborates with multiple companies to design a new product in an alliance or joint venture. Intellectual property and designs are assigned which, although controlled at a contractual level, do not have adequate security controls, and there is a risk of leakage of sensitive information. It is critical to ensure that only the right people access, monitor access or prevent access to information when the project is completed. |
| Information control in global engineering teams | When a new project to be designed is developed, people from different areas or business units must have access to it. The information is stored in different repositories, copied to local computers, etc. The more people access and the more distributed the information is, the greater the possibility that there may be leaks or loss of sensitive information. You need to control who can access it and if people on the team leave the organization, make sure they don't have access to CAD designs even if it has been copied to removable drives, etc. |
| Regulatory compliance, audits, export controls | The organization is exposed to regulatory controls by a particular client to keep their intellectual property safe. Violation of technical data export regulations or passing information control audits by customers must be avoided. It is necessary to have visibility into protected data and ensure that it is accessed by certain individuals in compliance with export regulations and controls. |
| Access by support or field technicians. | When deploying equipment, systems or machinery, field and support technicians must have access to very sensitive information that must be monitored. This is usually done by engineers working for suppliers who may leave these companies and move on to the competition. It is essential to be able to guarantee that people access it when they need to, even in places without internet connection, but to control that they only access what they need and access can be revoked if they stop working on the project. |


© SEALPATH TECHNOLOGIES S.L. – ALL RIGHTS RESERVED.

## BENEFIT SUMMARY

SealPath for AutoCAD provides the following benefits in summary:

- Prevent potential data leakage by controlling who can access designs and with what permissions.
- Ability to monitor access and have complete visibility throughout the supply chain and when collaborating with partners or global engineering teams.
- Ability to revoke access to information by preventing users from accessing it once they have left the organization or stopped collaborating with a partner.
- Ease of use and management, allowing users to work with native AutoCAD tools, without viewers, and with protection automation capabilities.




## ABOUT SEALPATH

SealPath is a leading data-centric cyber security company that enables companies to protect their sensitive information wherever it travels. SealPath's security travels with the documents and allows the owner of the documents to see who is accessing, when, with what permissions and to destroy the information remotely in the event that we cease to collaborate with a third party. Operating in more than 20 countries and with a strong focus on R&D to continuously improve its solutions, SealPath stands out for its ease of use and integration with other data protection tools present in the corporate environment.