

## MICROSOFT PURVIEW PROTECTION FOR CAD

### 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 CAD drawings 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

Microsoft PurView (formerly Microsoft Information Protection) is a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels. SealPath Protection for CAD, through its SealPath Security Sandbox technology integrated with Microsoft PurView, adds persistent Rights Management 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.

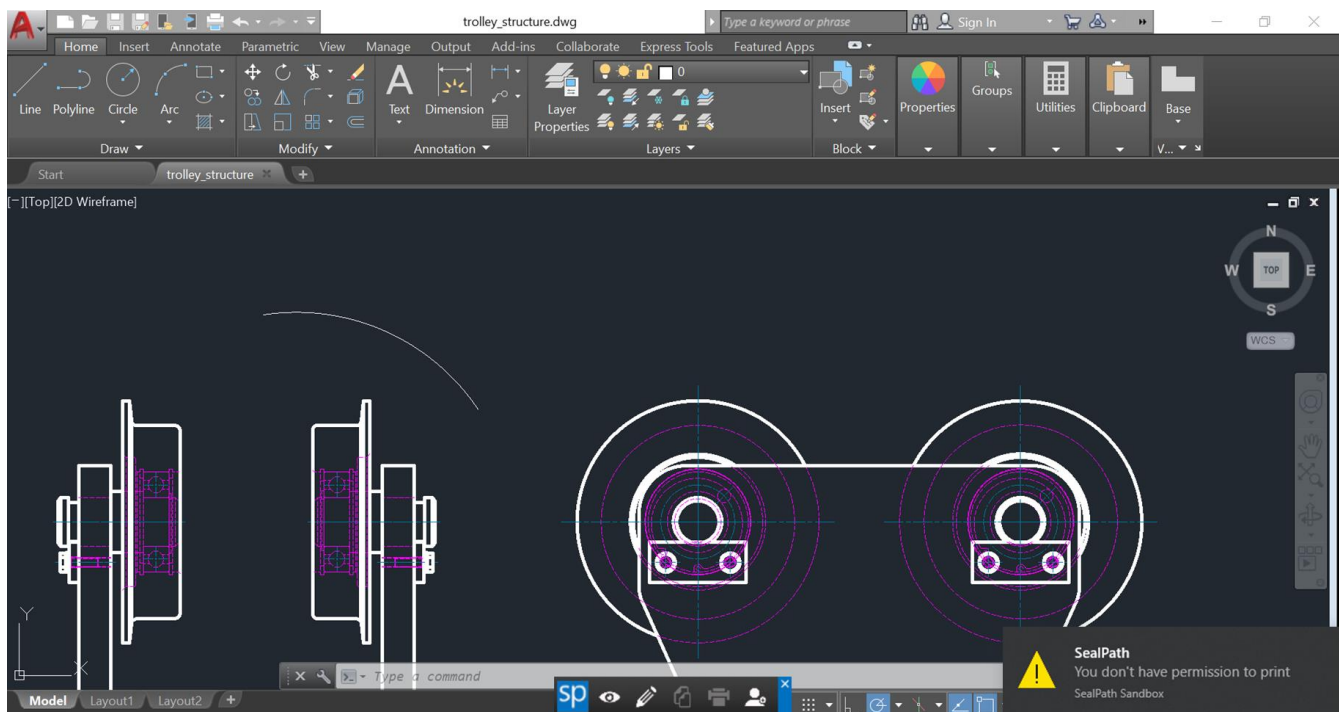
Even though they are shared, the company protecting them will retain ownership of these designs so that if there is a potential risk of data leakage, they can remotely delete these files or see who has attempted to access them without authorization. When you no longer wish to collaborate with these designs,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

## HOW IT WORKS

SealPath Protection for CAD is a solution that integrates with Microsoft PurView and extends it to CAD files. Users protect designs through the PurView client by indicating the users, groups or domains with access to the information and their permissions (e.g. view only, edit, print, etc.) through a specific label / protection policy.

Protection can be manual or automatic, integrated with different information repositories through the PurView Scanner. 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 through their regular CAD tools (i.e. AutoCAD, Inventor, SolidWorks, etc.), without external viewers. The user must first install the PurView Client or Viewer with the SealPath Security Sandbox software, 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 permission, etc. through the Microsoft PurView portal, ultimately having full control of their files regardless of where they are.

## AUTODESK CAD COMPATIBILITY CHART

Supported Suites and formats	<ul style="list-style-type: none"> <li>• AutoDesk AutoCAD: .DWG, .DWF, DWS, .DWF, or .DWT formats (Electrical, Map 3D, Mechanical, Civil, LT, etc.) or in applications such as TrueView.</li> <li>• AutoDesk Inventor 3D: .IPT, .IAM, .IDW, or .DWG.</li> <li>• AutoDesk Revit: .RVT, .RTE, or .RFA formats.</li> <li>• Siemens Solid Edge: .ASM, .DFT, .PAR, .PSM or .PWG formats.</li> <li>• Dassault Systèmes CATIA: .CATPart, .CATDrawing or .CATProduct.</li> <li>• Dassault Systèmes Solidworks: .slddrw, .sldprt, .sldasm or .sldxml formats.</li> <li>• Dassault Systèmes Draftsight: .dwg, .dws, .dwt or .dxf formats.</li> <li>• Grabert ARES Commander &amp; Kudo: dwg, .dws, .dwt or .dxf formats.</li> <li>• PLMs: AutoDesk Vault, SolidWorks PDM, Enovia, Ares Kudo.</li> </ul> <div>  <b>AUTODESK AutoCAD</b>  <b>AUTODESK Inventor</b>  <b>AUTODESK Vault</b> </div> <div>  <b>AUTODESK Revit</b>  <b>SIEMENS SOLID EDGE</b>  <b>SOLIDWORKS PDM</b> </div> <div>  <b>CATIA</b>  <b>SOLIDWORKS</b>  <b>ENOVIA</b> </div> <div>  <b>DraftSight</b>  <b>ARES® Commander DESKTOP CAD</b>  <b>ARES® Kudo CLOUD CAD</b> </div>
Versions	2018 - 2025. 32 y 64 bits.
Client platform	Windows 8-Windows 11.
Permissions	View, Edit, Export (STEP, PDF, Save As, etc.), Copy & Paste, Print (Plot, Batch Plot, 3D Print), Add Users.
Others	<ul style="list-style-type: none"> <li>• Support of CAD drawings with references to other parts or files.</li> <li>• Ability to import files with external extensions.</li> <li>• Possibility to export files to other formats (if you have permissions).</li> </ul>
Additional controls	<ul style="list-style-type: none"> <li>• Expiration by date, offline access to the design.</li> </ul>

## FEATURES

SealPath protection for CAD in conjunction with Microsoft PurView offers the following features:

✓	Protection of CAD designs by controlling the identity of the user and their permissions.
✓	Assigning permissions to individual users, AD groups, etc.
✓	Application of time controls, offline access, etc. to designs.
✓	Facilities for sharing with external users registered in Azure PurView
✓	Automatic protection of designs stored in repositories through the PurView Scanner.
✓	Manual protection through PurView client by the user or in batch mode through scripts.
✓	Monitoring of file access, blocked access attempts, etc.
✓	Real-time and remote file access revocation.
✓	Integration and automation with other systems through PurView SDK / MIP SDK.
✓	Backend based 100% on Microsoft PurView.

## USE CASES

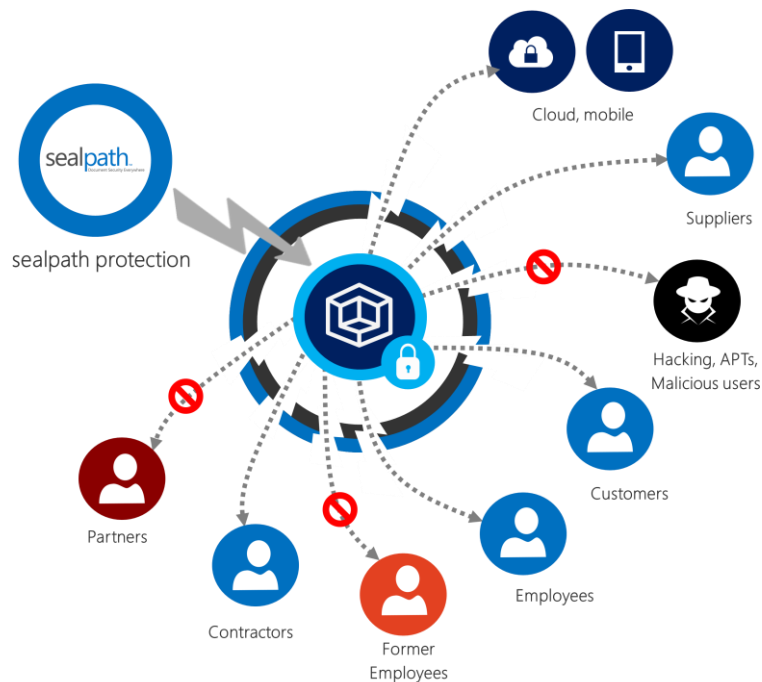
SealPath Protection for CAD enables the protection of designs and sensitive information in multiple use cases for engineering, manufacturing companies, etc. Some of them are:

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 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 sometimes done by engineers working for suppliers who may leave those companies and go 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.

## BENEFIT SUMMARY

SealPath Protection for CAD 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 CAD tools, without viewers, and with protection automation capabilities.



Do you want to know more? Contact SealPath at [www.sealpath.com](http://www.sealpath.com) | [sales@sealpath.com](mailto:sales@sealpath.com)