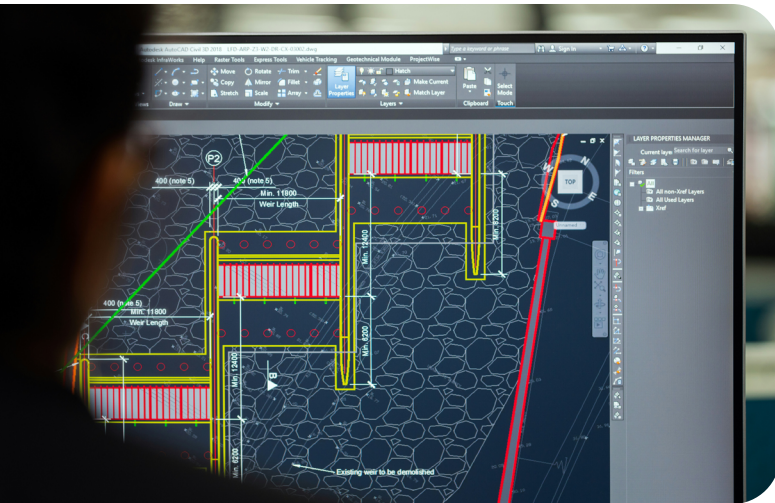


# Secure Every Step of the Design Process — From CAD Creation to PLM



## Design IP is your competitive edge—HaloCAD keeps it that way

Secude's HaloCAD embeds Microsoft Purview-powered Zero Trust protection directly into CAD files, securing sensitive designs across Autodesk, Siemens, PTC, and Dassault ecosystems. Whether inside your organization or shared externally, your CAD data stays protected—without disrupting native workflows.

### TRACK & REVOKE

#### Control Doesn't End When the File Leaves Your Hands

HaloCAD extends Microsoft's tracking and revocation capabilities—typically limited to Office files—to CAD files, enabling engineering teams to monitor usage and revoke access at any time, even after distribution.

#### Key Capabilities:

- Integrate with Microsoft Purview, Sentinel, or third-party SIEMs
- Revoke access to a CAD file via the "Revoke" button in the HaloCAD status pop-up
- Track file usage and access history inside and outside your organization
- Built on CAD SDK integrations—bringing Microsoft Purview's revoke functionality to engineering design filesWorks for both internal use (employee offboarding) and external collaboration (supplier or partner withdrawal)

#### Use Cases:

##### Revoke Access After Employee Departure

An engineer leaves the company and copies a design file to a USB drive. With HaloCAD, access to that file is revoked—rendering it unreadable even outside the network.

##### Contract Termination With a Supplier

A CAD file shared with a partner becomes sensitive after a deal falls through. HaloCAD allows immediate revocation of access—ensuring no further visibility into your IP.

### CLASSIFY

#### Apply Sensitivity Labels Automatically and Consistently

HaloCAD enables both **manual and automated classification** of CAD files—ensuring sensitive files are always labeled, encrypted, and handled correctly.

#### Key Capabilities:

- Automatically apply Microsoft Purview sensitivity labels (e.g., "Engineering Confidential") using Active Directory group mapping or file context
- Extend Microsoft Purview labeling to CAD and PLM files
- Label files at the point of export, creation, or check-out from PLM systems like Siemens Teamcenter or PTC Windchill
- Tailor DLP policies by department, project, or geography

#### Use Cases:

##### Protect Multi-CAD Data with Microsoft Purview

An aerospace firm uses HaloCAD to extend Microsoft Purview labels to CAD files across SolidWorks and Siemens NX. As files move through Teamcenter, sensitivity labels like "Export Controlled" are applied automatically—ensuring consistent encryption from design to supplier handoff.

##### CAD File Security with Ease of Use

Engineers and designers are not cybersecurity professionals. Sensitivity labels automatically added to CAD drawings when they're created, with familiar processes and controls (i.e. similar to Word or Excel) ensure engineers can collaborate seamlessly and securely - both with colleagues and external partners.

### Compatible Across Your Ecosystem

Supports major platforms: **Autodesk, Siemens, PTC, Dassault Systèmes** and more

## PROTECT & CONTROL

### Secure CAD Files Without Disrupting Engineering Workflows

HaloCAD empowers secure collaboration by protecting data at **the file level**—enabling access only when conditions are met and deny access when they aren't.

#### Key Capabilities:

- Enforce encryption and access controls based on sensitivity label
- Prevent copy, paste, print, or screen capture of sensitive files
- Revoke file access after project completion or contractor off-boarding

#### Use Cases:

##### Department-Based Access Control

A powertrain engineer attempts to access chassis design files. HaloCAD blocks access due to labeling and logs the attempt.

##### Time-Bound Supplier Access

A heavy equipment company limits access to design files shared with a third-party firm in India to 30 days on company-issued laptops.

##### Enable Secure Manufacturing Access

R&D teams work on designs labeled “Confidential – In Development,” while manufacturing receives only the final labeled version “Approved for Production.”

## Why Engineering Leaders Choose HaloCAD

- ✓ Automated classification and encryption via Microsoft Purview via PLM
- ✓ Persistent, file-level protection across CAD when checked out from PLM systems
- ✓ Seamless support for Autodesk, Siemens, PTC, and more
- ✓ Access follows the file—not the user or location
- ✓ Designed for compliance: CMMC, ISO-19650, NIS2

## Technical Information

- HaloCAD seamlessly extends MPIP security across product lifecycle management (PLM) systems and complex multi-CAD integrations, such as AutoDesk, PTC, Siemens or Dassault.
- HaloCAD's MPIP plug-in leverages Azure Rights Management Service (Azure RMS) protection and enhances Microsoft 365 E5 compliance to protect sensitive CAD files.
- HaloCAD modules can be used standalone, such as HaloCAD READER (enforces 'read only' privileges) or in combination with HALOCAD for PLM (which automatically locks access during the download process and unlocks access when returned to the PLM vault).
- HaloCAD extends CAD data protection and supports multi file formats that includes DWG, DXF, IPT, IAM, IDW, RVT, ASM, PRT, PAR, PSM, SLDPRT among others.

---

**Secude: Classify. Secure. Control. CAD & PLM, Protected by Design.**

For more information about Secude: [www.secude.com](http://www.secude.com)

**Phone:** USA/Canada: +1 800-900-9633 | **India:** +91 44 4777 9704 | **Switzerland:** + 41 41 510 70 70

**Email:** USA/Canada: [AmericasSales@secude.com](mailto:AmericasSales@secude.com) | **EMEA:** [EMEASales@secude.com](mailto:EMEASales@secude.com)

Secude, it's product names all rights reserved. Other product names in this publication are for identification purposes only. Other trademarks are the properties of their respective owners. 2025\_UC\_HaloCAD0\_0630\_ww

Member of  
**Microsoft Intelligent  
Security Association**

