HaloCONNECT provides zero-touch supply chain data security — enabling you to securely store, share, view and track sensitive files (i.e. CAD files) when collaborating.

HaloCONNECT

Do you collaborate seamlessly and securely with external partners?

From engineering to manufacturing, today's production chains rely on smooth digital workflows — especially when collaborating on CAD files. But when multiple users from multiple organizations using multiple systems collaborate on a project, it slows down production and increases the cybersecurity risk.

Streamlining workflows on critical infrastructure projects and defense contracts is particularly challenging. On the one hand, seamless data transfer and file access between project partners is essential for efficient third-party collaboration and providing a competitive edge. On the other hand, decrypting sensitive files (i.e. CAD files) or reducing barriers to sensitive data increases the risk of unauthorized access, which can lead to damaging cyber attacks, regulatory non-compliance (i.e. CMMC), IP loss and even national security crises.

It's therefore no surprise that strengthening access control policies (38%) and meeting compliance requirements (37%) are the top cybersecurity priorities for the Defense Industrial Base (DIB) in 2025. But file security cannot be considered separately to workflow efficiency: your access control policies should not impede your productivity.

Balancing efficiency and security is essential

From storing and sharing data (i.e. blueprints and contracts) to viewing and collaborating on key files (i.e. product designs and engineering drawings), multi-partner projects require seamless and secure data access along the production chain.

Given each project partner has a different set of users, roles, devices and systems, finding the right balance between security and efficiency has been difficult to achieve. For example, encrypting CAD data with sensitivity labels is vital for security, but can be inconvenient if external collaborators do not have CAD decryption software.

But with HaloCONNECT, you can now securely store, share, view and track sensitive files, including CAD, MS Office and PDF files, when collaborating without the need to download software or install a plug-in - making your external workflows seamless and secure.

Secude

HaloCONNECT, a joint collaboration between Secude and Gold Comet, enables you to:

- **Store and share files in a secure environment.** Upload files to HaloCONNECT's secure cloud storage using drag-and-drop, including HaloCAD-protected and unprotected CAD files, and share files with collaborators within a safe, centralized environment.
- **Set granular access controls.** HaloCONNECT automatically assigns access permissions to files based on roles (i.e. administrator or editor), user attributes (i.e. job title or department), time frames (i.e. business hours), specific devices or geographic locations.
- **Securely view files.** HaloCONNECT's Web Viewer enables your collaborators to securely view, rotate, zoom and measure key file types (i.e. 2D/3D images, MS Office files, PDFs) without needing to download decryption software.
- **Log and monitor data access.** HaloCONNECT records the time, date, and activity of each user and file in detailed logs, flags unusual behavior with automated alerts and enables real-time monitoring of data access.

Key Features

- **Download and installation free**
- **Enables secure web collaboration**
- **Stores files in a secure cloud environment**
- **Tracks file access and issues alerts**
- **Auto-assigns access permissions**
- **Logs data access for auditing/ reporting**

HaloCONNECT benefits

- **Present and future threat mitigation.** With full control over the collaboration experience and full visibility of data access, HaloCONNECT enhances your security posture, minimizes the risk of breaches and easily adapts to evolving threats.
- **Rapid incident response.** With real-time detection of suspicious behavior (i.e. large file downloads out of business hours), anomalies, unauthorized access or policy violations, HaloCONNECT enables you to identify, investigate and mitigate incidents promptly.
- **Simplified compliance.** With granular access control, tamper-proof access logs and detailed activity tracking, HaloCONNECT ensures data integrity and simplifies compliance assessments for legal, financial and regulatory obligations, such as CMMC.
- **Improved efficiency and transparency.** By automating access restrictions and data tracking, HaloCONNECT streamlines your engineering workflows and improves trust among customers, partners and regulators — particularly in regulated industries.

Technical information

HaloCONNECT is built according to the Zero Trust Model.

HaloCONNECT utilizes Quantum secure, 256-bit Object Level Encryption, Multi-Factor Authentication (MFA), and whitelisting.

All data storage, sharing, and messaging operations take place within the HaloCONNECT Secure Cloud.

HaloCONNECT stores any file type and enables secure viewing of CAD, MS Office and PDF files and more.

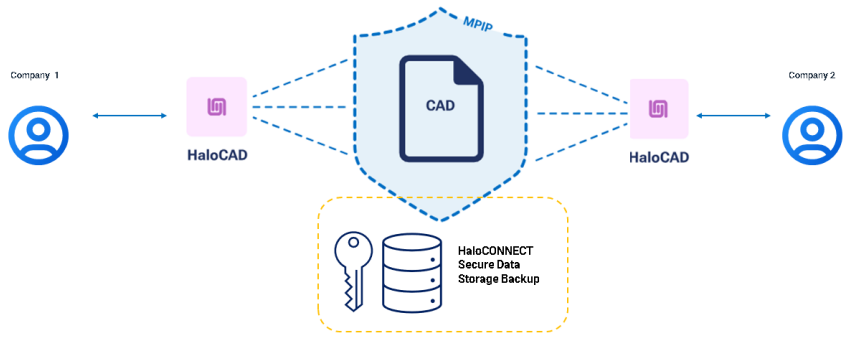
HaloCONNECT works with file formats from Autodesk, Dassault, Siemens and PTC products.

HaloCONNECT is 100% US based and operated.

With HaloCONNECT, there are no limitations on the regions or locations of users.

Access to the HaloCONNECT platform is browser-based and utilizes MFA authentication.

HaloCONNECT Overview



Member of
Microsoft Intelligent Security Association
Microsoft Security

Secude

Secude, a trusted Microsoft partner and CAD security provider, is a global leader for Zero Trust data protection and data governance.

Contact us: www.secude.com or email North America: AmericasSales@secude.com | EMEA: 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_SB_HaloCONNECT_0217_ww