HaloSHARE streamlines bulk file classification, labeling, encryption, annotation, and digital watermarking.

HaloSHARE

Is your sensitive data secure when collaborating externally?

Cyber attacks have increased 30% year-on-year with the average breach costing $4.88 million in 2024. But supply chain attacks have risen 2,600% since 2018 with an average $82 million cost to organizations in key industries, such as aerospace and defense.

As supply chains have become increasingly digitized, so have their vulnerabilities. Be it targeted attacks on shared software, accidental leaks by third-party partners or even data loss by fourth-party subcontractors, **you only need one security gap across the entire digital supply chain to cause a widespread data breach.**

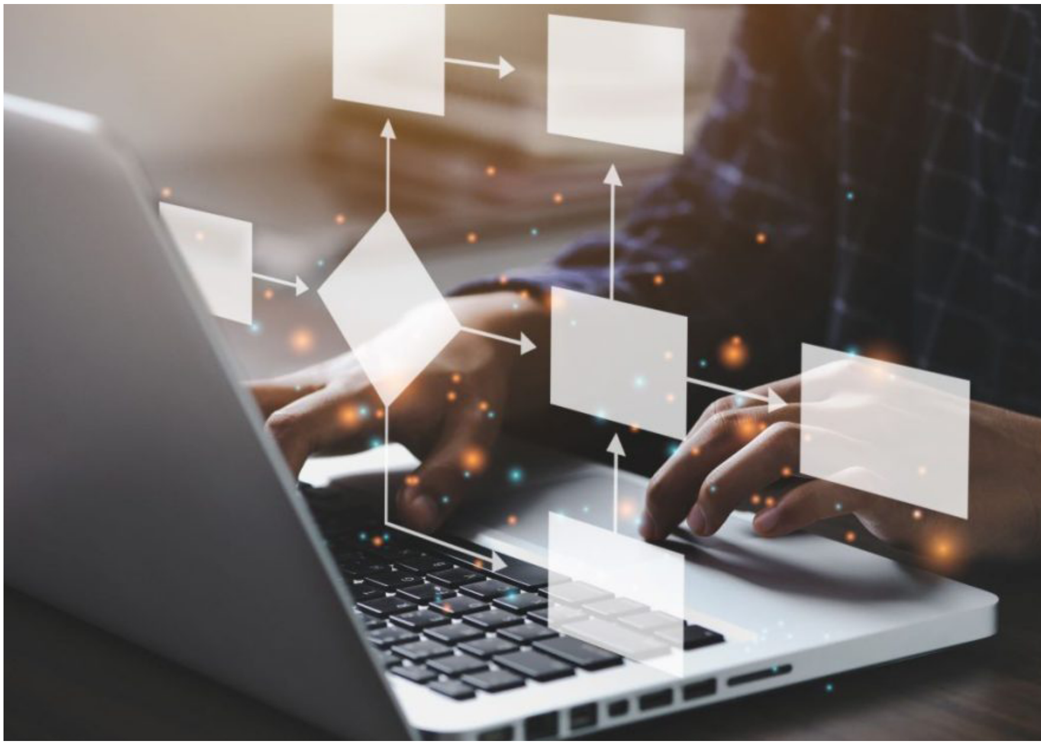
Given it's impossible to monitor every security touchpoint along the supply chain, Gartner predicts that 45% of organizations will suffer a digital supply chain attack by 2025.

Files in shared networks and cloud server folders are particularly vulnerable.

Today's multi-partner supply chains rely on seamless workflows, be it manufacturing production, federal government contracts or national infrastructure projects. However, when multiple users share access to a system, network or cloud server folder, you increase the possibility of unauthorized access to sensitive files - especially if a third-party partner is less security-focused than your organization.

By sharing unprotected files with supply chain partners, you not only risk the financial loss, operational disruption, and reputational damage from a potential data breach, but also lawsuits and fines from regulatory non-compliance. Even if shared files do not contain your sensitive IP, such as building blueprints or documents for a tender process, you still need controls to avoid accidental file modification or unauthorized transfers.

To ensure your business operations are safeguarded from malicious attacks or partner negligence along the supply chain without disrupting your workflows, you need to protect all shared project files by default - both at rest and in transit.



Secude's HaloSHARE simplifies bulk file management with classification, labeling, encryption, annotation, and digital watermarking - securing and streamlining your internal and external workflows.

- **Extend MPIP protection to shared folders.** HaloSHARE extends Microsoft Purview Information Protection (MPIP) to CAD, PDF and MS Office files placed within shared folders, encrypting sensitive information with adjustable sensitivity labels.
- **Classify, label and encrypt files in bulk.** HaloSHARE's labeling and relabeling solution enables you to encrypt hundreds of sensitive files in shared folders (i.e. OneDrive or SharePoint) using drag-and-drop.
- **Bulk watermark non-sensitive files.** HaloSHARE enables bulk watermarking of files with both visible and discreet markings, including traceability of who files are shared with and when (date stamped).
- **Customize protection for specific file types.** HaloSHARE enables MPIP administrators to configure encryption per file type within shared folders and allows users to create custom permissions for specific drawings or designs.

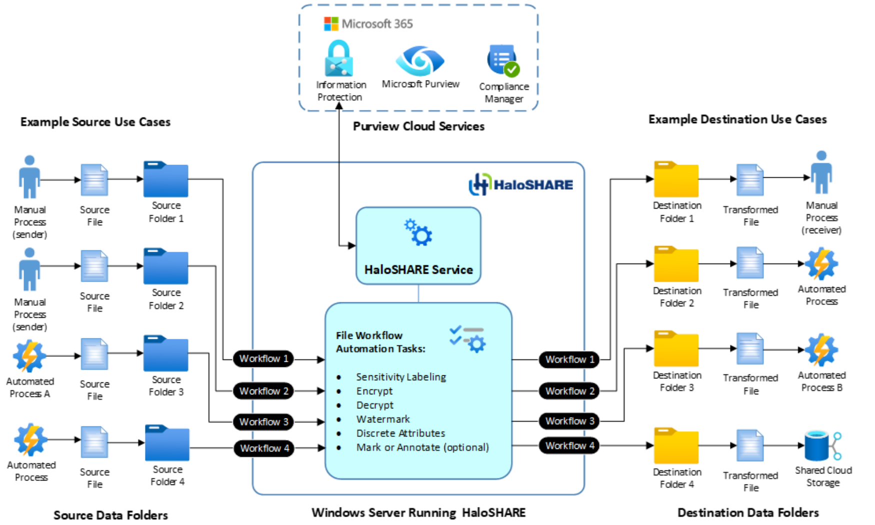
Key Features

- ✓ File-level data security
- ✓ Bulk file operations
- ✓ Fully customizable
- ✓ Additional metadata
- ✓ Watermarking
- ✓ Relabeling

HaloSHARE benefits

- **Secure collaboration.** HaloSHARE-configured folders automatically protect sensitive files from unauthorized access even when they travel outside of your organization. HaloSHARE's adjustable authorization labels, which can be revoked or set to expire, enable you to work closely and securely with external suppliers and vendors without impacting the end-user experience.
- **Shared files protected from misuse.** The greater the number of users sharing access to a system, network or folder, the greater the risk of accidental leaks, file modification or overwriting of files. But with HaloSHARE's customized authorization controls, shared files are always protected from malicious or unintentional misuse.
- **Seamless workflows.** HaloSHARE's labeling and relabeling solution enables you to bulk protect files using drag-and-drop, securing your production chain without impeding operational productivity. With HaloSHARE, you can also watermark non-sensitive files without encryption, enabling you to share and trace project files without slowing down workflows.

> *"Prior to HaloSHARE, it would take us days or weeks to mark the large quantity of documents we must share externally. Now we can mark those files in minutes."* Global Engineering Group



Secude, a trusted Microsoft partner and CAD security provider, is a global leader for Zero Trust data protection and data governance. For more information about Secude: 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 | **EMEA:** EMEASales@secude.com

Technical information

HaloSHARE must be registered in Microsoft Entra ID.

HaloSHARE communicates with the Microsoft Rights Management Service (RMS) to encrypt files in a specific folder using predefined MPIP labels or user defined custom permissions.

HaloSHARE users can create custom permissions through GUI and Azure labels, which are taken directly from the Entra ID portal.

HaloSHARE supports all native CAD file types, PDF files and MS Office files.

When a HaloSHARE-protected CAD file is shared with external partners, they can view the file by simply installing the HaloCAD add-on for CAD applications.

Member of
Microsoft Intelligent Security Association
Microsoft Security