

FASOO

CASE STUDY

Driving Innovation Securely:

How a Global Automotive Leader Protects Its IP



About The Customer

A leading global automotive supplier designs and manufactures advanced safety components, electronics, and driver assistance systems that support next-generation mobility. With operations across multiple regions and a wide supplier network, the company relies on fast, secure collaboration to stay competitive.

Challenges

As engineering programs expanded, the company faced increasing risks to intellectual property (IP). CAD designs, process documentation, and test data were shared across teams and partners, but perimeter defenses like firewalls, VPNs, and CASBs only worked within controlled systems. Once files were emailed or downloaded, visibility and control were lost. Without file-centric security, sensitive designs could be copied or shared without oversight. Administrators couldn't track who accessed or printed files, and screen captures or hard copies created further blind spots. Revoking access outside the network was nearly impossible, exposing IP to insider threats, supply chain risks, and compliance issues.

To address these challenges, the company required a solution that could:

- Shift from perimeter-based controls to persistent, file-level protection
- Automatically encrypt CAD and Office files across global teams
- Integrate with PLM systems without disrupting workflows
- Enforce dynamic policies and maintain full visibility across the supply chain
- Govern printing and screen activity to eliminate security blind spots

Industry

Manufacturing, Automotive

Use Case

- Inconsistent file protection once it leaves controlled systems
- Sensitive design files at risk across global teams and suppliers
- Limited control and visibility over screen and print activities

Solutions

- Applied file-level encryption and dynamic policies across CAD, Office, and process files
- Integrated PLM workflows with automatic encryption to secure designs without disruptions
- Enforced screen and print security with watermarks, monitoring, and access controls



Solutions

The automotive company implemented Fasoo's advanced data security platform, designed to provide persistent protection throughout the lifecycle of IP data, while minimizing insider threats, including protecting screens and printouts, through its innovative features.

I. Advanced Data Security

Recognizing that traditional perimeter-based security tools such as firewalls, VPNs, and CASBs could not adequately protect data once it left controlled environments, the company adopted a persistent data security approach. CAD, Office, and process files were automatically encrypted at the point of creation, with dynamic policies applied to each document that remained in effect throughout its entire lifecycle, regardless of where it traveled. Administrators gained centralized policy management, ensuring consistent security across the supply chain and enabling access to be revoked whenever necessary.

II. Seamless PLM Integration

Engineers often downloaded unprotected IP design files from the PLM system, creating a major risk once the files moved beyond its security perimeter. To address this issue, the customer integrated their PLM with Fasoo EDRM, using Fasoo's SDK encryption packager to automatically encrypt and assign ACL policies to all engineering drawings upon download. This ensured that every file leaving the PLM environment remained protected, while enabling engineers to stay productive without disruption or additional user intervention.

III. Proactive Screen Security

Another challenge came from remote or supply chain users potentially taking photo or capturing screenshots of sensitive data. To mitigate this risk, the company responded by applying visible screen watermarks that displayed dynamic user information directly on the screen. Screen capture prevention was also enabled, activating only when employees accessed PLM or CAD files. Also, captured content and activities were logged to empower auditability, ensuring complete screen security.

IV. Traceable Print Security

The company had no visibility on printing activities. To overcome this, the company deployed Fasoo's print security solution to enable secure printing, allowing only authorized users to print or print with watermark. Classified printouts included user-specific watermarking information, deterring misuse. In addition, the customer also gained complete visibility of sensitive files being printed, which minimized IP risks and ensured full traceability and compliance.

Results

The company experienced significant improvements after implementing Fasoo's data security platform.

It moved beyond perimeter-bound defenses to persistent, file-centric security. Intellectual property is now consistently protected across CAD, Office, and process documentation, no matter where files are stored or shared. Engineers and suppliers can securely collaborate with confidence, and administrators maintain full visibility into file usage across the enterprise.

The ability to revoke access and enforce dynamic policies has strengthened compliance and reduced the time needed for investigations, while closing the risks posed by uncontrolled printing and screen captures. Most importantly, these safeguards were introduced without disrupting the engineering workflows. By consolidating data, print, and screen security into a single platform, the company reduced risk exposure, improved data governance, and established a Zero Trust foundation that enables innovation with confidence.



With Fasoo, security follows the file itself.
Our engineers continue working as they always do,
while our designs and processes remain protected,
whether in the office, the cloud, or with suppliers.

FASOO

Fasoo provides unstructured data security, data governance, and AI-powered enterprise content platforms to help organizations discover, classify, protect, and manage critical information assets while boosting productivity. Our solutions enable secure information sharing, AI-ready data management, and simplified compliance with evolving security regulations.

Email : inquiry@fasoo.com Web : <https://en.fasoo.com/>