FASOO | AI

CASE STUDY

Powering AI Securely:

How an Energy Company Secures Critical Operational Data Across Its Value Chain

About the Company

A global energy provider operating across power generation, distribution, and infrastructure management is undergoing a large-scale digital transformation. With increasing adoption of AI and data-driven systems, it manages vast volumes of sensitive data, including engineering designs, operational procedures, and infrastructure documentation.

Challenges

As the company accelerated AI adoption and digital transformation initiatives, sensitive operational data such as plant schematics, grid operation data, and maintenance documentation was increasingly shared across systems, users, and external partners. However, traditional perimeter-based security controls could not adequately protect data once files moved beyond controlled environments. As data was shared across cloud and partner ecosystems, visibility and control were reduced. Without persistent, data-centric protection, sensitive information could be reused outside intended contexts, while unmanaged external access and screen-level exposure created additional blind spots. The organization also faced growing challenges maintaining visibility into how critical data was accessed and utilized across AI-driven workflows.

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

- Protect sensitive operational data used in AI-driven workflows
- Maintain persistent control over files shared across systems and partners
- Restrict unauthorized copying, downloading, and screen capture
- Revoke access dynamically as projects and partnerships change

Industry

Energy / Critical Infrastructure

Challenges

- Increased exposure of operational data with AI adoption
- Uncontrolled file sharing across partners
- Limited control and visibility after data leaves systems

Solutions

- Fasoo Enterprise DRM (FED)
- Fasoo Data Radar (FDR)
- Fasoo Smart Screen (FSS)

Results

- Secure AI-driven operations with continuous protection of critical data
- Full visibility and control over data across internal teams and external partners
- Stronger compliance and reduced risks without disrupting workflows

Solutions

The energy company implemented Fasoo's data-centric security platform to securely support AI adoption across operational environments, supply chains, and distributed workforces. By applying persistent protection directly to sensitive data, the company maintained visibility and control over critical operational information while enabling secure AI-driven workflows and collaboration.

Persistent AI Data Protection

The company deployed **Fasoo Enterprise DRM** to apply persistent encryption and dynamic access controls to sensitive operational data. This ensured only authorized users and AI systems could access critical information throughout its lifecycle.

AI-Ready Data Visibility and Classification

The company implemented **Fasoo Data Radar** to discover and classify sensitive data across its environment, providing visibility and enabling protection before the data was used by AI applications or shared externally.

Proactive Screen-Level Protection

To reduce screen-level exposure risks, the company deployed **Fasoo Smart Screen** to apply dynamic visible watermarks, block unauthorized screen captures, and log screen activities and capture attempts.

Continuous Protection Across the Data Lifecycle

By integrating persistent encryption, data visibility, and screen-level protection into a unified security strategy, the company ensured that sensitive operational data remained protected, controlled, and traceable throughout its lifecycle.

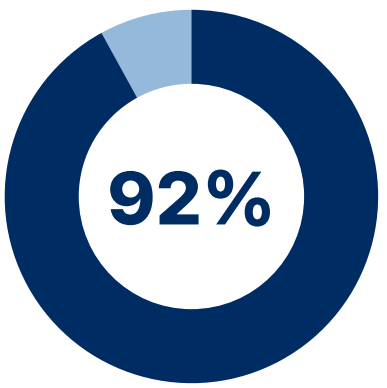
> AI is transforming how we operate, but it also increases the risks of exposing sensitive operational data. We needed to ensure that the data fueling our systems remained protected at all times.

Results

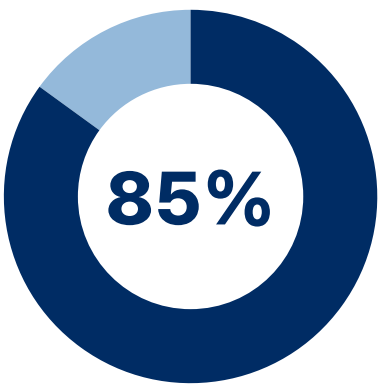
By embedding security directly into its data, the company was able to accelerate AI adoption without increasing risks. Sensitive operational data remained continuously protected across AI workflows, internal systems, and external collaborations, enabling the organization to innovate with confidence.

The company also gained end-to-end visibility into how data was accessed and used, including interactions involving AI systems. This improved its ability to enforce governance policies, detect potential risks, and meet regulatory requirements.

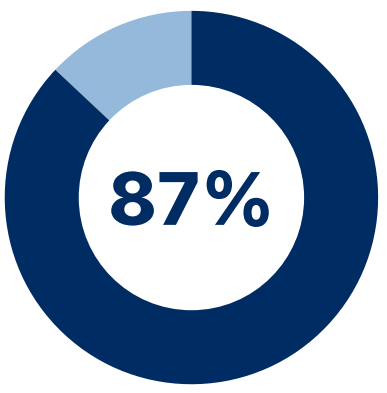
Ultimately, the organization established a secure foundation for AI-driven operations, balancing innovation with control and ensuring that the critical operational data remained protected across internal and external workflows.



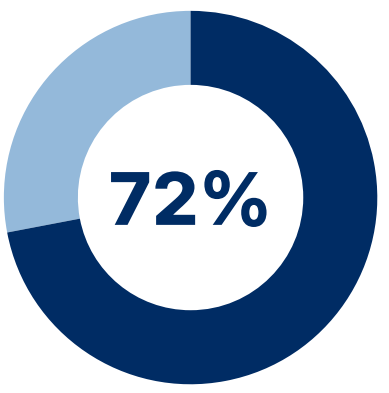
Reduction in unauthorized external data exposure risks



Improvement in visibility across AI-related data activities



Reduction in screen-level exposure incidents



Faster identification of sensitive operational data

FASOO | AI

Fasoo AI 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.ai Web : https://en.fasoo.ai/