Fasoo Addresses Critical GenAI Security Gap with Data-Centric ACL Management

BETHESDA, MD, UNITED STATES, February 24, 2026 /EINPresswire.com/ -- Fasoo, a leader in data-centric security and AI-ready data governance, today highlighted a fundamental security challenge facing enterprises deploying private large language models (LLMs): AI systems trained on

FASOO

Fasoo - a leader in data-centric security

internal documents often expose sensitive information to unauthorized employees, bypassing traditional access controls.

When organizations train AI on internal documents like HR salary data, financial projections, legal contracts, and product roadmaps, the LLM absorbs everything indiscriminately. An employee in Marketing queries the AI about the CMO's salary, and the system, having been trained on Finance's confidential data, provides answers the employee was never authorized to see. A second challenge: ensuring AI systems learn from correct document versions when contextual metadata is incomplete or stored separately from content.

"AI security must start at the data level, not the storage layer. Policies must travel with the information wherever it travels," said Ron Arden, EVP, CTO & COO of Fasoo.

Storage-Based Solutions Prove Unsustainable:

Many enterprises create segregated cloud folders and separate training datasets for each department. This approach fails as organizations evolve: documents move, permissions change, employees join or leave, and reorganizations occur. Within months, folder taxonomies become inconsistent. The fundamental flaw: metadata managed at the storage layer degrades over time because it's separate from the data itself.

Data-Centric Approach Embeds Governance in Content:

Fasoo's solution embeds access control lists (ACLs) and contextual metadata—permissions, ownership, version control, usage history—directly into documents. This metadata travels with content everywhere, ensuring consistent policy enforcement.

Fasoo's data-centric encryption-based solutions, Fasoo Data Radar (FDR), Wrapsody, and Fasoo Enterprise DRM (FED), all maintain per-file ACL policies that form the foundation for GenAI security. Together, they address both AI input and output: FDR discovers and classifies sensitive information, Wrapsody manages AI-ready content with embedded version control, and FED enforces persistent file-level access controls.

When unauthorized users attempt to include sensitive documents in AI queries, embedded ACLs block the attempt. When AI generates responses from protected sources, the system checks permissions in real-time and filters accordingly.

"Enterprise AI adoption requires a fundamental shift in how access control is designed and managed," Arden added. "Controls that are detached from the data cannot keep pace with dynamic organizational changes and large-scale AI workflows. Embedding ACLs and contextual metadata into each file establishes a consistent and scalable foundation for secure GenAI deployment across the enterprise."

For more information, visit https://en.fasoo.com/data-centric-acl-management-for-genai/.

About Fasoo:

Fasoo provides unstructured data security, privacy, and enterprise content platforms that securely protect, control, trace, analyze, and share critical business information while enhancing productivity. Fasoo's continuous focus on customer innovation and creativity provides market-leading solutions to the challenges faced by organizations of all sizes and industries. For more information, visit https://en.fasoo.com/.

Sonia Awan
Outbloom Public Relations
soniaawan@outbloompr.net
Visit us on social media:
LinkedIn
Facebook
YouTube
X