PBAC for GenAI and LLM Security

Identity-aware security, powered by Policy-Based Access Control (PBAC)

The AI Data Access Explosion: A Security & Compliance Risk

The explosion of identities accessing enterprise data has outpaced traditional access controls, creating security gaps and compliance risks. AI-driven tools such as GenAI, AI Agents, and Large Language Models (LLMs) improve efficiencies but can also expose sensitive data to both human users and non-human identities (NHI).

Enterprises risk data leaks, compliance violations, and security breaches as LLMs leveraging Retrieval-Augmented Generation (RAG) generate insights from integrated enterprise data sources such as customer records and financial reports. A scalable authorization framework ensures that both humans and NHIs can only access the data they are explicitly authorized for.

Improve Security for AI-driven Tools with PBAC

The PlainID GenAI Authorizer enforces granular access controls at every stage of the RAG pipeline, where vast amounts of enterprise data are accessed and generated. With PlainID, Authorization is dynamically enforced at three critical points in the AI workflow:

Secure Query Input by ensuring users can only ask questions within their authorized scope. By enforcing policies at the query level, PlainID prevents unauthorized attempts to extract sensitive data, reducing exposure risks before retrieval.

Control Access of AI Systems and AI Agents to documents and data, by applying dynamic access policies to determine who can access what and under which conditions. Data can be retrieved only when the identity is authorized, ensuring security and compliance.

Mask and Filter Data from Generated Responses by ensuring that AI-generated responses displayed to users align with their permissions. This prevents the LLM from exposing unauthorized insights, keeping response output secure, compliant, and controlled.

Control access dynamically in real-time to mitigate unauthorized access, secure sensitive data, and maintain compliance across AI-driven workflows for any identity, and at any scale.

Business Impact

Minimize Risk With Identity-First Security
Address Zero Trust and continuous Authorization in real-time, with context and consistency.

Standardize Enterprise Authorization
Deliver a modern and user-friendly authorization experience across all technology patterns at the application, API, service, and data layer.

Coarse & Fine-grained Authorization
Enforce fine-grained controls at a granular level by determining what rows/columns/cell data are exposed to the authorized user.

Address Compliance & Auditing
Ensure alignment with regulatory requirements by maintaining consistent, auditable access decisions across all enterprise systems.

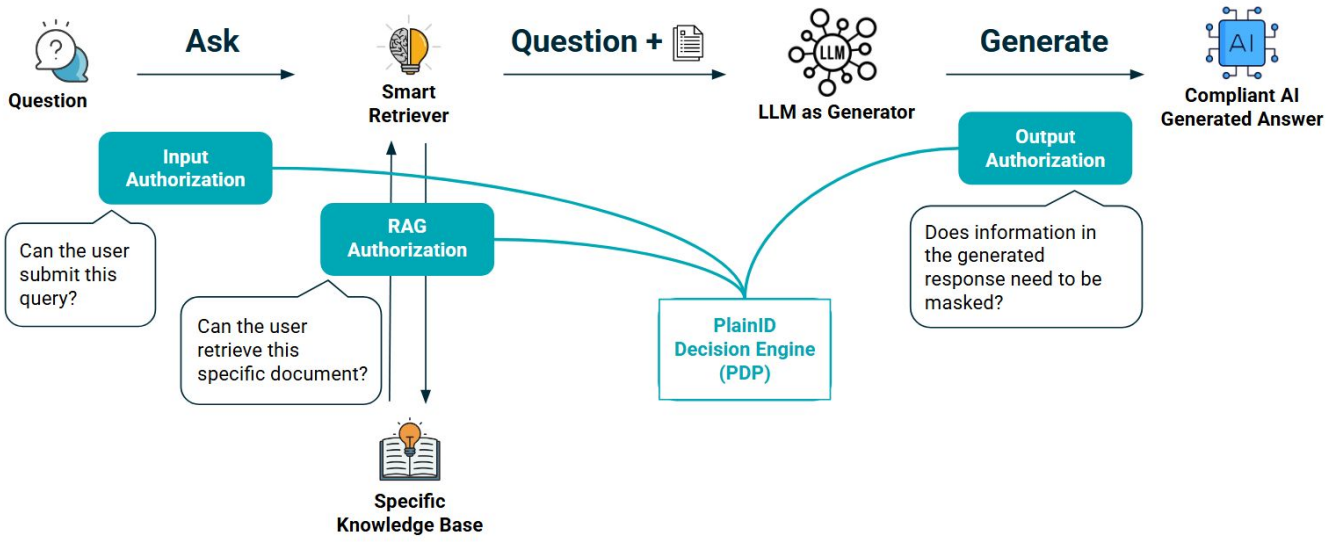
Technical Insight

Identity-aware Access Control Prevents AI Overreach

AI Agents function as NHIs, but what data they can access and do should be tied to the user they serve, ensuring permissions align.

Limiting AI access based on the user's identity (e.g. role, attributes, etc.) ensures NHIs do not exceed intended permissions.

How PBAC for the GenAI Pipeline Works



The GenAI pipeline implementing a RAG model involves several critical stages, each reinforced with robust security and access control measures powered by PlainID:

- **Query Authorization:** Verifying whether the user is authorized to ask a specific question before processing.
- **Document Retrieval:** Only documents that the user is authorized to access are retrieved.
- **Response Filtering:** Applying dynamic policies to mask or redact sensitive information before integrating it into AI-generated responses. This validates the final AI-generated output against enterprise security policies to prevent unauthorized data exposure.

Future-proof Your Enterprise

The **PlainID Integration Hub** is designed to address the complex challenges of enterprise access control. By offering out-of-the-box Authorizers™ and Integrations, it allows for a standardized approach across varied and distributed infrastructures – unifying disparate access controls under one platform.

PostgreSQL · amazon REDSHIFT · Google BigQuery · denodo · apigee · envoy · snowflake · Microsoft SQL Server · trino · Starburst · Kong · Power BI · Istio

Visit PlainID.com/integration-hub for more information

ABOUT PLAINID

PlainID is the world's leading provider of enterprise Authorization, helping enterprises address the complex challenges of Identity Security. The PlainID Platform allows you to discover, manage, and authorize access control policies for enterprise applications and data. Our solution is architected to protect against identity-centric security threats powered by Policy-Based Access Control (PBAC). Visit PlainID.com for more information.

plainID