plainID + databricks

SaaS Authorization Management™ for Databricks

Manage & Standardize on Authorization policies for SaaS Apps

Access Control Challenges in Databricks

Enterprises increasingly rely on Databricks as a strategic platform for storing, processing, and analyzing vast amounts of data. As data volumes grow and the need for granular access controls increases, ensuring only authorized users can access sensitive information becomes critical.

While Databricks offers native access control features, aligning these controls across large enterprise environments is complex and error-prone. The challenge many organizations face is that data access policies are often managed in silos. These silos lead to inconsistencies and potential security vulnerabilities, making it difficult for security teams to maintain oversight and ensure sensitive data isn't inadvertently exposed.

PlainID addresses this gap by centralizing Databricks' access controls through a unified Policy-Based Access Control (PBAC) framework. Through Policy Orchestration, the PlainID Platform empowers enterprises to centrally create and manage policies, which are then enforced by Databricks at the point of data access.

Centralized policy management ensures that access control policies are consistently managed and securely applied, whether data is accessed directly by users or indirectly through automated processes and service accounts. As a result, enterprises gain full visibility and control of their data access landscape, strengthening their security posture without disrupting business operations.

Business Impact

Streamline Access to Data
Centralize and automate policy management to reduce manual efforts required to enforce policies across the data ecosystem.

Reduce Risk of Exposed Data
Ensure consistent enforcement of data access policies and minimize the risk of data breaches and insider threats.

Gain Visibility & Monitoring
Track access policies from a single dashboard that provides reporting to inform administrators on policy changes.

Comply with Privacy Regulations
Standardize policies to comply with regulatory requirements such as GDPR, and HIPAA – and quickly adapt to evolving business needs.

Centralized Policy Management & Enhanced Data Security with PlainID

DATA ACCESS CONTROL

Centrally managed policies in PlainID can be deployed across enterprise data platforms, ensuring uniform and comprehensive data security throughout the enterprise's data environments.

SECURE DATA SHARING

Secure all types of data access, direct (users) and indirect (service accounts). Create policies to filter or mask sensitive data at the row-level and use Databricks' object tagging for selective data access.

SECURE DATA FABRIC

For enterprises adopting a data mesh approach, PlainID offers decentralized and scalable data access controls, supporting various analytical and operational use cases across multiple domains.

Key Features

Centralized Management & Policy Orchestration

- **Rapid Native Integration**: Integrate Databricks with PlainID within seconds and immediately discover existing policies.
- **Unified Control Plane**: Centralize the discovery and management of all Databricks access policies, including row-level filtering and masking.
- **Lifecycle Management**: Govern the full lifecycle of access policies, from creation to decommissioning, ensuring consistency and reducing risks of policy drift.

Dynamic Data Masking & Row-Level Filtering

- **Dynamic Masking**: Apply masking instructions such as tokenization, k-anonymization, and dynamic masking to protect sensitive data.
- **Row-Level Access Controls**: Define fine-grained row-level filtering policies that ensure users only access relevant subsets of data.
- **Leverage Object Tags**: Apply Databricks' object tagging to inform access policies, ensuring the correct data is protected across various datasets.

Improved Visibility and Compliance Auditing

- **Policy Auditing**: Generate real-time, consolidated audit trails across all Databricks environments, ensuring full visibility into access policy changes.
- **Policy Mapping**: Advanced visualization tools map out the relationships between policies and their impact on data being accessed.
- **Policy Investigation:** Simulate and test various levels of access control policies and their effects before moving to live production.

Secure Direct and Indirect Access to Databricks

- **Direct Access to Databricks:** Secure access to sensitive data for users and service accounts querying Databricks via the UI or programmatically.
- **Indirect Access to Databricks:** Combine with Dynamic SQL Authorization in the Microservices or Application layer to further reduce exposure by applying identity and context-aware security controls in combination with direct access restrictions on service accounts.

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 · databricks · 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