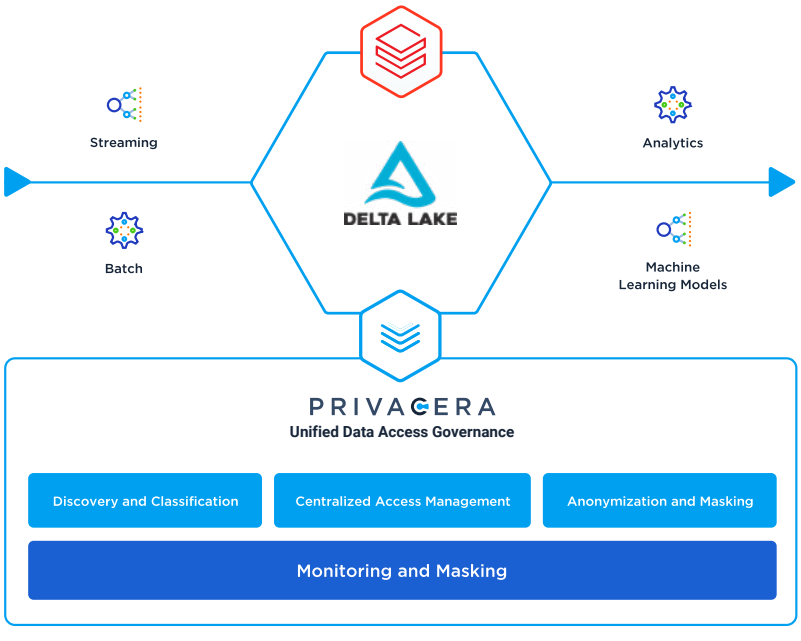
PRIVACERA AND DATABRICKS

Rapid Analytics with Unified Data Access Governance

Data is the most valuable asset for data science and analytics teams. It helps enterprises understand customers better, drive product innovation, and make faster business decisions to gain a competitive edge. But if data is siloed, inaccessible, or fragmented across business units, data teams can't rapidly access data they need to drive innovation or effectively control who accesses data for what purpose – leaving enterprises vulnerable to privacy or compliance violations.

To successfully balance rapid access to data with security and compliance, Privacera's native integration with Databricks centralizes data access governance across multiple workloads, including Spark SQL,ML/A and more, with automated sensitive data discovery, fine-grained access controls, dynamic masking and encryption, and detailed data access auditing – all from a single user interface.

Privacera-Databricks Architecture

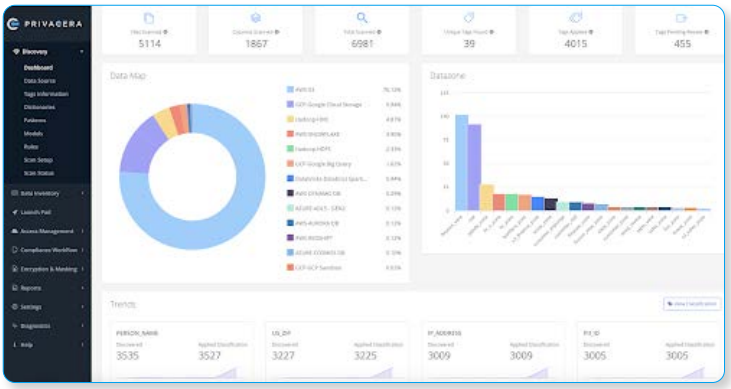


questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

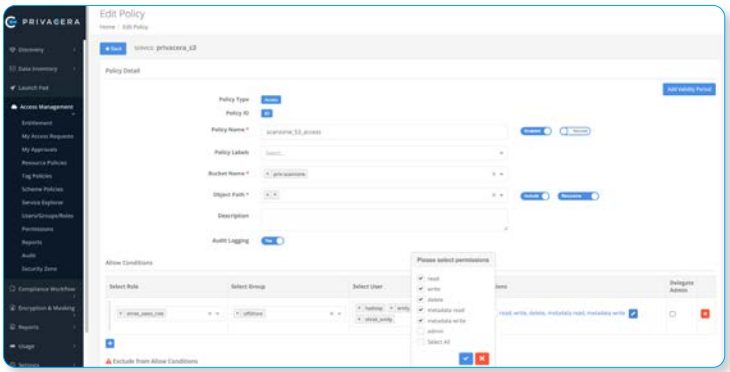
KEY FEATURES

Sensitive Data Discovery & Classification

- Automated discovery, tagging, and classification of sensitive data across repositories that serve as storage layers for Databricks deployments, including Amazon S3 and Azure Data Lake Storage
- Sophisticated rules, pattern matching, dictionaries, and algorithms
- Out-of-box reporting, custom reporting capabilities, and near real-time alerts give comprehensive visibility of sensitive data and its use



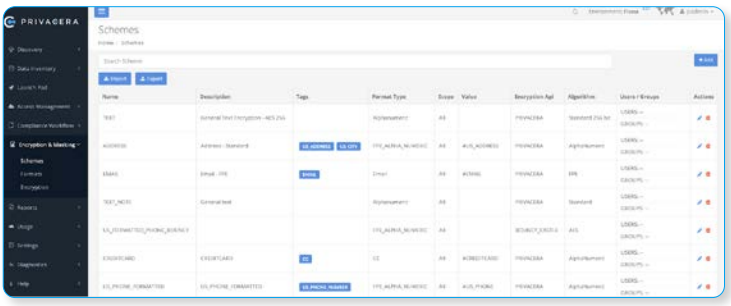
Fine-grained Access Control & Compliance Workflows



- Single-pane view to define and administer tag-based, role-based, or attribute-based data access policies across cloud databases, analytics services, and relational databases including Databricks on AWS or Azure Databricks
- Granular access control down to file, row, and column-levels
- Built-in workflows to ensure compliance with privacy and industry regulations
- Authentication support for LDAP, SAML, OAuth, and OpenID

Data Masking and Encryption

- Masking policies ensure analytics teams can extract insights from regulated data, while complying with privacy regulations
- Define which data fields are masked and what data is anonymized or pseudonymised
- Encrypt data at rest or in motion to secure migration of on-premise data, analytical workloads, and ETL processes

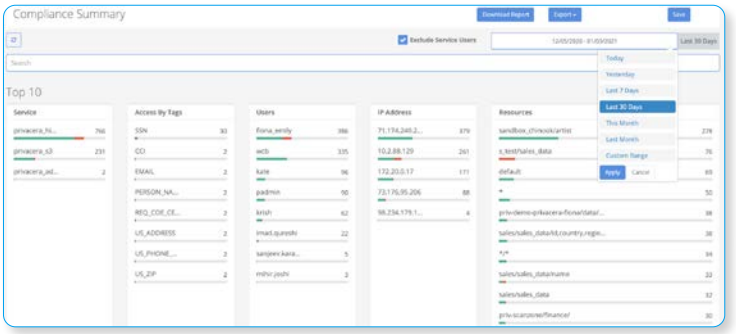


questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

PRIVACERA

KEY FEATURES

Data Auditing and Reporting



- Real- time audits of all data access requests
- Rich event metadata with details of who tried to access what data, when, and from which environment, as well as tenant, security zone, or cluster
- Ability to forward audit logs to downstream systems like Kafka, AWS Kinesis, Azure EventHubs, and more, or SIEM and cybersecurity systems

KEY BENEFITS

Accelerated Digital Transformation

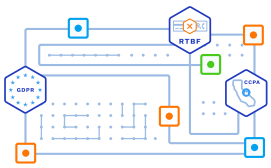
Onboard users faster by rapidly migrating analytic workloads and access policies to Databricks without manually copying or re-writing access policies

Rapid, Self-Service Analytics

Implement customizable policies, rules, and privileges to ensure only the right users have access to the data they need to derive better business, product, and customer insights

Governed Data Sharing

Leverage Privacera's integrations with Databricks' Unity Catalog and Delta Sharing to enable internal and external data sharing without compromising security or compliance



Automated Security and Compliance

Control and enforce data access across on-prem, cloud, and analytical sources from a single location & ensure compliance with real-time reporting

Ready to get started with Privacera and Databricks? Visit https://privacera.com/partners/databricks/ to learn more, or contact us at sales@privacera.com.

questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

PRIVACERA