

PRIVACERA AND STARBURST DATA

Securely Query Anything, Anywhere, and Ensure
Consistent Governance and Compliance



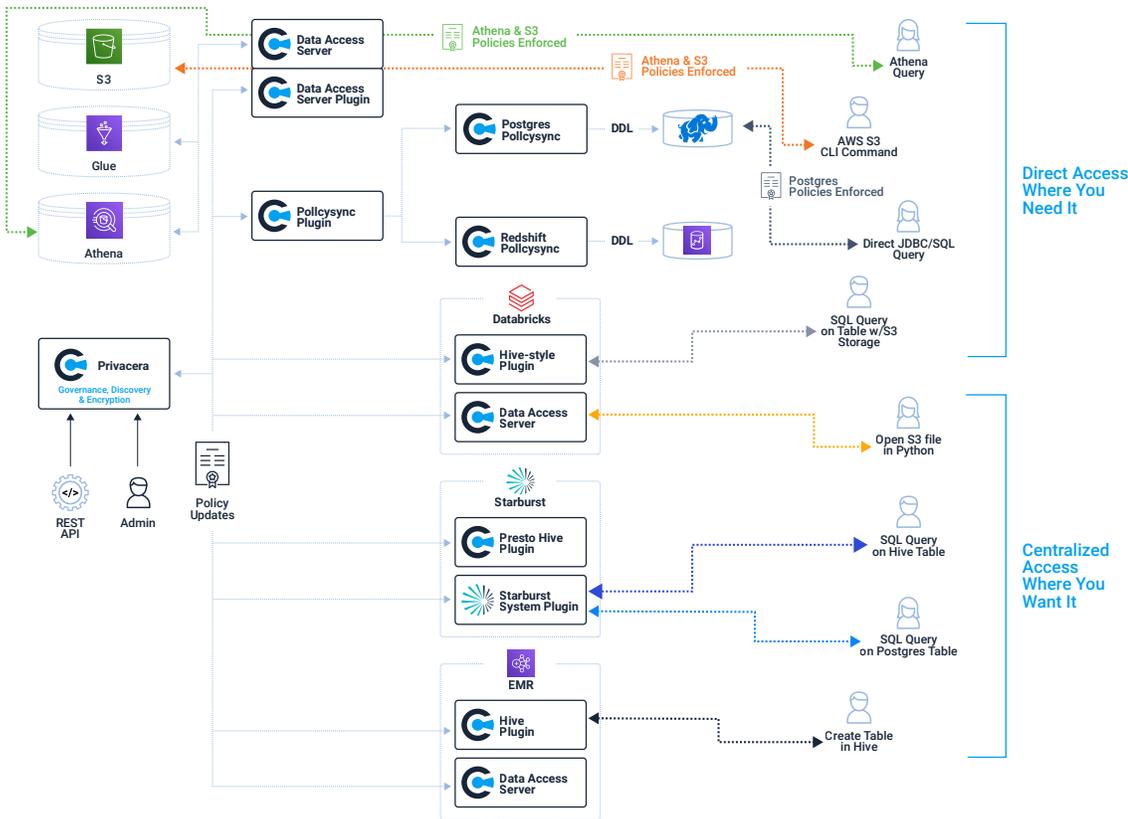
As the number of organizations migrating their analytical workloads to the cloud continues to increase and the volume of data stored continues to grow exponentially, simply moving data into a single-source-of-truth warehouse is no longer viable. In multi-cloud or hybrid cloud infrastructures where data is distributed across multiple platforms, enabling rapid access to data is vital to derive valuable analytics, drive innovation, and improve business operations.

At the same time, automating access control and governance policies across data sources becomes even more complex and difficult as new technologies are added—leaving legal, compliance and data teams overburdened with manual processes and exposing enterprises to potential privacy breaches and compliance violations.

- ⊕ Moving data from various sources into a data warehouse or data lake can be costly and take months
- ⊕ Data engineers spend 57% of their time moving data
- ⊕ Data scientists spend 23% of their time on collection and preparation

To combat these challenges, Privacera and Starburst Data together provide organizations with centralized data access and automated governance across their federated query environments – enabling fast, SQL-based access to data; fine-grained access controls to protect sensitive data from unauthorized access; and detailed auditing and reporting to easily comply with regulations like CCPA, HIPAA, GDPR, and LGPD.

Privacera-Starburst Data Architecture



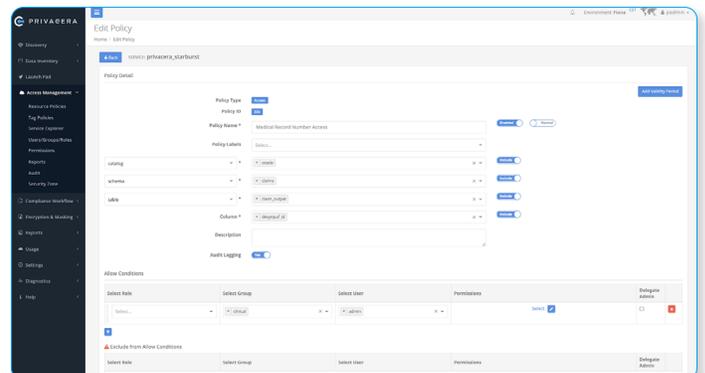
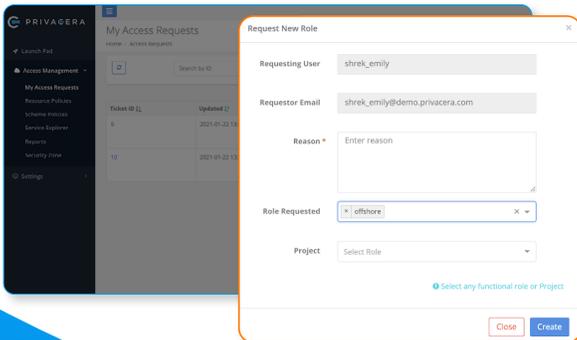
KEY FEATURES

Fine-grained Access Control

- ⊕ Control data access down to the file, row, and column level
- ⊕ Grant access based on roles, projects, data sharing agreements, engagements, classifications, or à la carte requests for specific resources

Automated Policy Migration And Provisioning

- ⊕ Existing on-prem policies are automatically migrated to the cloud and immediately enforced in Starburst
- ⊕ Maintain policies for legacy systems and Starburst catalogs
- ⊕ No rewriting Apache Ranger policies from scratch or duplicating data
- ⊕ Extensive APIs for automation and monitoring



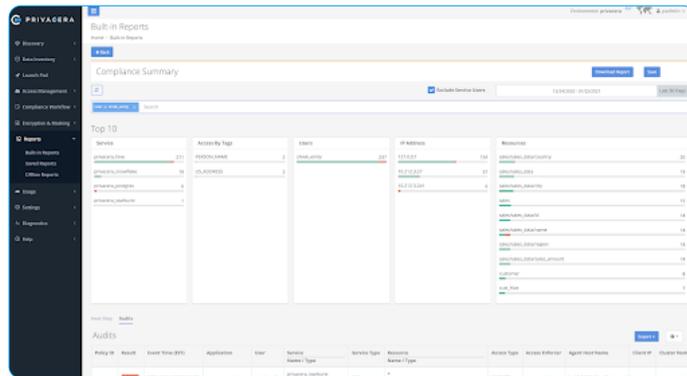
questions@privacera.com
privacera.com
510.413.7300

privacera @privacera

KEY FEATURES (CONT.)

Centralized Auditing And Reporting

- + Get detailed reports and audit trails to understand what data was accessed, by whom, when, and why to easily meet legal, regulatory, and corporate compliance requirements
- + Interactively drill into access and administrative details for auditing or forensic analysis
- + Combine Starburst audit data with access audits from cloud-based data platforms, data warehouses, and databases

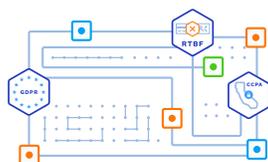


KEY BENEFITS



Ease of Use

Single-pane visibility of data and seamless integration leveraging Apache Ranger plug-in



Automated Compliance

Simplify and automate compliance workflows for Right to be Forgotten (RTBF) requests, data encryption, and anonymization to help meet GDPR, CCPA, PIPEDA, and LGPD requirements



Reduced Manual Processes

Implement bulk access requests, single-click approvals, and automated provisioning



Empowered Data Teams

Fast, secure access to data distributed across multiple sources to derive valuable business insights and analytics

Ready to get started with Privacera and Starburst?

Visit <https://privacera.com/our-partners/> to learn more, or contact us at sales@privacera.com

questions@privacera.com
privacera.com
510.413.7300

in privacera @privacera

PRIVACERA