PROTEGRITY

Databricks Solution Brief

Strengthen Data Security and Compliance for Enhanced Analytics and AI

As organizations in highly regulated industries like healthcare, financial services, and insurance increasingly embrace cloud technologies, they face significant challenges around data security and privacy. Despite the rapid acceleration of cloud adoption, with Gartner forecasting cloud computing as a "business necessity" by 2028[1], the migration of sensitive workloads still presents several concerns.

For example, enterprises want to leverage sensitive data for insights that can drive revenue and improve customer service, however, regulatory compliance requirements can make accessing data for analytics a daunting prospect.

Protegrity provides the critical connection that helps enterprises protect data and maintain compliance–while advancing analytics and artificial intelligence (AI) capabilities. By offering a comprehensive, data-centric solution, Protegrity empowers organizations to fully harness the operational flexibility of the cloud while ensuring stronger data privacy and security.

WHAT MAKES DATA PROTECTION SO COMPLEX?

- Large, distributed teams are cumbersome and expensive to manage
- Data siloed by region can inhibit secure access and comprehensive analysis
- Ad hoc understanding of local compliance regulations weakens governance
- Inadequate tools prevent control of personally identifiable information (PII) across international boundaries
- Increasing costs can result from compliance penalties or outsized resources invested in solutions that don't scale

Protegrity Data Protection Is Trusted Worldwide by

8 of the largest global banks with **500+ million customers** across 160 countries

4 of the 10 largest NA retailers driving **$1.1+ trillion** in revenue

3 of the world's largest government agencies covering **450+ million citizens**

4 of the largest health insurers protecting **200+ million** patients' health records

SIMPLIFY AND STRENGTHEN DATA SECURITY

An effective data protection architecture offers a unified view of data across all workloads and systems. Protegrity makes this possible, while ensuring that sensitive information is protected seamlessly across cloud, hybrid-cloud, and on-premises environments.

Protegrity's tailored approach also eliminates gaps in one-size-fits-all solutions, providing comprehensive security that adapts to the breadth and complexity of today's enterprise environments. Partnering with Protegrity means enhancing security and compliance throughout your data's lifecycle, wherever it may go.

FORTIFY COMPLIANCE

Organizations need a customized, data-centric security approach aligned with corporate policies, government regulations, and evolving customer expectations for data privacy. Protegrity offers a holistic approach to safeguard sensitive data, including PII, payment card industry (PCI) data, and protected health information (PHI), across all environments.

With Protegrity, enterprises get precise data-driven compliance that goes beyond encryption and continuously protects sensitive data with vaultless tokenization. Protegrity's solution also includes the Enterprise Security Administrator (ESA), a user-friendly interface designed to provide centralized oversight of data security policies. ESA meets stringent security standards and boasts built-in backup and recovery options, meticulous access controls, and role separation. It also provides auditing and reporting to promote transparency of various teams' compliance policies and processes.

Protegrity also offers data protection that is embeddable throughout enterprise architecture to help meet strict compliance mandates, such as General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

ENSURE DATA SECURITY IN AI

Empowering teams to use AI can revolutionize your data strategy. But first you must establish the right foundation with proper data protection. Protegrity helps ensure data privacy and mitigates risks associated with the handling of sensitive data in AI applications by minimizing data collection and enabling the use of sensitive data to create richer AI experiences.

Just a Few of Protegrity's Data Security Strengths

Centrally managed security policies
Ensure robust data protection and access control across diverse cloud systems and applications.

Increased situational awareness
Enrich security information and event management (SIEM) threat hunting with centralized logging and monitoring for PII security.

Fine-tuned and field-level protection
Enable secure sharing and tailored access for enhanced business value.

Reduced complexity to minimize mistakes
Provide consistent data security across environments, avoiding configuration errors.

GET MORE FROM SENSITIVE DATA WITH PROTEGRITY AND DATABRICKS

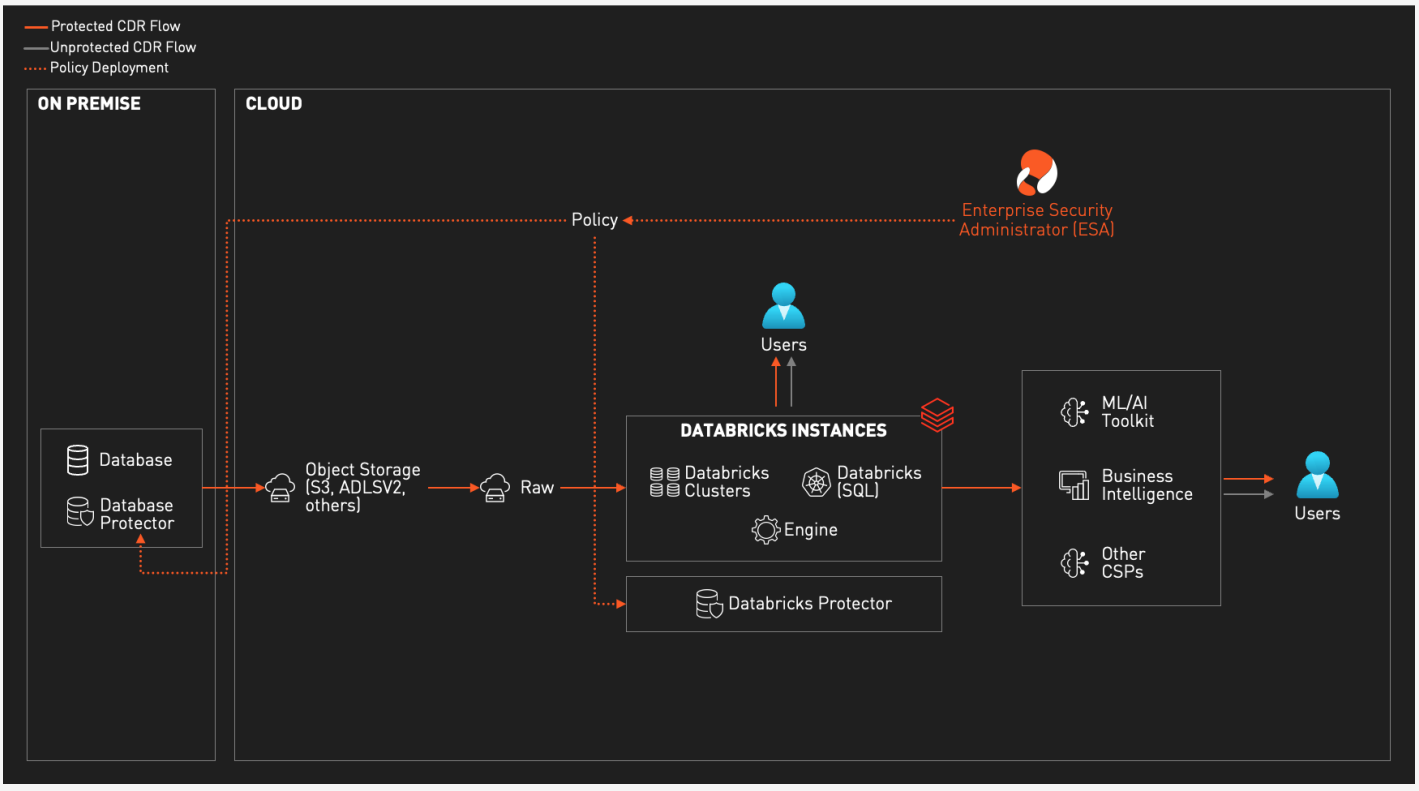
Together, Protegrity and Databricks help customers extract optimal value from their sensitive data assets, facilitating secure utilization of Databricks' analytical capabilities and achieving heightened results.

With a Protegrity and Databricks solution, companies can integrate data protection with cloud data processing and data lakehouses. This makes it possible to protect massive amounts of sensitive data with the flexibility to access, analyze, and monetize it more effectively.

The Databricks Protector simplifies the management and enforcement of data protection across cloud-native, hybrid-cloud, and on-premises deployments and protects data as it moves across operational and analytic systems within hybrid-cloud environments. With Protegrity's centralized policy shared across the enterprise, data is secured prior to being ingested into the Databricks environment and can be protected at rest. User-defined functions (UDFs) can be created in Databricks, which can use Protegrity policy to protect or unprotect data. This minimizes risk, as data is only accessed by authorized users.

The Protegrity and Databricks solution helps data teams fill their data protection gaps and scale across the organization, achieve secure accessibility and transparency, gain clearer data analytics and insights, meet compliance requirements, and simplify day-to-day processes for consistent and trusted results.

Databricks Reference Architecture



PROTEGRITY AND DATABRICKS UNITY CATALOG

Unity Catalog provides centralized access control, auditing, lineage, and data discovery capabilities across Databricks workspaces. Protegrity can leverage Unity Catalog to automate the data protection steps being used within Databricks.

SUPPORTED DATABRICKS CLUSTERS

- Databricks Dedicated Compute
- Databricks Standard Compute
- Databricks SQL Warehouse (Serverless & Non-Serverless)

BENEFITS AT A GLANCE

Improve insights from Databricks

Protect data as it moves or rests in data lakes

Meet compliance requirements across programs and systems

Secure account information and PII at all access points

Maintain customer trust with enhanced data security and privacy

Achieve cost savings and enable growth opportunities

About Protegrity

For more than two decades, Protegrity has been a global leader in data security, protecting the sensitive data of the largest brands in the world. We provide the only platform that lets enterprises decide and classify specific sensitive data sets, allowing them to control how they safeguard that data. With Protegrity, companies can leverage protected data securely and compliantly wherever it's stored. Now, organizations have unrestricted enterprise access to all generally available data security technology, today and in the future, including advisory services and 24/7 support.

READY TO LEARN MORE?

Discover how you can benefit from combining Protegrity data protection and Databricks solutions.

For more information, email **info@protegrity.com** or visit **www.protegrity.com**

PROTEGRITY PARTNER NETWORK MEMBER

databricks

1 "Gartner Says Cloud Will Become a Business Necessity by 2028," Gartner, Nov. 29, 2023