

Delphix Compliance Services

Automatically De-Risk Cloud Data in Microsoft Fabric & Azure Data Flows

The cloud is filled with personally identifiable information (PII) and other confidential information, fueling privacy and security risk. Sensitive data from every production app flows to 10+ downstream systems for dev/test and analytics. Organizations often manage these risks manually—or sometimes not at all. Delphix Compliance Services automates data compliance and security to unblock data movement and accelerate innovation.

Speed Up Compliance in Fabric and Azure

Delphix Compliance Services automatically masks PII within your Fabric and Azure Data Factory (ADF) pipelines. Delphix replaces sensitive data values with fictitious, yet realistic ones while also maintaining multicloud referential integrity. Organizations mitigate risk while ensuring analysts can easily and quickly consume the right data.

How it Works: Discover, Mask and Move Data in Three Steps

Select source and target

Using a pre-built template, select sources and targets, leveraging over 170+ Fabric and Azure-supported connectors, including Snowflake and Databricks. Delphix Compliance Services can mask data from any of these sources and provide masked data within Fabric and Azure ETL data flows.

Discover sensitive data and apply compliance rules

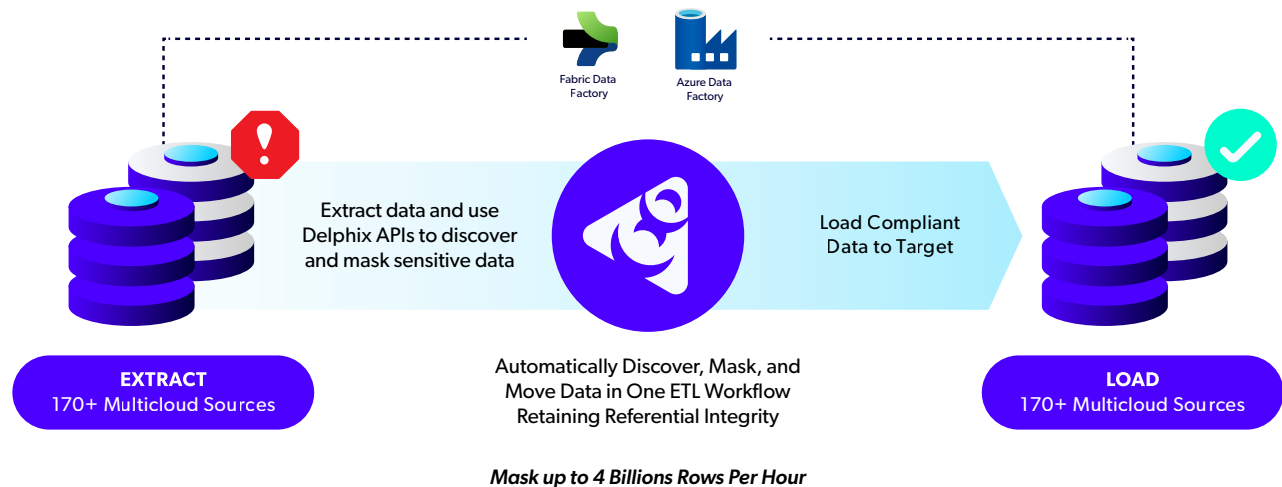
Next, automatically scan the data being passed through the pipeline using out-of-the-box sensitive data discovery capability. Once sensitive data is identified, masking algorithms are automatically assigned to protect that data or algorithms can be defined by the user. These algorithms will replace sensitive data with fictitious, yet realistic values, and do so consistently across all data flows being masked.

Run the data flow to deliver compliant data

Finally, run the data flow to mask data prior to delivery to the selected target. Masked data maintains multicloud referential integrity, is production-like in quality, and remains fully functional for accurate analysis, development, or testing. The service can run any number of concurrent masking jobs to meet the scale needed for enterprise data movement.

Delphix Key Capabilities

- **Regulatory compliance**
Automatically discover and mask data governed by privacy laws such as GDPR, CCPA, and HIPAA
- **Remove data friction**
Automate compliance in Azure and Fabric ETL flows to eliminate data bottlenecks
- **Analytics consistency**
Mask and tokenize data with algorithms designed to preserve analytical meaning
- **Multicloud referential integrity** Leverage the same secure algorithms across clouds and data centers



Feature Overview

- Sensitive data discovery**
 Automatically identify sensitive data fields subject to privacy and industry laws.
- Automated masking within ETL data flows**
 Apply masking rules to data within ETL streams to deliver compliant data where and when it's needed.
- Quality data with realism**
 Transform sensitive values into realistic yet fictitious data, to enable meaningful and accurate analytics.
- Multicloud referential integrity**
 Consistently mask data across PaaS, SaaS, and on-premises sources for improved quality of development and analytics.
- Extensive masking algorithm library**
 Use a comprehensive set of pre-built, customizable masking algorithms to accelerate compliance with privacy or industry regulations and corporate policies.
- Incremental masking**
 Mask only incremental data, using change data capture (CDC) functionality for supported connectors, like Cosmos and Azure SQL. This accelerates pipeline speed and data refresh while reducing storage space and costs.
- Pre-built integrations and templates**
 Use code-less templates and pre-built integration with Fabric and ADF to automatically integrate data compliance into end-to-end data flows.
- Universal multicloud connectivity**
 Leverage 170+ Azure and Fabric connectors to move compliant data where it's needed.

Discover, mask, and move data in Fabric pipelines for your analytics and AI project.

