# SYNTHETIC DATA MASKING

Overview

Organizations globally are moving away from traditional test data management solutions to synthetic test data. But there are use cases where you need to use all or a subset of production data. Organizations must ensure that they are not using Personally Identifiable Information (PII) data that may be within the production data. Violations of PII laws (GDPR, CCPA, HIPPA, etc.) may result in monetary penalties and long-lasting reputational damage that is difficult to repair.

Many traditional masking solutions use replacing certain values with "X"s or other obfuscation methods, sometimes making the data unusable in testing. With GenRocket's Synthetic Data Masking (SDM) feature, you can create realistic looking synthetic replacement value that is usable and secure.

Most common SQL databases are supported (Oracle, MS SQL, IBM DB2, PostgreSQL, MySQL). SDM can also be used to mask secure values in most common file types (Any delimited files such as CSV or fixed files such as VSAM, X12 EDI, JSON, XML, ORC).

Sensitive data is "masked" using **Synthetic Data Replacement**
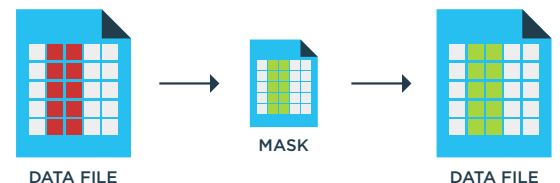
Key Features

- Specify values to replace based on meta data of database or columns in a file
- Supports replacing values in database or files
- Define the characteristics of the replacement data (using GenRocket's 730+ generators)
- Combine with database subset or masking only

Benefits

- GenRocket doesn't need to look at data values, just the metadata, making it more secure
- Can define the exact characteristics of the replaced data value to meet test case requirements
- Obtain test data with greater volume and variety by augmenting masked data

For More Information about **Synthetic Data Masking**, visit the **GenRocket Knowledge Base**

LEARN MORE