DBMasking Overview

Database masking technology refers to the process of replacing sensitive or confidential data in database, such as name, ID, address, phone number, and even credit card number/account number, with random data or special characters to obfuscate the output. By masking the sensitive data, it prevents unauthorized access and protects enterprises from potential damages caused by data breaches.

DBMasking technology enables the de-identification of sensitive data. For instance, an ID number "A123456789" can be masked as "A12345****", and a phone number "0912345678" can be masked as "091234****". With this technology, even if a customer's personal information is leaked, it will not cause harm. Furthermore, the DB Masking technology preserves the characteristics and integrity of the original production data.

Common Threats to Database

Database Vulnerability

Sensitive Data Mismanagement

Improper Authority Control

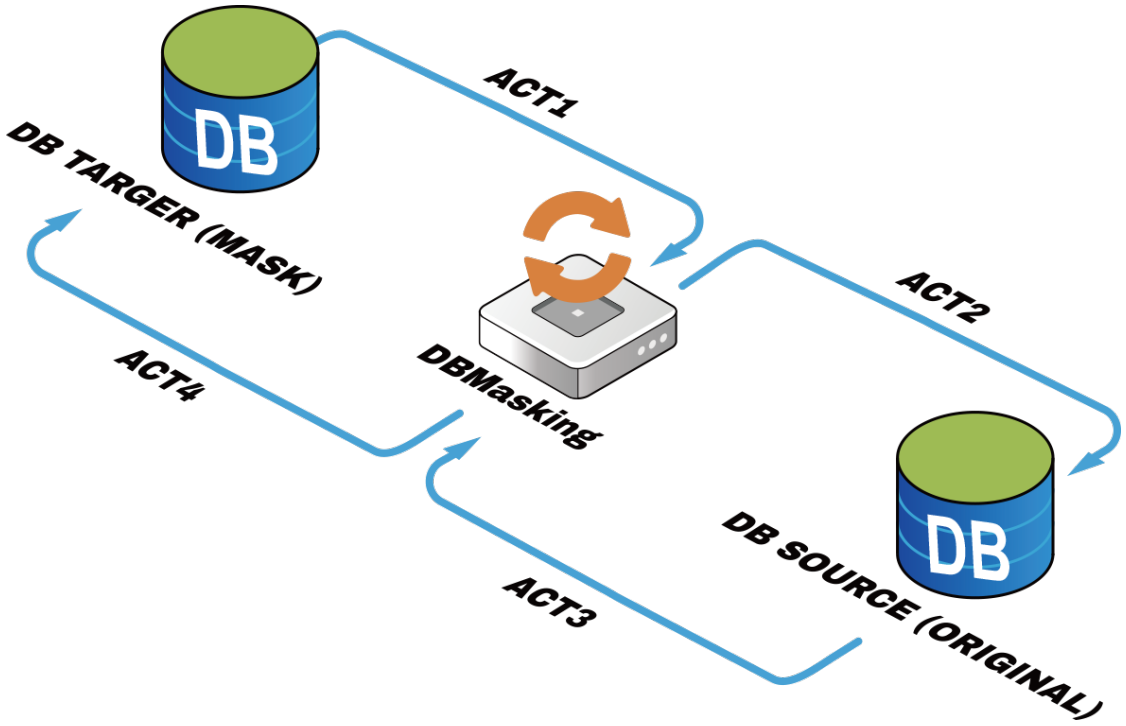
Malware Infiltration

Supported Database

MariaDB

MySQL

DBMasking Architecture



Benefits Of DBMasking

Protecting Data Security

Through DBMasking, data can be effectively protected to prevent data leakage, hacker attacks, intentional misuse of data, and other security threats.

Reduce Burden

With the absence of traditional methods, personnel are not required to modify AP and DB, which reduces the burden on the modifying staff.

Compliance

Comply with international data security regulations, such as GDPR, NIST, PCI DSS, and HIPAA.

Reducing Litigation Risk

Implementing masking mechanisms to anonymize personal and sensitive data can lower the risk of personal data-related litigation.

Keep the original data

DBMasking preserves the structure and format of original data, ensuring the integrity of the original production data.