Informatica Persistent Data Masking

Minimize Risk of Unauthorized Access by Masking Sensitive Data

Informatica Persistent Data Masking is scalable data masking software that lets you create safe and secure copies of data by anonymizing and encrypting information that could threaten the privacy, security, or compliance of critical data. You can use these copies for test, research, analytics, and other nonproduction environments.

The software shields confidential data such as credit card information, Social Security numbers, names, addresses, and phone numbers by preventing unauthorized viewing. It provides scalability, robustness, and connectivity in traditional databases and Apache Hadoop and cloud environments.

Informatica Persistent Data Masking provides a consistent data masking policy across the enterprise with a single audit trail, and it enables you to track procedures for protecting sensitive data through comprehensive audit logs and reports. It provides simulation of masking rules before actual execution to validate privacy policies, and defines and reuses data masking rules to adhere to privacy policies and produce quick results with support for in-place and in-stream masking.

Informatica Persistent Data Masking minimizes the risk of unauthorized data access by masking test, analytics, or development data sets created from production data, regardless of database, platform, or location. The software provides sophisticated but flexible masking rules that allow your IT team to apply different types of masking techniques to various data used in testing, training, and other nonproduction environments.

Benefits

- Reduce the risk of data breaches
- Improve development, testing, and training quality
- Simplify test data management
- Support data privacy compliance
Informatica Persistent Data Masking lets you create policies for masking specific types of sensitive data.

Informatica Persistent Data Masking features robust masking algorithms including substitution, blurring, key masking, and other special techniques for credit card numbers, Social Security numbers, account numbers, and financial information to enable IT and security organizations to maintain structural rules to de-identify values.

**Key Features**

**Single, Scalable Data Masking Environment**
Create and centrally manage masking processes from a single, high-performance environment that readily handles large data volumes. Leverage the scalability and robustness of the Informatica Intelligent Data Platform® and its enterprise-wide connectivity to mask sensitive data regardless of database (Oracle, DB2, SQL Server, Sybase, Teradata), platform (Windows, UNIX/Linux, z/OS, Hadoop), or location.

**Robust Data Masking and Encryption Support**
Maintain structural rules to de-identify values by using masking algorithms such as substitution, blurring, sequential, randomization, and nullification, plus special techniques for credit card numbers, SSNs, account numbers, and financial data. Substitute production information with realistic prepackaged or user-defined data sets. Encryption is provided with a NIST-standard format preserving encryption (FPE) transformation, supporting needs for reversible masking for analytics or privacy needs, such as GDPR (pseudonymization of data).
Broad Connectivity and Custom Application Support
Quickly apply masking algorithms to any sensitive data, in any format. Access and mask a wide variety of databases, mainframes, and business applications, including Oracle, IBM DB2, Microsoft SQL Server, IMS, VSAM, JD Edwards, and Baan. Create data masking rules and standards across all enterprise systems.

Key Benefits

Reduce Risk of Unauthorized Data Access
Creating consistent masking policies across the enterprise with a single audit trail dramatically decreases your organization’s risk of a data breach. With Informatica Data Masking, your database administrators can preview masking policies and rules before data is actually masked. The software simplifies the maintenance and administration of privacy policies.

Improve the Security of Test and Analytics Environments
The software masks sensitive or confidential application data so you can replicate it safely to nonproduction systems. You can preserve the original information characteristics and maintain data and referential integrity. The realistic yet de-identified data enhances the quality of test data for improved development, testing, and training.

Support Compliance with Data Privacy Mandates and Regulations
With access to realistic yet de-identified or pseudonymized data, your IT organization can comply with privacy regulations—including GDPR, HIPAA, PCI DSS, and GLBA—and with data governance policies.