Informatica Persistent Data Masking

Benefits

- Reduce the risk of data misuse or loss
- Support data privacy in application develop and test, and analytic data sets
- Simplify test data management
- Support data privacy compliance

Protect Personal and Sensitive Data With Data Masking

Informatica® Persistent Data Masking is a scalable data masking software product that creates safe and secure copies of data by anonymizing and encrypting information that could threaten the privacy, security, or compliance of personal and sensitive data. You can use these copies for analytics, test, development, and other nonproduction environments.

The software anonymizes personal and sensitive data such as credit card information, Social Security numbers, names, addresses, and phone numbers. Informatica Persistent Data Masking also provides scalability, management, and connectivity for traditional databases, Apache Hadoop, and cloud environments.

Informatica Persistent Data Masking provides consistent data masking policies across the enterprise with a single audit trail, enabling you to track procedures for protecting sensitive data through comprehensive audit logs and reports. It simulates masking rules before they run, so you can validate privacy policies, define and reuse data masking rules that comply with these policies, and produce quick results with in-place and in-stream masking.

Informatica Persistent Data Masking protects data from unauthorized access by masking analytics, test, 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 data privacy and protection teams to apply different masking techniques based on the types of data used in test, development, training, and other nonproduction environments.
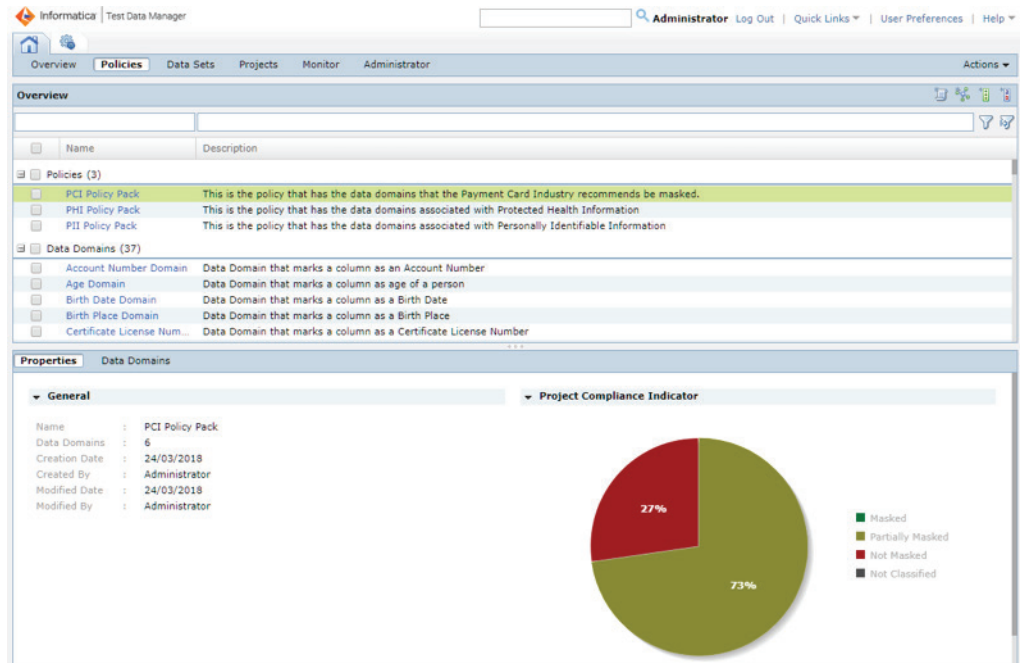
Figure 1: Informatica Persistent Data Masking lets you create policies for masking specific types of personal and sensitive data.

Informatica Persistent Data Masking features robust masking algorithms including format-preserving encryption (FPE), substitution, blurring, key masking, and other techniques for specific data such as credit card numbers, Social Security numbers, account numbers, and financial information. These comprehensive and flexible masking capabilities enable data privacy and protection teams to maintain structural rules that 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 volumes of data. Leverage the scalability and robustness of the Informatica Intelligent Data Platform™ and its enterprise-wide connectivity to mask personal and 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, FPE, blurring, sequential, randomization, and nullification, plus masking techniques specific to credit card numbers, SSNs, account numbers, and financial data. Substitute production information with realistic prepackaged or user-defined data sets. The software provides a NIST-standard FPE transformation that supports reversible masking for analytics or privacy needs, such as GDPR (data pseudonymization).

Broad Connectivity and Custom Application Support

Quickly apply masking algorithms to any personal or 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

Protect Data From Unauthorized 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 Persistent Data Masking, your database administrators can preview masking policies and rules before data is 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 characteristics of the original information while maintaining 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, CCPA, HIPAA, PCI DSS, and GLBA—and with data governance policies.

![Informatica logo] Informatica®