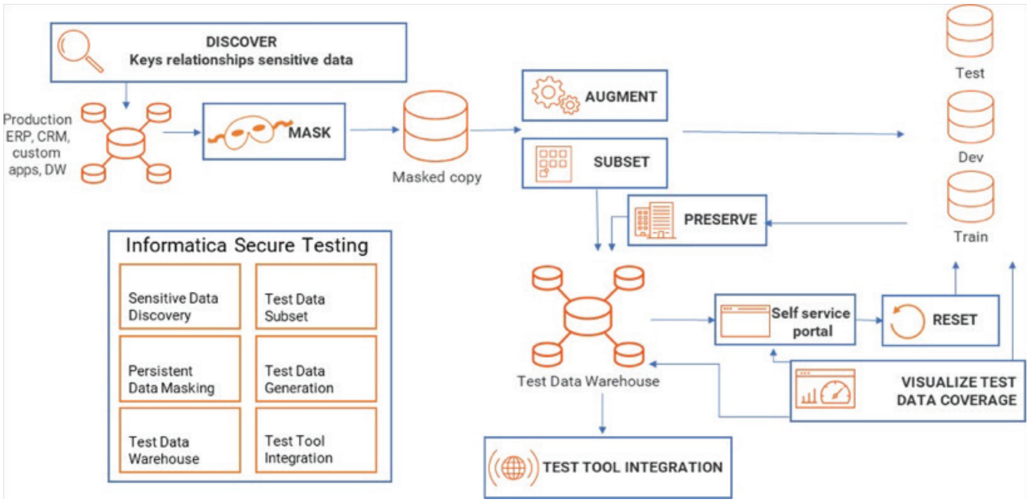
Informatica Secure Testing Solution

Key Benefits

- Improves overall software quality with better test data
- Reduces costs by enabling outsourcing and offshoring of test/development with de-identified sensitive data
- Ensures regulatory compliance and privacy protection in test data environments
- Enables DevOps with automated test data lifecycle management
- Provides self-service test data
- Supports collaboration among multiple testers working on the same test environment

Organizations face increasing challenges for their distributed teams to develop, test, and release software with demanding delivery schedules, complex requirements, and privacy regulations. To meet these demands, organizations seek solutions that accelerate and simplify test data provisioning, provide automated and self-service models for improved tester productivity, and protect personal and sensitive data.

The Informatica® Secure Testing solution provides capabilities for achieving on-time, high-quality results for continuous delivery of software while ensuring that the development and testing process does not threaten privacy compliance by exposing sensitive data to unauthorized access or use. What matters most is getting the right test data to the right teams as accurately and quickly as possible, without violating internal policies or regional and industry regulations.



Informatica Secure Testing

Sensitive Data Discovery	Test Data Subset
Persistent Data Masking	Test Data Generation
Test Data Warehouse	Test Tool Integration

Figure 1: The Informatica Secure Testing solution provides scalable capabilities for sensitive data discovery, masking, subsetting, and validation; automatic generation of anonymized test data; robust test tool integration; visualizations; and a self-service portal.

Sensitive Data Discovery and Test Set Subsetting

The Informatica Secure Testing solution is scalable and highly visual software that enables IT organizations to define subsets of test data from production environments and create a gold copy with desensitized PCI, PHI, and PII data. These smaller datasets additionally minimize infrastructure requirements while optimizing performance. Persistent data masking provides advanced masking of sensitive data that supports privacy and regulatory compliance.

Data discovery and classification automates the identification of sensitive data locations for consistent masking within and across databases. Data validation verifies that sensitive data is masked and compares expected test results with the results of test scripts. Masking sensitive data in test and training environments eliminates test data risks of noncompliance with standards and regulations such as the Federal Communications Commission (FCC), Customer Proprietary Network Information (CPNI), General Data Protection Regulation (GDPR), or the California Consumer Protection Act (CCPA).

Protection of DevOps/Test Environments With Persistent Data Masking

Regardless of the test environment, user role, or data type, data must be protected so that personal and private data of customers and employees is used only in accordance with an organization's security and privacy policies. Persistent Data Masking provides sophisticated but flexible masking rules that allow your IT team to apply different masking techniques to various data used in testing, training, and other nonproduction environments. It anonymizes personal and sensitive data such as credit card information, social security numbers, names, addresses, and phone numbers while preserving the data's format and referential integrity. Testing teams can rely on this anonymized data for accurate and thorough applications testing without jeopardizing privacy or security.

Synthetic Test Data With Test Data Generation

Test Data Generation improves data privacy, mitigates sensitive data risk and increases test result accuracy by creating synthetic test data where data sets do not exist or where access to production data is not feasible. Test Data Generation enhances test data by following the business rules, customizations, anomalies, and error conditions in the associated production data.

Test Data Warehouse

Test Data Warehouse stores test data sets in a central repository that the testing community can access, share, and provision. These capabilities enable test data administrators and QA engineers to collaborate and improve testing productivity. The solution's collaboration tools include marking, metadata tagging, and searching across test data sets with on-demand provisioning and re-set capabilities. Test teams can provision data within shared test environments without the risk of testing collisions, data corruption, or exposing sensitive and private data. The repository maintains test data sets for reuse, ensuring high-quality, on-time software delivery.

Test Data Warehouse further increases testing productivity with a self-service portal that allows testers to request, manipulate, and provision data sets on new or existing nonproduction environments without help from a testing engineer.

Test Tool Integration

The Secure Testing solution provides industry-leading connectivity for managing heterogeneous test tool application environments from a single testing environment.

Key Features

Sensitive Data Discovery and Classification

Test Data Management automates the identification of sensitive data locations for consistent masking within and across databases. It can be deployed on premises, or in cloud data warehouse or data lake environments.

Powerful Masking Capabilities

Enhance software testing privacy by de-sensitizing and pseudonymizing data for privacy compliance and analytics. Persistent Data Masking pseudonymizes analytic data with a NIST-standard format-preserving encryption (FPE) transformation, supporting reversible masking or privacy requirements, such as GDPR compliance, or for medical or legal research.

Performance

Persistent Data Masking can scale to mask terabytes of data for large test, outsourcing, or analytic projects. Data Subset provisions smaller datasets based on test plan requirements to minimize infrastructure requirements and speed performance.

Data Connectivity

Informatica provides comprehensive integrations and connectors to ensure application integrity and speed deployments across various distributions, including mainframe, relational databases, NoSQL databases, cloud applications and databases, and big data sources.

Self-Service and Reuse

With Test Data Warehouse, testers can store, augment, share, and reuse test datasets to improve their testing efficiency.

Automated Test Data

Test Data Generation rapidly automates the creation of complex test data sets when copies of production data are incomplete, unavailable, or cannot guarantee data privacy.

Monitoring and Compliance Reporting

Data security and privacy professionals can ensure ongoing alignment with data governance initiatives.

For more information, please visit our website to explore additional resources and connect directly with our team.

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category, or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities, or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

Informatica®

Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA   Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871