Security threats and the continued expansion of regulations worldwide have increased the focus on ways to reduce exposure of sensitive information to people inside and outside of the business. At the same time, proliferation of stored sensitive data is expanding the security and compliance boundary and increasing the likelihood of data breaches. Oracle Data Masking and Subsetting Pack provides a flexible automated solution that extracts and sanitizes sensitive production data, allowing the data to be safely shared and reused across organizations.

**Introduction to Data Masking and Subsetting**

Oracle Data Masking and Subsetting enables entire copies or subsets of application data to be extracted from the database, obfuscated, and shared with partners inside and outside of the business. The integrity of the database is preserved assuring the continuity of the applications. Oracle Data Masking and Subsetting improves security by reducing the scope of data exposed to partner organizations. Compliance costs are lowered by narrowing the compliance boundary for test and development groups.

**Sensitive Data Discovery and Modeling**

Knowing where sensitive data resides is a non-trivial exercise in today’s complex applications. Oracle Application Data Modeling helps to automate the discovery of database table columns holding sensitive data and the corresponding parent-child relationships defined in the database. The discovery process uses built-in, extensible patterns such as credit card numbers and national identifiers to identify the table columns. The resulting data model is centrally stored within the Oracle Enterprise Manager repository and is updatable whenever the underlying metadata changes.
Masking Sensitive Data

Oracle Data Masking and Subsetting reduces the exposure of sensitive data to test and development organizations with its powerful, flexible, and repeatable masking transformations. Sensitive data such as credit card numbers, social security numbers, national identifiers, and other personally identifiable information can be easily masked with an extensive out-of-the-box library of masking formats. The library can be extended with customized formats for repeated use. Advanced masking techniques include masking based on a condition, deterministic masking, reversible masking, and more. Deterministic masking ensures consistent outputs for a given input. Reversible masking encrypts and transforms the original data based on a regular expression.

Data Subsetting

Oracle Data Masking and Subsetting automates the creation of subsets of application data for sharing with internal and external partners. Data targeted for subsetting can include all database tables or specific tables based on conditions, percentage of database size, and more. Oracle Data Masking and Subsetting provides up-front estimates of the resulting subset size. These features are useful for test data management, where a reduced amount of data is passed to quality analysis teams. Furthermore, subsetting can accelerate servicing e-discovery legal requests.

Centralized Administration and Flexible Execution

Oracle Data Masking and Subsetting Pack is installed by default with Oracle Enterprise Manager. Masking and subsetting can be performed on a cloned copy of the original data, eliminating any overhead on production systems. Alternatively, masking and subsetting can be performed during database export, eliminating the need for staging servers. Subsetting and masking can be performed on data in non-Oracle databases by staging the data in an Oracle Database using the relevant Oracle Database Gateway.

Integrated Masking and Subsetting

Subsetting and masking can be performed in a single workflow. Masking can be automatically initiated when cloning databases using Oracle Database Lifecycle Management Pack. It also can be initiated along with Oracle Data Integrator, applying masks while incrementally synchronizing data with another database.