Oracle Advanced Security Data Redaction

Oracle Advanced Security Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed and redacted on-the-fly before it leaves the database. Data Redaction reduces exposure of sensitive information and helps prevent exploitation of application flaws that may disclose sensitive data in application pages. It is well suited for both new and legacy applications that need to limit exposure of sensitive data without invasive application changes. Oracle Data Redaction is particularly suited for reporting applications and other applications that are read-only.

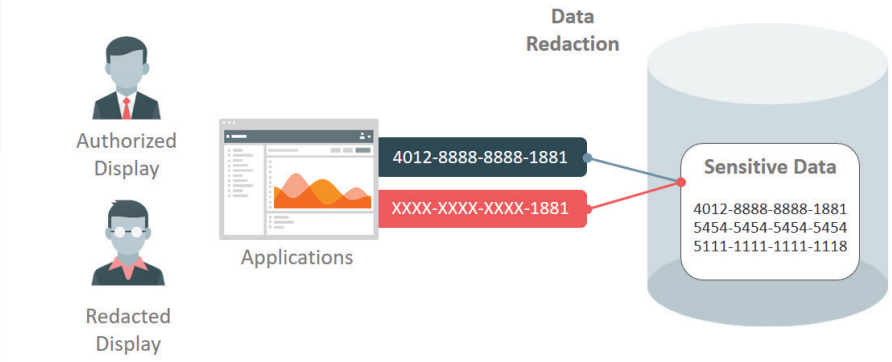

Figure 5. Redacting sensitive data displayed by applications using Data Redaction

Policies and Transformations

Oracle Advanced Security Data Redaction supports a number of different transformations that can redact all data in specified columns, preserve certain pieces of the data, or randomly generate replacement data. Examples of the supported data transformations are shown below.

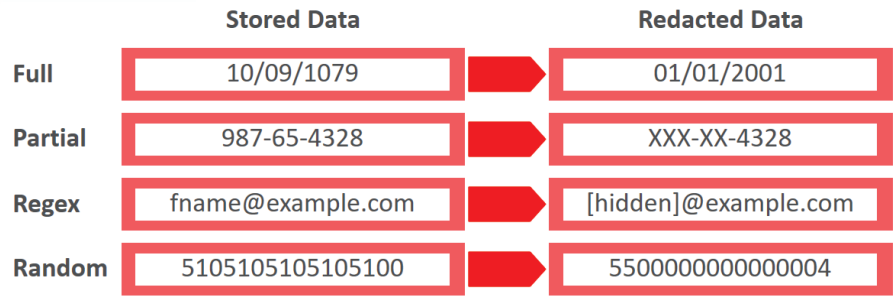

Figure 6. Example Data Redaction transformations

Data Redaction makes the business need-to-know decision based on declarative policy conditions that utilize rich runtime contexts available from the database and from the applications themselves. Examples include user identifiers, user roles, and client IP addresses.

Context information available from Oracle Application Express (APEX), Oracle Real Application Security, and Oracle Label Security also can be utilized to define redaction policies. Redacting APEX