ORACLE

ORACLE Database 23ai

Oracle Advanced Security

Oracle Advanced Security with Oracle Database 23ai delivers industry-leading encryption and data redaction capabilities, vital to protecting sensitive application data. Transparent Data Encryption helps prevent unauthorized access to sensitive information from the operating system, backup media, and database exports. Data Redaction provides dynamic masking for data for application interfaces. Oracle Transparent Data Encryption works with Oracle Database technologies such as RMAN, RAC, Advanced Compression, Oracle Sharding, Data Guard, GoldenGate, and Multitenant, delivering high performance on Oracle's engineered systems.

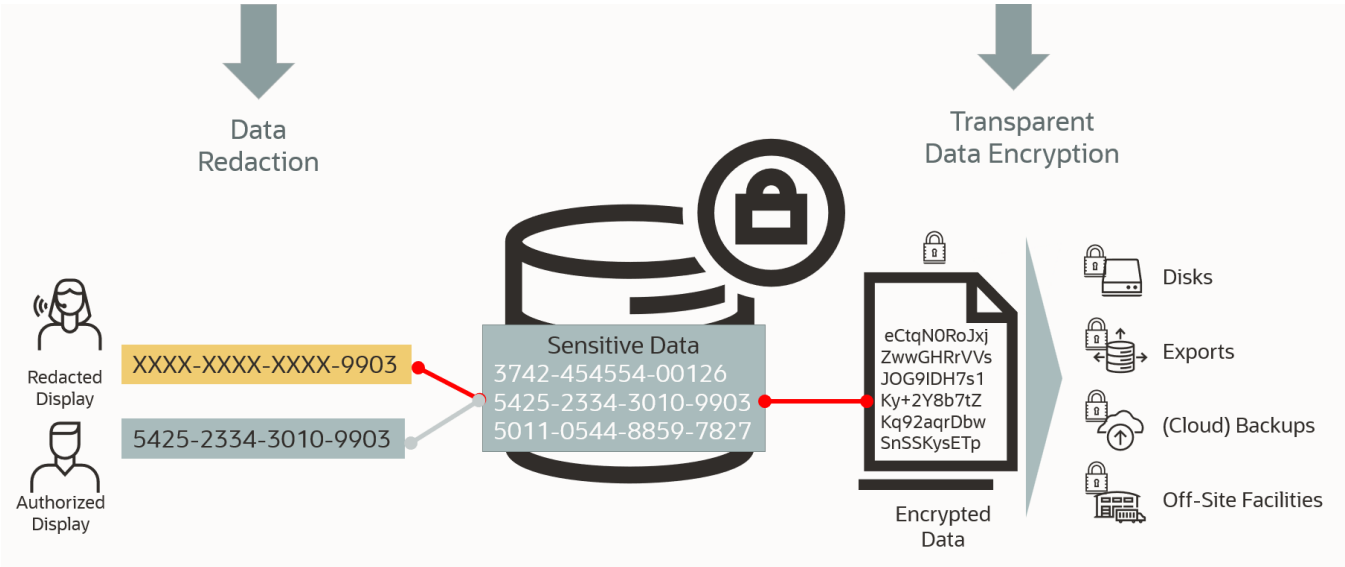
Key Business Benefits

- Protects sensitive data and provides an easy, cost-efficient route for compliance with PCI-DSS, HIPAA, EU GDPR data encryption provisions, and other regulations.
- Helps manage business risk of data breaches due to sensitive data exposure.
- Keeps encrypted data secure and available throughout the data management lifecycle.
- Reduces deployment and operational costs with minimal changes required to applications and databases.
- Improves governance with a single point of management for redacting data across applications and users.
- Enables secure data isolation with full support for the Oracle Multitenant option.

Encryption and Data Redaction for privacy and compliance

Oracle Advanced Security combines two essential data security solutions to help address numerous regulatory requirements, prevent data breaches, and protect privacy-related information. Using Oracle Advanced Security, sensitive application data can be automatically encrypted in storage and, when retrieved, decrypted and redacted on the fly before leaving the database in query results. These two capabilities are critical for complying with privacy regulations and standards such as the Payment Card Industry Data Security Standard (PCI-DSS).

Figure 1. Oracle Advanced Security overview.



Transparent Data Encryption

Transparent Data Encryption safeguards sensitive data against unauthorized access from online storage by encrypting data at rest. It prevents privileged operating system users from directly accessing sensitive information by bypassing access controls and inspecting the contents of database files. Transparent Data Encryption protects against theft, loss, or improper decommissioning of database storage media and backups.

The solution is transparent to applications because data is automatically encrypted when written to storage and decrypted when read from storage. It is also transparent to access controls enforced at the database and application layers. No application code or configuration changes are required.

The encryption and decryption processes are fast because Transparent Data Encryption leverages Oracle Database caching optimizations. In addition, Transparent Data Encryption utilizes CPU-based hardware acceleration available in Intel®, AMD, and Oracle SPARC CPUs, including Oracle Exadata and SuperCluster. Exadata Smart Scans of encrypted data are accelerated by decrypting data in parallel on multiple storage cells. Exadata Hybrid Columnar Compression runs efficiently by reducing the number of required cryptographic operations.

Transparent Data Encryption implements a two-tier encryption key management architecture consisting of data encryption keys and master encryption keys. Administrators can manage master keys locally in an Oracle Wallet or centrally in Oracle Key Vault. Built-in functionality manages keys across their lifecycle and provides easy key rotation without the overhead of re-encrypting all your data.

Transparent Data Encryption deploys quickly and is included by default with the database installation. Users can encrypt existing tablespaces online with zero downtime on production systems or offline with no storage overhead during a maintenance window. Transparent Data Encryption works out of the box with Oracle Data Guard, Oracle Real Application Clusters (RAC), and multitenant databases. Oracle Database Configuration Assistant (DBCA) can automatically encrypt existing databases or create encrypted databases.

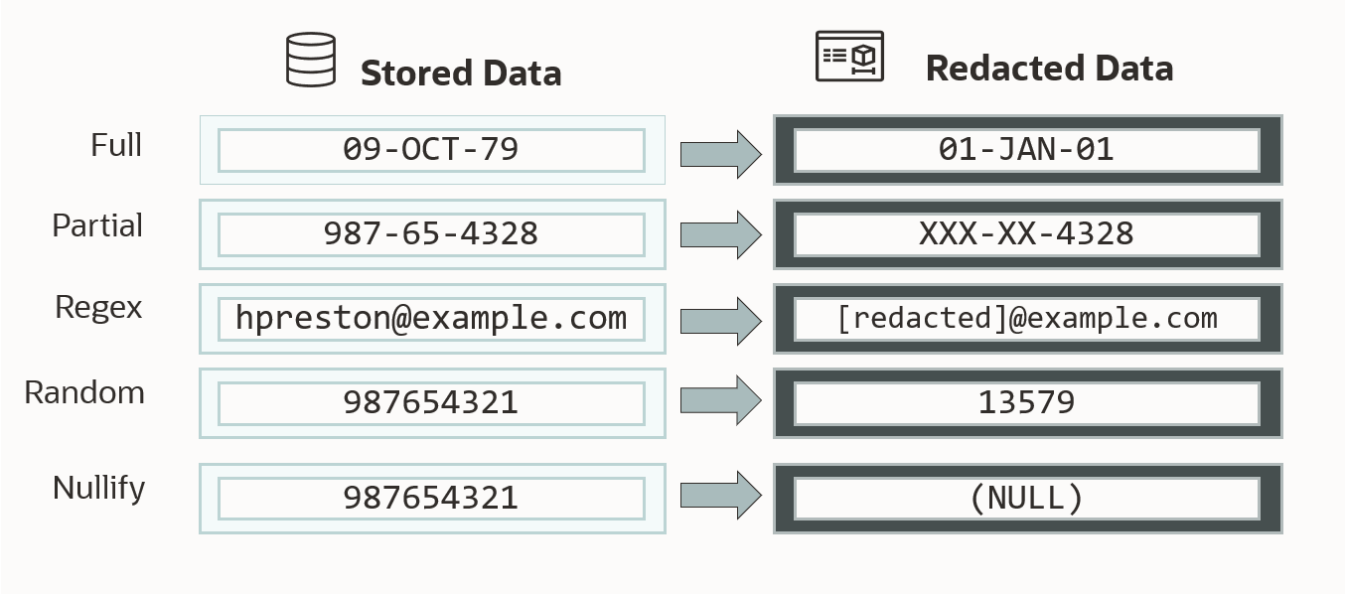
Key features of Transparent Data Encryption

- Encrypts application data with no application changes.
- Supports online and offline encryption of existing tablespaces.
- Built-in encryption key lifecycle management with assisted key rotation.
- Supports industry-standard encryption algorithms, including AES (128, 192, and 256-bit keys) with XTS cipher mode, ARIA (128, 192, and 256-bit keys), and Triple DES (168 bits).
- Works with Oracle Key Vault to provide efficient key management for any number of encrypted databases.
- Leverages hardware acceleration on Oracle SPARC CPUs, Intel® and AMD® (AES-NI).
- Direct integration with Oracle Database technologies such as RMAN, ACFS, RAC, Advanced Compression, Data Guard, Oracle Sharding, and GoldenGate.
- Supports isolation of keystores between pluggable databases.

Redacting sensitive data in applications

Data redaction provides selective, on-the-fly redaction of sensitive data in query results for display in custom applications so that unauthorized users cannot view the sensitive data. It enables consistent redaction of database columns across application modules accessing the same data. Data redaction minimizes the need for changes to applications because it does not alter actual data in internal database buffers, caches, or storage, and it preserves the original data type and formatting of the transformed data returned to the application. Data redaction does not impact database operational activities such as backup and restore, upgrade and patch, and high availability clusters.

Figure 2.Data Redaction transformations.



Unlike approaches that rely on application coding or additional software components, Data Redaction policies are enforced directly in the database kernel. Declarative policies can apply different data transformations, such as partial, random, and full redaction. Redaction can be conditional, based on various factors tracked by the database or passed to the database by applications such as user identifiers, application identifiers, or client IP addresses. A redaction format library provides pre-configured column templates for common types of sensitive data, such as credit card numbers and national identification numbers. Once enabled, policies are enforced immediately, even for active sessions.

Key features of Data Redaction

- On-the-fly redaction to limit exposure of sensitive information in applications.
- Declarative redaction policies are managed centrally in the database.
- Multiple redaction transformations for different application scenarios.
- Redacts unstructured data in LOBs (CLOB/NCLOB) using regular expressions.
- Policy administration using Oracle Enterprise Manager and integration with Oracle SQL Developer.

Protecting sensitive data on-premises and in the cloud

Transparent Data Encryption and Data Redaction are easy to deploy and administer as part of a defense-in-depth security strategy. Oracle Cloud Databases are encrypted using Transparent Data Encryption by default, and deploying encryption to on-premises databases helps ensure seamless security across the hybrid enterprise. Oracle Enterprise Manager provides a convenient and comprehensive management console for defining and applying policies across your fleet of databases. Command-line APIs are also available to facilitate automation.

Transparent Data Encryption and Data Redaction complement other database features while integrating with Oracle Database tools. For example, Transparent Data Encryption tablespace encryption works seamlessly with Oracle Recovery Manager to produce encrypted and compressed backups.

Oracle Advanced Security fully supports Oracle Multitenant, enabling data security isolation between database tenants. Transparent Data Encryption and Data Redaction remain in place when pluggable databases are moved to new multitenant container databases, protecting them while in transit.

Oracle Advanced Security is the only data protection solution for the Oracle Database that delivers application transparency and coverage throughout the data lifecycle without performance penalties or the requirement to expand computing resources. Organizations preparing to move to the cloud can leverage the same data protection solutions with all their databases, both on-premises and in the cloud.

Related products

Oracle Database 23ai defense-in-depth solutions

- Oracle Key Vault
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting Pack
- Oracle Audit Vault and Database Firewall
- Oracle Data Safe

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle