19c ORACLE Database

Oracle Advanced Security

Oracle Advanced Security with Oracle Database 19c Release delivers industry leading encryption and data redaction capabilities, vital to protecting sensitive application data. Transparent Data Encryption and Data Redaction help prevent unauthorized access to sensitive information at the application layer, in the operating system, on backup media, and within database exports. Oracle Advanced Security fully supports Oracle Multitenant and is integrated with Oracle engineered systems for unparalleled performance.

ENCRYPTION AND DATA REDACTION FOR PRIVACY AND COMPLIANCE

Protecting data requires a defense-in-depth approach that includes preventive, detective, and administrative controls. Oracle Advanced Security delivers preventive controls to help address numerous regulatory requirements, prevent data breaches, and protect privacy related information. For example, credit card 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).

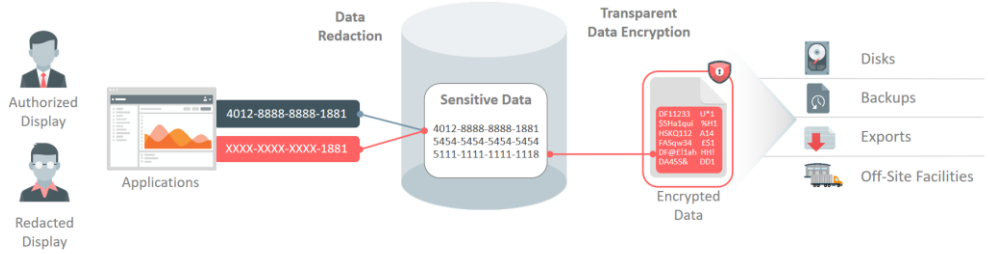

Figure 1: Overview of Oracle Advanced Security

Key Business Benefits

- Protects sensitive data and provides an easy, cost-efficient route for compliance with data encryption provisions of PCI-DSS, HIPAA, EU GDPR 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 Oracle Multitenant option

ORACLE

TRANSPARENT DATA ENCRYPTION

Transparent Data Encryption safeguards sensitive data against unauthorized access from outside of the database environment by encrypting data at rest. It prevents privileged operating system users from directly accessing sensitive information by bypassing controls and directly inspecting the contents of database files. Transparent Data Encryption also 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. Access controls that are enforced at the database and application layers remain in effect. SQL queries are never altered, and no application code or configuration changes are required.

The encryption and decryption process is extremely fast because Transparent Data Encryption leverages Oracle Database caching optimizations. In addition, Transparent Data Encryption utilizes CPU-based hardware acceleration available in Intel® AES-NI and Oracle SPARC platforms, including Oracle Exadata and SuperCluster. Transparent Data Encryption further benefits from Exadata Smart Scans, rapidly decrypting data in parallel on multiple storage cells, and from Exadata Hybrid Columnar Compression, reducing the total number of cryptographic operations that need to be performed.

Transparent Data Encryption provides a two-tier encryption key management architecture consisting of data encryption keys and master encryption keys. The master keys are stored outside of the database in an Oracle Wallet or in Oracle Key Vault. Built-in functionality manages keys across their lifecycle and provides assisted key rotation without the overhead of re-encrypting all of the data.

Transparent Data Encryption deploys easily and installs by default as part of the database installation. Existing tablespaces can be encrypted online with zero downtime on production systems or encrypted offline with no storage overhead during a maintenance period. Additionally, Transparent Data Encryption works out of the box with Oracle Automatic Storage Management to protect data in ASM file stores.

REDACTING SENSITIVE DATA IN APPLICATIONS

Data Redaction provides selective, on-the-fly redaction of sensitive data in query results prior to display by 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 when transformed data is returned to the application. Data Redaction has no impact on database operational activities such as backup and restore, upgrade and patch, and high availability clusters.

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 different factors that are 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 which can be applied to common types of sensitive data such as credit card numbers and national identification numbers. Once enabled, polices are enforced immediately, even for active sessions.

Key Features

Transparent Data Encryption

- Encrypts application data in database columns, tablespaces or entire databases with no application changes required
- Supports online encryption of existing tablespaces
- Built-in encryption key lifecycle management with assisted key rotation
- Uses industry-standard encryption algorithms including AES (128, 192, and 256 bit keys) as well as regional encryption algorithms such as ARIA, SEED and GOST
- Works with Oracle Key Vault to provide efficient key management for hundreds of encrypted databases
- Leverages hardware acceleration on Intel® AES-NI and Oracle SPARC T-Series
- Direct integration with database technologies such as Oracle RMAN, ASM, RAC, Advanced Compression, Data Guard, and GoldenGate
- Supports creation of a keystore for each pluggable database if isolation of keystores between pluggable databases is desired
- Supports creation of user-defined master encryption key

Data Redaction

- On-the-fly redaction to limit exposure of sensitive information in applications
- Declarative redaction policies managed centrally in the database
- Multiple redaction transformations for different application scenarios
- Redacts unstructured data in LOBs (CLOB/NCLOB) using regular expressions

PROTECTING ENTERPRISE DATA ON PREMISE 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. Data in Oracle Databases in Oracle Cloud is always encrypted using Transparent Data Encryption. Oracle Enterprise Manager provides a convenient and comprehensive management console for defining and applying policies. Command-line APIs also are available.

Transparent Data Encryption and Data Redaction complement other database features while integrating with frequently used 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 to enable data security isolation between database tenants. Both Transparent Data Encryption and Data Redaction remain in place when pluggable databases are moved to new multitenant container databases, and they protect pluggable databases 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 penalty or the requirement to expand computing resources. For organizations preparing to move to the cloud, the solution lets them leverage the same data protection solutions with their assets both on-premises and in the cloud.

- Policy administration using Oracle Enterprise Manager, and direct integration with Oracle SQL Developer

Related Products

Oracle Database 19c Defense-InDepth Security Solutions:

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

19c ORACLE Database

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/cloudsecurity/db-sec

 facebook.com/oracle

 twitter.com/oracle

Integrated Cloud Applications & Platform Services

 Oracle is committed to developing practices and products that help protect the environment

ORACLE