ORACLE ADVANCED SECURITY

ENCRYPTION AND DATA REDACTION FOR PRIVACY AND COMPLIANCE

ENCRYPTION FEATURES

- Encryption of application data in database columns or entire tablespaces
- Built-in encryption key lifecycle management, with assisted key rotation
- Industry-standard algorithms including AES (128, 192, and 256 bit keys)
- Hardware acceleration from Intel® AES-NI and Oracle SPARC T-Series
- Oracle Exadata integration, and direct integration with database technologies such as Oracle RMAN, ASM, RAC, Advanced Compression, Active Data Guard, and GoldenGate

REDACTION FEATURES

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

CUSTOMER BENEFITS

- Transparent and consistent data security across current and legacy applications
- High-speed implementations
- Easy to deploy and manage
- Fully supports Oracle Multitenant option

Oracle Advanced Security with Oracle Database 12c 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 option and is integrated with Oracle engineered systems for unparalleled performance.

Overview of Oracle Advanced Security

Protecting data requires a defense-in-depth approach that includes preventive, detective, and administrative controls. Oracle Advanced Security preventive controls 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, at the same time, redacted on-the-fly before leaving the database in query results. These two capabilities are critical for complying with privacy regulations and the Payment Card Industry Data Security Standard (PCI-DSS).

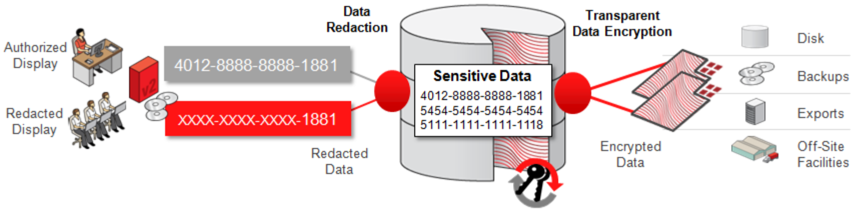

Figure 1. Oracle Advanced Security

Transparent Data Encryption

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

The solution is transparent to applications because data is encrypted automatically 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 TDE leverages Oracle Database caching optimizations. In addition, TDE utilizes CPU-based hardware acceleration in Intel® AES-NI and Oracle SPARC T-Series platforms, including Oracle Exadata and SPARC SuperCluster. TDE 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 performed.

RELATED PRODCUTS

Oracle Database 12*c* Defense-In-Depth Security Solutions:

- Oracle Database Vault
- Oracle Data Masking
- Oracle Label Security
- Oracle Audit Vault and Database Firewall

TDE 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. Built-in key management functionality provides assisted key rotation without re-encrypting all of the data and management of keys across their lifecycle.

TDE can be deployed easily. It is installed by default as part of the database installation. Existing data can be encrypted with zero downtime on production systems using Oracle Online Table Redefinition or encrypted offline during a maintenance period. Additionally, TDE works out of the box with Oracle Automatic Storage Management.

Redacting Sensitive Data for Display

Data Redaction provides selective, on-the-fly redaction of sensitive data in query results prior to display by 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 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 historical approaches that relied on application coding and new 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 to choose from for common types of sensitive information such as credit card numbers and national identification numbers. Once enabled, polices are enforced immediately, even for active sessions.

Protecting Enterprise Data

Both TDE and Data Redaction are easy to administer as part of a defense-in-depth security strategy. Oracle Enterprise Manager provides a convenient and comprehensive management console. Command-line APIs also are available.

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

Oracle Advanced Security fully supports Oracle Multitenant option. Both TDE and Data Redaction remain in place when pluggable databases are moved to new multitenant container databases, and they protect pluggable databases while in transit.

Contact Us

For more information about Oracle Advanced Security, including Transparent Data Encryption and Data Redaction, visit oracle.com/database/security or call +1.800.ORACLE1 to speak with an Oracle representative.

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

Hardware and Software, Engineered to Work Together

ORACLE