# ORACLE ADVANCED SECURITY

## KEY FEATURES AND BENEFITS

- Transparently encrypt data without application changes
- Built-in key management
- Encrypt entire application tables or individual columns
- Encrypt database exports and RMAN backups
- Encrypt Oracle SQL*Net network traffic
- Fully interoperable with Oracle Advanced Compression technologies
- Fully Interoperable with Oracle GoldenGate 11.1.1.1
- Exadata X2 'Smart Scan' and EHCC support
- Cryptographic acceleration with AES-NI on Intel® XEON® 5600
- Industry standards – AES, 3DES, PKCS#11,PKCS#12, X.509v3

*Oracle Advanced Security helps customers address regulatory compliance requirements by protecting sensitive data on the network, on storage media and within the database from unauthorized disclosure. Transparent Data Encryption, a major component of Oracle Advanced Security, provides the industry's most advanced database encryption solution for protecting sensitive information without requiring changes to applications.*

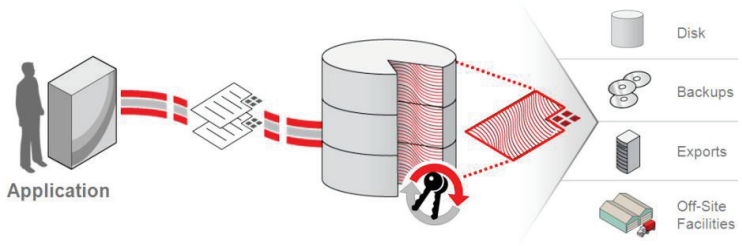
## Overview

Oracle Advanced Security is an option to the Oracle Database 11g Enterprise Edition that helps address privacy and regulatory requirements including the Payment Card Industry Data Security Standard (PCI), Health Insurance Portability and Accountability Act (HIPAA), and numerous breach notification laws. Oracle Advanced Security provides data encryption and strong authentication services to the Oracle database, safeguarding sensitive data against unauthorized access from the network and the operating system. It also protects against theft, loss, and improper decommissioning of storage media and database backups.

## Transparent Data Encryption

62

Transparent data encryption (TDE) encrypts data before it is written to storage and automatically decrypts data when reading it from storage without any changes to existing applications – no triggers, views or other costly changes. Access controls that are enforced by the Oracle database, including object grants, roles, virtual private database and Oracle Database Vault, still remain in effect.




62

TDE supports two modes: tablespace encryption and column encryption. TDE *tablespace* encryption, introduced with Oracle Database 11g, provides an efficient solution for encrypting entire application tables. TDE tablespace encryption fully supports Exadata X2 including Smart Scan and Hybrid Columnar Compression (EHCC). Starting with Oracle Database 11.2.0.2, TDE tablespace encryption automatically utilizes the hardware acceleration of the Intel® Xeon® 5600 CPUs with AES-NI, enabling Oracle Database 11g to encrypt and decrypt data up to 10 times faster on Intel® platforms, including the Oracle Exadata Database Machine. TDE *column* encryption, introduced with Oracle Database 10g Release2, provides an efficient solution for encrypting individual data elements such as credit card and social security numbers. For TDE column and tablespace encryption, frequently

## Protecting Sensitive Data Using TDE Column Encryption

Oracle Advanced Security also provides TDE column encryption. TDE column encryption can be used to encrypt specific data in application tables such as credit card numbers and U.S. Social Security numbers. Customers identify columns within their application schema containing sensitive or regulated data, and then encrypt only those columns. This approach is useful when the database tables are large, only a small number of columns must be encrypted, and the columns are known. TDE column encryption is typically useful for warehouse applications where each query is likely to return a very different set of data. Data encrypted using TDE column encryption remains encrypted on backup media and discarded disk drives, helping prevent unauthorized access and potential data breaches that bypass the database.

### Performance Characteristics

TDE's cryptographic operations are extremely fast and well integrated with related Oracle Database features. TDE leverages CPU-based hardware cryptographic acceleration available in Intel® AES-NI and Oracle SPARC T4 and newer platforms to increase performance significantly. The block-level operations of TDE tablespace encryption receive an additional performance boost from database buffering and caching. Tablespace encryption integrates seamlessly with Oracle Advanced Compression, ensuring that compression occurs before encryption. Tablespace encryption also integrates with the advanced technologies in Oracle Exadata such as Exadata Hybrid Columnar Compression (EHCC) and Smart Scans, which offload certain cryptographic processing to storage cells for fast parallel execution.

### Built-In Key Management

Key management is critical to the security of the encryption solution. Oracle Advanced Security TDE provides an out-of-the-box, two-tier key management architecture consisting of data encryption keys and a master encryption key. The data encryption keys are managed automatically by the database and are in-turn encrypted by the master encryption key. The master encryption key is stored and managed outside of the database within an Oracle Wallet, a standards-based PKCS12 file that protects keys, or in Oracle Key Vault, a centralized key management platform that complies with the industry standard OASIS Key Management Interoperability Protocol (KMIP). Keeping the master key separate from the encrypted data mitigates attacks because both the keys and the encrypted data must be separately compromised to gain access to clear data. The two-tier key architecture also enables rotation of master keys without having to re-encrypt all of the sensitive data.

Either to help you to address regulatory requirements or to comply with your own company policy, Oracle Database 18c introduced support for Bring Your Own Key (BYOK). This feature allows you to bring a user-generated key and use it as the master encryption key for Advanced Security Option Transparent Data Encryption. Those external keys can be ingested by TDE directly, or they can be batch-uploaded into OKV for later use by TDE-enabled databases.

Oracle Database has a dedicated SYSKM privilege that may run all key management operations including initializing TDE, rotating master keys and changing the keystore password. This role can be optionally delegated to a designated user account to enable separation of duty for these functions. Oracle Enterprise Manager provides a convenient graphical user interface for creating, rotating, and managing TDE master keys as shown in the figure below.

Oracle Key Vault is the only enterprise-grade key management platform that provides continuous key availability by clustering up to 16 active OKV instances across geographically distributed datacenters; it is a full-stack, security-hardened software appliance which provides centralized management of encryption keys, Oracle Wallets, Java Keystores, ACFS volume encryption keys, Solaris crypto keys, and credential files. Oracle Key Vault works with Oracle Database and MySQL TDE to automate the management of TDE master keys including creation, rotation, and expiration. Oracle Key Vault