RELATED PRODUCTS

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

accessed data blocks are cached in memory in the same manner as traditional non-encrypted data blocks. This efficient use of native database performance optimizations enables TDE to minimize overhead. TDE tablespace and column encryption also can be used in combination within the same database for hybrid encryption solutions.

Key Management

Oracle Advanced Security provides a built-in, two-tier key management architecture, consisting of a master encryption key and one or more data encryption keys. The TDE master encryption key is used to encrypt and protect the data encryption keys. The master encryption key resides outside of the database in the Oracle Wallet.

Strong Protection for Data In Transit

Oracle Advanced Security provides standards-based network encryption for protecting all communication to and from the Oracle Database. Connections can be rejected from clients that have encryption turned off. No changes to existing applications are required, allowing businesses to easily deploy network encryption.

Strong Authentication Replaces Password Based Authentication

Oracle Advanced Security provides strong authentication to the database using Kerberos, PKI or RADIUS. Oracle Advanced Security interoperates with the Microsoft Kerberos and MIT Kerberos v5. With Oracle Advanced Security, customers can require their users to plug-in a Smart Card (CAC, HSPD-12) as part of their SSL-based authentication to the Oracle Database.

Strong Protection for Database Backups

64

Data encrypted with TDE remains encrypted when the database files are backed-up to disk with Oracle RMAN. Oracle RMAN can also use TDE during the backup process to encrypt the entire database backup, including the SYSTEM and SYSAUX tablespaces. In addition, Oracle RMAN compression and TDE can be used together to generate backups that are both compact and secure.

Application Certification with Transparent Data Encryption

Oracle Advanced Security TDE is certified with many applications, including Oracle E-Business Suite, Oracle PeopleSoft Enterprise, Oracle Siebel CRM, Oracle JD Edwards EnterpriseOne and SAP.

Contact Us

For more information about Oracle Advanced Security, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

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

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

centrally manages TDE master keys over a direct network connection, eliminating the need for local wallet files, reducing operational and security challenges of wallet file management such as periodic password rotation, wallet file backups, and wallet file recovery. Using Oracle Key Vault with TDE enables sites to scale their TDE deployments to hundreds or thousands of databases in different locations while improving operational efficiencies, reducing TCO, and enabling consistent key management policies. A RESTful API allows for secure, automated on-boarding of any number of current or future TDE-enabled databases without any further intervention by the OKV administrators.

Oracle Key Vault also integrates with popular Hardware Security Modules (HSM) from nCipher and Safenet (now Thales) to establish a Root of Trust (RoT) relationship where the secret that unlocks OKV is stored on a tamper-resistant, specialized, FIPS 140-2 level 3 certified hardware module.

Oracle Key Vault supports hybrid cloud deployments, so organizations migrating to the Oracle Cloud can use it to support TDE deployments in both their cloud and on premises databases.

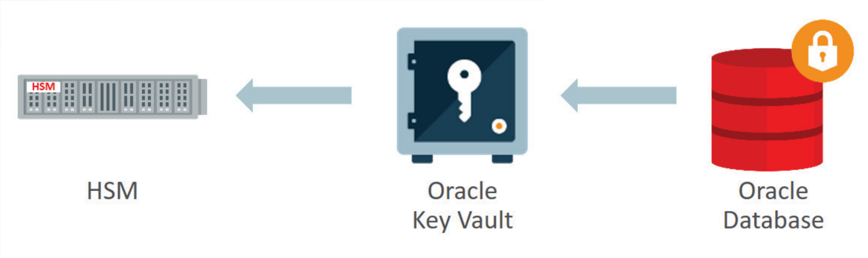

Figure 3. Oracle Key Vault and HSM as Root of Trust for TDE

Encryption Impact for Common Operational Activities

Essential day-to-day database operational activities can potentially leak sensitive data when not performed properly, making bypass easy. Examples of these activities include database backup and restore, data movement, high-availability clustering, and replication.

Example integrations with Oracle Advanced Security TDE

64

DATABASE TECHNOLOGIES	EXAMPLE POINTS OF INTEGRATION	TDE SUPPORT
High-Availability Clusters	Oracle Real Application Clusters (RAC), Oracle Data Guard	✓
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	✓
Export and Import	Oracle Data Pump Export and Import	✓
Database Replication	Oracle GoldenGate	✓
Pluggable Databases	Oracle Multitenant	✓
Engineered Systems	Oracle Exadata Smart Scan	✓
Storage Management	Oracle Automatic Storage Management (ASM) and ASM Cluster File System (ACFS)	✓
Data Compression	Oracle Standard, Advanced , and Hybrid Columnar Compression	✓