Solution Brief

Securing Database Data and Demonstrating Compliance on Oracle Exadata

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Optimized, high-performing databases are essential for all organizations. Often these organizations process significant quantities of data—such as online payment transactions—quickly. Much of this data tends to be highly sensitive and subject to data privacy and security regulations. Oracle's native encryption functionality for Exadata—also known as Transparent Data Encryption (TDE)—is an important tool for protecting this sensitive, regulated data. Oracle TDE on Exadata encrypts data at the tablespace with very little impact on the applications accessing that protected data. While TDE secures data at rest, it is an incomplete protection strategy by itself because it stores encryption keys locally in software, on the database server. Local key storage is especially problematic when regulatory compliance is a consideration.

Fortunately, Thales solves this problem for Oracle TDE On Exadata customers with its CipherTrust Data Security Platform.

Separating encryption keys from encrypted data is a best practice and the foundation of an effective security strategy. Organizations that choose Oracle TDE on Exadata can use CipherTrust Application Key Management (CAKM) with CipherTrust Manager (CM) to secure their database encryption keys to ensure that their database data cannot be accessed without proper authentication and the Master Encryption Key (MEK) to decrypt the Data Encryption Keys (DEKs). Such a strong barrier to entry both secures data and serves as a deterrent to any would-be attackers. Compliance is a significant concern for many Oracle Exadata customers. Requirements such as the Payment Card Industry Data Security Standard (PCI-DSS) state that keys should be secured in separate hardware devices ultimately pushing customers to look for complementary solutions to Oracle TDE.

Benefits

Transparent and Efficient Encryption

- Transparently encrypt sensitive data in Exadata environments
- Secure data without making application changes

Compliance Made Straightforward

- Address compliance requirements for data encryption, separate key storage, and separation of duties

High Performance Security

- Local memory key cache accelerates servicing multiple database unlock request
- Persistent key cache enables faster database start-up, even as the overall network is completing initial boot-up
- Built-in connection pooling, health checking, and multi-tiered load balancing maintain high performance

Risk Mitigation with Maximum Key Security

- Built-in tamperproof hardware options or hardware root of trust integration with Thales Luna HSM address FIPS 140-2 Level 3 and FIPS 140-3 Level 3 requirements

Thales CipherTrust Application Key Management (CAKM) and CipherTrust Manager (CM)

CipherTrust Application Key Management (CAKM) secures Oracle TDE On Exadata keys in their software wallet with a master encryption key, held externally within the confines of a physical appliance or hardened virtual machine. CipherTrust Manager is a centralized platform for managing cryptographic keys, and is capable of running on–premises, in the cloud, in hybrid environments, and is available as a cloud-based service. Available in multiple options, organizations can choose from amongst a range of FIPS 140-2 Level 1 or Level 3 options.

CipherTrust Application Key Management (CAKM) supports TDE key management for the following database versions:

Supported Oracle Database

- Oracle Database 19c (validated with 19.16.0.0.0)

Supported Platforms

- Windows Server 2022 and 2019, 64 bit (validated with Windows Server 2022)
- RHEL 9.x, 64-bit
- RHEL 8.x, 64-bit (validated with RHEL 8.7)
- RHEL 7.x, 64-bit (validated with RHEL 7.9)
- Oracle Linux 8.x, 64-bit (validated with OEL 8.6)
- Oracle Linux 8.x, 64-bit (validated Dataguard on OEL 8.x)
- Oracle Linux 8.x, 64-bit (validated Oracle 19c ExaCC on OEL 8.9)
- Oracle Linux 7.x, 64-bit (validated with OEL 7.9)

Supported CipherTrust Manager

- CipherTrust Manager 2.5.2 and higher

CipherTrust Application Key Management (CAKM) Benefits

Persistent Data Protection

With Oracle TDE and Thales CipherTrust Application Key Management (CAKM), Exadata customers can use encryption and key management to secure database data throughout its at-rest lifecycle, wherever it is copied or transferred. With CipherTrust Application Key Management (CAKM), authorized users and processes readily have appropriate levels of access to the information they need for their roles even as the data remains secured.

Facilitate Compliance

Oracle Exadata databases' ability to quickly store and categorize large quantities of data—much of it sensitive—make it a target for hackers and an important compliance concern for organizations. Oracle TDE secures data while CipherTrust Application Key Management's logging capabilities and remote key storage in CipherTrust Manager allow administrators to demonstrate control over their data per compliance requirements. With CipherTrust Application Key Management (CAKM), organizations can also address a host of miscellaneous internal policy requirements and relevant regulatory obligations such as; the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA), Digital Operational Resilience Act (DORA), and the General Data Protection Regulation (GDPR).

Streamline Key Management Across the Enterprise

With Thales CipherTrust Manager (CM) and CipherTrust Application Key Management (CAKM), customers can strictly control access to their Oracle TDE On Exadata encryption keys within an easy to use platform. As part of the CipherTrust Data Security Platform, Thales also offers products that can protect a wide range of environments, including, self-encrypting drives, tape archives, Storage Area Networks, and a growing list of vendors supporting the Key Management Interoperability Protocol (KMIP) standard.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us