cpl.thalesgroup.com

THALES

Securing Oracle Database Data and Demonstrating Compliance on Amazon Web Services (AWS)

For many, the most valuable data resides in databases running on AWS. It's no secret that data breaches are becoming more common. Organizations that want to protect their reputation and bottom line must implement adequate security. Oracle's native encryption functionality—also known as transparent data encryption (TDE)— serves as a fundamental tool for protecting sensitive data. Oracle TDE provides tablespace encryption that can be implemented with very little impact on applications accessing data protected by encryption. While TDE provides encryption it is an incomplete protection strategy by itself due to local database encryption key storage and management. This is especially the case if regulatory compliance is a consideration, because TDE encryption keys are stored locally in software on the same server as the database.

Fortunately, Thales solves this problem for TDE customers with its CipherTrust Manager enterprise key management platform.

Separating encryption keys from the encrypted data is a best practice and the foundation of an effective encryption strategy. Organizations that choose Oracle TDE can secure and manage their database encryption keys with CipherTrust Manager to ensure that an encrypted database cannot be accessed without CipherTrust Manager authentication. The barrier to entry both secures data and serves as a deterrent to any would-be attackers.

For many Oracle TDE customers regulatory compliance is a significant concern. Requirements such as the Payment Card Industry Data Security Standard (PCI-DSS) state that keys should be secured in separate hardware devices.

Benefits

Transparent and Efficient Encryption

- Transparently encrypt sensitive database data
- No need to make application changes

Achieve Compliance

- Meet compliance mandates, such as PCI DSS and HIPAA, that require encryption of data and separation of duties

Streamline Ongoing Management Activities

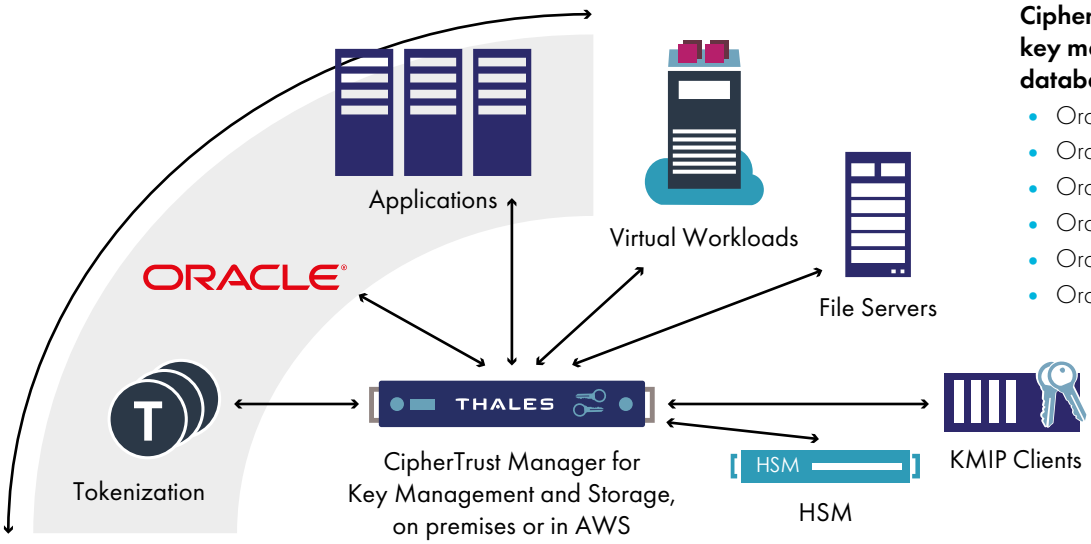
- Built-in, seamless key rotation and data re-keying
- Reduce administration and overhead costs with centralized policy and key management
- With software installed on virtual machines in AWS to enforce data security and compliance policies, deployment is scalable and fast.

High Performance Security

- Perform cryptographic operations locally or offload to CipherTrust Manager to leverage external processing power
- Built-in connection pooling, health checking, and multitiered load balancing

Risk Mitigation with Maximum Key Security.

- Tamperproof hardware options supporting a hardware root of trust with Thales Luna HSM



CipherTrust Manager supports TDE key management for the following database versions:

- Oracle 11g: 11.1.0.6—11.1.0.7
- Oracle 11g: 11.2.0.1—11.2.0.4
- Oracle 12c: 11.1.0.1—12.1.2.0
- Oracle 12c: 12.2.0.1 0 12.2.0.1.0
- Oracle 18c
- Oracle 19c

CipherTrust TDE Agent and CipherTrust Manager

The CipherTrust TDE Agent secures Oracle TDE keys in their software wallet, with a master encryption key, on CipherTrust Manager. CipherTrust Manager is a centralized platform for managing cryptographic content (keys and related data) that is capable of running on–premises, in AWS or hybrid environments. Available as a physical or virtual appliance, customers can choose from flexible options spanning FIPS 140-2 Level 1 or 3 versions.

Thales Oracle TDE Connector Benefits

Persistent Data Protection

With Oracle TDE and CipherTrust Manager running on AWS, customers can ensure encrypted database data remains secure throughout its lifecycle, wherever it is copied or transferred. Though secured, authorized users and processes still have appropriate levels of access to the information they need for their roles when they need it. Full lifecycle protection improves overall security and facilitates collaboration by eliminating points of vulnerability outside the database.

Ensure Compliance

Oracle databases' ability to store and categorize large quantities of information—much of it sensitive customer data—make it a central compliance concern for customers. Oracle TDE secures data per compliance requirements while CipherTrust Manager's logging capability allows administrators to demonstrate control over their data to regulators to aid compliance efforts. With CipherTrust Manager, organizations can also effectively address their internal policies and relevant regulatory mandates such as; the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR).

Streamline Key Management Across Solutions

With CipherTrust Manager, customers can consolidate their Oracle TDE keys into an easy to use management platform along with keys from a wide variety of encryption products including the CipherTrust Data Protection Portfolio, self-encrypting drives, tape archives, Storage Area Networks, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

Granular Access and Authorization Controls to Separate Administrative Duties.

Organizations can unify key management operations across Oracle TDE and other encryption deployments and products, across AWS, while ensuring administrators are restricted to roles defined for their scope of responsibilities—all from a centralized management console. CipherTrust Manager can utilize existing LDAP or AD directories to map administrative and key access for databases, applications and end users.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

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