Vormetric Data Security

Understanding and Selecting Transparent Data Encryption: Native vs External Approaches

Vormetric, Inc.
Tel: 888.267.3732
Email: sales@vormetric.com
www.vormetric.com
Table of Contents

Executive Summary ......................................................... 3
Native Database TDE Overview .......................................... 3
Native Database TDE Security Challenges .............................. 3
Expanding Security Coverage with External TDE ....................... 5
Conclusion .................................................................... 7
Executive Summary

Enterprises have a variety of drivers to encrypt information stored in their databases, from regulatory compliance to executive mandates, and a variety of options to evaluate in protecting that information. One of the options considered when securing database information is the Transparent Data Encryption (TDE) provided by the database vendor. This paper discusses the TDE technology and explains the strengths and limitations that TDE faces in meeting the needs of today’s enterprises. It also explains how Vormetric Data Security provides necessary security and operational benefits while avoiding the limitations of native database TDE solutions.

Native Database TDE Overview

TDE protects data at rest inside of the database through native encryption functions within the database. Some database vendors offer encryption at the column and tablespace level, but it has become increasingly common to apply encryption to all of the data in the database. TDE is referred to as “transparent” since for some implementations, it can secure the data at rest without requiring application changes to take advantage of the encryption functionality. The major reason for using encryption is to avoid compromise of database files in storage. TDE avoids the possibility of someone stealing database files or storage media containing the database files and subsequently attempting to restore the data or browse the files.

TDE implementations are designed to protect raw data at the operating system and storage tiers, while allowing applications and DBA’s to continue to interact with the database, as usual. TDE is not a replacement for good application security and database access controls.

Key management is a major concern for any encryption project and crops up when considering TDE. While database vendors might use common encryption algorithms, how encryption keys are shared, archived, secured and accessed varies between vendors. Some database vendors providing native encryption rely on simple access controls tied to administrative accounts, some encrypt individual user keys with a single master key, and others permit no key access at all and instead use a proxy to perform key operations.

Native Database TDE Security Challenges

Some implementations of TDE within the database engine have the benefit of transparency by avoiding application or database changes; however, like any technology, there are limitations. What follows are some of the most significant challenges to consider when evaluating Transparent Data Encryption.

Unprotected Unstructured Data: Ancillary Data Surrounding The Database

While databases frequently capture the attention of auditors and IT management, the database is part of a web of information flows that include backups, archives, Extract-Transform-Load (ETL) files, and reports. Hackers, bad guys and misguided Database Administrators (DBAs) recognize that security is only as good as its weakest link, and can search out the unencrypted weak link to obtain valuable data. While the database might be secure, the spreadsheet report extracted from the database containing sensitive data also needs to be considered when evaluating data security.
TDE protects sensitive data within the database, however TDE cannot be extended to protect unstructured data outside of the database. Compliance requirements and executive mandates typically impact data no matter where it might reside and include structured data inside the database as well as unstructured data outside of the database. Consequently, the narrow TDE approach cannot extend to protect unstructured information outside of the database.

Unstructured data can take a variety of forms, from images containing sensitive information such as a scanned personal check to spreadsheets or pdf reports containing the results of queries from the database. It can also take the form of database-generated trace files, alert logs or audit logs that are likely to contain sensitive data extracted from the database.

**Administrative Burdens: Native Database Encryption in a Heterogeneous World**

Enterprises have adopted various database technologies for different applications over time. A typical enterprise has accumulated different databases from different vendors. This heterogeneous world means that an enterprise looking to secure databases with native encryption will need to factor in increased costs and administrative resources required from managing multiple encryption solutions. TDE consequently requires training and processes that are specific to each database vendor and goes not generate the economies that come from a single solution protecting multiple databases.

**Insufficient Key and Policy Management**

Database vendors providing TDE typically provide minimal key management functionality and point to Hardware Security Modules (HSMs) or third-party Key Managers to provide the necessary key management. Such key management functionality can become painful when enterprises need to wrestle with large deployments involving tens or hundreds of servers, each having an encryption key to manage. TDE can enable encryption that is transparent to an application, but the management burden needs to be considered to arrive at an accurate understanding of the feasibility and total cost of a solution.

**Performance**

Encryption operations impose an incremental performance requirement on systems. This performance requirement applies regardless of the approach to encryption, whether application-level, database-level (TDE), or file/OS-level. The performance overhead required for TDE varies significantly depending on the workload, with a recent Microsoft paper pegging the overhead at 3-5% for TDE for a database and up to 28% for “cell-level” (column) encryption.²

---


Legacy Database Migration

Enterprises typically have a variety of database versions and grapple with the challenge of supporting a number of older database versions that do not include TDE functionality. While the latest and greatest database versions might offer TDE, legacy packaged applications come bundled with older versions of a database that lack TDE to encrypt columns or tablespaces. It is frequently impossible to migrate such older database versions to more recent versions offering TDE given the constraints of the packaged application the database supports.

In addition, the effort to encrypt the data once the database itself is migrated can include an even more significant body of work. This migration of legacy databases is something that will pose a testing and operational burden.

Expanding Security Coverage with External TDE: Vormetric Data Security

Vormetric Data Security enables enterprises to meet their data security compliance requirements and executive mandates with superior manageability and extensibility compared to native database Transparent Data Encryption. Vormetric protects information stored in databases by transparently encrypting data at the file or volume manager level and can be applied to all databases irrespective of the vendor. In addition to securing database information, Vormetric can also secure unstructured data outside of the database without application or IT operational changes. Vormetric Data Security protects data in physical, virtual and cloud environments while avoiding any changes to the application, database or infrastructure. This approach allows enterprises to achieve security and operational efficiency while avoiding the deficiencies of native TDE provided by a database vendor.
Understanding and Selecting TDE: Native vs External Approaches

Extensible Solution for Structured and Unstructured Data

Vormetric Data Security can secure structured and unstructured data to satisfy rigorous audit requirements and provide comprehensive protection for sensitive data. While data at rest inside of the database can catch the attention of auditors, the data inserted into the database and extracted from the database can be of equal importance to the auditor validating security.

Vormetric can protect sensitive data residing in reports, spreadsheet extracts, archives, Extract-Transform-Load (ETL) data or pdf files. Hackers and rogue employees can use such data stored outside of the database to obtain sensitive information.

Vormetric can evolve as your enterprise’s security requirements evolve in ways that are not possible with native database encryption. While TDE can protect data within the database, Vormetric can protect data inside and outside of the database on all major operating systems including Windows Linux and Unix (AIX, HP-UX, and Solaris) irrespective of whether the server is physical, virtual or in the cloud.

One Solution for All Databases

Vormetric Data Security minimizes administrative overhead and support burdens with a single key and policy management console providing a secure, easy method of administering encryption keys. This enables organizations using databases from different vendors to establish consistent and common best practices for managing the protection of both structured and unstructured data. The Vormetric approach provides for a single console to establish policies and manage database encryption across all database platforms, from Oracle to SQL Server to MySQL to DB2.

Operational Efficiency through Encryption Key & Policy Management

Vormetric Data Security provides secure key management along with granular and configurable auditing and reporting of access requests to protected data, as well as changes to policies and keys. The system’s audit management reduces audit scope, integrates with existing Security Information & Event Management (SIEM) solutions, and aids compliance with industry and regulatory practices regarding the handling and protection of private and confidential information.

Exceptional Performance

Benchmarking from a variety of customers has demonstrated the Vormetric solution provides superior performance over native database TDE. Vormetric performs encryption and decryption operations at the optimal location of file system or volume manager and consequently minimizes performance overhead. Vormetric’s extensive OS and filesystem expertise provides for the best possible system performance while minimizing the encryption CPU requirement.

Major Vormetric Data Security Benefits

Reduced Administrative and Operational Costs

- Protects structured and unstructured data accessed by Linux, UNIX and Windows systems in physical, virtual and cloud environments
- Complete encryption solution includes integrated key management that avoids the cost of acquiring and managing HSMs and third-party key management software typically needed for TDE

Reduced Risk through a Unified Data Security Solution

- Controls privileged user access (System Administrators, etc) and allows them to perform tasks without exposing sensitive data
- Single solution provides common policy framework for accessing both structured and unstructured data

Rapid, Cost-Effective Deployment:

- Vormetric Data Security is transparent to user operations, applications, databases and storage operations
- High performance encryption maintains service level agreements
Future-proofed Transparent Encryption

IT infrastructure and security is changing at a rapid pace with a steady flow of new applications and evolving compliance mandates. To maximize their return on IT investments, enterprises need data protection solutions that can evolve as their requirements change. The solution for protecting a database today might expand to include different vendor databases or “big data” in the future.

Vormetric Data Security functions at the operating system level to encrypt data irrespective of database version or functionality. Vormetric can encrypt legacy databases, today’s current version, and tomorrow’s future data repository to grow as your enterprise grows.

Conclusion

The data within enterprise databases is the lifeblood that permits efficient operations and the sensitive information such databases hold frequently requires protection. An optimal solution to securing database information needs to provide operational efficiency and robust security. While TDE can appear to solve an immediate data security hole, a careful evaluation of technology alternatives can ensure that your business also selects an approach that minimizes operational costs and maximizes business flexibility as business requirements change.

Vormetric enables operational efficiency with a single solution protecting both structured and unstructured data combined with integrated key management. Unlike TDE which secures a single vendor’s database and lacks significant key management, Vormetric delivers manageable data security for complex, heterogeneous environments and can evolve as enterprise requirements change.

With Vormetric Data Security, enterprises can transparently protect their data today with the extensibility to evolve to meet tomorrow’s needs for encrypting data in different vendor databases and also secure unstructured data. Vormetric enables your business to minimize operational costs of securing data while providing the flexibility to evolve as your data protection requirements evolve.

About Vormetric

Vormetric is the leader in enterprise encryption and key management for physical, virtual and cloud environments.

For more information, please call (888) 267-3732 or visit www.vormetric.com.

Copyright © 2011 Vormetric, Inc. All Rights Reserved.

Vormetric is a registered trademark of Vormetric, Inc. in the U.S.A. and certain other countries. All other trademarks or registered trademarks, product names, company names and logos cited are the property of their respective owners.