thalesgroup.com

THALES

Thales Database Encryption Solutions

Database Security Challenges

In today's enterprises, databases house some of the most highly sensitive, tightly regulated data—the very data that is sought after by malicious insiders and external attackers. Many well-publicized database attacks have occurred in recent years, exposing hundreds of millions of records and resulting in financial and reputational damage to the affected organizations.

Central Point of Failure

Databases represent a central aggregation point—and a focal point for thieves. Databases are where a wide range of corporate assets reside, including sensitive, regulated resources, like customer payment data, patient records and intellectual property. In short, your databases, whether on-premises or in the cloud, hold the data that matters to your business and that is prized by would-be attackers.

Insufficient Security Controls

Insufficient security controls expose your organization to fraud and data breaches. For example, when both database encryption and the corresponding key management is handled within the database, the database administrator (DBA) has control of both the data and key. Database encryption solutions often disregard the potential for insider abuse, as well as advanced persistent threats, where an attacker imitates a privileged user.

Complex and Inefficient Key Management

As database environments expand, so do key management challenges. Using multiple key management tools is complex and creates more opportunities for errors and fraud. While database vendors offer key management functionality, this only works when the enterprise uses that vendor's specific databases. Given that each instance of a vendor's database requires a separate encryption key, managing the keys for disparate databases results in more complexity and exacerbates the risks of having keys lost or stolen. Read the Aberdeen report on the remarkable cost of disparate key management.

Is TDE Sufficient?

Oracle and Microsoft SQL Server databases provide Transparent Data Encryption (TDE) functionality, enabling encryption at the database or cell level. It is very likely, however, that you will also need to encrypt the log and report files that contain sensitive data about these databases. And for many organizations, data in other applications and databases will need to be encrypted as well, requiring investments in multiple encryption products, key management and storage systems, and implementation efforts.

The Limitations and Risks of Traditional Approaches

Traditionally, security teams have focused on establishing and shoring up perimeter defenses. However, these defenses leave your organization's databases exposed to a range of insider threats:

- Privileged users can exploit their visibility and permissions to access private data, sabotage configurations and hide their tracks
- Other staff can abuse their access privileges, or they may inadvertently circumvent policies and leave data exposed
- External attackers who gain access to administrator or user credentials can exploit these permissions to wage attacks

To comply with both organizational policies and regulatory mandates, your security team needs to address these threats by establishing strong defenses for your databases.

Database Encryption and Key Management with Strong Access Controls

With solutions from Thales, your organization can establish a strong, comprehensive defense for databases and the assets they contain. Thales solutions feature robust encryption and key management, granular access controls and logging to help protect your on-premises and cloud database environments. Your security teams can encrypt sensitive data and apply granular policies that limit who has access to decrypt that data.

Database Encryption Solutions

Vormetric Data Security Manager

The Vormetric Data Security Manager, or DSM, provides a central platform for managing encryption, policies, keys and security intelligence. Offered as a physical or virtual appliance, the DSM enables your administrators to centrally manage encryption across thousands of databases, and is FIPS 140-2 certified (all 3 levels).

Vormetric Transparent Encryption

Vormetric Transparent Encryption equips your security team with file-level encryption, access control and security intelligence. Vormetric Transparent Encryption can be deployed without having to re-architect applications, infrastructure or practices. Databases may be protected at the file or volume level.

Vormetric Application Encryption

Vormetric Application Encryption makes it easy to add column-level encryption to an existing database application. Development teams can implement the solution without having to acquire encryption or key management expertise. With Vormetric Application Encryption, your organization can secure sensitive data in fields or columns in any database. You can encrypt data before it is written into the database—and ensure data is encrypted at the application server, in transit and in the database.

Vormetric Tokenization with Dynamic Data Masking

Vormetric Tokenization makes it easy to protect sensitive fields in databases. It also provides protection for data in use with policy-based dynamic data masking.

CipherTrust Cloud Key Manager for Cloud Services

With the CipherTrust Cloud Key Manager, your organization can establish strong controls over encryption keys and policies for databases encrypted by cloud services. CipherTrust Cloud Key Manager centralizes encryption key management across multiple cloud environments, providing a range of key life cycle automation capabilities.

Thales Database Encryption Benefits

Thales database encryption solutions offer several key benefits:

Administrative Simplicity

The solutions help minimize the time and effort associated with implementing and maintaining your database encryption with a unified and centralized platform for managing data-at-rest encryption and key management across an enterprise.

Flexible Implementation and Broad Environment Coverage

By leveraging Thales flexible implementation of centralized policy and key management, you can address security policies and compliance mandates across databases and files—whether they are located in the cloud, in virtual infrastructures, or in traditional infrastructures. Thales solutions offer significant flexibility in implementing security in the cloud, whether you want to use keys generated in your own HSM, manage keys created at your cloud provider or encrypt data on site before sending it to the cloud. Whatever approach you require, your organization retains control over keys and data.

Granular Privileged User Access Policy Enforcement

With Vormetric Transparent Encryption, security teams can enforce granular, least-privileged user access policies—by user, process, file type, time of day and other parameters. Security teams can control not only whether users are granted access to clear-text data, but what file system commands are available. Organizations can create a layer of separation between systems and the data they hold. In this way, security teams can enable administrators to manage configurations and ongoing maintenance on specific database servers, without being able to view the sensitive data that resides on those systems in the clear.

Structured and Unstructured Data Support

Thales database encryption solutions provide your IT organization a consistent and repeatable method for managing encryption, keys, access policies and security intelligence for all structured and unstructured data.

Comprehensive Compliance Controls and Audit Trails

Detailed data access audit logs delivered by Vormetric Transparent Encryption help address many general compliance and regulation controls for data encryption, data sovereignty, least-privileged policy and data access auditing. Intelligence logs can prove to an auditor that encryption, key management and access policies are working effectively. Logs also reveal when users and processes accessed data, under which policies, whether requests were allowed or denied, and even when a privileged user submits a command like "switch user" in order to attempt to imitate another user. Finally, pre-built integration to leading Security Information and Event Management (SIEM) systems mean the log data is immediately actionable.

Supported Data Environments

Database: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase, Big Data: Hadoop, NoSQL, SAP HANA, Teradata

Learn More

Please visit www.thalesgroup.com to learn more about how we can help you secure your sensitive databases.

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.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com