cpl.thalesgroup.com

THALES

Thales Database Protection 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.

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 perimeter and endpoint defenses, leaving an organization's data exposed when those defenses fail.

- **Lack of Visibility**
  Organization can't protect their sensitive data effectively, if they don't know where it resides across different databases.
- Reliability and Performance Issues
  Enterprise often suffer from performance impact to real-time access to data, when they implement poorly designed database encryption.
- **Insufficient Security Controls**
  Native database encryption tools suffer from insider abuse, since the database administrators has access to both encrypted data and encryption keys.
- **Complex Key Management**
  As database environments expand, so do the key management challenges. Using multiple key management tools offered by each database vendor increases cost and complexity.

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 data discovery and classification, robust encryption, tokenization 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

CipherTrust Manager

CipherTrust Manager enables organizations to centrally manage encryption keys, provide granular access controls and configure security policies. It is available in both virtual and physical form factors that are FIPS 140-2 compliant up to level 3.

CipherTrust Data Discovery and Classification

The crucial first step in compliance is to understand what constitutes sensitive data, where and how it is stored, and who can access it. Efficient scans enable you to build a strong foundation for your overall data privacy and security. No need to go to different vendors for disjointed solutions. Thales CipherTrust Data Discovery and Classification can efficiently locate most types of data across file servers and traditional databases including Oracle, IBM DB2 and Microsoft SQL Server.

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption delivers data at rest encryption, privileged user access control and detailed access audit logging. It can be deployed at the file or volume level without modifying applications or databases. With CipherTrust Transparent Encryption, you can secure sensitive data in databases across your enterprise, whether you're running Oracle, IBM DB2, Microsoft SQL Server, MySQL, Sybase, NoSQL environments, or any combination thereof.

CipherTrust Application Data Protection

CipherTrust Application Data Protection delivers crypto functions for key management, signing, hashing and encryption services through APIs, so that developers can easily secure data in application or database servers. The solution comes with supported sample code. It accelerates development of customized data security solutions, while removing the complexity of key management from developers.

CipherTrust Database Protection:

CipherTrust Database Protection provides high-performance, column-level database encryption with an architecture that can provide high-availability to ensure that every database write and read happens at almost the speed of an unprotected database. databases with secure, centralized key management and without the need to alter database applications. Granular access controls ensure only authorized users or applications can view protected data. Granularity can be assured with a specific key for each column, and CipherTrust Manager provides a range of powerful access controls for each key while simultaneously assuring separation of duties, a crucial aspect of data security.

CipherTrust Tokenization

CipherTrust Tokenization offers both vaulted and vaultless ways of tokenizing sensitive data. The vaultless tokenization offering includes dynamic data masking, whereas vaulted requires use of environment specific APIs.

CipherTrust Cloud Key Manager for Cloud Services

Streamline bring your own key (BYOK) management for multi-cloud environments, such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, Salesforce and IBM Cloud. The solution provides comprehensive cloud key lifecycle management and automation to enhance security team efficiency and simplify cloud key management.

CipherTrust Database Protection Benefits

Thales database encryption solutions offer several key benefits:

Database Protection Without Noticeable Performance Impact

Thales CipherTrust Data Security Platform solutions are highly scalable and offer protection of your database environment without compromising performance. CipherTrust Transparent Encryption has been field tested in performance-intensive environments, with proven scalability to support 50,000 cryptographic transactions per second.

Seamless Implementation

Thales CipherTrust Data Protection enables high-performance, column-level database encryption without changes to your applications, infrastructure, or business practices, and makes it simple to extend application-layer encryption across virtual, cloud, big data, and traditional environments.

Improved Compliance Posture

Thales CipherTrust Data Discovery and Classification provides data discovery and classification, risk assessment, rich visualizations and detailed reports that enables rapid identification of regulated data, highlights security risks, and help you uncover compliance gaps. This makes it easy for your organization to uncover and close privacy gaps, prioritize remediation, and make informed decisions about privacy concerns.

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 cpl.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.

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