thalesgroup.com

THALES

A Comprehensive Guide to Securing Data with Database Encryption

White Paper

Contents

Today's enterprise security teams are being tasked with supporting a rapid expansion of database encryption use cases. This paper offers a detailed look at why the demand for database encryption is growing more critical and more challenging to contend with. The paper offers an overview of the key approaches required to address this increased demand, and it outlines the different types of encryption approaches—helping IT architects, CISO's, and database security experts ensure they're using the right tools for the right purposes. Finally, this paper offers a look at Thales' extensive portfolio of data protection solutions, and reveals how these solutions enable security teams to address their database security objectives in an efficient, holistic manner.

Why the Demand for Database Encryption is Growing, and Growing More Difficult

For today's modern businesses, virtually every critical digital business asset ultimately makes it into corporate databases. Not surprisingly, these repositories often represent the most sought-after targets of malicious insiders and cyber attackers—and it's a database compromise that tends to pose the most devastating strategic and financial penalties to victimized businesses.

Given these realities, business security policies and regulatory mandates have increasingly stressed the importance of employing encryption to establish strong safeguards around data in databases.

However, while the need to secure data in databases continues to grow more urgent, it also continues to grow more challenging. As the use of big data grows, so too do the number of disparate repositories that access and leverage databases—which significantly expands the number of systems that need to be secured as well as the potential threat vectors. Organizations have grown reliant upon an increasingly diverse range of internal, external, and hybrid computing models—which means more databases need to be secured in more environments and more complex ecosystems. Further, extra safeguards need to be implemented to mitigate the risks inherent in cloud environments, including additional layers of administrative risks and potential exposure should a cloud provider be subpoenaed.

As they seek to contend with this expanding and increasingly urgent demand for database encryption, many security teams are being hampered by their existing tools and approaches. In many organizations, the implementation of encryption has been more tactical in nature, driven by efforts associated with specific project teams, compliance mandates, and technology silos. This has resulted in encryption deployments that can't be centrally operated and administered. Particularly when it comes to key management, the disparate, fragmented nature of these implementations has started to create a number of challenges, including escalating key stores, costs, and risks.

Determining How to Encrypt Database Data

The Requirement: A Holistic Approach to Database Protection

To address all the challenges outlined above, it's essential for enterprise security teams to institute more strategic, enterprise-wide protection strategies. Therefore, security teams need to leverage platforms that provide central, efficient administration of keys and policies across the enterprise, while also having the diverse capabilities and flexible solutions required to institute encryption in the most effective manner for each unique use case.

Overarching Requirements

Any solution employed needs to equip security teams with the following fundamental capabilities:

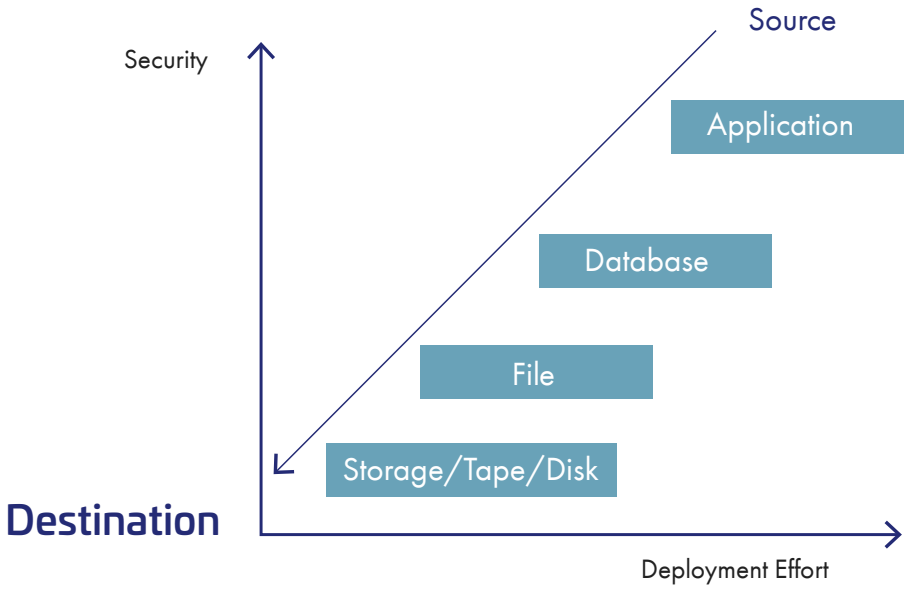
- Securing data and controlling access to that data.
- Applying strong controls to safeguard keys, and to efficiently manage them across the lifecycle.
- Storing and managing keys in a manner that is physically and logically isolated from data repositories.

Choosing the Right Approach for Each Use Case

When it comes to encrypting database data, security teams have a number of approaches and solutions to choose from. Decision makers need to select the solutions that address the most critical channels of attack, while also balancing factors like cost, integration and administration effort, and user service levels and convenience. Following is an overview of some of the approaches available and their relative strengths and weaknesses:

- **Application-layer encryption and tokenization.** By leveraging application-layer encryption and tokenization, organizations can often achieve the highest levels of security. With this approach, organizations can secure sensitive assets across their entire lifecycle, from the point of initial creation or capture until deletion. On the other hand, this approach tends to require the highest level of implementation effort.
- **Database-layer.** By encrypting at the database layer, organizations can secure specific columns within the database. For example, they could encrypt a column that holds employee social security numbers, while leaving other data in the clear. This approach may offer easier implementation than application encryption, but it may not address as many potential threats.
- **File-system layer.** With this approach, organizations encrypt the entire database file. This approach may not offer the broad protection that application- and database-level encryption can provide, but it can be an optimal way to secure database files before or as they are exported, backed up, and archived to storage. Compared to the prior approaches, this alternative is often much easier to employ and manage.

Where to Encrypt and Manage Keys

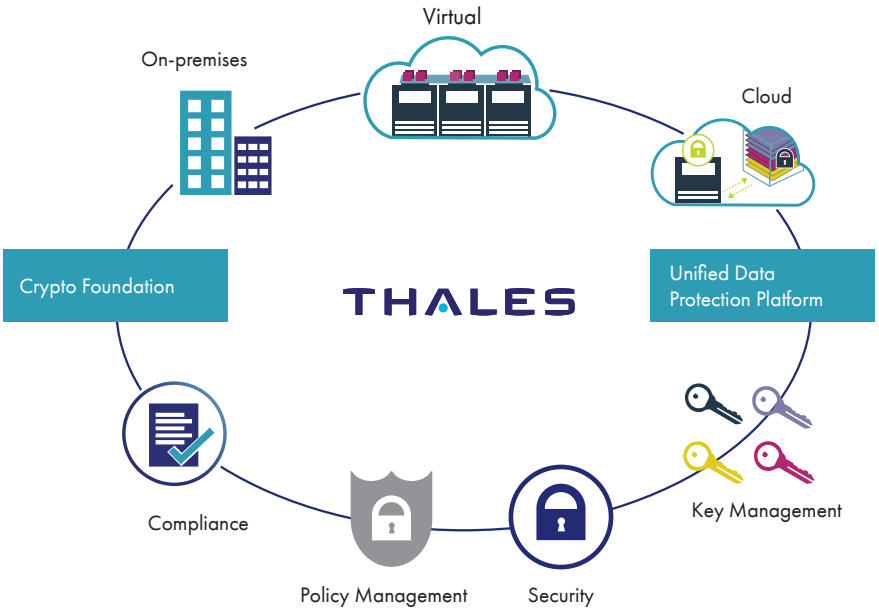


In general, employing encryption higher in the computing stack offers stronger security, while requiring more deployment effort.

Thales Database Protection Solutions

With Thales' portfolio of Thales data protection solutions, your organization can establish a comprehensive, strategic approach to protecting database data across your enterprise. The portfolio offers a comprehensive range of solutions for encryption and tokenization, and it offers central key management solutions that enable your security team to efficiently manage all your organization's encryption implementations and keys. Thales data protection solutions feature these unique advantages:

Unified Data Protection



Thales provides a complete portfolio of solutions that enables unified data protection across an enterprise.

- **Robust, centralized key management.** All Thales data protection solutions are deployed with KeySecure, which offers highly secure, centralized management of encryption keys across the enterprise. By offering centralized key and policy management and enabling automated key rotation and data re-keying, the solution helps strengthen security while reducing administrative effort.
- **Efficient implementation and operation.** Thales data protection solutions offer centralized administration, policy management, and auditing and reporting, which promotes consistent policy adherence and more streamlined administration. With these solutions, you can leverage an efficient architecture that minimizes the performance impact of encryption.
- **Broad environment support.** These solutions offer support for a range of computing environments and models, including multiple public cloud services, virtualized systems, traditional data centers, hybrid infrastructures, and big data implementations.
- **Multi-layer encryption support.** With Thales data protection solutions, security teams can employ a number of approaches, including encrypting columns, files and folders, and entire virtual machines or instances. The suite features databaselevel offerings and application-level solutions for encryption and tokenization.
- **Comprehensive database support.** Your organization can encrypt data in NoSQL databases, including Cassandra, MongoDB, and HBase; and SQL databases, including Microsoft SQL Server, Oracle, IBM DB2, MySQL, and PostgreSQL.

Solutions for Protecting Select Columns in Databases

ProtectDB: Column-level Encryption

ProtectDB delivers column-level encryption for structured data and SQL databases. ProtectDB enables organizations to address a range of security objectives, including securing financial data, complying with PCI DSS, and safeguarding PII.

The solution features transparent and efficient encryption capabilities. With ProtectDB, security teams can institute granular access controls, including by role, user, time of day, and other variables. The solution offers strong safeguards, for example, enabling your security team to prevent a database administrator from impersonating another user to gain access to sensitive data. For added security, automated key rotation and data re-keying are built into the solution, as well as comprehensive logging and reporting.

ProtectApp: Application-level Encryption

ProtectApp encrypts data at the application level, before it is saved to the database. The solution also offers an interface for key management operations.

Many organizations use ProtectApp to secure sensitive information—such as intellectual property or personally identifiable information (PII)—and to address compliance and regulatory mandates.

The solution supports NoSQL and SQL databases and it can protect structured and unstructured data. Encryption is performed on the Thales KeySecure platform, which helps ensure optimal performance and enables centralized key and policy management.

With ProtectApp, organizations can transparently secure data across its entire lifecycle, no matter where it is sent, stored, or copied. The solution offers the following features and capabilities:

- APIs that help streamline integration across multi-vendor application server infrastructures.
- Granular access controls that enable security teams to ensure that only authorized users and applications can gain access to decrypted data.
- Comprehensive auditing and logging.
- Built-in, automated key rotation and data re-keying

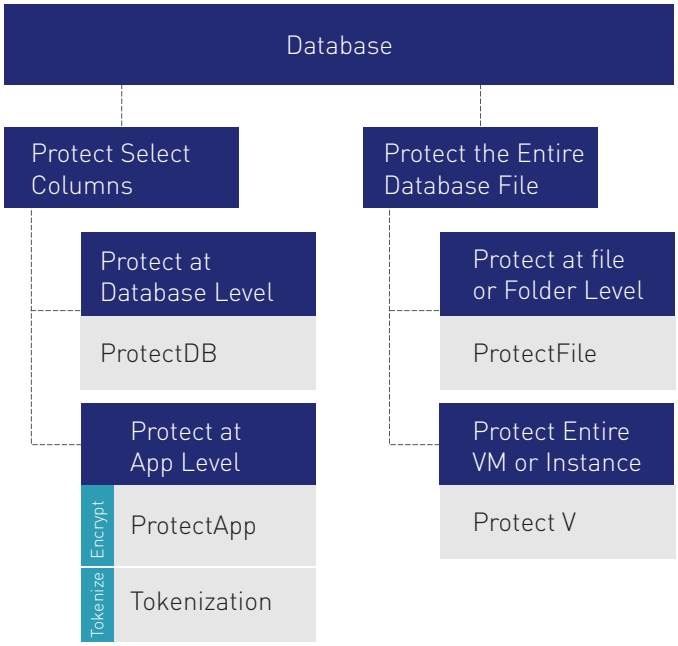
Tokenization: Application-level Tokenization

When organizations employ Thales Tokenization, they can replace sensitive pieces of data with a token, a value that has no meaning or value should it be accessed. The solution tokenizes data before it is stored in the database.

Tokenization offers the flexibility to use standard or customized formats. The solution's format preserving tokenization capabilities enable you to ensure this tokenized data retains similar properties to the original value, which helps minimize any potential impact on associated processes and applications that may access the data. Tokenization features granular access controls and comprehensive logging and auditing capabilities. The solution offers a range of capabilities that streamline deployment, including support for Web services, bulk tokenization, and batch API support.

Tokenization can be used to tokenize any type of sensitive data, including account numbers, credit card numbers, social security numbers, and so on. Many organizations use Tokenization to secure primary payment card account numbers to achieve compliance with the Payment Card Industry Data Security Standard (PCI DSS). In addition, the solution enables organizations to protect PII, and sensitive data in big data environments. Finally, organizations can use the solution to secure data in non-production environments, including those used for application development and testing, research, and more.

Database Encryption Options



The portfolio of Thales data protection solutions enables organizations to leverage an array of approaches for securing data in databases.

Solutions for Protecting the Entire Database File

Thales ProtectFile: File System-level Encryption

ProtectFile applies transparent encryption to the entire database file. The solution offers support for SQL and NoSQL databases and it can encrypt unstructured files. With ProtectFile, security teams can use such file sharing protocols as Common Internet File System (CIFS) and Network File System (NFS) to secure database files that reside on direct-attached storage (DAS), storage area network (SAN), and network-attached storage (NAS) server environments.

The solution offers strong safeguards against insider abuse, for example, restricting a rogue administrator from being able to impersonate a user in order to gain access to encrypted data. For added security, automated key rotation and data re-keying are built into the solution, as well as comprehensive logging and reporting.

ProtectFile represents an optimal solution for securing database files, including files that are used for exports, archives, and backups. The solution also offers effective security in big data implementations, including those running on Apache Hadoop and IBM InfoSphere Big Insights.

Thales ProtectV: Full Disk Virtual Machine Encryption

ProtectV enables organizations to encrypt entire virtual machines, including associated storage volumes, instance snapshots and backups, and partitions. The solution can encrypt unstructured files in NoSQL and SQL databases.

Thales data protection Solutions at a Glance

Solution	Implementation level/type	Databases	Data Types	Environments
ProtectApp	Application-level encryption	NoSQL and SQL	Structured and unstructured	• Public clouds • Virtual environments • Traditional data centers • Hybrid environments • Big data implementations
Tokenization	Application-level tokenization	NoSQL and SQL	Structured	
ProtectDB	Column-level encryption	SQL	Structured	
ProtectFile	File- and folder- level encryption	NoSQL and SQL	Unstructured	
Transparent Data Encryption	Enterprise key management for native database encryption	SQL	Structured	
ProtectV	Virtual machine encryption	NoSQL and SQL	Unstructured	Virtual environments and select public clouds, including Amazon Web Services, Microsoft Azure, IBM SoftLayer Cloud, and VMware

With the solution, organizations can effectively secure virtualized and cloud environments. Security teams can maintain ownership and control of data and encryption keys at all times, and they can institute controls in order to authorize the launch of virtual machine instances. They can also can audit and report on all access to keys, and revoke key access in the event of a breach. ProtectV works with KeySecure to enable centralized key and policy management.

Robust, Centralized Enterprise Key Management

Thales KeySecure

KeySecure is a FIPS 140-2 validated platform that enables you to create a centralized cryptographic service that streamlines encryption deployments across your enterprise. KeySecure seamlessly integrates with the suite of Thales encryption solutions, including ProtectApp, ProtectDB, ProtectFile, ProtectV, and Tokenization.

KeySecure also provides a wide range of standard APIs and development libraries, and it offers support for the Key Management Interoperability Protocol (KMIP) standard. As a result, your organization can realize optimal deployment efficiency, no matter when, where, and how you integrate encryption.

Manage Transparent Data Encryption Keys with KeySecure

Today, many versions of Oracle and Microsoft SQL Server databases offer Transparent Data Encryption (TDE) functionality, which enables organizations to employ encryption of data in databases. However, when TDE capabilities are employed, the cryptographic keys that are generated are stored within the database, along with the encrypted data, which leaves the organization vulnerable to breaches and failed compliance audits. With KeySecure, organizations can leverage native TDE capabilities, while managing keys in a separate and more secure fashion. Further, this approach is transparent to the applications and users that access secured data.

Conclusion

For today's enterprises, demands for securing data in databases continue to grow more urgent. With the Thales porfolio of data protection solutions, your organization can leverage the capabilities it needs to address this demand, and do so with unparalleled efficiency. With these solutions, you can harness capabilities for centralized, unified key and policy management, while implementing database protection approaches that are optimally aligned with your organization's specific risks, technologies, compliance mandates, and business objectives.

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.

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) Ltd
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
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <