Trusted Cyber Technologies

THALES
Building a future we can all trust

Understanding Data Security for SAP

White Paper

Contents

Executive Summary

SAP provides the operational lifeblood of many enterprises with SAP modules providing essential functions that run the gamut from enterprise resource planning (ERP) to Human Resources (HR).

SAP modules can contain sensitive data affected by internal governance mandates or external regulations. Such compliance drivers motivate enterprises using SAP to evaluate methods of securing data and achieving compliance.

This paper describes the unique challenges involved in securing SAP data. It highlights and compares the various technologies that can be used to secure SAP data along with the trade-offs posed by the different approaches. It illustrates how CipherTrust Data Security Platform from Thales provides protection for data in SAP environments.

SAP Data Security Challenges

SAP provides the operational heartbeat for many enterprises, and the data processed by SAP frequently contains sensitive data affected by internal data governance mandates along with industry or government regulations. SAP data can include employee data containing medical or health information that falls under the US Health Insurance Portability and Accountability Act (HIPAA).

Employee personally identifiable information (PII) would be affected by European regulatory regimes such as the UK Data Protection Act and EU Data Protection Directive and General Data Protection regulation (GDPR) protecting individual's information as well as data breach laws passed by various US states including Massachusetts, Nevada and California that require notifications in the event of a data breach. Such legislation typically has "safe harbor" exclusions if organizations can demonstrate that compromised data was encrypted.

SAP data has increased in sensitivity as Human Resources modules can now contain employee health information that might be impacted by national legislation such as the US HIPAA/HITECH Act or EU Data Privacy Directive and GDPR. If SAP holds credit card information, such information is typically affected by Payment Card Industry—Data Security Standard (PCI-DSS). Executive management can deem certain information to be sensitive, resulting in executive mandates to protect this information.

Data in SAP environments can be categorized into two broad categories: structured data and unstructured data. Structured data typically resides inside of the database in the form of tables, columns and rows.

Unstructured data comes in the form of reports, log files, database extracts such as Extract- Transform- Load (ETL) files, and data archives.

Enterprises need to ensure that data is protected against both theft and misuse. Since SAP does not provide such in-depth data security functionality, enterprises rely on the SAP partner ecosystem that provides data protection including protecting data at rest or in use. Tools such as Database Activity Monitoring (DAM) can protect against misuse of data in use, but DAM does not address regulatory requirements for data privacy and security addressed by encryption. Encrypting sensitive data at rest can minimize the possibility of data breaches and satisfy audit requirements. DAM typically works in conjunction with encryption to secure data and help achieve compliance.

Challenges in protecting SAP Data

- **Dispersed Data** — Sensitive data of multiple data types can be spread across multiple columns in 100s of databases throughout the enterprise and cloud environments.
- **Heterogeneity** — Enterprises not only have to protect structured data within databases, but also protect unstructured data, such as log files, reports, and archives outside SAP.
- **Risks of Co-location of Encryption keys and Encrypted Data** — Encryption keys are typically stored with the encrypted data in SAP, which leads to a single point of failure - when keys are exposed sensitive data is also exposed.
- **Performance Impact** — SAP is the operational heartbeat of today's enterprises, and degrading performance or interrupting operations can have catastrophic consequences.
- **Supportability** — Modifying SAP applications or altering database tables risks jeopardizing support agreements
- **Expense and Total Cost of Ownership** — Custom development for data encryption and key management can be expensive given the breadth of SAP applications

Maximizing data security with minimal operational impact

Any strategy for securing data in SAP environments needs to minimize the impact on SAP applications and IT operations. Minimizing any change to an SAP environment allows for rapid implementation of a data security solution and avoids burdening IT with significant ongoing management costs. Burdens to consider can come in the form of changing SAP integration, testing, or modifying the underlying hardware topology.

Considering and controlling such changes results in a higher probability of success. To the degree changes can be avoided, a project can roll out more quickly and with a higher probability of success.

Technology approaches to encrypting SAP data

Storage Encryption

Storage-level encryption refers to encrypting storage at the storage subsystem or storage area network (SAN) switch to protect against theft. Storage encryption can satisfy some audit requirements and protects against the risk of physical theft of storage media. While this approach encrypts the entire storage subsystem and provides protection against data theft, it does not provide for a granular separation of duties between IT security and IT operations nor can it provide auditing of data access. Another challenge with storage encryption is that it can require significant modifications to storage infrastructure that can be costly and time-consuming to implement.

Transparent Data Encryption

Encrypting the database, typically called "Transparent Data Encryption" (TDE), refers to the approach used by some database vendors to encrypt database content. TDE typically works within the database to encrypt content at the tablespace or column level. TDE is usually specific to a particular database vendor, usually lacks centralized security management and does not lend itself to a crossplatform approach across database platforms. While TDE can encrypt data inside of the database, it does not encrypt unstructured data outside of the database that can take the form of reports, archives, Export-Transform-Load data or log files.

File-level Encryption

File-level Encryption can be delivered transparently without requiring any changes to applications. It enables organizations to protect data in files, folders, volumes, and big data environments. In addition, it can generate security intelligence logs to speed up threat detection and streamline compliance reports.

Database Encryption

Database encryption, sometimes referred to as "cell or column-level encryption", can encrypt specific columns containing sensitive data. Such approaches can preserve the format of the column while encrypting the data contained in the column. Column- level encryption has proven useful when a business knows the specific column containing sensitive data (example: credit card number, Social Security Number) and needs to reduce the scope of an audit by encrypting such information. Column-level encryption can be implemented with database triggers, views and stored procedures and typically requires intrusive database changes. Third party column encryption solutions can have a network encryptor element, and such approaches can impact performance due to the network latency inherent in network access.

Column-level encryption in the context of SAP environments has multiple challenges to address. Sensitive data in SAP is scattered throughout the database, so understanding which columns to encrypt can be an issue. Column-level encryption can also pose a significant burden on system resources, particularly when multiple columns are encrypted. Any column-level approach can require more time for integration and testing compared to alternative approaches that encrypt the entire database. Column-level approaches do encrypt structured data in specific database columns, however such an approach cannot address the need to secure unstructured SAP data outside of the database including reports, archives, log files or ETL data.

Application-level Encryption

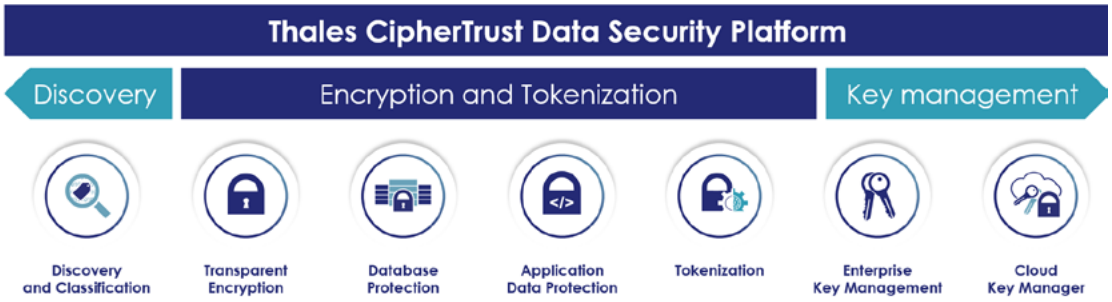
Application-level encryption typically provides a method for securing data at the application layer. Such approaches are frequently found in custom or "homegrown" applications where developers can build in the necessary encryption, however such an approach is not an alternative for SAP data. SAP is a packaged application and SAP has not permitted third parties to encrypt SAP data at the application level. Any attempt to build encryption into the SAP application layer risks invalidating support agreements.

Tokenization

Tokenization refers to the process whereby sensitive data, such as credit card data or a Social Security number, is represented with a surrogate value, called a token. Tokenization provides a way for organizational to minimize the scope of audits since the actual sensitive data is held in a secure repository while a representation of the data (the "token") resides in the database table.

Tokenization functions optimally in situations where one or a handful of database columns need to be secured such as a single database column containing credit card numbers. However, the tokenization approach does not lend itself to complex database schemas. SAP databases can have sensitive data spread among multiple database tables and columns. Tokenization protects structured data inside of a database, but does not apply to unstructured data including reports or log data.

CipherTrust Data Security Platform for SAP



CipherTrust Data Security Platform for SAP applies the same data security and separation of duties (SoD) model used by thousands of Thales customers to SAP data. This proven approach satisfies compliance requirements by encrypting all database files along with reports and log data.

Transparent, rapid implementation

CipherTrust Transparent Encryption, which is part of the CipherTrust Data Security Platform, encrypts databases and files "in place" and avoids the need to re-architect databases, files, or storage networks. Inserted above the file system and/or logical volume layers, CipherTrust Transparent Encryption does not require any applications or databases to be modified to enable data encryption. It requires no ABAP coding, no modification to SAP modules or the database, and consequently deployments can be managed in weeks rather than months.

SAP Environments supported by CipherTrust Transparent Encryption

- Databases including Oracle, DB2, Informix, SAP MaxDB, SAP HANA, SQL Server
- Operating systems including Unix, Linux, Windows
- Files located in physical, virtual and cloud environments

Structured and unstructured data

CipherTrust Transparent Encryption can secure structured and unstructured data to satisfy rigorous audit requirements and provide comprehensive protection for sensitive data. SAP generates and manipulates both structured and unstructured data, and sensitive data is spread across all SAP modules in the database. This can pose challenges for encryption approaches focused on encrypting databases since this approach does not provide support between database platforms and does not protect unstructured data outside of the database.

Multi-Cloud Control

The CipherTrust Platform offers several options to securely move SAP workloads from on-prem to the multi-cloud and hosted environments, yet retaining custodianship of encryption keys, by supporting BYOK use-cases.

Live Data Transformation

CipherTrust Transparent Encryption safeguards SAP HANA data and log volumes, without any changes to SAP HANA or the underlying database or hardware infrastructure. It provides automated key management, key rotation with zero-downtime for initial encryption and mandated key rotation.

Batch Data Transformation

The static data masking capability in the CipherTrust Platform enables you to mask sensitive information in databases before sharing with third-party developers and big-data environments, while maintaining data integrity and still support mission critical testing and analytical activities.

High performance

The Thales solution has no discernable performance impact for SAP end users.CipherTrust Data Security Platform performs encryption and decryption operations at the optimal location of file system or volume manager, and consequently minimizes performance overhead. This approach leverages the I/O profile of SAP databases by only encrypting and decrypting the storage blocks needed for a particular operation.

Centralized management in hetergeous environments

CipherTrust Data Security Platform minimizes administrative overhead with key and policy management providing a secure, easy method of administering encryption keys. It enables organizations deploying SAP to establish consistent and common best practices for managing the protection of both structured and unstructured data accessed by SAP in Linux, UNIX and Windows systems.

Robust auditing

The CipherTrust Data Security Platform provides 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 and Event Management (SIEM) solutions, and aids compliance with industry and regulatory practices regarding the handling and protection of private and confidential information.

Scalability

Organizations can scale the CipherTrust Platform in large and complex SAP environments including thousands of systems and files.

Extensibility

The CipherTrust Data Security Platform lends itself particularly well to protecting SAP data, but can be extended to other applications, files or databases requiring data security.

The CipherTrust Data Security Platform can be used for multiple data types, platforms and use cases beyond securing SAP data. A benefit of such extensibility is that administration and support costs can be minimized since security policies, encryption keys are maintained in one central repository rather than being dispersed among different encryption platforms.

The CipherTrust Data Security Platform protects SAP Data

Top 3 Global Convenience Food Company

- Business Need: Compliance with corporate governance mandate
- Technology Need: Non-intrusive encryption providing high performance
- Solution: The CipherTrust Data Security Platform with Oracle database on HP-UX Server

Leading Global Medical Technology Company

- Business Need: Adhering to multiple compliance initiatives, including PCI and HITECH, protecting intellectual property and personally identifiable information.
- Technology Need: Ensuring security of structured and unstructured SAP data with rigorous separation of duties for system administrators and database administrators (DBAs)
- Solution: CipherTrust Transparent Encryption with Oracle database on Solaris Server

Top 3 Global Beverage Company

- Business Need: Fulfilling executive mandate to protect sensitive data
- Technology Need: Securing SAP data without changing existing environment
- Solution: The CipherTrust Data Security Platform with IBM DB2 database on AIX server

Conclusion

SAP data provides the heartbeat of today's enterprises and the sensitive information it holds frequently requires protection. Given the criticality of SAP deployments, the optimal solution to secure SAP data needs to overcome the challenges including minimizing project risk, protecting dispersed data that can be structured or unstructured, maximizing SAP system performance and scalability, and providing the necessary audit and SoD functionality. CipherTrust Data Security Platform for SAP is a proven solution that enables enterprises to protect their SAP data while meeting these challenges.

The CipherTrust Platform from Thales encrypts data and prevents unauthorized data access using latest encryption technology and centralized key management with CipherTrust Manager, included in the CipherTrust Platform. The CipherTrust Manager integrates with an embedded or network attached Luna Hardware Security Module that is FIPS 140-2 level 3 certified. Either on-premises or in the cloud, the customer can prevent (by policies) system administrators/root user/privileged users from accessing the data in HANA. This is done on the level of the file system and will be used for the SAP HANA data volume and/or log volumes.

SAP has reviewed and qualified the CipherTrust Data Security Platform to protect mission-critical SAP HANA and other SAP environments.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

THALES

Building a future we can all trust

Contact us

www.thalestct.com