THALES

www.thalesesecurity.com

‹Thales eSecurity›

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 then highlights how Vormetric Data Security Platform from Thales eSecurity provides protection for SAP data.

SAP data security challenge

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.

SAP data 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 for SAP 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 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.

MAXIMIZING SECURITY, MINIMIZING THE SECURITY BURDEN

Any strategy for securing SAP data needs to minimize the impact on SAP 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.

DISPERSED DATA

While SAP is an exceptionally comprehensive system, the structure of SAP databases is such that sensitive data in multiple datatypes can be spread throughout the database. One Thales customer mentioned finding that their ERP implementation had sensitive data of various datatypes spread over 200 database columns.

For example, SAP Human Capital Management (HCM) module data may contain sensitive information about employee health records as well as Personally Identifiable Information (PII) in multiple database locations.

SECURING STRUCTURED AND UNSTRUCTURED DATA

While securing dispersed data inside of SAP poses challenges, enterprises also need to consider protecting unstructured data outside of SAP. Optimal solutions for SAP security need to protect structured information as well as unstructured data that can take the form of log files, reports, ETL data for data warehousing, and archive files.

MAXIMIZING SYSTEM PERFORMANCE

SAP is the operational heartbeat of today's enterprises, and degrading performance or interrupting operations can have catastrophic consequences. Any solution to securing SAP data needs to minimize its particular performance overhead so that the SAP system maintains the necessary responsiveness.

AUDITING AND SEPARATION OF DUTIES

Meeting compliance requirements is frequently a major driver behind SAP data security initiatives and SAP security projects typically need robust separation-of- duties (SoD) model along with rigorous auditing to meet those requirements.

Such auditing and SoD functionality protects data while addressing the concern of insider threats.

COMPLIANCE DRIVERS FOR SECURING SAP DATA

- Enterprise business governance mandates
- Government Health Information Regulations including HITECH Act applying to employee health-related information
- Government Industry Regulations including Food and Drug Regulatory Rules including Title 21 of the Code of Federal Regulations (CFR) Part 11 for the United States
- National privacy mandates including UK Data Protection Act and EU Data Protection Directive
- "Safe Harbor" provisions for data privacy between US and European Union
- US state data breach laws (California, Illinois, Massachusetts, Nevada, etc.)

Technology approaches to encrypting SAP 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 "home-grown" 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.

COLUMN-LEVEL ENCRYPTION

Column-level encryption, sometimes referred to as "cell-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 can pose unique performance challenges since data cannot be indexed while it is encrypted; a WHERE clause query using an encrypted column can be time-consuming as the entire encrypted column must first be decrypted.

Column-level encryption also increases storage requirement since a clear text column becomes far larger size/type to accommodate encrypted cipher text.

Column-level encryption in the context of SAP 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.

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.

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 cross-platform 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.

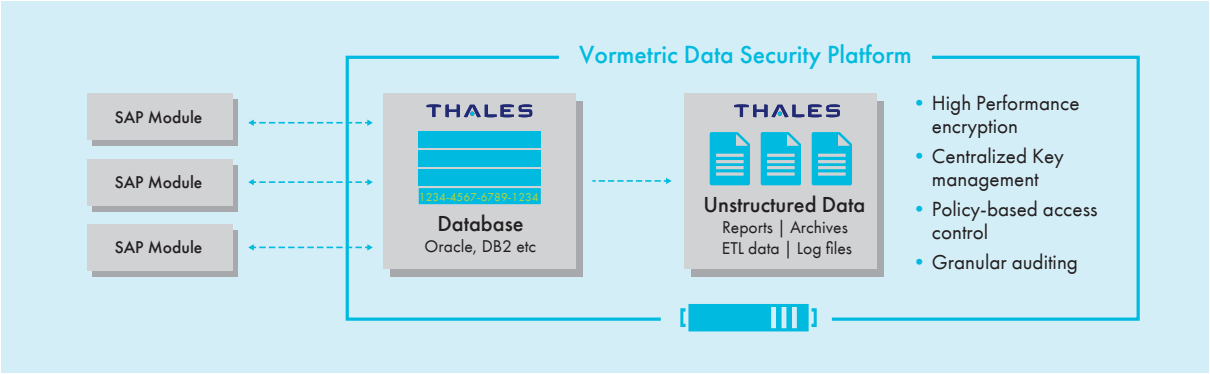
STORAGE ENCRYPTION

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.

CHALLENGES IN PROTECTING SAP DATA

- **Dispersed Data** — Hundreds of database columns may contain sensitive information, making database column-level encryption or tokenization unwieldy
- **Performance** — Maintaining maximum SAP database responsiveness when implementing encryption
- **Supportability** — Modifying SAP application or altering database tables risks jeopardizing support agreements
- **Heterogeneity** — Need to protect both structured data (database files) and unstructured data (log files, Extract-Transform-Load data files, etc.)
- **Expense and Total Cost of Ownership** — Custom development for data encryption and key management can be expensive given the breadth of SAP applications

Vormetric data security platform for SAP



Vormetric Data Security Platform for SAP applies the same data security and separation of duties (SoD) model used by hundreds 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

Vormetric 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, Vormetric Data Security Platform is transparent to users, applications, databases and storage subsystems. 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 Vormetric Data Security Platform

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

STRUCTURED AND UNSTRUCTURED DATA

Vormetric Data Security Platform 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 product unstructured data outside of the database.

HIGH PERFORMANCE

The Thales solution has no discernable performance impact for SAP end users. Vormetric 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

Vormetric 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.

FINE-GRAINED AUDITING

Vormetric 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 Vormetric Data Security Platform in large and complex SAP environments including thousands of systems and files.

EXTENSIBILITY

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

Vormetric 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 VORMETRIC 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 Vormetric 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: The Vormetric Data Security Platform 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 Vormetric 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. Vormetric Data Security Platform for SAP is a proven solution that enables enterprises to protect their SAP data while meeting these challenges.

The Vormetric Data Security Platform from Thales encrypts data and prevents unauthorized data access using latest encryption technology and external key management. The external key manager is FIPS 140-2 Level 1, Level 2, and 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 determined that the Vormetric Data Security Platform software is helpful for mission-critical SAP customer running Linux environments. SAP will fully support this solution on any of the SAP-certified Linux platforms. In order to achieve a full support, SAP and Thales have defined an advanced support ticket handling process (using BC-OP-LNX) for all Linux customers.

THALES

www.thalesesecurity.com

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • 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