cpl.thalesgroup.com

THALES

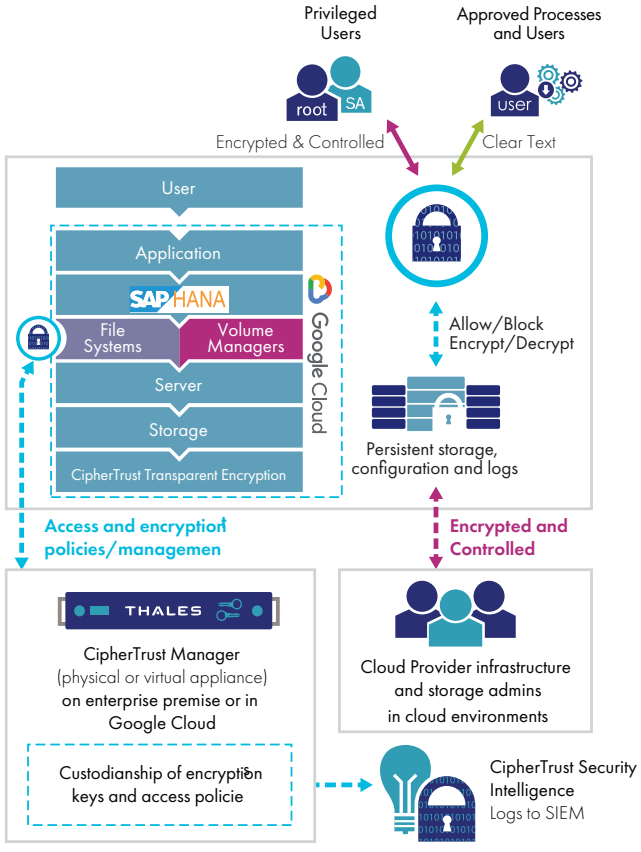
Make SAP HANA Secure and Compliant on Google Cloud with CipherTrust Transparent Encryption

Securely Adopt SAP HANA on Google Cloud

- Encrypt structured and unstructured data and files in place
- Avoid need to re-architect databases or storage in the cloud
- Migrate SAP HANA to the cloud without downtime
- Provide granular and configurable auditing and reporting
- Facilitate compliance to growing data security mandates

The problem: Compliance obligations increase the need to secure SAP HANA Data

SAP HANA repositories often contain large quantities of highly regulated data. Threats to this data, along with increased pressure from regulatory bodies, is prompting enterprises to adopt strong data security controls, including encryption of data-at-rest. These needs become extra important when databases deploy in cloud environments - such as the Google Cloud - where customers are not in control of the underlying infrastructure. Regulatory regimes like the US Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) act, as well as European legislation such as the UK Data Protection Act and EU Data Protection Directive, and the General Data Protection Regulation (GDPR), call for safeguarding individual data. However, security is often difficult to control in remote Cloud environments where the customer also has to worry about the Cloud Service Providers access to their data.



CipherTrust Transparent Encryption protects data and prevents unauthorized access, facilitating regulatory compliance without having to change database or hardware.

The challenge: Securing sensitive data without affecting performance

Securing dispersed structured and unstructured data in cloud environments is a high-visibility task that must be done carefully. The approach should satisfy security and audit requirements without impacting the database application, architecture, or IT or Cloud operations. Organizations that move their SAP HANA infrastructure into the Google Cloud without adequate security controls not only put their sensitive data at risk, but also risk falling afoul of regulators. Simply put, cloud adoption isn't feasible for large enterprises unless security concerns are adequately addressed.

The solution: Thales' CipherTrust Transparent Encryption secures SAP HANA to make Google Cloud migration possible

CipherTrust Transparent Encryption (CTE) and CipherTrust Manager offer organizations encryption and policy based access controls to SAP HANA and prevent unauthorized cloud administrators, root users, and other privileged users from gaining access to data - whether SAP HANA is deployed on-premises or in Google Cloud. CTE secures data without requiring changes to the underlying database, application or hardware infrastructure. CipherTrust Manager provides customers with granular and configurable auditing and reporting of data access requests, and changes to policies and keys in order to meet governance requirements. Whether securing an existing SAP deployment, or upgrading to a new version, CTE delivers a proven approach that can scale to thousands of systems and files and quickly secure SAP data in Google Cloud while ensuring continued operation at optimal performance.

Why use CipherTrust Manager with SAP HANA database?

Inserted above the file system and/or logical volume layers, CTE is transparent to users, applications, databases, and storage subsystems. In short, it secures data without impacting a user's experience.

With CipherTrust Transparent Encryption, organizations can:

- Protect against privileged escalation by OS root users
- Minimize encryption impact on service level agreements and need for additional computer resources through use of a distributed agent-based deployment model
- Manage security and encryption policies, as well as, aggregate logging and reporting from a central location
- Mitigates the risks of increasingly sophisticated advanced persistent threats

Ensure Control of Your Data in the Google Cloud

Organizations that use CTE to provide their own encryption to secure SAP HANA ensure that they are solely in control of their sensitive data. CTE agents secure SAP HANA files in conjunction with CipherTrust Manager which stores encryption keys in a physically and logically separate location. Customers deploy CipherTrust Manager in a location they control to ensure that the Cloud Service Provider will never have access to both encrypted data and their corresponding keys at the same time. Such separation allows organizations to adopt the Google Cloud while both staying compliant with their regulatory obligations and protected from the risk that the service provider will turn over their data in the event they are served with a lawful subpoena.

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.

SAP

As a market leader, SAP develops enterprise software to manage business operations and customer relations. SAP is at the center of today's business and technology revolution with innovations that help over 350,000 customers worldwide to work more efficiently and use business insight more effectively. For more detailed technical specifications, please visit www.cpl.thalesgroup.com or www.saphana.com

> cpl.thalesgroup.com <

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