cpl.thalesgroup.com

THALES
Building a future we can all trust

Global Energy Leader Secures High Value Data in the Cloud with Thales CipherTrust Platform

The Business Challenge

A highly regulated global energy company with operations in multiple countries needed to protect high-value data across multiple platforms. The organization was concurrently migrating most of its data centers to the cloud. The company had hundreds of Microsoft Azure subscriptions, and each used several key vaults, increasing the complexity for managing keys. The customer wanted a vendor-agnostic solution able to centrally manage and store keys on premises for multi-cloud deployments leveraging the bring your own key (BYOK) model.

Moreover, the global energy leader wanted the highest level of security for its most sensitive "Tier 1" data to protect against not only external attacks, but also insider privilege abuse and have the ability to comfortably comply with government subpoenas. The IT department also needed to ensure no downtime when encrypting sensitive production data.

The Solution

In order to manage encryption keys from a single pane of glass across all its Azure subscriptions, the energy company deployed Ciphertrust Cloud Key Manager (CCKM). In addition, they deployed CipherTrust Transparent Encryption to protect a wide variety of file formats and data stores, and Live Data Transformation to protect production data and perform key rotation with minimum possible downtime.

CipherTrust Cloud Key Manager

CipherTrust Cloud Key Manager (CCKM) provides the global energy company with simplified management and control over BYOK keys managed on-premises with FIPS 140-2 Level 3 certified Hardware Security Modules guaranteeing high entropy key generation and secure key storage.

Specially designed to reduce the complexity of managing cryptographic keys in multi-cloud environments, CipherTrust Cloud Key Manager enables centralized key management and gives users complete control of the encryption keys used by their Cloud Service Providers (CSPs).

Offering seamless support for the BYOK APIs provided by CSPs, CipherTrust Cloud Key Manager automates key lifecycle management, enables key generation, usage logging and reporting, and facilitates 'keys decoupling' by securely storing the keys separately from the encrypted data. These features provide stronger controls over encryption key lifecycles for the data encrypted by the CSPs than native encryption.

With on-premises hosting of CipherTrust Cloud Key Manager, the energy company gained full ownership of its encryption keys resulting in complete visibility into how its encryption keys were created, used, and managed in the cloud.

CipherTrust Transparent Encryption

CipherTrust Transparent Encryption includes granular controls that allow only authorized users and processes to decrypt specified data when needed, while keeping all sensitive data encrypted whether the data is on-premises or in the cloud.

CipherTrust Transparent Encryption delivers data-at-rest encryption, privileged user access controls, and detailed data access audit logging. Agents protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers in cloud and big data environments.

The CipherTrust Transparent Encryption feature Live Data Transformation enables minimal downtime encryption deployments, by encrypting and re-keying data without taking applications offline. Live Data Transformation allows deployment of encryption while respecting business continuity and high availability.

CipherTrust Transparent Encryption ultimately delivers the highest level of security in the cloud, called "Bring Your Own Encryption or BYOE." BYOE protects customers not only against external threats, but also against internal threats such as privileged account abuse and even subpoena of a cloud service provider for a customer's data.

The Results

- Addressed global and regional regulatory requirements, mandates and standards including Federal Energy Regulatory Commission (FERC) and General Data Protection Regulation (GDPR).
- Achieved complete visibility and control over key management across multiple cloud subscriptions used by several business units and subsidiaries.
- Automated key lifecycle management, simplifying generation, rotation, backup, and revocation of millions of keys.
- Ensured developer-friendly environment with REST APIs allowing new applications to easily tap into CCKM for key management.
- Achieved protection in the cloud against external and internal threats, and CSP subpoena with BYOE platform for multiple cloud instances.
- Enabled the dynamic protection of live data without moving databases offline for critical systems with large and essential datasets such as SAP Hana -- both on premises and in the cloud.

CipherTrust Cloud Key Manager together with CipherTrust Transparent Encryption with Live Data Transformation provided a secure path to cloud migration with minimum disruption for even the most sensitive data for this global energy provider.

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.

© Thales - April 2022 • RMv3