cpl.thalesgroup.com

THALES
Building a future we can all trust

Banking and Finance Sector
Cloud Security & Key Management Challenges

The move to the cloud has had a profound effect on all industries, and the Financial sector is no exception. Financial companies want to leverage the benefits of the cloud but security concerns and issues around data sovereignty are providing barriers and confusion. Sensitive internal and client data previously managed by in-house resources will now be handed over to a third party, which raises a host of new questions - What controls do they put in place? What if there's a data breach by a rogue administrator? Can they uphold confidentiality commitments? Will the cloud provider be compelled to divulge client data as a result of a government request? How can encrypted data be moved between cloud providers?

How can Banks and Financial Institutions retain control of their client data in the cloud?

By correctly deploying a centralised key management and encryption technologies, which provides an easy to deploy Bring Your Own Key (BYOK) when Cloud's Native encryption is turned on, Bring Your Own Encryption (BYOE) or Hold Your Own Key (HYOK); you can retain control of your keys and therefore the data it protects. This ensures you have sovereignty and exclusive control over the data.

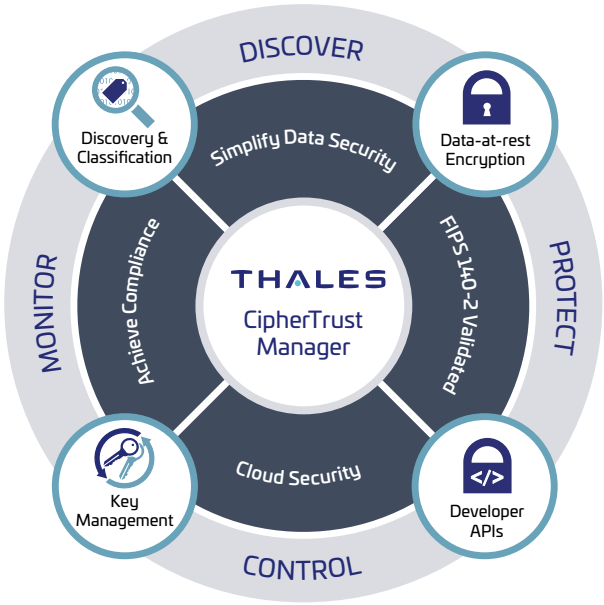
How Thales helps the Banking and Finance sector use these technologies to move to the cloud:

The Need for Customer Key Control

The requirement to protect sensitive data across Infrastructure, Platform, and Software-as-a-Service (IaaS, PaaS, and SaaS) has resulted in broader cloud provider encryption offerings. Meanwhile the Cloud Security Alliance and industry analysts state that cloud encryption keys should be managed by the data owners. The challenges of holding keys grow with up to hundreds of master keys per subscription to be secured and managed across multiple clouds. There is also the imperative of knowing how, when, and by whom encryption keys are used. CipherTrust Cloud Key Manager provides comprehensive key lifecycle management to fulfill requirements for safe, comprehensive key management across multiple clouds.

Supported clouds include:

- Microsoft Azure
- AWS GovCloud
- Microsoft Azure GovCloud
- Microsoft Azure China
- Microsoft Azure Germany
- Google Cloud
- Amazon Web Services
- Microsoft Azure Stack
- AWS China
- IBM Cloud
- Salesforce.com
- Salesforce Sandbox



Delivering Enhanced IT Efficiency

CipherTrust Cloud Key Manager offers multiple capabilities in support of enhanced IT efficiency:

- Centralised cloud key management provides access to each cloud provider from a single browser window, including across multiple accounts or subscriptions
- Full management of native cloud keys enables multicloud key management even without BYOK.
- Automated synchronisation ensures that cloud console-specific key operations are reflected in centralised key management
- Automated key rotation including support for expiring keys can ensure compliance while saving up to thousands of valuable hours per year
- With cloud providers using varying key technologies and terminology, CipherTrust Cloud Key Manager presents key operations in the semantics of the cloud provider, saving time and training

Strong Encryption Key Security

Customer key control presents requirements for secure key generation and storage. CipherTrust Cloud Key Manager leverages the security of the CipherTrust Manager and Luna Network HSM, to create keys with up to FIPS 140-2 Level 3 security. Key source compatibility with clouds and cloud keys varies. Please see the CipherTrust Data Security Platform Data Sheet for details.

The Compliance Tools You Need

CipherTrust Cloud Key Manager Logs and prepackaged reports enable fast compliance reporting. Logs may also be directed to a syslog server or SIEM.

Flexible deployment options

CipherTrust Cloud Key Manager is available in multiple form factors to meet any organisation's needs. Both CipherTrust Cloud Key Manager and its key sources are available in all-software, cloud-friendly offerings and may be found in several cloud provider marketplaces for fast instantiation. Further, deployment in any cloud is wholly separated from cloud provider access, and, keys can be managed in the cloud in which the solution is deployed as well as any other reachable, supported cloud. For example:

- A key source may be on-premises for compliance
- A CipherTrust Cloud Key Manager instance may be deployed in Amazon Web Services or any other cloud supported for deployment
- From where it is deployed it can manage keys in AWS, Salesforce or Azure or other supported clouds

Many other deployment architectures are available.

Multi-cloud data security solutions

CipherTrust Cloud Key Manager simplifies the need to hold and manage encryption keys for cloud services, a critical solution for fulfilling industry and organisational data protection mandates.

Additional Thales multi-cloud security products, including Bring Your Own Advanced Encryption, all with centralised key management, enable you to encrypt and control cloud storage to reduce the chance of your sensitive data being leaked.

Thales CipherTrust Transparent Encryption solution

In addition to the cloud key management; part of the CipherTrust Data Security Platform, also offers encryption of data at rest using file-system level encryption. This combined with centralised key management, access control and policy enforcement, audit and reporting; provides Insurance companies with a full comprehensive Data Security Platform and is endorsed by the major cloud providers.

Why you should care?

By implementing CipherTrust Data Security Platform, Insurance companies can:

- Prevent data breaches which can result in fines and reputational damage
- Provide assurance to clients and ensure their compliance to regulatory requirements
- Retain exclusive control and sovereignty of data
- Ensure compliance to recognised security standards e.g. ISO 27001 /FIPS 140-2 / GDPR
- Provide an encryption platform which is neutral and independent of the cloud provider

Thales encryption technology has been trusted to secure some of the world's most sensitive data for more than 40 years. Organisations such as Insurance, Banks, Government, Military / Law Enforcement, Healthcare, Retail, Manufacturing and more trust Thales to help them secure their mission-critical information, wherever it is created, shared or stored.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organisations 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