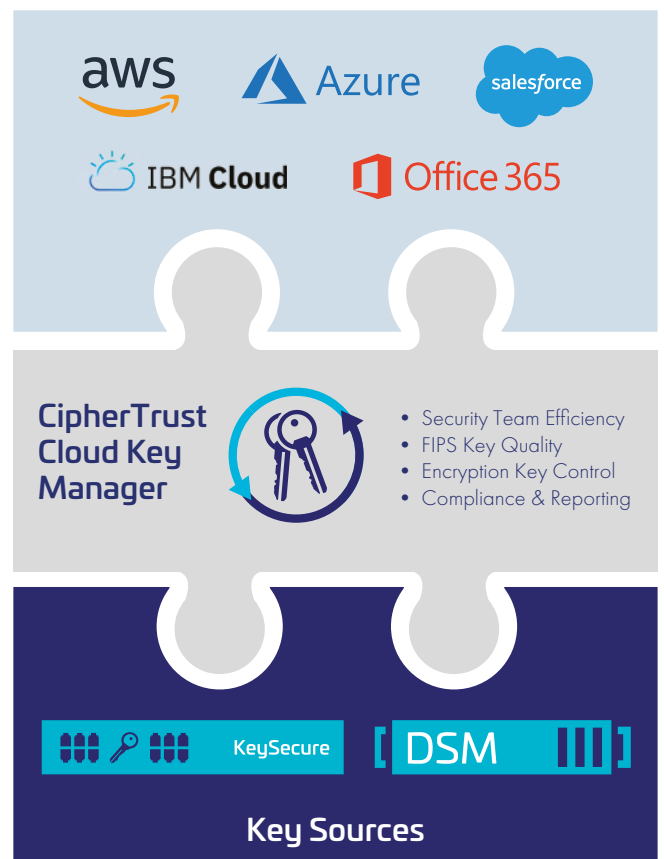**THALES**

CipherTrust Cloud Key Manager

Many infrastructure-, platform-, and software-as-a-service providers offer data-at-rest encryption capabilities with encryption keys managed by the service provider. Meanwhile, many industry or internal data protection mandates, as well as industry best practices as defined by the Cloud Security Alliance, require that keys be stored and managed remote from the cloud service provider and the associated encryption operations. Providers can fulfill these requirements by offering "Bring Your Own Key" (BYOK) services to enable customer control of the keys used to encrypt their data. Customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create them.

Leveraging cloud provider BYOK API's, the CipherTrust Cloud Key Manager reduces key management complexity and operational costs by giving customers lifecycle control of encryption keys with centralized management and visibility.

Take control of your cloud encryption keys

- Leverage the value of "Bring Your Own Key" services with full-lifecycle cloud encryption key management
- Gain higher IT efficiency with centralized key management across multiple cloud environments, automated key rotation and key expiration management
- Comply with the most stringent data protection mandates with up to FIPS 140–2 Level 3 validated key origination and storage

aws Azure salesforce
IBM Cloud Office 365

CipherTrust Cloud Key Manager

- Security Team Efficiency
- FIPS Key Quality
- Encryption Key Control
- Compliance & Reporting

KeySecure DSM

Key Sources

The key control imperative

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 encryption keys should be held by customers. 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. The 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
- Microsoft Office365
- Microsoft Azure Stack
- Microsoft Azure China and Germany National Clouds
- Amazon Web Services
- IBM Cloud
- Salesforce.com
- Salesforce Sandbox

Enhanced IT efficiency

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

- Centralized Key Management gives you access to each cloud provider from a single browser window, including across multiple accounts or subscriptions
- Automated key rotation offers IT efficiency and enhanced data security
- Cloud service logins are authenticated and authorized by the service provider—no login database nor AD or LDAP configuration is required
- For workloads that require it, CipherTrust Cloud Key Manager can request creation of native cloud provider keys and provide full lifecycle management for them
- With varying key technologies and terminology, CipherTrust Cloud Key Manager presents key operations in the semantics of the cloud provider
- Already created thousands of keys at your cloud provider? CipherTrust Cloud Key Manager will synchronize its database with keys created at the cloud provider

Strong encryption key security

Customer key control presents requirements for secure key generation and storage. CipherTrust Cloud Key Manager leverages the security of the Vormetric Data Security Manager, Thales KeySecure, or supported hardware security modules (HSMs)

to create keys and store them with FIPS 140–2 security. With the requirement for key security mechanisms such as safe storage of cloud backup keys, CipherTrust Cloud Key Manager acts as a key escrow for supported clouds and allows for full key metadata control both during upload and for keys in use.

The compliance tools you need

CipherTrust Cloud Key Manager cloud-specific logs and prepackaged reports offer fast compliance reporting. Logs may also be directed to a syslog server or SIEM.

Implementation Choices that Match Your Needs

CipherTrust Cloud Key Manager offers several convenient implementation choices to meet your security and deployment needs:

- All-software is available with FIPS 140–2 Level 1-certified key security. The CipherTrust Cloud Key Manager Virtual Appliances and either the Data Security Manager or KeySecure virtual appliances can be instantiated in Amazon Web Services or Microsoft Azure, or deployed in any public- or private cloud leveraging VMware.
- Customers that require FIPS 140-2 Level 3 can deploy or utilize existing Data Security Manager or KeySecure appliances at that level as a key source for CipherTrust Cloud Key Manager. In addition, the FIPS 140-2 Level 3 certified Thales Luna Network HSM can be deployed as a root of trust for the virtual appliance key sources.

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

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.