ESG SHOWCASE

# The Thales CipherTrust Cloud Key Manager for Multi-cloud Environments

**Date:** July 2020 **Author:** Doug Cahill, Senior Analyst

**ABSTRACT:** The broad use of multiple cloud services, including software-as-a-services (SaaS) applications and infrastructure-as-a-service (IaaS) platforms, has become the new normal of corporate computing. Users are increasingly relying upon these cloud-delivered applications and cloud-resident workloads for business-critical purposes, resulting in sensitive data being stored across multiple public cloud environments and on-premises, resulting in both multi-clouds and hybrid clouds. As such, the same enterprise-class data security and compliance tools and processes employed to protect on-premises data to meet and maintain compliance with industry regulations must be applied to this hybrid and multi-cloud reality.

While many cloud services now offer native and third-party encryption options, including bring-your-own-key (BYOK) services, challenges remain, such as operationalizing encryption key lifecycle management centrally, across multiple cloud services. The CipherTrust Cloud Key Manager from Thales separates encrypted data from its encryption keys for organizations seeking the combination of compliance, enhanced security, and operational efficiency to protect data assets in a multi-cloud environment.

## Compliance and Operational Key Management Challenges for Cloud-resident Data

Today, multiple IT meta trends, including mobility and cloud adoption, are simultaneously and fundamentally changing how corporate data is stored, accessed, and secured, challenging perimeter-centric security models and complicating compliance with industry regulations. At the same time, the threat landscape continues to evolve with bad actors employing new attack vectors and methods and internal threats exercising new data exfiltration techniques. But one constant remains: Security should be applied as close to the data as possible, an especially relevant consideration for data stored by cloud services in physical locations into which the customer lacks visibility and control.

### Multi-cloud Adoption Increases Cloud Data Security Concerns

IT is evaluating many new projects through the lens of cloud-first initiatives, which is driving the wide adoption of cloud services. In fact, according to ESG research, 94% of IT professionals surveyed said that their organizations currently use public cloud services.[1] While the use of multiple SaaS applications has been commonplace for years, the use of services from multiple infrastructure-as-a-service providers has grown in popularity as well. In fact, 76% of the participants in research conducted by ESG who indicated they were using IaaS services reported consuming these services from two or more cloud infrastructure services providers.[2]

This broad consumption of cloud services has created an acute concern around storing sensitive data in one or more public clouds due to its strategic and, thus, intrinsic value to a company. As such, it is quite disconcerting that 53% of the

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey* , March 2019.

respondents who participated in another ESG study indicated that more than 30% of their organization's cloud-resident sensitive data is insufficiently secured.[3] In response, according to additional ESG research, both cloud security and data security are two of the most commonly selected areas of cybersecurity in which organizations expect to make significant investments in 2020 (see Figure 1).[4]

**Figure 1. Most Common Areas of Significant Investment Related to Cybersecurity in 2020**


*Source: Enterprise Strategy Group*

## Complicating Compliance

Many regulations are infrastructure-agnostic in that they require organizations to apply the same processes and controls independent of whether the data in scope is on-premises, in the cloud, or both. For example, PCI DSS requires dual control with respect to the separation of data and keys, as well as separation of duties in the form of role-based access to key management software. PCI DSS, along with GLBA/FFIEC and FISMA, requires the use of NIST-certified AES encryption and FIPS 140-2-compliant key management. Meeting and maintaining compliance with such industry regulations can be complicated by the prevalent use of cloud services. Furthermore, regional laws and regulations that govern data sovereignty and privacy, including the European Union's General Data Protection Regulation (GDPR), are increasingly relevant to conducting business internationally, typically requiring both access controls and custodianship of data and keys.

[3] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.
[4] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

### Cloudy Key Management and Custodianship

While many cloud service providers (CSPs) offer native encryption, that capability, in and of itself, does not address all use cases or compliance requirements. Co-located encryption keys provide access to encrypted data and raise questions and concerns over separation of duties, lack of dual controls between data and keys, and operational aspects of key management including key rotation, deactivation, and more. For these and many other reasons, industry best practices, such as those from the Cloud Security Alliance, simply state that encryption keys should be held remote from the cloud provider. If the CSP holds the keys, then the customer should be rightfully concerned about what happens in the case of a court serving the CSP a subpoena requiring access to the data. Key management and clarity on which party—the CSP or the customer—should be the custodian of the keys is an important factor for security professionals given prescribed guidelines and regulatory requirements.

## The Requirements for Multi-cloud Key Management

Given the general importance of key custodianship along with the clear acknowledgement of best practices that the CSPs themselves acknowledge and in some cases helped create, some CSPs address at least a subset of cloud encryption issues with bring-your-own-key (BYOK) services to give customers more control over their keys. The services are fine on a small scale and at one cloud provider at a time, but in multi-cloud environments, centralization across cloud services and additional capabilities are required.

### Coverage across Multiple Cloud Services

The ongoing shortage of cybersecurity skills and the need for the definition and application of consistent security policies and controls across disparate environments make support for multiple cloud services a central requirement for modern encryption key management solutions. While most organizations subscribe to dozens, and often hundreds, of cloud applications, those which store sensitive data, such as IaaS and PaaS-resident databases, AWS S3 buckets, customer relationship management (CRM) and office productivity SaaS applications, are the types of apps that are most relevant to those requirements.

### Separation of Data and Keys

Augmenting a BYOK service should allow organizations to implement the encryption best practice of separating the location of data from that of the encryption keys. This best practice of data and key separation is a compliance requirement for many industry regulations. However, such separation does not address the issue of custodianship, also a compliance requirement for some industry regulations.

### Deployment Flexibility for both Management Plane and Key Sources

Customer-managed does not necessarily mean custodianship. Cloud-delivered encryption services allow for customer-dedicated vaults in the form of a hardware security module (HSM), but the keys in that HSM still reside in the CSP's data center when in use. Organizations most sensitive to this fact are typically those subject to certain industry regulations that require them to be the physical custodians of their keys. Extending a CSP's BYOK capability should include the option of deploying the management server and key vault on-premises where the customer controls the creation, backup, and usage, and in contrast with HSM BYOK, key revocation and lifecycle management of CSP-delivered backup keys.

## Extending BYOK with Flexibility of the CipherTrust Cloud Key Manager for Multi-clouds

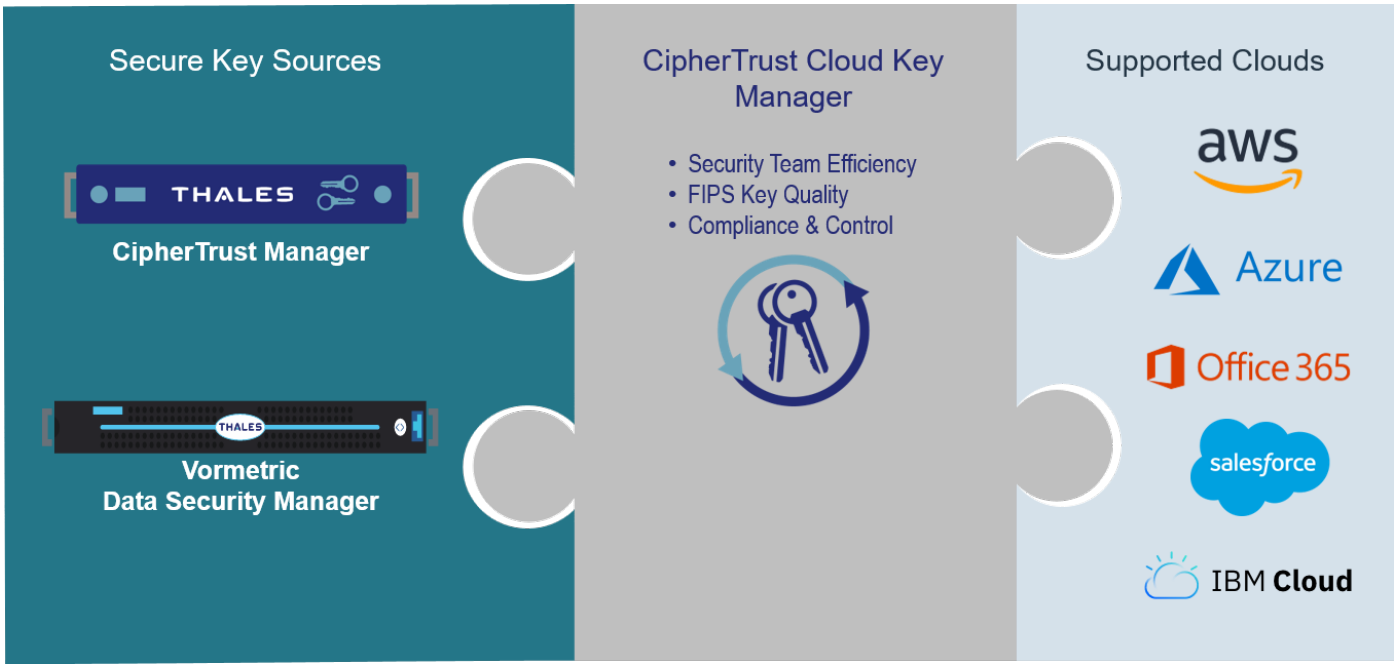
The CipherTrust Cloud Key Manager from Thales extends native BYOK offerings with full capabilities across multiple cloud services, and is offered in a range of flexible customer-management deployment modes.

### Support for Multiple Cloud Services

The CipherTrust Cloud Key Manager allows organizations to bring their own encryption keys and centrally manage the lifecycle of those keys across many of the most broadly used and business-critical cloud services (see Figure 2).

- Software-as-a-service (SaaS): The CipherTrust Cloud Key Manager supports Salesforce via integration with Salesforce Shield's BYOK service (including Salesforce Sandbox) as well as Microsoft's Office 365 office productivity suite.
- Infrastructure-as-a-service (IaaS): The CipherTrust Cloud Key Manager supports and extends the BYOK services of Amazon Web Services (AWS), Microsoft Azure, Azure Stack, and IBM Cloud.

**Figure 2. CipherTrust Cloud Key Manager for Multiple Cloud Services**




*Source: Thales*

### Flexible Control Plane and Key Store Deployment Options

CipherTrust Cloud Key Manager can be deployed on premises or in private cloud environments, or instantiated in public cloud environments as a shared Amazon Machine Image (AMI) or from the Azure or Azure Stack Marketplace. CipherTrust Cloud Key Manager also offers customers several choices for key sources including the CipherTrust Manager and the Vormetric Data Security Manager. CipherTrust Cloud Key Manager and its key sources offer easy-to-use graphical user interfaces to remove much of the complexity often associated with key management. The result is centralized key management across multiple cloud services that can simplify compliance and regulation audits for PCI DSS, FISMA, HIPAA, and GDPR.

These flexible deployment options represent a notable consideration for organizations evaluating key management solutions for cloud-resident data: Some customers can opt for the efficiencies of a full or partial cloud deployment; others

can choose the on-premises option when custodianship of the keys is a requirement for internal security policies or compliance considerations. All options are single-tenant, including cloud deployment, which keeps key control in the hands of the customer with the cloud service provider having no access to either the management plane or the key source/vault.

Irrespective of the deployment model, customers can take advantage of utility-based subscription licensing, if desired. Licensing flexibility includes subscription-based bundles for both the management plane and key vault, standalone subscriptions for CipherTrust Cloud Key Manager, and perpetually-licensed key sources.

### RBAC-based Key Lifecycle Management

The CipherTrust Cloud Key Manager provides a full set of key management functionality including: key creation, rotation, deactivation, and revocation. These management capabilities also include the ability to automatically sync key stores to facilitate migrating cloud-resident keys to customer-managed key store vaults. To ensure such key management activities are authorized, Thales integrates with federated login APIs to enable tenant secret management based on cloud provider, rather than local database, controls. In addition to key creation in its secure key sources, the product can provide full key management for cloud-native keys. Finally, CipherTrust Cloud Key Manager retains backup keys for services that enable restoration of keys erroneously deleted by cloud administrators.

## The Bigger Truth

The foundational concept in cloud security is the shared responsibility model that defines the demarcation line of the division of labor between the cloud service provider and the customer for securing and protecting the cloud service. For all types of cloud services, from infrastructure platforms to software-as-a-service, the model is clear: The customer is responsible for securing data that is stored in a public cloud. While CSPs offer some native controls, including the abilities to encrypt data, upload your own keys via a BYOK service, and store those keys in either a multi-tenant environment or dedicated HSM, the customer is responsible for both employing these services and managing the process. The use of multiple, discrete, native data encryption-related services increases management complexity while customers in certain industries also require the ability to store encryption keys on-premises to meet regulatory compliance requirements, which, together, create the requirement for efficiency and flexibility.

With the CipherTrust Cloud Key Manager, which supports multiple SaaS apps and IaaS platforms, Thales has delivered on operationalizing the management of encryption keys to efficiently and effectively protect data assets stored by critical cloud services that increasingly represent the core of modern IT environments. The combination of visibility into key origination usage and management, along with the optionality of cloud-delivered and on-premises deployment models, will help organizations satisfy auditors when it comes to meeting and maintaining compliance. By providing both a range of flexible deployment models and choices of key sources and licensing options, CipherTrust Cloud Key Manager allows organizations to leverage the agility of the cloud while effectively protecting cloud-resident data assets.



**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188