Trusted Cyber Technologies

THALES
Building a future we can all trust

Best Security Practices for milCloud Data Migration

In December 2022, the Defense Information Systems Agency (DISA) announced that it planned to cease the use of milCloud 2.0 cloud services on May 20, 2022[1]. This means that all milCloud 2.0 users will have to migrate their data to either a commercial cloud or another environment before the deadline. The impending deadline brings attention to the security implications associated with the use of commercial clouds by the Department of Defense (DoD).

Security is a Shared Responsibility

The Cloud Security Alliance emphasizes the importance of shared responsibility in its latest Security Guidance v4.0. Shared responsibility means that Cloud Solution Providers (CSPs) own the responsibility to secure the infrastructure that runs their cloud services. Data owners are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud.

Securing data in the cloud properly requires that data owners own—and can prove that they own—their data, from inception to deletion. That means that data owners—not their cloud provider—must protect their sensitive data by deploying a cloud security ecosystem where data and cryptographic keys are secured and managed, and access is controlled.

Cloud Security Best Practices

Defense agencies can ensure that their data is properly protected in commercial cloud environments by applying the following cloud security best practices.

- Data owners need to directly manage, if not own, their encryption to ensure that their data is protected as it is stored in and moves to and from the cloud.
- Data owners need to own the generation and administration of the cryptographic keys used to encrypt data in the cloud.
- Data owners need to ensure that only validated and authorized users can access sensitive data in the cloud.

Depending on the sensitivity level of the data stored in the cloud, agencies may choose to deploy either just a few or even all of the aforementioned best practices. However, managing data security across multiple clouds with different cloud storage options quickly gets complex. Therefore, data owners need cloud independent security solutions that can be applied across private, hybrid, public, and multi-cloud environments

Thales TCT Cloud Data Protection Solutions

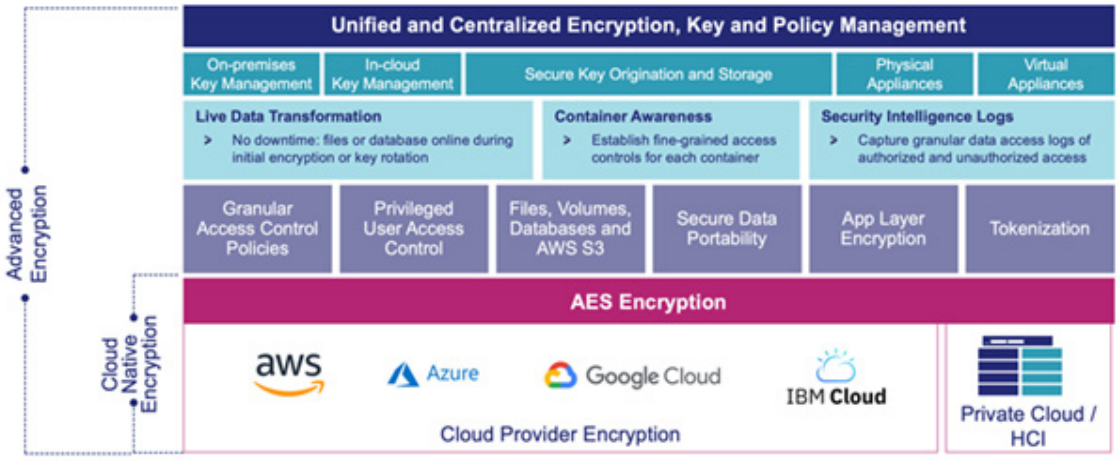
Thales Trusted Cyber Technologies (TCT), a U.S. provider of cybersecurity solutions dedicated to the U.S. Federal Government, offers cloud independent encryption and key management solutions that enable defense agencies to safely store sensitive data in the cloud. Our solutions allow users to effectively manage their security when working in different environments, across different platforms, and with multiple cloud providers. Our cloud data protection solutions can be deployed in public clouds including AWS, Azure, Google Cloud, and IBM Cloud as well as in private or hybrid cloud infrastructures.

[1] https://www.meritalk.com/articles/dod-plans-to-exit-milcloud-2-0-contract-by-may-2022/

Bring Your Own Encryption (BYOE)

For the highest level of data security in the cloud, users should deploy advanced BYOE tools in their cloud environments. Thales TCT offers advanced multi-cloud BYOE tools through **CipherTrust Data Security Platform** to secure data and rapidly reach compliance. Compared to the native encryption solutions available from cloud providers, Thales TCT BYOE through CipherTrust Data Security Platform delivers:

- High-performance AES encryption enhanced by hardware acceleration and granular access control policies, including privilege user access control. BYOE controls who, through what process and at specified times, can see specific data.
- An architecture that secures unstructured files, structured databases, and big data environments and also enables users to migrate data between cloud environments and on-premises servers without the time and cost of decryption.
- Easily add tokenization, or format preserving or traditional encryption to applications using RESTful APIs or the industry's most powerful and secure encryption libraries for additional granular controls and regulatory compliance.
- BYOE extensions enable use of data during encryption and rekeying operations with patented **Live Data Transformation** or, to isolate and secure container environments by creating policy-based encryption zones. BYOE monitors and logs file access to accelerate threat detection with Security Intelligence Log integration with popular SIEM tools.
- Simplified key management across on-premises and multi-cloud deployments by centralizing control on **CipherTrust Manager**.



Bring Your Own Key (BYOK)

For cloud deployments where security is less critical, agencies may choose to rely on a CSP's native encryption and deploy BYOK services. BYOK services enable users to separate key management from provider-controlled encryption, offering a crucial layer of separation of duties and control.

CipherTrust Cloud Key Manager from Thales TCT delivers key generation, separation of duties, reporting, and key lifecycle management that help fulfill internal and industry data protection mandates, with optional FIPS 140-2-certified secure key sources. 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.

CipherTrust Cloud Key Manager supports a growing list of IaaS, PaaS and SaaS providers. SaaS solutions include Microsoft Office365, Salesforce.com and Salesforce Sandbox. Supported IaaS/PaaS solutions include Amazon Web Services, AWS GovCloud, Microsoft Azure, Azure Stack, Azure GovCloud, IBM Cloud, Google Cloud Platform, and Google Workspace Client-side encryption, Salesforce.com, SalesForce Sandbox and SalesForce GovCloud Plus.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the field with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com