Trusted Cyber Technologies

THALES
Building a future we can all trust

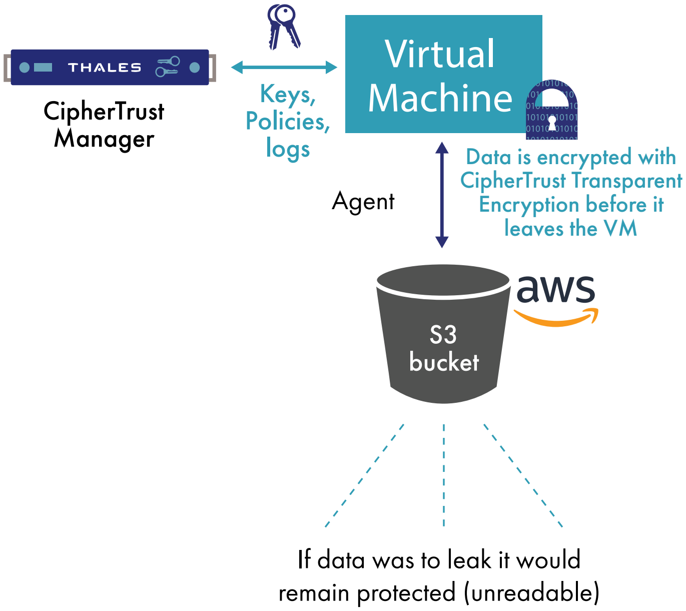
Advanced data protection for AWS S3 with CipherTrust Transparent Encryption

CHALLENGE: Avoid Data Breaches Caused by Misconfigured AWS S3 Security Settings

Amazon Web Services (AWS) Simple Storage Service (S3), one of the leading cloud storage solutions, is used by companies all over the world to power their IT operations for a variety of use-cases. AWS S3 buckets have become one of the most commonly used cloud storage repositories for everything from server logs to customer data. However, poorly configured S3 buckets have been the cause of a large number of data breaches. AWS does provide a range of security services and features that its customers can use to secure their assets, but ultimately the cloud service provider places responsibility for protecting the confidentiality, integrity, and availability of data in the cloud, and for meeting specific business requirements for information protection, in the hands of its customers.

SOLUTION: CipherTrust Transparent Encryption for AWS S3

To fully secure data in an untrusted and multi-tenant cloud environment, organizations must secure sensitive data and maintain complete governance and control of their data- and the associated encryption keys and policies. Thales simplifies securing AWS S3 objects and helps achieve compliance with data security regulations with the CTE for AWS S3 solution. CTE operates seamlessly on objects in AWS S3 delivering transparent and automated encryption of sensitive data stored in S3 buckets without any changes to applications, databases, infrastructure, or business practices.


THALES
CipherTrust Manager
Keys, Policies, logs
Virtual Machine
Agent
Data is encrypted with CipherTrust Transparent Encryption before it leaves the VM
S3 bucket
aws
If data was to leak it would remain protected (unreadable)

Highlights:

- Transparent encryption of data in the cloud. Provides transparent and automated encryption of sensitive data stored in AWS S3 buckets
- Customer-owned key security. Maintain control and ownership of encryption keys on-premises or in the cloud
- Fast deployment and implementation. Utilize automation tools for fast and easy deployment
- No re-architecting required. Minimal changes to your existing AWS environment are necessary

Benefits

CipherTrust Transparent Encryption for AWS S3:
Strengthens data security with operating-system-level controls against unauthorized access based on granular access policies, including user identity (for example for administrators with root privileges), and processes, among many others.

- New S3 bucket access controls to restrict access to only authorized hosts.
- Attackers will be denied access to protected buckets, even if the buckets are misconfigured and wide open.
- Accelerates breach detection and satisfies compliance mandates with detailed file access logs directed to your Security Information and Event Management (SIEM) system.
- Delivers a fast return on investment with a non-intrusive, flexible implementation. Encryption agents operate on Amazon EC2 compute instances and other servers accessing S3 buckets, Elastic Block Storage (EBS), and on-premises storage.

Features

- Transparent encryption and access control for data residing in S3 buckets.
- Privileged user access controls allow root users to do their job, without abusing data.
- Data access audit logging accelerates threat detection and eases forensics.
- Employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange.
- Simplified key management across on-premise and multi-cloud deployments by centralizing control on the FIPS 140-2-compliant CipherTrust Manager.

CipherTrust Manager

The CipherTrust Manager centralizes key, policy, and log management for CipherTrust Transparent Encryption. It is available in both virtual and physical form-factors for securely storing master keys with an elevated root of trust. These appliances can be deployed on-premises as well as in private or public cloud infrastructures. This allows organizations to address compliance requirements, regulatory mandates and industry best practices for data security

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com