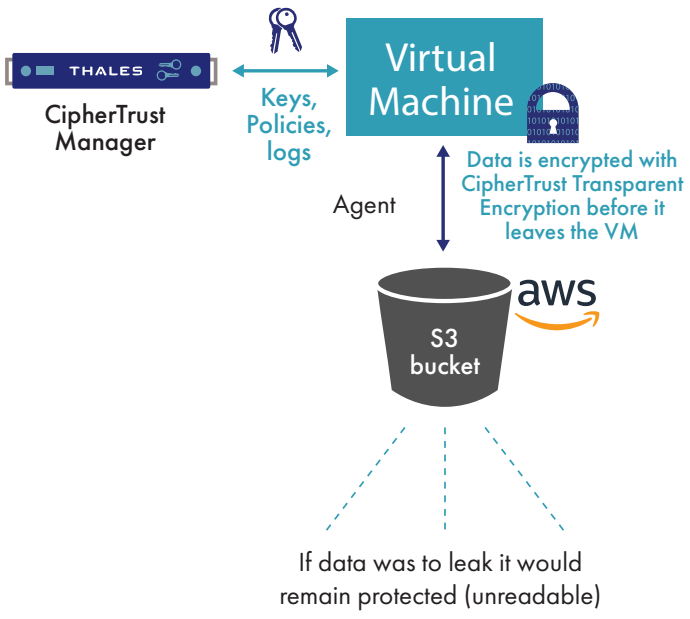
cpl.thalesgroup.com

THALES

Advanced data protection for Amazon S3 with CipherTrust Transparent Encryption

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

Amazon Simple Storage Service (S3), is one of the leading cloud storage solutions used by companies all over the world to power their IT operations for a variety of use-cases. Amazon 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. Amazon 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 Amazon S3

In a public 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 Amazon S3 objects and helps achieve compliance with data security regulations with CipherTrust Transparent Encryption. CipherTrust Transparent Encryption operates seamlessly on objects in Amazon S3 delivering transparent and automated encryption of sensitive data stored in S3 buckets without any changes to applications, databases, infrastructure, or business practices.

Highlights:

- **Transparent encryption of data in the cloud.** Provides transparent encryption of sensitive data stored in Amazon S3 buckets.
- **Customer-owned key security.** Maintain control and ownership of encryption keys on-premises or in the cloud with a FIPS 140-2 compliant solution.
- **Fast deployment and implementation.** Easy to deploy agents run on Amazon EC2 and on-premises servers with no need to change applications or database schema.
- **Segregation of duties.** Add granular access management and privileged user access controls controlled by the security team.

Benefits

CipherTrust Transparent Encryption for Amazon S3. Strengthens data security with 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.
- Simplifies key management across on-premises 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

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us