cpl.thalesgroup.com

THALES

# Security and Compliance for MinIO Cloud-Native Object Storage

## Thales CipherTrust Manager for MinIO Encryption

## The Problem: Sensitive Data Needs Protection

Simple Storage Service (S3) is used by companies all over the world to power their IT operations to store everything from server logs to customer data. In general, data breaches have been steadily increasing year-over-year with breaches becoming more severe in the process. Misconfigured S3 buckets have been behind a significant number of data breaches. Organizations risk exposing themselves to fraud and data breaches when they implement insufficient security controls.

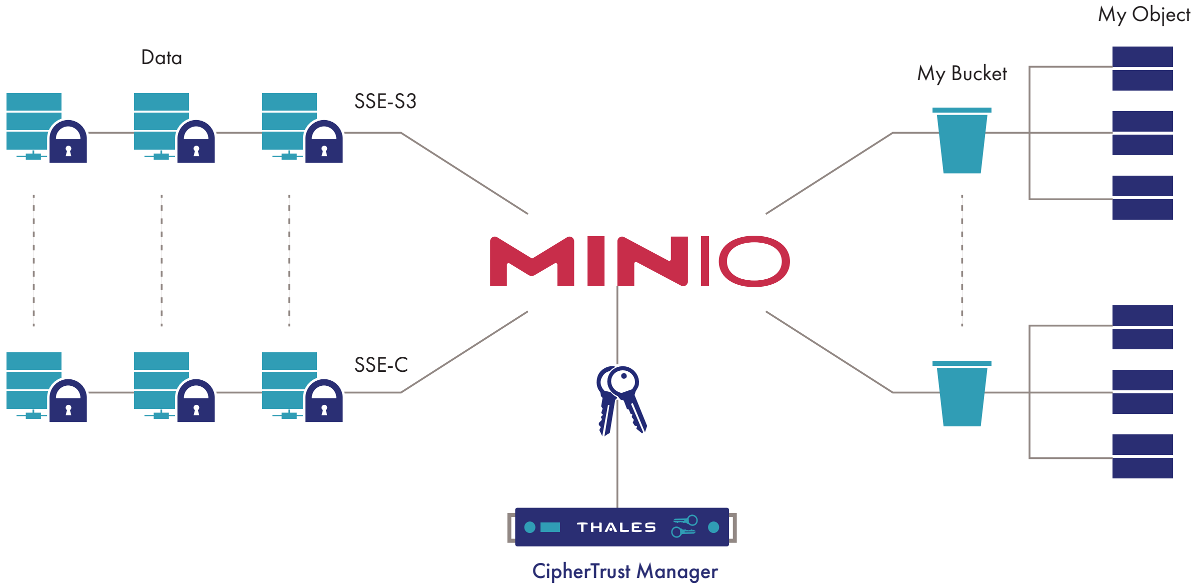
With sensitive data consolidated and stored in S3, object storage becomes a highly attractive target to those seeking to steal or compromise the data. S3 stored data can vary widely and include sensitive, regulated resources, like customer payment data, patient records and intellectual property. Amid all of these operational and security considerations, organizations must also consider their compliance obligations many of which detail how data must be kept secured from unauthorized users.

Fortunately, MinIO and Thales work together to solve these security and compliance concerns.

## The Solution

MinIO is an open-source, software-defined, distributed object storage system for industry standard hardware that was designed to be the standard in private cloud object storage. As a cloud-native solution that is simultaneously performant, scalable and lightweight, MinIO addresses traditional use cases like secondary storage, disaster recovery and archiving while overcoming the private cloud challenges associated with machine learning, analytics and cloud-native application workloads. MinIO addresses data confidentiality, integrity and authenticity by supporting multiple sophisticated server-side encryption schemes with negligible performance overhead.

Thales' CipherTrust Key Management platform integrates with MinIO for external key management. The MinIO server encrypts each object using a unique object key which is protected by a master key stored and managed for its entire lifecycle within the CipherTrust Manager. Centralizing key storage and management improves security by making surveillance, rotation, and deletion easier. Access control features allow organizations to separate duties so that no single administrator is responsible for both data and the keys securing that data. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible when demonstrating regulatory compliance.



## Why Use CipherTrust Manager with MinIO S3 Encryption?

When customers use MinIO with CipherTrust Manager, they can securely adopt S3 object storage in their private cloud environments. Whether using S3 for backup storage or as the foundation for a big data implementation, MinIO and Thales combine to ensure that data remains secure and the organization compliant as sensitive data is stored in, and used from, these repositories. Organizations can use CipherTrust enterprise key management to incorporate MinIO encryption seamlessly into their larger encryption strategy. Through Thales' access controls and detailed audit logging, organizations can separate security and administrative platform duties, increase visibility of the data's security and mitigate privileged insider risk.

### Policy Management and Separation of Duties

With CipherTrust Manager, administrators can dictate which users and processes can access data in clear text through defined authentication and authorization policies.  Such controls offer organizations tighter governance of their sensitive data. Finely tuned policy-based access controls are an important layer of protection for organizations looking to comply with security mandates that require robust separation of duties between IT and security administrators.

### Logging, Auditing, and Reporting

CipherTrust Manager records detailed key and access information in centralized logs to simplify auditing and reporting access to data and encryption keys. Tracking this information from a centralized location gives organizations increased security around their data and the ability to readily demonstrate compliance with regulatory obligations.

### Streamlined, Simplified Encryption Administration

Vendor provided encryption can easily turn into a collection of security silos if not managed well. The CipherTrust Manager consolidates MinIO encryption keys into an easy to use management platform where organizations can manage them along with keys from a wide variety of encryption solutions including: the Thales Data Security Portfolio, self-encrypting drives, tape archives, Storage Area Networks, Cloud Service Provided encryption, and an ever growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

## 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.

## About MinIO

MinIO is a high performance, distributed object storage system. It is software-defined, and runs on standard hardware. Because MinIO is purpose-built to serve only objects, a single-layer architecture achieves all of the necessary functionality without compromise. The result is a cloud native object server that is simultaneously performant, scalable and lightweight.

For more detailed technical specifications, please visit https://cpl.thalesgroup.com/ or https://min.io/.