Encrypting your data

IBM® Cloud Object Storage provides several options to encrypt your data.

By default, all objects that are stored in IBM Cloud Object Storage are encrypted by using randomly generated keys and an all-or-nothing-transform (AONT).

While this default encryption model provides at-rest security, some workloads need full control over the data encryption keys used. You can manage your keys manually on a per-object basis by providing your own encryption keys - referred to as [Server-Side Encryption with Customer-Provided Keys (SSE-C)](https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-sse-c).

With Object Storage you also have a choice to use our integration capabilities with IBM Cloud® Key Management Services like IBM® Key Protect and Hyper Protect Crypto Services. Depending on the security requirements, you can decide whether to use IBM Key Protect or IBM Hyper Protect Crypto Services for your IBM Cloud Object Storage buckets.

[IBM® Key Protect for IBM Cloud™](https://cloud.ibm.com/docs/services/key-protect?topic=key-protect-about) helps you provision encrypted keys for apps across IBM Cloud® services. As you manage the lifecycle of your keys, you can benefit from knowing that your keys are secured by FIPS 140-2 Level 3 certified cloud-based hardware security modules (HSMs) that protect against the theft of information.

[Hyper Protect Crypto Services](https://cloud.ibm.com/docs/services/hs-crypto?topic=hs-crypto-overview) is a single-tenant, dedicated HSM that is controlled by you. The service is built on FIPS 140-2 Level 4-certified hardware, the highest offered by any cloud provider in the industry.

Refer to product documentation on [IBM® Key Protect for IBM Cloud™](https://cloud.ibm.com/docs/services/key-protect?topic=key-protect-about) and [Hyper Protect Crypto Services](https://cloud.ibm.com/docs/services/hs-crypto?topic=hs-crypto-overview) for a detailed overview of the two services.