# **Amazon S3 security**

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](https://aws.amazon.com/compliance/shared-responsibility-model/) describes this as security *of* the cloud and security *in* the cloud:

**Security of the cloud**

AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely.

# **Protecting data using encryption**

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption. You have the following options for protecting data at rest in Amazon S3:

* Server-Side Encryption – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.  
  To configure server-side encryption, see [Specifying server-side encryption with AWS KMS (SSE-KMS)](https://docs.aws.amazon.com/AmazonS3/latest/userguide/specifying-kms-encryption.html) or [Specifying Amazon S3 encryption](https://docs.aws.amazon.com/AmazonS3/latest/userguide/specifying-s3-encryption.html).
* Client-Side Encryption – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.