Customer-Managed KMS Keys

Last Modified on 11/28/2023 9:41 am EST

Overview

Customers who opt-in to use a Dedicated Environment or Database also have the option to manage their own KMS Key. This article breaks down what a KMS Key is, how to securely manage a KMS Key, what happens if a KMS Key is deleted or lost, and customer responsibilities.

Key Management Service (KMS) Key

A KMS Key is a cryptographic key that encrypts data in an Amazon Web Services (AWS) cloud environment. When used with a cryptographic algorithm, the key encrypts or decrypts data within a Dedicated Environment or Database, giving a user secured access to the data. KMS Keys are generated randomly to ensure that the contents of the key remain secure.

You must use an AWS account to create a KMS Key.

Managing a KMS Key

An internal management system is required to keep your KMS Key secure and to maintain your AWS account. Educating your employees on the importance of a KMS Key will also ensure that the key is not lost, deleted, or compromised.

Resolver® recommends that a company using KMS Keys have a knowledgeable, dedicated internal resource (employee) to manage the KMS Key and AWS account.

Lost or Deleted KMS Keys

If a KMS Key is lost or deleted, all data on a Dedicated Environment or Database is permanently lost. Resolver and its employees cannot reproduce a lost or deleted KMS Key and have no means of retrieving any data from a Dedicated Environment or Database.

Resolver and its employees are not responsible or liable for interruptions, data loss, or inability to access data caused by the Customer’s management of KMS Keys.

Customer Responsibility

Customers who agree to manage their own KMS Key are responsible for the following conditions:

- The Customer must follow Resolver’s technical processes and procedures for customer key management.
- The Customer must notify Resolver if Customer Keys are lost or compromised.