

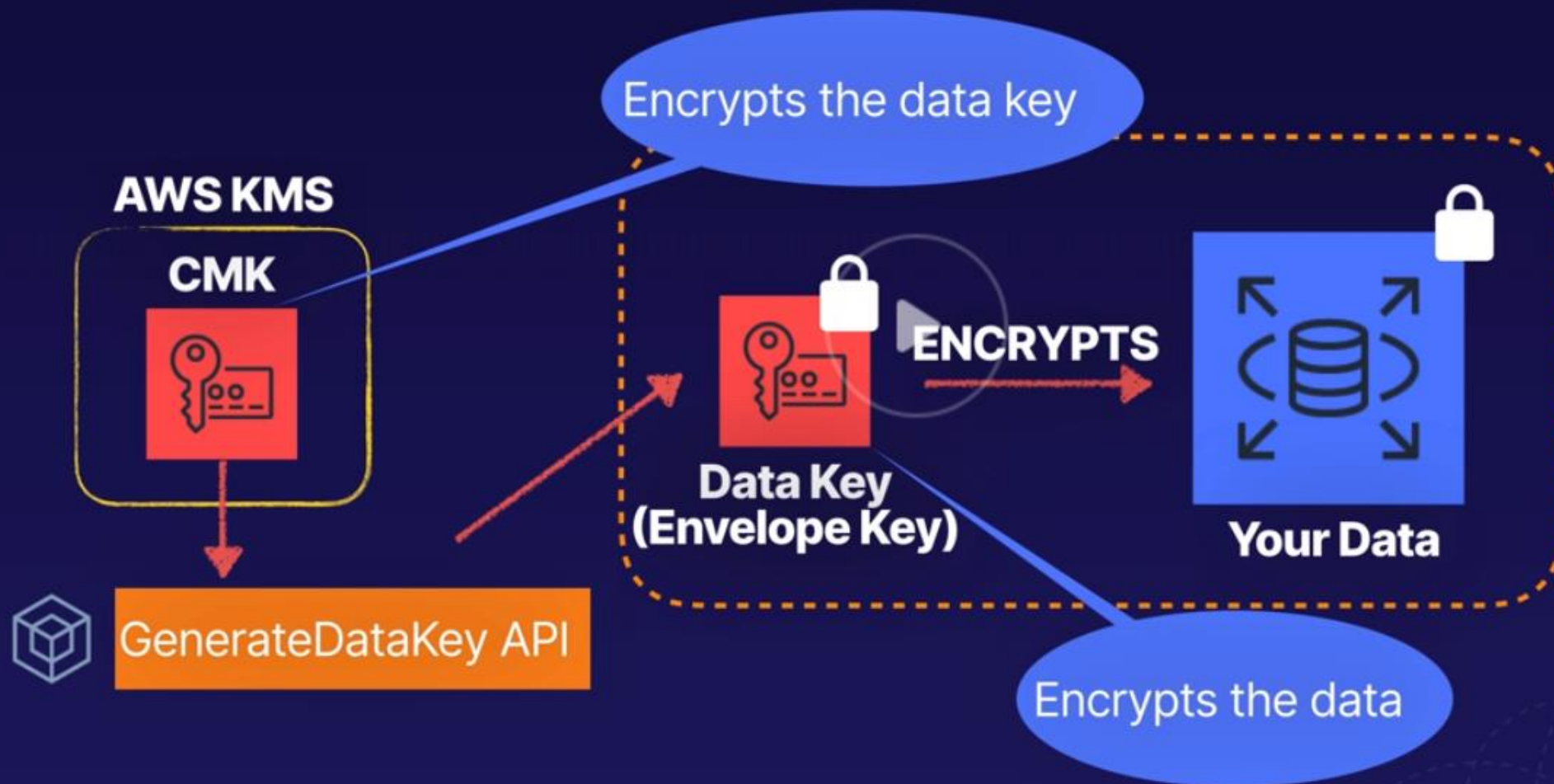
What Is Envelope Encryption?

A process for encrypting your data. It applies to files > 4 KB.



Envelope Encryption in Action

THE ENVELOPE ENCRYPTION PROCESS



THE KMS DECRYPTION PROCESS



At the end of the process, it
Deletes the plain text from the
memory

THE KMS DECRYPTION PROCESS



Why Envelope Encryption?

Why not encrypt the data using the CMK directly?



Network

When you encrypt data directly with KMS it must be transferred over the network.



Performance

With envelope encryption, only the data key goes over the network, not your data.



Benefits

The data key is used locally in your application or AWS service, avoiding the need to transfer large amounts of data to KMS.

Envelope Encryption

Encrypting the key that encrypts our data.

The CMK is used to encrypt the data key (or envelope key).

The data key encrypts our data.

Used for encrypting anything over 4 KB.

Using envelope encryption avoids sending all your data into KMS over the network.

Remember the `GenerateDataKey` API call.