

The background features a complex, abstract pattern of overlapping, translucent geometric shapes, primarily triangles and polygons, in various shades of blue and purple. These shapes create a sense of depth and movement, radiating from the right side of the frame towards the left.

AWS re:Inforce

JULY 26 – 27, 2022 | BOSTON, MA

DPP331

Best practices for cutting AWS KMS costs using Amazon S3 bucket keys

Aarti Parupudi

Technical Account Manager
AWS

Syed Shareef

Control Engineer
AWS



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Speaker bios

- Technical Account Manager
- Serverless expert and SQS SME
- AWS tenure – 4.5 years
- Harry Potter fan
- Love hiking, being in nature, and devouring books



Speaker bios

- A member of the AWS Control Tower team
- Security SME with a heavy financial services industry background
- At AWS for 3+ years in field teams
- Amateur woodworker, coffee snob, and gearhead



“I dislike saving money”

Nobody Ever

Data protection terms



Envelope encryption

The practice of encrypting plaintext data with a data key, then encrypting the data key under an AWS Key Management Service (AWS KMS) key



AWS KMS key (envelope key)

Protect data keys; uniquely identified by an ARN; sits at the top of your key hierarchy



Data key

Encryption keys that you can use to encrypt your plaintext data



Plaintext

Unencrypted information that you wish to protect, pending input into cryptographic algorithms



Ciphertext

Encrypted information unreadable by a human or computer without decryption

Enabling Amazon S3 default encryption

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

☐ Disable

☒ Enable

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

☐ Amazon S3 key (SSE-S3)

An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

☒ AWS Key Management Service key (SSE-KMS)

An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key

☐ AWS managed key (aws/s3)

arn:aws:kms:us-east-1:418866442500:alias/aws/s3

☒ Choose from your AWS KMS keys

☐ Enter AWS KMS key ARN

AWS KMS key

Choose AWS KMS key ▼

↻

Create key

Bucket Key

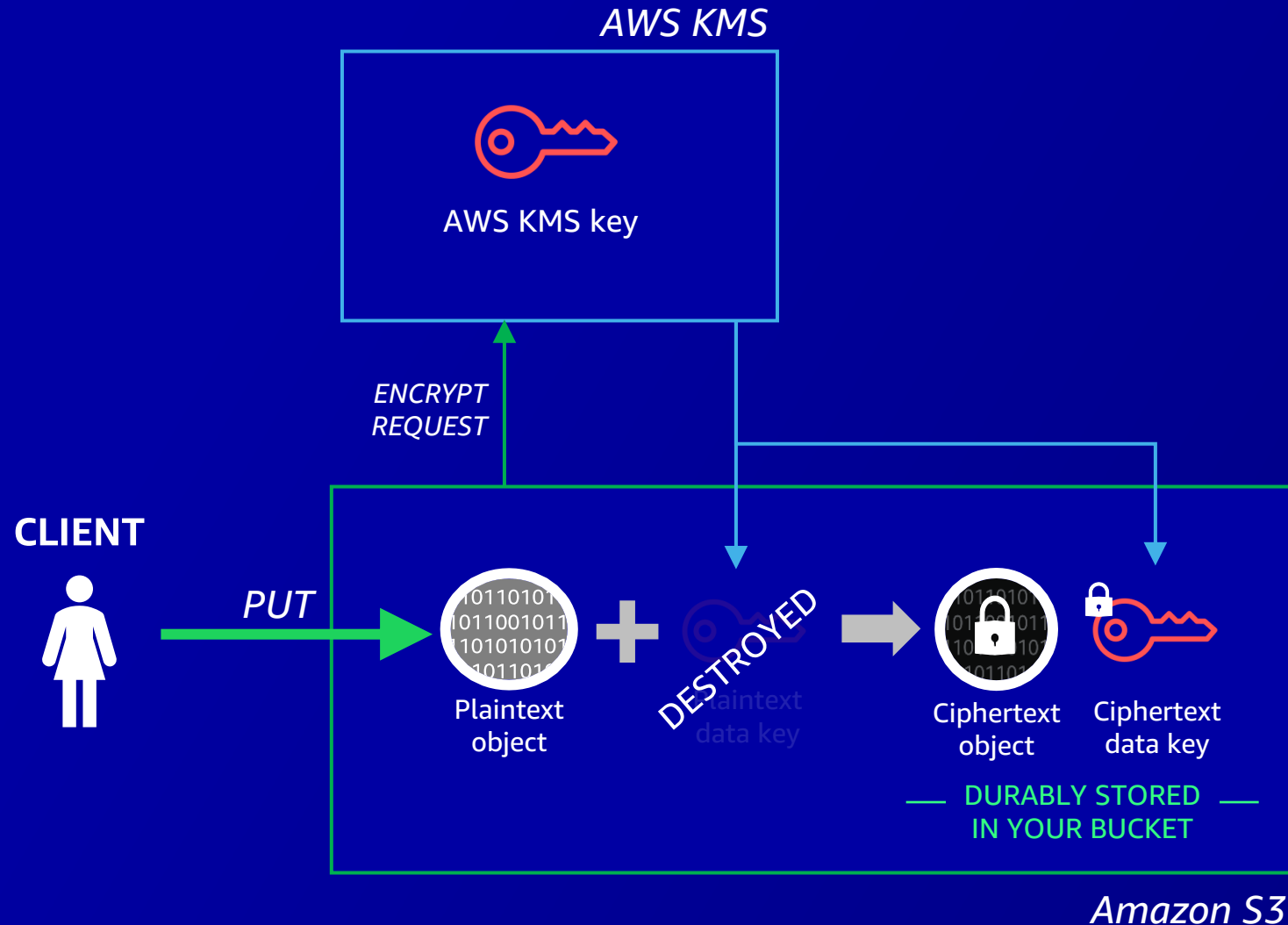
Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)

☐ Disable

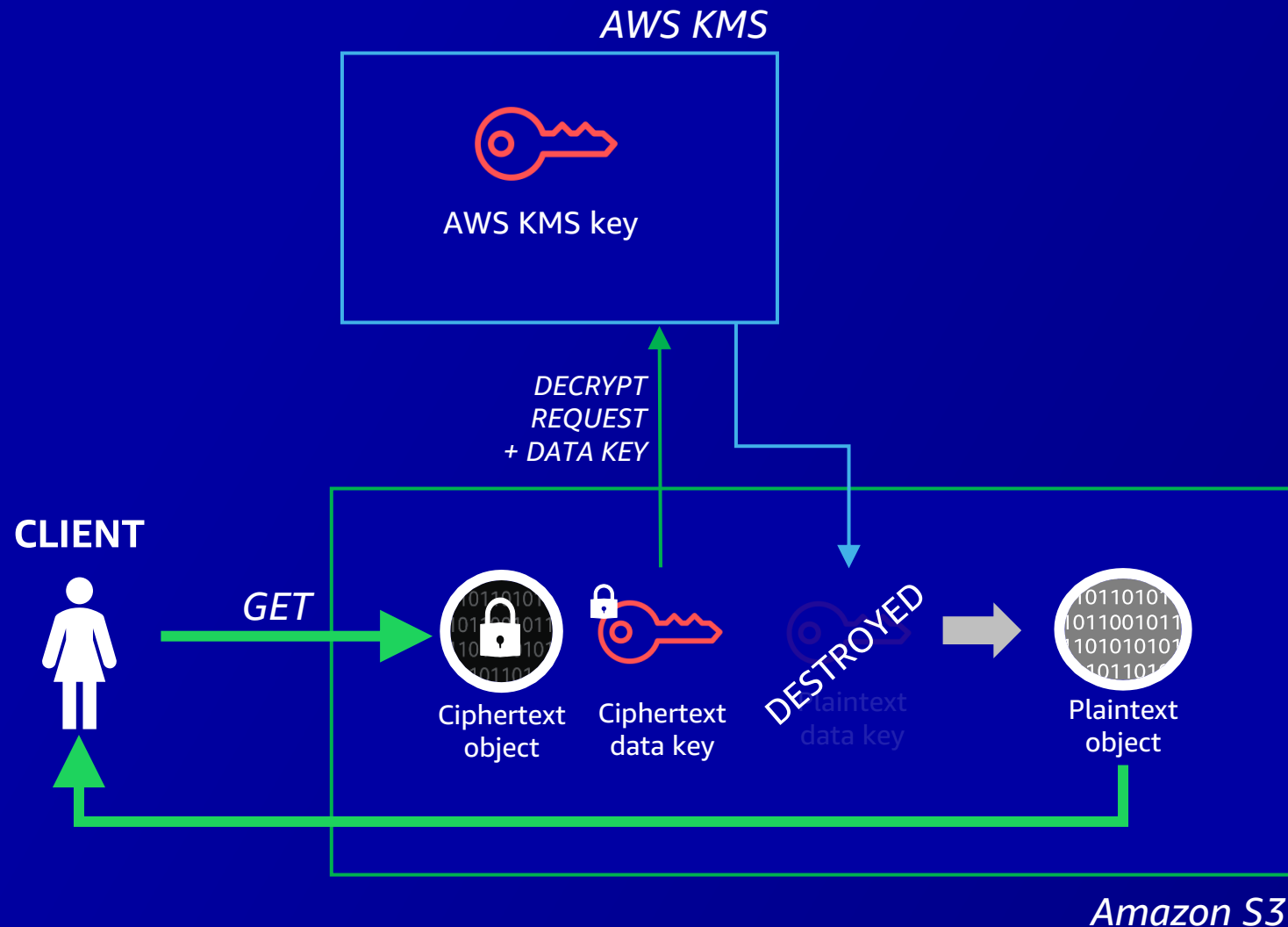
☒ Enable

- One-time bucket-level setup
- Specify key management strategy
- If AWS KMS, then specify a key
- Reduce AWS KMS costs with a bucket key

How an encrypt request works with AWS KMS



How a decrypt request works with AWS KMS



AWS KMS pricing – US East (Ohio)

Key storage

- \$1 per month, per AWS KMS key
- No charge for deleted keys or keys scheduled for deletion
- AWS-managed KMS keys are **free** to create and store

Key usage

Each API call to AWS KMS incurs a transaction cost (above **Free Tier**)

- **\$0.03** per 10,000 requests
- **\$0.03** per 10,000 requests involving **RSA 2048** keys
- **\$0.10** per 10,000 **ECC GenerateDataKeyPair** requests
- **\$0.15** per 10,000 **asymmetric requests except RSA 2048**
- **\$12.00** per 10,000 **RSA GenerateDataKeyPair** requests



AWS KMS pricing – Amazon S3 example

1 KMS key used to encrypt 10M unique files that are collectively decrypted for access 100M times per month

Monthly cost:

1 AWS KMS key - \$1

10M encrypt requests (1 request x 1M objects)

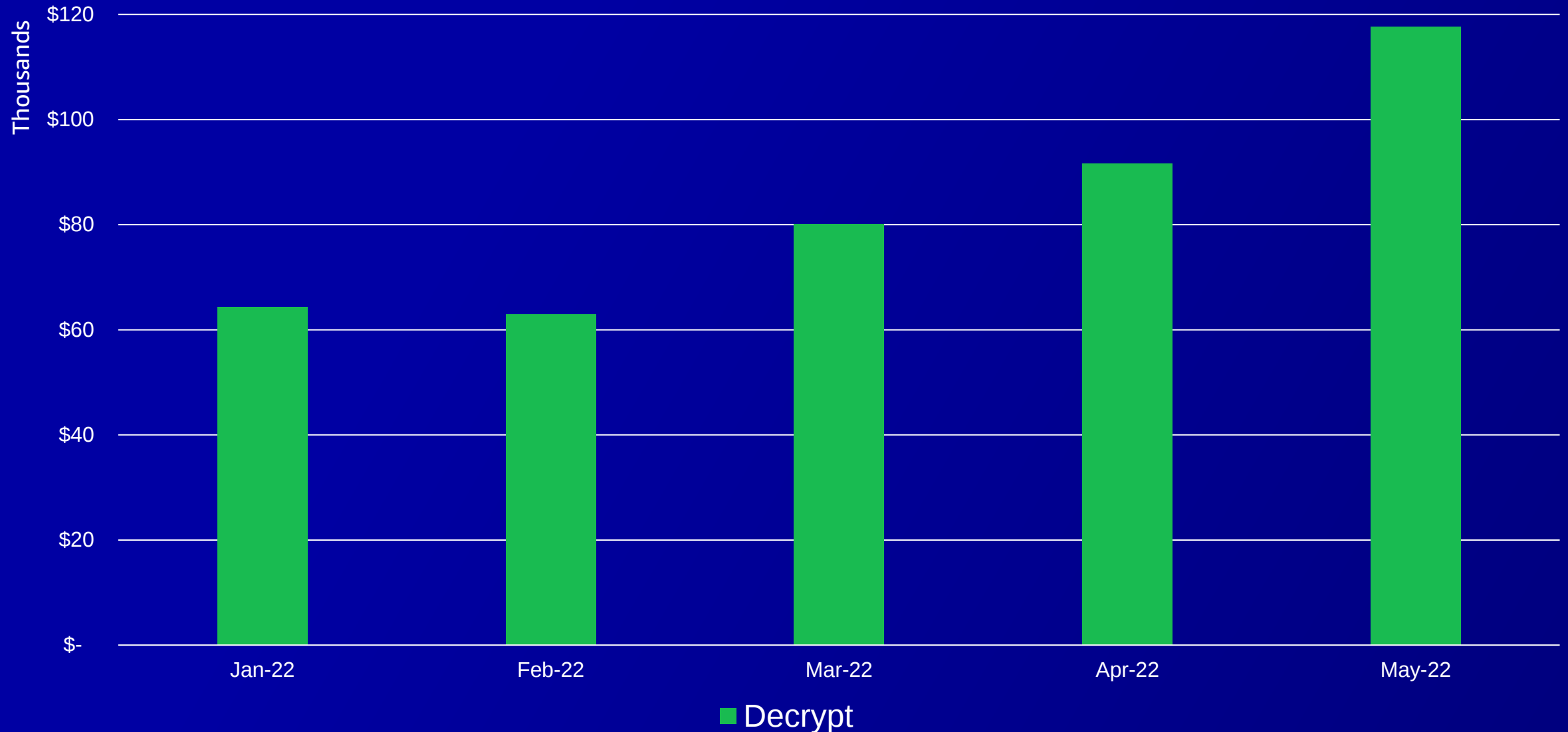
100M decrypt requests to access the objects

110M total requests - **\$331.94** (excluding free tier requests of 20K per month)

Free Tier – AWS Key Management Service provides a free tier of 20,000 requests/month calculated across all regions that the service is available



A real world scenario



Sample queries

List buckets with the highest number of AWS KMS calls

```
filter (eventName="GenerateDataKey"
or eventName="Decrypt" or
eventName="Encrypt") and
`requestParameters.encryptionContext.aws:s3:arn` like
`arn:aws:s3:::/
|parse
`requestParameters.encryptionContext.aws:s3:arn` 'arn:aws:s3:::*/' as
s3bucket
|stats count(*) by s3bucket
|sort by `count(*)` desc
```

s3bucket	# of AWS KMS Calls
s3-kms-test-2	20M
s3-kms-test	10M
s3-kms-test-4	7M
s3-kms-test-1	6M
s3-kms-test-3	2M

List S3 objects with the highest number of AWS KMS calls

```
SELECT
count(*) as Count,
json_extract(requestparameters, '$.encryptionContext["aws:s3:arn"]') AS [s3
Object], eventname AS [Event Name]
FROM
<Athena CloudTrail table>
WHERE
eventsource = 'kms.amazonaws.com'
AND
json_extract(requestparameters, '$.encryptionContext["aws:s3:arn"]' is not
null)
AND
eventtime > '1776-07-04T00:00:00Z'

GROUP BY
json_extract(requestparameters, '$.encryptionContext["aws:s3:arn"]'),
eventname

ORDER BY cnt DESC
```



Output

Count	Amazon S3 object	Event name
8M	"arn:aws:s3::s3-kms-test-1/File5.rtf"	Decrypt
4M	"arn:aws:s3::s3-kms-test/File2.rtf"	Decrypt
2M	"arn:aws:s3::s3-kms-test/File6.rtf"	GenerateDataKey
2M	"arn:aws:s3::s3-kms-test/File3.rtf"	GenerateDataKey

.....



Count of AWS KMS calls incurred by Amazon S3

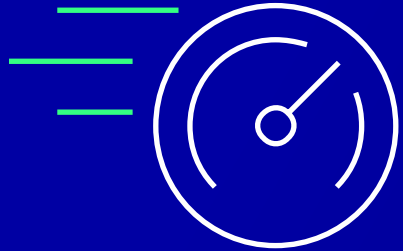
```
SELECT
count(*) as cnt
FROM
<Athena CloudTrail table>
WHERE
eventsource = 'kms.amazonaws.com'
AND
eventname = 'Decrypt'
AND
json_extract(requestparameters,
'$ .encryptionContext["aws:s3:arn"]') is not null
AND
eventtime > '2022-06-01T00:00:00Z'
```

#	cnt
1	91M

Amazon S3 bucket keys



Amazon S3 bucket keys



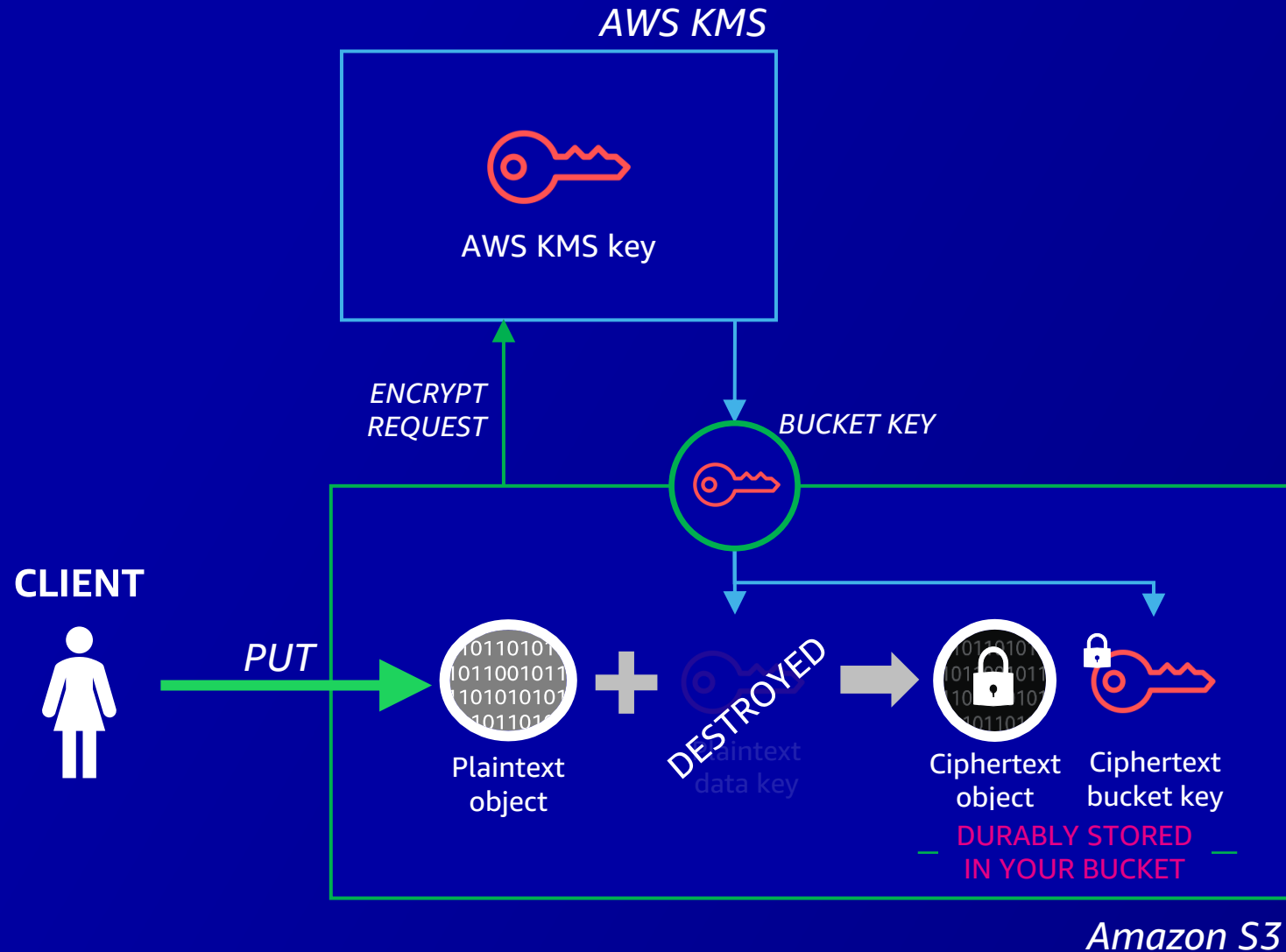
Increase
performance
for encryption



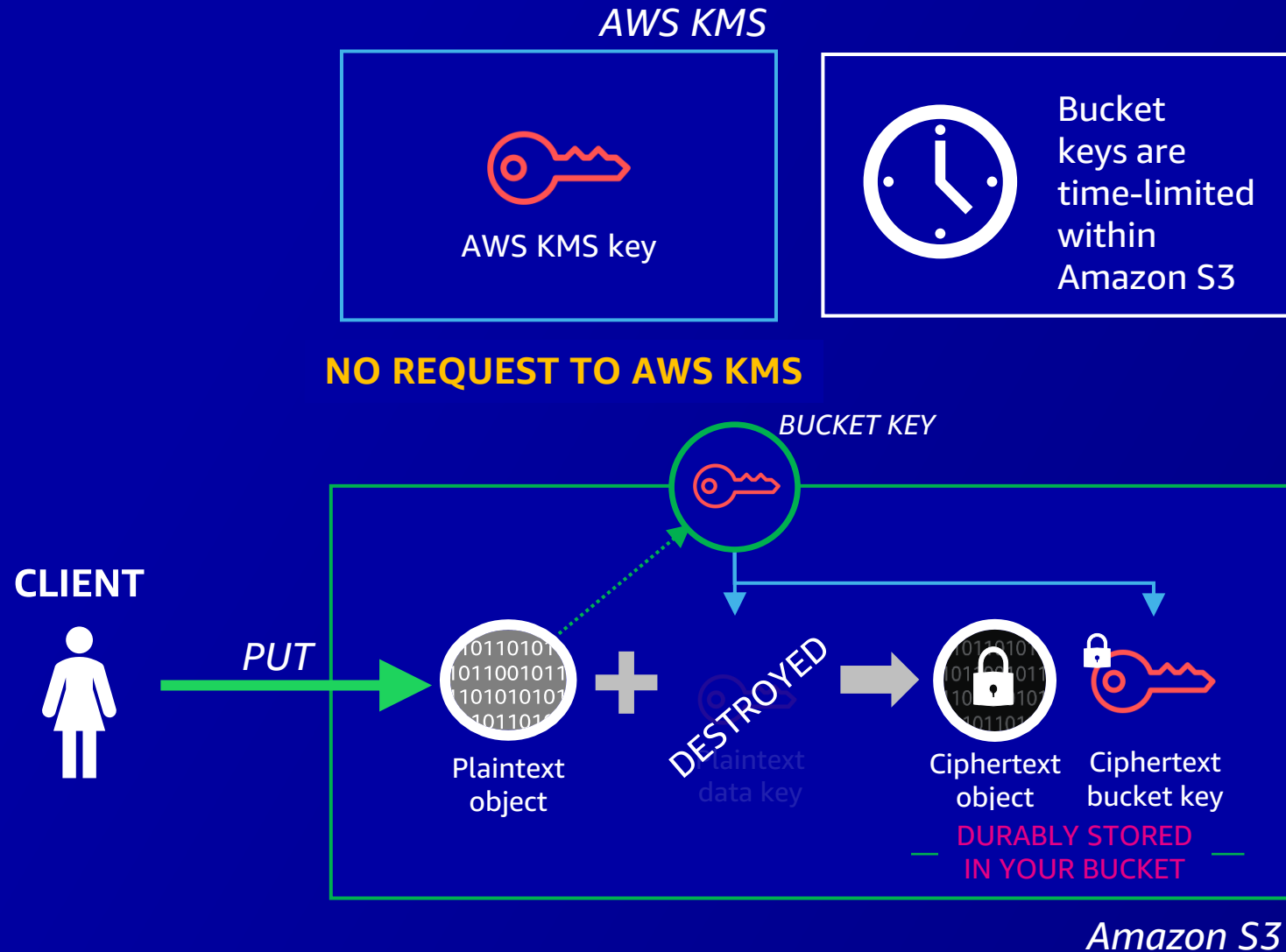
Reduce request costs for
AWS KMS-backed
server-side encryption by

up to 99%

How Amazon S3 bucket keys work (1st request)



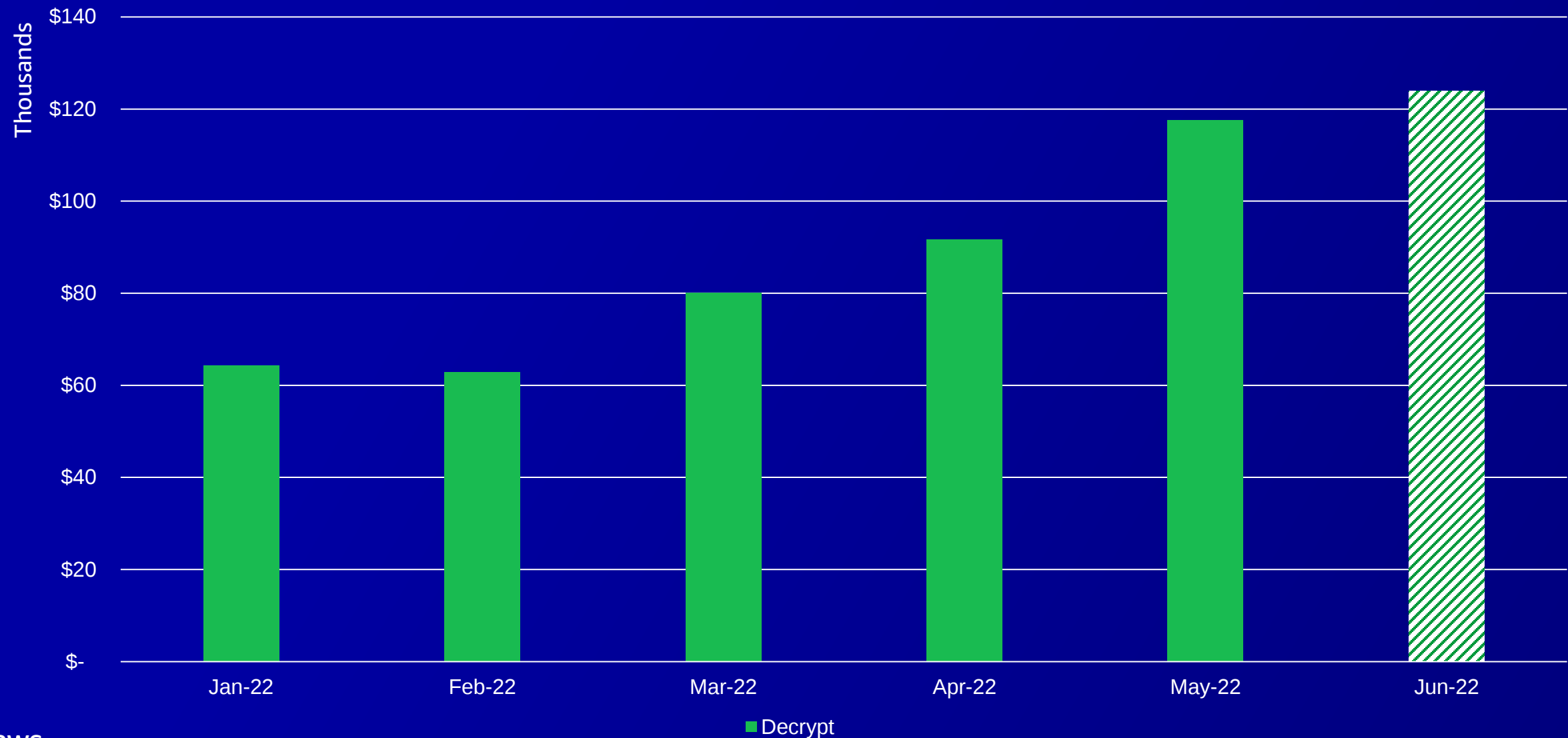
How Amazon S3 bucket keys work (N^{th} request)



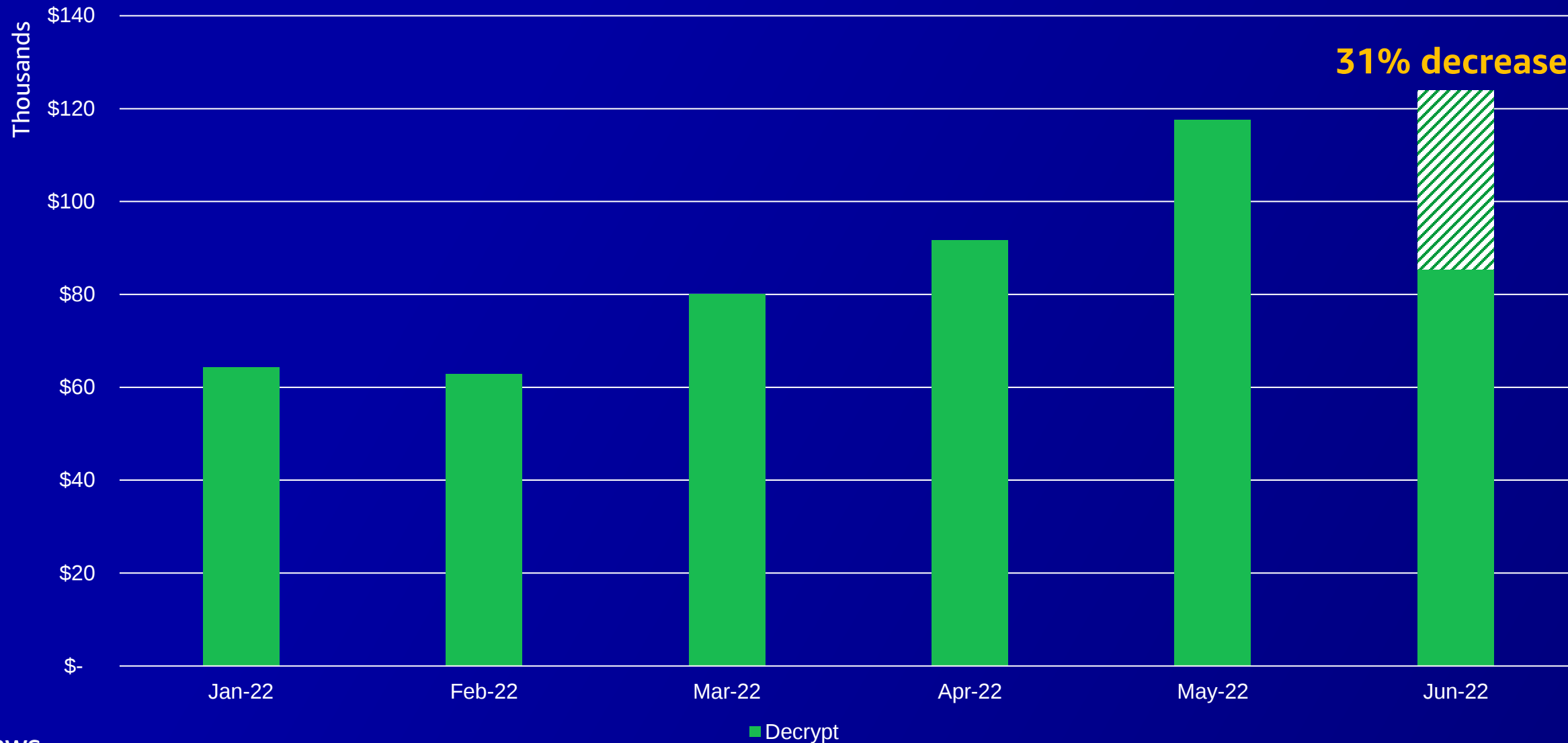
The results



Forecasted value – Status quo



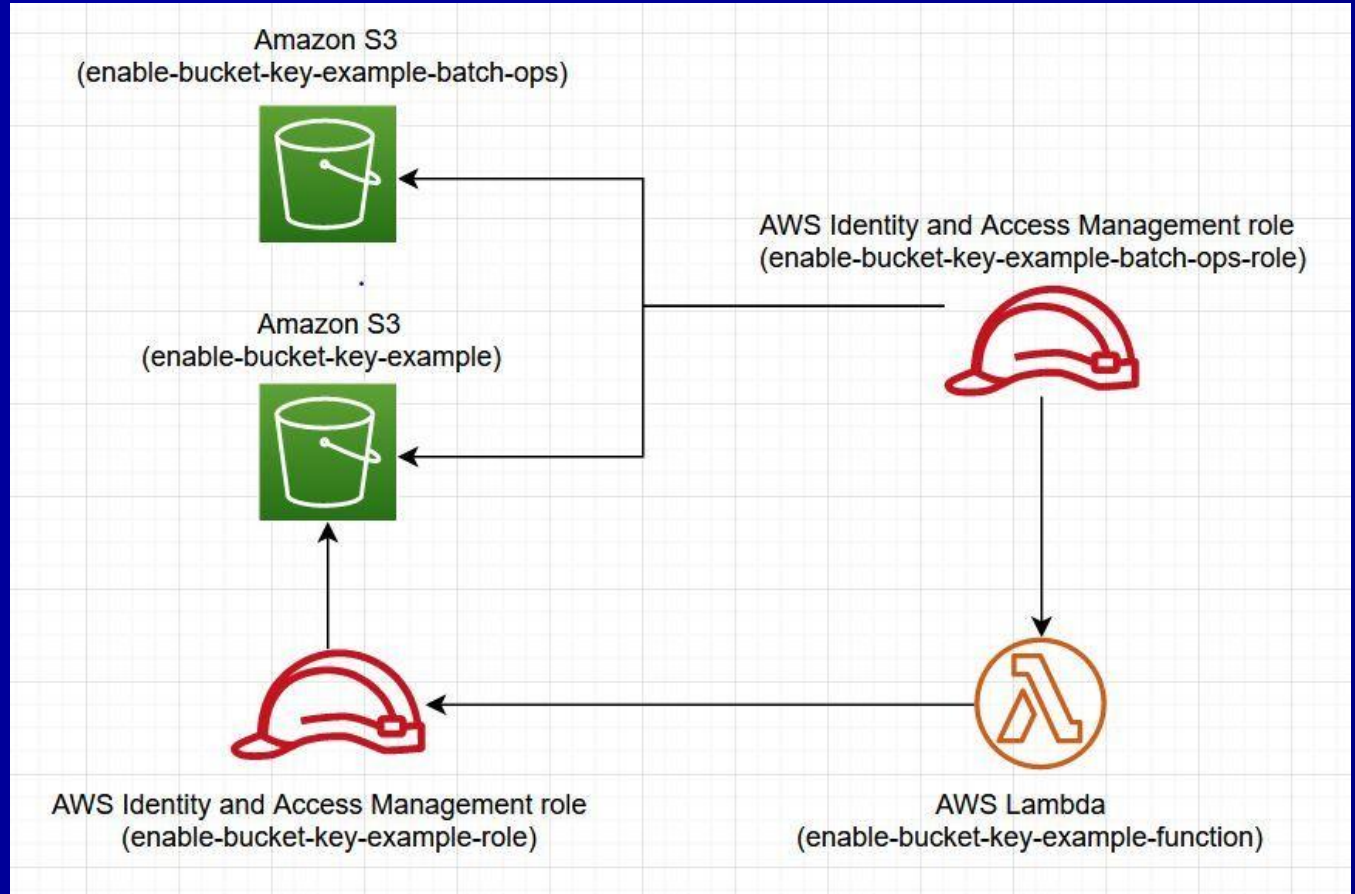
Actual value – Bucket keys enabled



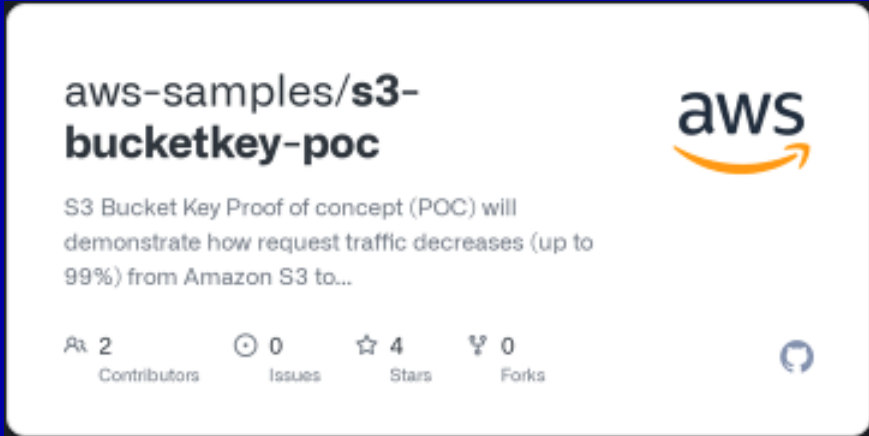
Existing objects?

Amazon S3 inventory

Amazon S3 batch operations



Additional resources



<https://bit.ly/3nSwlom>

Amazon S3 bucket key docs



<https://go.aws/3uFi8EE>



Connect with us

Aarti Parupudi



<https://www.linkedin.com/in/aarti-parupudi-62b4a3a8>

Syed Shareef



<https://www.linkedin.com/in/techsherrif>

Thank you!

