IRONCORE LABS

SaaS Shield CMK for Amazon S3

A quick overview of the IronCore Labs SaaS Shield CMK for Amazon S3, available in AWS Marketplace.

SAAS SHIELD FOR AMAZON S3: WHAT IS CMK?

Your enterprise customers want better data control and visibility into their data stored with SaaS partners. Customer Managed Keys (CMK) allows these customers to either hold their own encryption keys or to manage those keys themselves. A highly sought after feature, CMK is often offered at a sharp premium by SaaS providers who upsell to privacy minded enterprises.

HOW CMK TRADITIONALLY WORKS

In CMK, you encrypt sensitive customer data before you store it using per-customer keys. Your application can still see the unencrypted data, but the customer gets a full audit trail of access and can revoke that access at any time. In revoking access, it is revoked everywhere, including in backups.

More recent versions of CMK allow the customer to hold their encryption keys in their own Key Management Server or Hardware Security Module. This gives them ultimate control of everything from key rotation and algorithm choice to revocation without having to trust their provider. They get transparency into who is accessing their data.

One of the biggest benefits of CMK is that your customers can use their infrastructure and tooling already in place, making it easy for your customers to implement.

CMK USED TO BE A CUSTOM-BUILT FEATURE

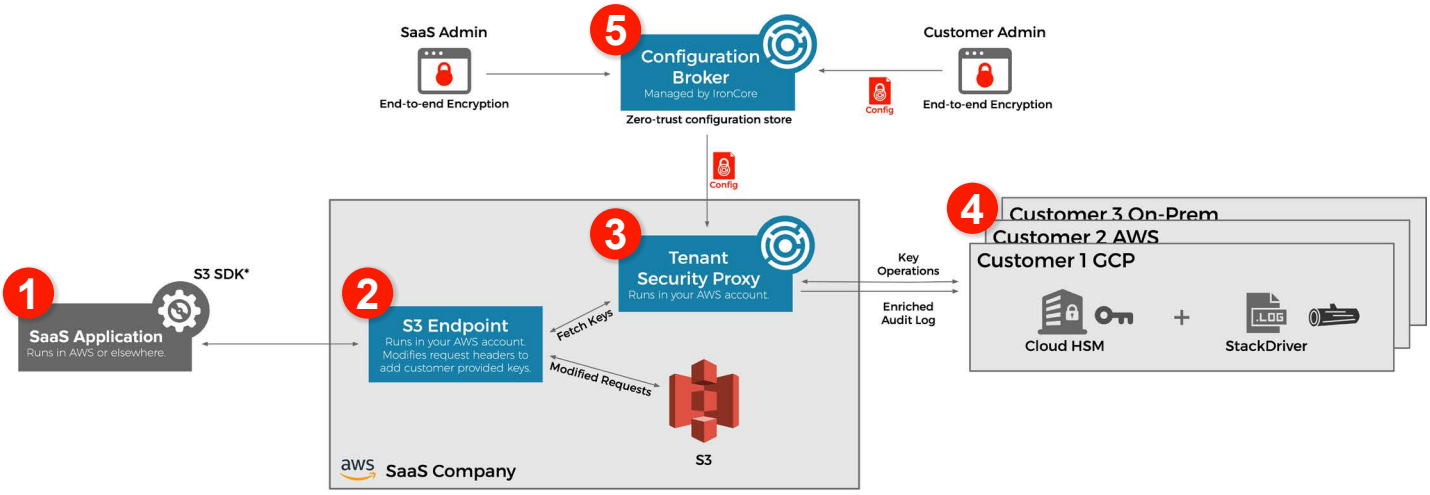
In recent years, top SaaS companies have started offering CMK, which they've built in-house at great cost but the payoff is revenue growth.

Hiring a team of applied cryptography experts and building your own custom version of Customer Managed Keys is no longer your only choice. IronCore's SaaS Shield lets teams build in CMK best practices in a fraction of the time and cost. With IronCore's SaaS Shield CMK for Amazon S3, you don't even need to get on the engineering roadmap.

INTRODUCING SAAS SHIELD CMK FOR AMAZON S3

IronCore Labs' SaaS Shield CMK for Amazon S3 is a simplified way to add customer managed keys to your SaaS application to protect your customers' files stored in S3.

SaaS Shield CMK for Amazon S3 can be installed with a simple CloudFormation template or using the AWS Marketplace. Once installed, the diagram below shows how your application interacts with S3 through a new proxy.



* Uses the standard AWS SDKs. No IronCore SDK required. SDK may be used anywhere with only configuration changes..

1. Your SaaS app can live anywhere and continues to use the AWS SDK to interact with S3. You simply change the endpoint and credentials used by your application.

2. IronCore's S3 Endpoint runs in your AWS account. The S3 Endpoint intercepts calls to S3, and for calls that upload or download files, it adds a header with a per-file encryption key that Amazon uses to encrypt/decrypt the file and then discards.

3. The S3 Endpoint determines the current Tenant ID and asks the IronCore Labs Tenant Security Proxy to provide the per-file key for encryption or decryption.

4. The TSP calls out to the customer's Key Management Server (if needed) to fetch the keys and to their logging service to push audit trails. If key leasing is turned on, rich audit trails are still sent, but far fewer calls to the KMS are required.

5. The TSP periodically fetches the latest configuration information from the IronCore Labs Config Broker, which holds the encrypted connection information for how to connect to a given customer's KMS and logging infrastructure.

Get Started

ABOUT IRONCORE

We are a data privacy platform for application layer encryption and customer managed keys (CMK). We enable software developers and businesses to rapidly build enterprise applications with strong data control. Data owners decide who can access their data, monitor how it's used, when, where, and by whom, and can revoke that access at any time. We are the fastest and easiest way to control data in multi-cloud and SaaS environments.

IronCore Labs
1750 30th Street #500
Boulder, CO 80301, USA

Inquiries
Email: info@ironcorelabs.com
Phone: +1.415.968.9607

CONNECT WITH US

- blog.ironcorelabs.com
- linkedin.com/company/ironcore-labs
- twitter.com/ironcorelabs
- ironcorelabs.com