box

Box KeySafe

Easy, cost-effective independent control of your encryption keys

The need for digital transformation has never been more urgent — where businesses need to operate faster than ever, employees need to be able to work anytime, on any device, and companies need to grapple with new cyber threat risks. To address these trends effectively, companies need a single content platform in the cloud to accelerate intelligent and collaborative business processes, and drive employee productivity. Despite these clear benefits of cloud content management, some companies are hesitant about moving certain workloads to the cloud due to prevailing security and privacy concerns.

This is why we developed Box KeySafe, a solution that enables organizations to maintain full control over the encryption keys that protect their content. Box KeySafe builds on top of Box's strong encryption and security capabilities to provide:

- complete, independent control over your encryption keys
- no impact to user experience
- unchangeable audit log of key usage
- ability to cut off access to content immediately
- physical and legal separation between encryption keys and content

With simple set up, and configuration in 30 minutes, IT teams of any size can deploy KeySafe within a few days.

Customers who use Box KeySafe

FICO flex intuit

METROPOLITAN POLICE schellman servicenow

SOCIETE GENERALE SUNTRUST ZURICH

How enterprises use Box KeySafe

Customers around the world and in highly regulated industries can take full control over their data for important security and compliance use cases

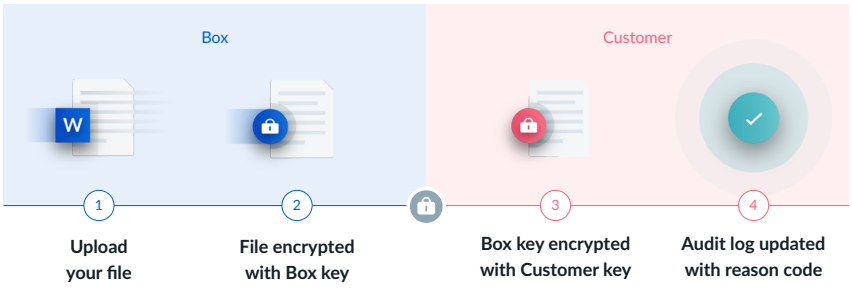
- **Client contractual compliance**
  For law, financial and consulting firms that are required to maintain control over client data at all times
- **Trade secret collaboration**
  For manufacturers working on highly sensitive research and development with partners around the globe
- **Data privacy compliance**
  For multinational firms to unify their global workforce on a single collaboration platform
- **Separation of duties**
  For security and IT teams required to meet this and other standards for data control and key management
- **Data access transparency**
  For organizations seeking greater control over their data and transparency into how their keys are used
- **Content access control**
  For security teams to control when cloud providers can access data, with ability to cut off access at any time

How Box KeySafe works

Box partnered with Amazon Web Services to provide on-demand management of keys through AWS KMS (Key Management Service) to support customers' requirements for security, control, legal separation and reliability.

When a file is uploaded into Box, the file is encrypted with a Box key through our native encryption service. With Box KeySafe, the Box key is then encrypted with the Customer key that is hosted at Amazon. The customer is the only entity that has access to that key. When the Customer key is used to encrypt or decrypt a file, an unchangeable audit log is updated with reason codes that identify why keys are being used.

Encryption flow



Customer keys are hosted by our partner, AWS, in systems that are designed with 99.99999999% durability and deployed in multiple availability zones. Decrypted data and encryption keys (both the Customer key and the Box key) are only stored in memory and never stored on disk.

Available Box KeySafe options

Box KeySafe is available in three versions, so that you can own your own encryption in the way that works for your organization.

Box KeySafe with AWS Key Management Service

This is the simplest, most cost-effective solution for customer-managed encryption for Box. KeySafe with AWS Key Management Service enables you to control your encryption keys by leveraging a software service — Key Management Service (KMS) from Amazon Web Services (AWS). KMS leverages multi-tenant HSMs.

Box KeySafe with AWS KMS Custom Key Store

With this option, Box customers can manage their own encryption keys using a simple-to-use AWS KMS interface — while storing encryption keys in AWS CloudHSM. KeySafe with AWS KMS Custom Key Store can be used to meet any security and compliance requirements for private key storage, without the operational overhead of managing on-premise hardware.

Support for KeySafe with AWS KMS Custom Key Store is coming in early 2019

Box KeySafe with AWS GovCloud

Box KeySafe with AWS GovCloud lets agencies ensure compliance with ITAR/EAR and IRS-1075 requirements as they move highly-sensitive workloads into the cloud. This offering leverages AWS KMS in the AWS GovCloud region, and enables government agencies and organizations that work with the U.S. government to gain independent control over their content encryption keys.

To learn more about how to leverage Box KeySafe, watch our on-demand webinar Own Your Keys to the Cloud

Visit www.box.com/security to read up on how we embed security, compliance, and resilience into our product foundation so that you can secure and manage your content