FINALCODE FOR BOX

QUICK OVERVIEW

PERSISTENT SECURITY FOR SENSITIVE FILES LEAVING THE BOX REPOSITORY

Box provides an intuitive cloud file sharing and collaboration platform with comprehensive file management and governance capabilities. But once files leave the secure box repository, data protection is lost. FinalCode for Box addresses this file data leakage challenge by ensuring persistent access, usage control and deletion of shared files leaving the box repository and in a way that is seamless to Box collaborators.

With FinalCode, organizations gain strong file encryption, dynamic permission setting, and lifecycle activity tracking – directly invoked within the Box interface as an added SaaS offering. Users can manage and change permissions to view or edit files by simply updating Box collaborator types which are linked to FinalCode's file security settings – it's that simple. After files leave the Box container, FinalCode file security controls stays persistent.

Easily Apply Security Right within Box GUI

Instantly Change Policy or Remotely Delete Files

Visibility and Control of Files Leaving Box Container

File Security Right Out of the Box

- Apply persistent security to files and folders leaving the secure box container
- Seamlessly manage and change permissions to view or edit files by simply updating file and folder Box collaborator types which are linked to FinalCode security settings
- Leverage intuitive Box workflow, user and security management

Dynamic Collaborator File Control

- Readily change, lock or revoke collaborator access and usage permission to shared files and entire folders
- Remotely delete files on recipient's device, on demand or on access attempt violation, even after files have been removed from box
- Security policy inheritance as files and folders move within the Box folder hierarchy
- Negate collaborator means to revert back to original unprotected files uploaded to Box

Extend Box File Governance

- Track the details on who, when and where shared files are opened, modified, printed and remotely deleted
- Preserves Box indexing metadata while ensuring encryption and usage control of files outside of Box
- Gain unified audit records within box and within log management platforms

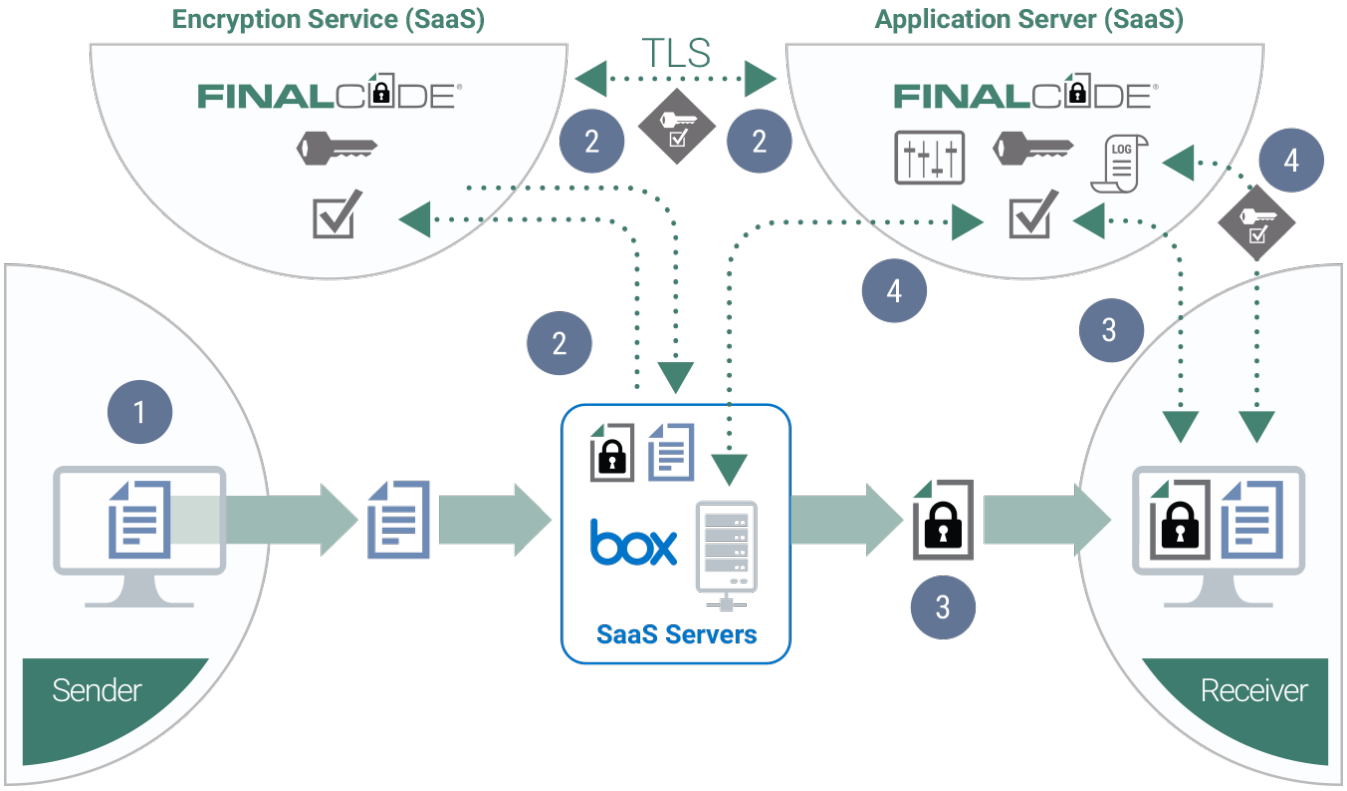
Like Box – Pay for Use, Cost-effective

- Licensed by internal user for project, department or enterprise-wide implementation
- NO COST for collaborators outside the organization
- Available to Box Business or Box Enterprise edition users

By separating file security management from file storage, distribution and content management, FinalCode makes secure file collaboration easy, cost-effective and in a way that works preserves your investment in Box and collaborator's user experience. As a result, companies can share files in confidence and reduce data leakage risks with an accelerated time to value.

FINALCODE®

www.FinalCode.com



1. Send

For files that the Box user would like to securely share, the Box user uploads files to the secure Box repository as they normally do. Box users can manually secure a file or folder, set folders for automatic security. FinalCode file security settings are pre-mapped to Box Collaborator types. Security settings are inherited as files more within the Box folder hierarchy.

2. Secure

FinalCode Encryption Service monitors for request to secure new files within the Box repository. FinalCode Encryption Service requests and receives a unique file encryption key and identifies from the SaaS Application Server. The Encryption Service never write to disk, but secures the file only in memory. The Encryption service replaces the original file with a FinalCode secured file and removes previous versions of the file within the Box repository. All original Box tags of the file are preserved.

3. Receive

Box Collaborator requests a FinalCode-secured file within the box repository which requires a local Client to open. Recipient one-time downloads and installs lightweight FinalCode Client (two-phase authentication, no administrator privileges are required). On attempted local secured file access, FinalCode Client will contact the FinalCode Server to verify access authorization.

4. Control

FinalCode Server will will check the Box Collaborators and respective roles linked to the file. If the recipient is authorized, FinalCode Server will send the security meta data to the FinalCode Client to enforce file access and usage control of the file. File security, access and usage activities are kept in the Server logs. On demand or upon an authorized recipient attempt to open the secured file, FinalCode Client will deny access, delete the file locally, and log the illicit action.

EASY, POWERFUL, INTEGRATED AND COST-EFFECTIVE

Security

Access and usage control for files leaving Box repository. AES-256 encryption and persistent protection with remote file deletion. Negate collaborator means to revert back to original unprotected files uploaded to Box.

Flexibility

Readily works with Box Enterprise and Box Business. Scale as needed by project, department or enterprise-wide.

Control

File access and usage settings applied by owner or administrator according to files and files in folders. File controls (e.g. open, edits, save, only in secured file, print) mapped to Box collaborator settings.

Intelligence

Comprehensive tracking across the file lifecycle including security being applied to files within the Box repository and access activity of files removed from the Box repository. Events captured in activity log support SYSLOG.

Rapid Deployment

Delivered as SaaS option for Box. Activated through Box administrator interface. Settings invoked within Box interface. Collaborators utilize lightweight software client to access FinalCode secured files.

TAKE THE NEXT STEP AND VISIT FINALCODE.COM

FINALCODE

www.FinalCode.com