Your Digital File vs. Dropbox

The Cryptoloc Advantage

Document Security

your Digital file® SMARTER SECURITY

Dropbox

At-Rest (HDD)

All documents stored on Your Digital File's servers are protected using our patented Cryptoloc technology, securing each file with a unique 256-bit AES key.

In the unlikely event our servers were to be compromised, the content of all users' documents remain confidential as we do not store or have access to the complete document encryption keys.[1]

"We (Dropbox) store your file data using 256-bit AES encryption [...]. You can securely access files and folders any time from our desktop, web, and mobile applications, or through third-party apps connected to your account."[2]

"Dropbox file data is stored in discrete file blocks that are fragmented and encrypted using 256-bit AES."

Documents stored on Dropbox's infrastructure are encrypted using 256-bit AES encryption. As files can be downloaded using only a web browser from Dropbox's servers, they must be decrypted by Dropbox. This means that Dropbox, not the user, controls the document encryption keys.

In-Flight (TLS)

As documents are protected using Cryptoloc technology, even if the Transport Layer encryption is broken, documents are still protected and can only be decrypted on the client's computer.[1] In addition, we specifically select the highest grade cipher suites and mandate server-side selection of cryptographic cipher protecting user's web access using the strongest available encryption algorithms.

"We (Dropbox) [...] use an SSL/TLS secure tunnel to transfer files between you and us. You can securely access files and folders any time from our desktop, web, and mobile applications, or through third-party apps connected to your account."

*"To protect file data in transit, Dropbox uses SSL/TLS for file transfer, creating a secure tunnel protected by 128-bit or higher AES encryption. [...] Not all mobile media players support encrypted streaming, so media files streamed from our servers **aren't always encrypted**."*

Content Confidentiality

your Digital file® SMARTER SECURITY

Dropbox

Can the system view my documents?

No The Your Digital File system and staff cannot decrypt your documents and view the content. All user documents are always stored in encrypted form on our servers. Documents can only be decrypted on the user's computer.[1]

Yes Documents are decrypted by Dropbox (server side) to support sharing, streaming and access via web browsers.

[1] Except for SecureShare. We have access to a document's encryption key only at the instant a share is created and or accessed by the recipient. We have access to the document in its complete, unencrypted form only at the instant a recipient downloads the shared document. In contrast, DocuSign has the ability to access the entire, unencrypted document at all times.

[2] Excerpt from "What does Dropbox do to protect my stuff?" – https://www.dropbox.com/security

Content Confidentiality

Personally Identifiable Information

Users who have not been fully identified cannot directly interact with other users unless they have been explicitly trusted by a fully identified user.

Users have full control over whether they are searchable by other authenticated (logged-in) users and even then, only their name, username, position and company is ever displayed to other users.

Dropbox claims a strong position on protecting the user's privacy[3], however, their privacy policy[4] states your information may be shared with Dropbox staff, users, applications and externally to Dropbox.

Document Content

All documents stored on Your Digital File's servers are protected using our patented Cryptoloc technology, securing each file with a unique 256-bit AES key.

In the unlikely event our servers were to be compromised, the content of all users' documents remain confidential as we do not store or have access to the complete document encryption keys.[1]

"Dropbox file data is stored in discrete file blocks that are fragmented and encrypted using 256-bit AES."

*"[...] Not all mobile media players support encrypted streaming, so media files streamed from our servers **aren't always encrypted**."*

This means that if Dropbox's servers are compromised, by external or internal threat actors, user data is exposed and document confidentiality cannot be guaranteed.

Additionally, media data that is shared via Dropbox **may be sent unencrypted to recipients, with no guarantees of any protection once leaving Dropbox's servers**.

Document Integrity

Client-side Hash Generation

SHA-2, 512-bits. A hash is calculated twice for each document on the user's computer, once before it is encrypted and again after it is encrypted. These are then signed by the user prior to uploading to Your Digital File to ensure "fingerprint" integrity.

Not available.
Dropbox does not provide this functionality.

Server-side Hash Generation

SHA-2, 512-bits. Your Digital File performs server-side hashing for documents uploaded via SecureShare. These documents are still protected by transport-layer security, and upon receipt by Your Digital File, are twice hashed, signed and encrypted using the same patented Cryptoloc security algorithms.

As Dropbox encrypts all documents on their servers and they provide *implicit* integrity checking upon decryption, i.e. if an encrypted file has been modified, it cannot be decrypted.

No *explicit* integrity protection is provided (such as digital signature technology), meaning that **Dropbox does not provide any protection against documents being modified or corrupted in transit or prior to encryption**.

[3] Excerpt from "How does Dropbox protect my privacy?" – https://www.dropbox.com/security#privacy

[4] Excerpt from Dropbox's "Privacy Policy" – https://www.dropbox.com/privacy

Document Versions and Data Recovery

your Digital file® SMARTER SECURITY

Dropbox

Deletion recovery and version history

Your Digital File supports recovery of an unlimited number of document versions for every account.

Additionally, deleted files, including all versions, can be recovered.

"By default, Dropbox saves a history of all deleted and previous versions of files, and allows you to restore them for up to 30 days. Unlimited recovery is available as an add-on for Dropbox Basic and Pro accounts, and is included with Dropbox for Business."[2]

How does Your Digital File deliver Advanced Key Management for maximum information security?

Advanced (Document) Key Management is provided by our patented Cryptoloc technology and is superior to Dropbox as users' document encryption keys cannot be decrypted by our servers.

- ✓ Your Digital File's Document Encryption Keys are never stored in a complete form and cannot be decrypted by a single party.
- ✓ Each Document Encryption Key is made up of three master keys, which are shared between the three parties defined in the system (user/service/escrow), two of which must collaborate to decrypt a document.

The Cryptoloc Advantage

- ✓ Advanced Document Key Management and simplicity of use.
- ✓ Integrity and validation of all important user actions (all critical user actions such as sharing & authorising, nominating, signing and all permissions require the User's private key).
- ✓ A Data Legacy service, enabling your data to be accessible to authorised parties in the event you or your business ceases to exist.

Where is your data stored?

Your Digital File's servers are based in ***Australia*** where data is governed by ***Australian law***.

All files stored online by Dropbox are encrypted and stored with a managed service provider in data centres across the United States.[5]

Data stored on overseas servers is *not* governed by Australian law.

[5] Excerpt from "Where does Dropbox store everyone's data?" – https://www.dropbox.com/en/help/7