Viivo and Dropbox

How Viivo works with Dropbox

Overview :: The Dropbox Problem

Dropbox is an excellent service that providers easy file-sync-and-share capabilities to its users. While Dropbox's security is "good enough" for most users due to encrypting data both in transit (SSL) and at rest (AES256) it remains a hands-off technology for many business users for a few simple reasons:

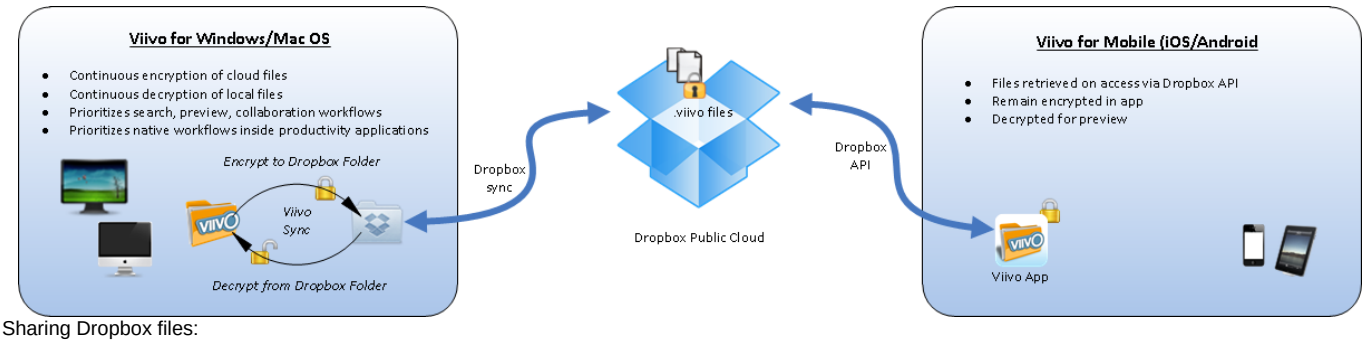
1. Dropbox at rest encryption is performed with encryption keys that the user does not control.
2. Dropbox is prone to security problems that leave your data vulnerable

Viivo makes an already great service better by giving end-users control over their encryption. With Viivo, all data is protected on the client device before the Dropbox synchronization service replicates it to the Cloud. While Viivo can protect many public cloud storage providers it has special support for Dropbox through integrated and seamless key management. This means you can share your files using the native Dropbox sharing process without having to perform extra steps often associated with secure sharing. Each participant in a Viivo secured Dropbox share has their own security credentials for accessing that share. End users are not required to communicate and share passwords or go through extra steps.

Viivo sync-based encryption/decryption

Your personal Dropbox files:

The Viivo program creates a folder named "Viivo" in the root of your user profile directory. Any unencrypted files placed in this folder cause Viivo to create compressed and encrypted copies in a Viivo-Encrypted folder in the root of your Dropbox directory. These secured files are what the Dropbox software and service synchronize to the Dropbox Cloud and any devices you choose to connect to it. The Viivo service keeps both of these folders in sync so that when you edit content on other devices, saved changes are securely synchronized through Dropbox and seamlessly decrypted with Viivo. This approach allows your computer to index plaintext content for searching and allows productivity applications to interact directly with plaintext data with no extra manual steps to decrypt beforehand and encrypt afterword. As soon as any file is "saved" to the Viivo folder, a compressed and encrypted copy is instantly created in Dropbox.



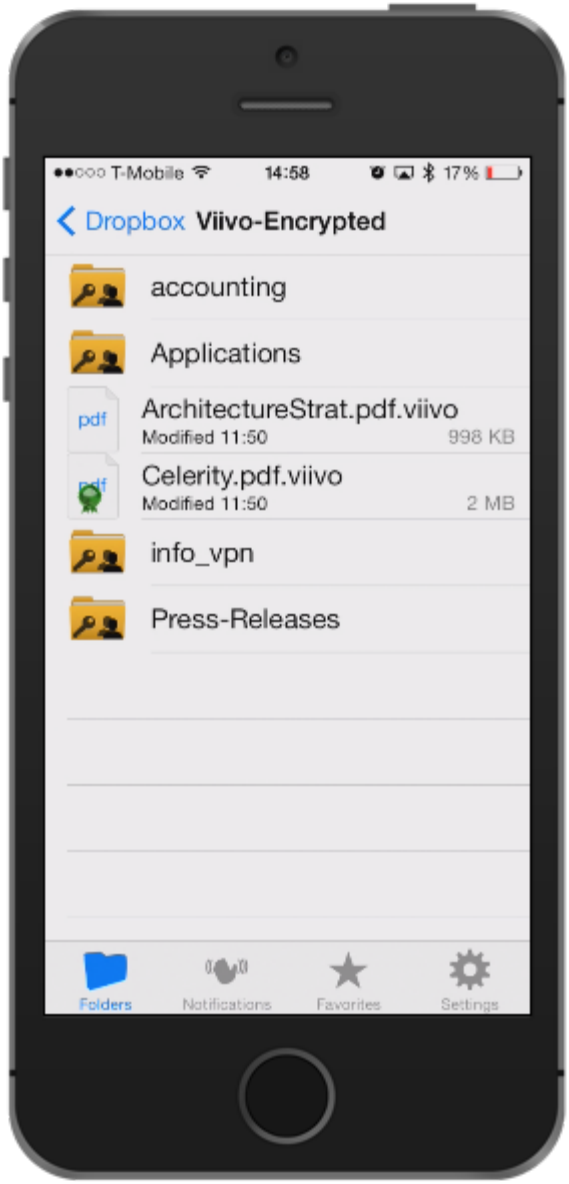
Sharing Dropbox files:

Dropbox supports two types of sharing. Public links and Dropbox shared folders. Viivo's key management has been designed to work with the latter. When you share a folder of Viivo encrypted files with another Dropbox user via Dropbox sharing, they will be required to install Viivo in order to decrypt them. Before decryption can occur, a collaborators Viivo client will generate an access request which presents itself to the content owner as a notification asking them if they would like to Allow or Deny each collaborator decryption keys for the files. Viivo generates unique keys for each Dropbox share. At no time are your private keys shared with any other Viivo user, cloud storage administrator or PKWARE staff member.

Support for decrypting from the Dropbox Web Interface

If someone sends you a public link to a Dropbox file you will need Viivo installed in order to decrypt it. If you do not already have the public key of the Asset associated with the file, your client will generate a signed key request which will trigger an Allow/Deny notification in the owners Viivo client.

Decryption with Viivo on iOS & Android



The Viivo Mobile app is available on the iTunes App store for iOS and Google Play for Android.

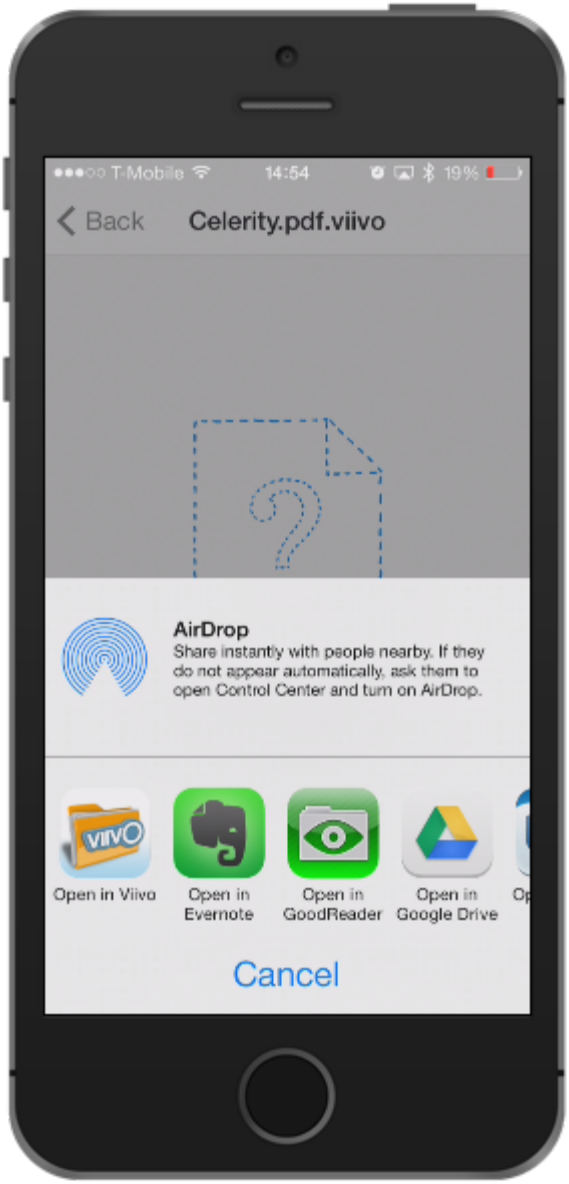
Connecting the Viivo App to Dropbox:

In the screen on the left, the mobile app connects directly to Dropbox via their API and will access your data directly. When you select an encrypted file, Viivo will download, decrypt and preview it for you. You may "Favorite" frequently accessed files or choose to open them in other applications if Viivo Preview is unable to display your particular file.

Viivo App pass-thru decryption:

Use this option for cloud storage providers that Viivo does not have API support for. Good examples are Email apps, Google Drive and SkyDrive. You simply use the native cloud storage app to locate your encrypted .viivo file and use the "Open In" function available from the OS. Selecting Viivo will cause your OS to pass the secure file to our App where it will be decrypted and previewed.

All data on mobile is encrypted at rest. Unencrypted contents are destroyed on close.



For a quick demonstration, checkout the Viivo + Dropbox demonstration video here.