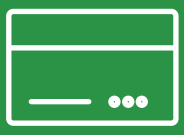
Dataguard™

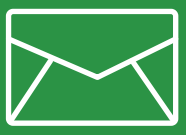
We provide digital and operational security solutions dealing with resilience and risk

Dropbox explained

How safe is your data?
Where does it go?
Who can see it?



Dataguard ePay
Encrypted Payslips



Dataguard eMail
Encrypted eMail

Dataguard eBox
Encrypted Storage

Dropbox explained

How safe is your data in Dropbox? Where does it go? Who can see it? There have been concerns raised about Dropbox's security in the past, so we're going to take a look and see if such concerns are justifiable.

Dropbox

What is Dropbox for?

Dropbox synchronises your files across multiple devices. Just put a file in the Dropbox folder and voila! It puts a copy on all your computers. And when you make changes to a file, it makes the same changes on all the others.

There are many services that offer this functionality (Cubby, SpiderOak, Google Drive, Microsoft SkyDrive, etc), but Dropbox was the first to make it big.

How Dropbox implements security

You can probably spot the weaknesses in the process. Any time you send your data anywhere on the internet, you can assume there's risk. What's more, your data is stored on a central computer over which you have no control. This requires that you trust in the company to treat your data properly.

So is Dropbox doing everything the right way? Let's take a look at their security process:

1. The Dropbox client (program) is installed on your computer. It is this program that creates a secure connection between your computer and their servers.
2. Dropbox encrypts the data on your computer in preparation to send it over the internet using the industry standard SSL/TLS with AES 128-bit encryption.
3. Your data is copied to the Dropbox servers and decrypted once it reaches its destination. Thanks to the encryption performed in the previous step, no eavesdroppers will be able to read your data in transit over the internet.
4. Your data is then encrypted again for storage with AES 256-bit. This is to prevent hackers from seeing your data if it's stolen from their servers.
5. The data is then copied from the servers to your other devices over the internet. Again, using SSL/TLS encryption.
6. Once on your computer, your data is then decrypted and stored on your hard drive.

What's the Problem With Dropbox's Security?

All that encryption sounds pretty safe. So what's the problem?

The biggest issue raised with most services like Dropbox is that you're not the only one with access to your data, despite all the fancy encryption manoeuvres. It's actually possible for Dropbox to manually decrypt and look at your data while it's on their servers. This can lead to several issues:

1. **A rogue Dropbox employee who decides he wants your data -** Of minimal concern since very few employees typically have the access rights. But still, you should be aware that it's possible for others to see your data.
2. **Hackers getting their hands on your encryption key -** Since Dropbox stores the keys for all its users, it's possible that a database breach could result where everyones' encryption keys are stolen. This would appear to be an unlikely scenario as the keys are probably stored far away from your actual data, but it is, at a minimum, a theoretical risk.
3. **Dropbox voluntarily disclosing your information to a third party -** This is the real concern. The question is whether companies like Dropbox should have the right to give away your data.

   For instance, Dropbox has already specified that were they to receive a subpoena by law enforcement, they would willingly decrypt your data and hand it over. And what would you be able to do about it? Probably nothing, even though Dropbox's own *Terms of Service* specify that you maintain full ownership of your data while it's stored on their servers.This may not rile you too much since you probably have nothing to hide from the cops. But it's worth noting that nothing you put in Dropbox is private. Other eyes may someday see what you put in there.

Dataguard™

Where Dataguard eBox differs

- We encrypt the data on the move at 256 AES and DO NOT rely on industry standard SSL/TLS with AES 128-bit encryption (HTTPS) which isn't secure!
- One of the most criticised facts about cloud services is the lack of security of stored data. In order to make sure that your eBox data is always secured, eBox does encryption and decryption on the fly so that no one is ever able to peek into your files. Data stored is encrypted with a unique key. We cannot access the contents and do not even know the file names.

Dataguard Security Ltd
Bloxham Mill | Bloxham | Banbury | Oxfordshire | OX15 4FF
+44 1295 724 101 | dataguard-uk.com