Confidentiality and Data Protection in Microsoft OneDrive

OneDrive is a cloud-based storage platform offered by Microsoft. Think of it as a hard drive in the cloud, which you can use to store your data on. In contrast to a any local storage you can conveniently access your data from virtually any device – desktop, smartphone, tablet – and from anywhere, over the internet. Data stored in the cloud is exposed to greater risks and therefore needs extra protection. Client-side encryption is a viable means of protection that can ensure that data is kept safe even when stored in hosted environments like OneDrive in Microsoft Cloud.

How can you protect data with conpal LAN Crypt?

conpal LAN Crypt is a client-side encryption solution that provides file-level encryption. Its powerful key and policy management functionality supports encrypting data using different keys for business, personal and shared data. Encryption and decryption take place on the local device. Hence, data is protected on the local machine, when it leaves the client, and in transit. Neither Microsoft nor anyone else has access to the plaintext data or to the key used for encryption. conpal LAN Crypt helps organizations keep their data secure and confidential even in cloud-hosted environments.

Enable Protection

1

Define what data to protect

In the conpal LAN Crypt Admin console, define an encryption rule for OneDrive. A single rule using the <OneDrive> placeholder is sufficient to encrypt all your data uploaded to OneDrive. Define additional rules if you plan to share data in the specified folders. That's all you need for now. If you are not happy with the result, you can always come back later and fine-tune the protected locations to suit your needs.

2

Activate the Policy

On your client, make sure that the conpal LAN Crypt client is installed. You can easily do this by checking for the app on your phone, the app-icon in the System Tray (Windows) or in the menu bar (Mac). Next, refresh the policy to have the encryption rules defined just before be applied to the system. All data you create in your local OneDrive Sync folder will be encrypted.

Upload to OneDrive

3

Connect to OneDrive

On your client, make sure that the Microsoft OneDrive client is installed. You can easily do this by checking for the app-icon in the system tray (Windows) or the menu bar (Mac). Login to your OneDrive account and start the upload. That's all - You are all set and good to go.

Access Anywhere

4

Windows or Mac

Use your local sync folder to access files stored in your OneDrive. Encryption and decryption take place on-the-fly and happen in the background, unnoticeable by the user. Data is encrypted before it is uploaded into the cloud. You can also share documents, even if they are encrypted. Just keep in mind that your partner needs to have access to the encryption key used for the shared document.

5

Smartphone or Tablet

The conpal LAN Crypt app allows you to browse and open your files stored on OneDrive. Launch the app and navigate through your folders. Files can be opened conveniently from within the app. Encrypted files are decrypted on the fly before being displayed. Encryption is done locally in the app to ensure that confidential data remains what it is – confidential.