Confidentiality and Data Protection in Microsoft Teams

Microsoft Teams is the hub for teamwork in Microsoft 365. It enables instant messaging, online meetings with audio and video calling support and offers extensive web conferencing capabilities. In addition, Teams provides file and data collaboration and on-line storage. For core productivity scenarios Microsoft Teams relies heavily on online services like SharePoint and Exchange Online. Data shared via Teams is stored in SharePoint and can be accessed from virtually any device and from anywhere. Stored in the cloud, it is exposed to greater risks and therefore needs extra protection. Client-side encryption is a viable means of ensuring protection of data stored in hosted environments such as Microsoft Teams and SharePoint Online.

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 supports use cases like data sharing where different keys should be used for business, personal and shared data. Encryption and decryption take place exclusively on the endpoint. Hence, data is protected on the local machine, when it leaves the client, and in transit. Neither Microsoft services in the cloud nor others have access to the "plaintext" data or the key used for encryption. conpal LAN Crypt helps organizations to keep their data safe and confidential even in cloud-hosted environments.

Enable protection

1

Define what Teams or Channels to protect

In the conpal LAN Crypt Admin console, define an encryption rule for the Teams or Channels you want to protect. A single rule covering all Teams is sufficient to ensure all data uploaded to Teams is encrypted. Define additional rules for individual Teams and/or Channels if you require more granular control. 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 the app on your mobile device, the app icon in the system tray (Windows) or in the menu bar (Mac). Next, have the policy refreshed. This will apply the encryption rules just set to your system. That's all – You are all set and good to go. All data you create in your local sync folder will now automatically be encrypted.

Sync with Microsoft Teams

3

Connect to the Teams File Storage

On your client, make sure that the conpal LAN Crypt client is installed. You can easily do this by checking for the presence of the app icon on your mobile device, in the system tray (Windows) or the menu bar (Mac). Enable local sync for those Teams/Channels you want your data to get encrypted in.

Access Anywhere

4

Windows or Mac

Use your local sync folder to access files stored in Teams. Encryption and decryption take place on the fly and happen in the background, invisible to the user. Client-side encryption ensures that data is encrypted before it is uploaded to the server or into the cloud. Documents can be shared, even if they are encrypted. Just keep in mind that the sharing partner needs to have access to the same encryption key used for the shared document.

5

Smartphone or Tablet

The conpal LAN Crypt app allows you to open encrypted files stored via Teams. Launch the Teams app and navigate through your folders. Files can be opened via the conpal LAN Crypt app or directly from within the Teams app. Encrypted files are decrypted on the fly before being displayed. Encryption is done locally within the app to ensure confidentiality of your data.