Dropbox detection and remediation

Dropbox does not support malware detection. Coro detects malware in these files as soon as they are uploaded from an external source or from the user's device to cloud storage.

Coro creates a quarantine folder (named "Suspected folder") at the point of malware detection. This folder is visible within the respective cloud storage service and Coro recommends that administrators restrict access in line with your organization's security policies. Coro moves malicious files to the "Suspected folder" and creates a ticket for the event. The admin user has the following remediation actions available:

- **Approve file**: The file is returned to its original location on the cloud drive. The admin user has the option of immediately closing the current ticket and all related tickets.

- **Delete file**: Permanently deletes the file. The file is removed from the "Suspected folder".