Salesforce detection and remediation

Salesforce does not provide malware detection.

Because Salesforce does not maintain a clear folder structure behind the scenes, Coro's automatic remediation process differs from the other protected apps. For Salesforce, Coro secures potentially harmful files by archiving them and making them inexecutable, preventing further damage. After being archived, these files are no longer visible in Salesforce 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 the archived 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".