Box detection and remediation

By default, Box does not detect malware, but it offers a paid feature, *Box Shield*, that detects malware in Box storage and restricts downloading and sharing. Regardless of the subscription type, Coro detects malware in all box 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".

Malware identified by Box

In some cases, malware might have been identified by Box prior to Coro and blocked from being sent to the quarantine folder. This can mean that, while Coro still identifies the malware event and raises a ticket in the Ticket Log, no remediation action on the file is performed.

When this happens, an admin user can still review tickets raised by Coro to notify about the malware identification, and can still perform actions such as suspend the user or close the ticket. However, as Box has already dealt with the threat, the **Approve file** and **Delete file** actions are not presented.