Microsoft 365 detection and remediation

Microsoft 365 offers limited malware detection, typically occurring 15 minutes or more after a file download. If a scan identifies a file as malicious, the system restricts its sharing capabilities, and a warning appears in the OneDrive interface, indicating the file cannot be shared.

In Addition, there are file types that Microsoft 365 does not detect. Coro detects malware in these files as soon as they are uploaded from an external source or 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.

> **Note**
>
> File deletion is currently not available via the Microsoft API.

Malware identified by Microsoft 365

In some cases, malware might have been identified by Microsoft 365 prior to Coro, and therefore 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 by Coro.

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 Microsoft 365 has already dealt with the threat, the **Approve file** and **Delete file** actions are not available.