

Overview of malware detection in cloud drives

Most types of files are susceptible to malicious code. In most cases, when a file containing such code is opened, the malware process is triggered, and can then infect an entire connected ecosystem. In other words, when a file with malware is uploaded to a cloud app, or downloaded from an app to a device, the risk escalates.

The majority of cloud applications natively offer some level of protection against these risks. Coro enhances malware detection and remediation across all supported cloud applications based on the specific level of protection offered by each. Coro searches for and removes files containing malware to prevent the spread of malware via cloud drives. The cloud applications currently monitored by Coro are:

- Microsoft 365
- Google Workspace
- Dropbox
- Box
- Salesforce
- Slack

Coro enhances malware detection and remediation across all cloud applications, based on what each application provides natively.