# CDR (Content Disarm and Reconstruction): What it is, why it helps, and how it works

Gridinsoft Help Center

## What it is

## Why it matters

Most attacks now hide in everyday files-invoices, resumes, PDFs, Office docs. CDR turns those high-risk attachments into safer versions, so a single click doesn’t become a compromise.

## How it works (30-second tour)

- Ingest: the file is opened in a controlled space.

- Disarm: active content and suspicious structures are removed or neutralized.

- Rebuild: a clean copy (same text/images/layout) is produced for the user. Some solutions sanitize by policy (always remove macros), others use allow-lists (keep only known-good elements).

## What CDR is great at

- Stops file-borne malware without waiting for signatures.

- Helps with zero-day file exploits.

- Reduces help-desk tickets from "I opened a bad attachment."

## What CDR is not

- A replacement for AV/EDR or sandboxing-CDR is one layer in the stack.

- Perfect fidelity: complex files may lose non-essential features (e.g., macros, embedded media).

## When to use it

- Email gateways and file-upload portals (support, HR, vendor portals)

- Shared folders, cloud drives, and collaboration tools

- High-risk roles opening lots of external documents

## Quick start

- Choose where to enforce (email, uploads, shared drives).

- Set a simple policy: remove macros/active content by default.

- Log what was removed; allow users to request the original if truly needed.