GLASSWALL

USE CASE

Metadata Removal

Reduce the risk of sensitive information being leaked to a third party with Glasswall CDR (Content Disarm and Reconstruction).

Discover proactive file protection

Most file formats have associated metadata that comes with the visual data. While this information can be helpful, it also poses a security risk. For example, personally identifiable information in metadata may change the classification of a business process and data storage from a compliance and security viewpoint. Tracked-changes in a file that undergoes review stages may become prejudicial in a commercial or legal context once the document has changed hands or moved to a different trust zone.

Glasswall CDR offers proactive protection to reduce the risk of accidental information being leaked. It instantly cleans and rebuilds files to match their known good manufacturer's specification – automatically removing potential threats. This simple approach ensures every document in your organization is safe, without sacrificing productivity.

Key Benefits

Reduce the risk of accidental information leakage

Eliminate potential for confusion from inaccurate data that detracts from the main visual layer

Key Features

Remove data about who, how, when and where a file was created

Discard commentary or user tracking about the data contained in the body of the document

How It Works

Glasswall CDR technology instantly cleans and rebuilds files to match their known good manufacturer's specification – automatically removing potential threats. This simple approach ensures every file in your organization is safe, without sacrificing productivity.

Inspect

files digital DNA

Clean

risky content (by policy)

Rebuild

to known good standard

Deliver

safe, visually identical file

GLASSWALL

glasswall.com
info@glasswall.com