
See Glasswall CDR in action: Compare this document before and after processing. This file includes a few examples of non-malicious content:

### Hyperlinks

Hyperlinks are commonly used in targeted phishing attacks. While links may appear innocent on the surface, the link itself may take the user to a different destination, designed to start a chain of malicious events.

> **Example:** http://www.glasswall.com/ In the original file, the actual URL is google.com – not what's displayed on screen. (Note: Your document reader may make valid URLs clickable in the processed version.)
>
> **Example:** Link within this document

### Metadata

Metadata can contain information an organization does not wish to disclose publicly, such as review comments, tracked changes, and the names of the file's authors.

## Supported file types and policy management

Glasswall CDR can support cleaning many more kinds of risky content than you see in this file. Several kinds are so risky that they appear malicious, and we can't include them here.

Visit https://docs.glasswall.com/docs/glasswall-supported-file-types to:

- See the full list of supported file types
- Learn what risky active content can be removed in each file type
- Find out how Glasswall can help reduce your organization's risk