GLASSWALL

USE CASE

Malware Risk Removal

Reactive detection-based security methods can't keep up with today's increasingly complex threats. Discover proactive protection with Glasswall CDR (Content Disarm and Reconstruction) for Malware Risk Removal.

Discover proactive protection against malware

In 2020, ransomware attacks increased by 66% to 304.6 million*. Detection-based solutions can't keep up with the sheer number of malware variations created each day. Businesses are at risk with popular file formats (e.g. PDFs, Word and Excel files) offering many places for malware to hide.

*Source: https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf

It's time for a better way. Glasswall CDR offers proactive protection that ensures every file in your organization is safe. 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

Trust your files again. Glasswall CDR disarms and secures every file in real-time

No more system crashes from malformed files. Glasswall CDR cleans and rebuilds files to their manufacturer's standard specification

De-risk documents in real-time, for security at the speed of business

Protect against future unknown attacks with CDR's proactive approach

Key features

- Supports a wide array of file formats
- Signature-less and can run in an air-gapped environment without needing regular updates
- Supports embedded SDK or Kubernetes-based architecture where throughput of files requires the ability to rapidly scale
- Cloud native and open architecture without risk of platform lock-in to any particular cloud service provider
- No quarantining files – every file is cleaned and rebuilt into a visually-identical file that's secure

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