USE CASE

# File Uploads and Downloads

File uploads are an integral feature of most web applications, however this leaves them open to potential vulnerabilities and attacks. They are designed to be permeable and receive inputs from users, many of which are mission critical. Examples include:

- Upload of resumes by candidates to recruiting sites
- Claims information being uploaded into insurance portals
- Proofs of identity uploaded into banking portals
- Document sharing via portals for M&A due diligence
- Or more generally, scanned documents and completed forms

For files uploaded to web applications, there is a high likelihood that a new file-based threat won't be identified by reactive endpoint protection, leaving the business exposed to exploits by hackers and could lead to malware, unauthorized server access, attacks to website visitors, the hosting of illegal files and much more.

## Reduce risk of file-based threats

The most obvious way to protect the underlying software applications from file-based threats is by facilitating the interception and disarming of files, by the application itself. This approach relies on proxies and firewalls, which can leave certain holes that still leave an application vulnerable.  Files can also be disarmed as they are retrieved from storage but there may still be some attack techniques that are best addressed at the web application layer.

According to Gartner® Content Disarm and Reconstruction (CDR) is cited as the strongest option for filtering threats at the application, gateway and storage layers.

"CDR provides the highest security" to limit the risk of malware upload.
- Gartner® "Quick Answer":  Protect Web Applications Against Malicious File Uploads, October 2021

Glasswall CDR (Content Disarm and Reconstruction) doesn't rely on the detection of 'known' threats, it works by proactively looking for 'known good'. The Glasswall CDR Platform inspects, cleans and rebuilds the file - automatically removing potential threats and delivering a secure, visually-identical file. It happens in real time, so users won't even notice Glasswall is there and provides protection against completely new attack types.

With Glasswall CDR you give users the freedom to instantly upload or download files from the internet without putting your organization at risk and without the latency of reactive detection-based solutions.

## Key benefits

- ✓ "CDR provides the highest security " to limit the risk of malware upload - Gartner®
- ✓ Remove threats from all files being uploaded and downloaded into your organization
- ✓ No more system crashes from malformed files – Glasswall CDR cleans and rebuilds files to their known good manufacturer's standard specification
- ✓ Give users the freedom to use the internet without being slowed down by less effective detection-based solutions
- ✓ Zero latency for maximum protection against the most evasive malware

## Key features

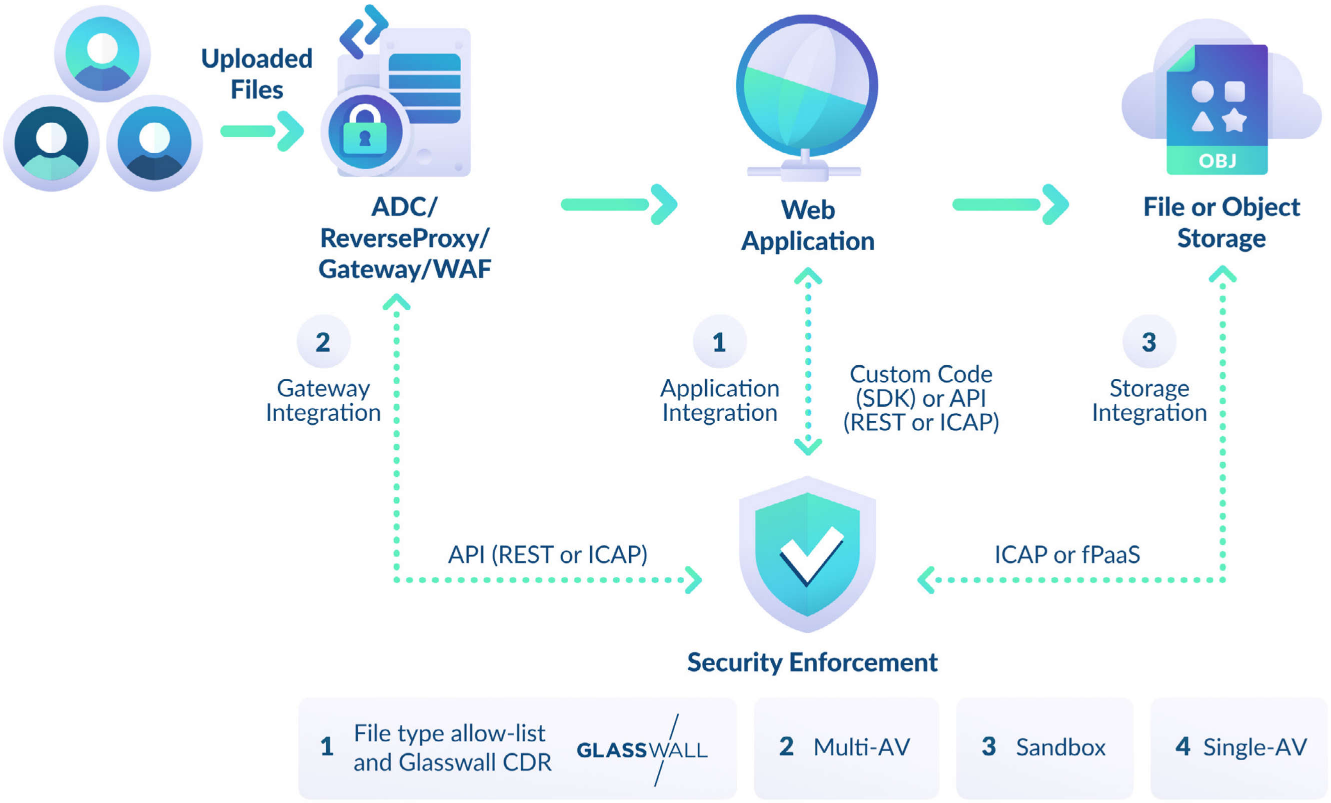
- Integration to network appliances that support industry standard ICAP
- Rapid integration into the web development process with code patterns and
- OpenAPI compliant endpoint contract

## How it works

Glasswall CDR Platform sanitizes files to prevent both known and unknown threats from entering your IT infrastructure.  Glasswall provides a public synchronous or asynchronous Cloud API to trial our CDR service through.

Additionally a public version of Glasswall's Clean Room application, a reference UI implementation that can perform CDR on files, displaying results to the user or silently making every file safe for downstream processing.

Check out our Guide to making File Uploads in Software Applications Safer for more detail on how to neutralise the threat of malware entering your organization.



GLASSWALL

glasswall.com
info@glasswall.com