GLASSWALL

Financial Organizations

Secure file uploads

with CDR (Content Disarm and Reconstruction) zero-trust file protection

glasswall.com
info@glasswall.com

File portals

Financial organizations around the globe encourage users and customers to upload files as part of everyday business operations. This can include a wide variety of sensitive documents, ranging from mortgages and new accounts to loans and filing claims (among many others).

To address a range of important cybersecurity concerns, they frequently rely on detection-based technologies – such as antivirus and sandboxing solutions – to protect their networks. These are designed to identify and remove potentially harmful content such as macros, malicious scripts, or malware, that may be uploaded by a cybercriminal via an online portal.

The problem with detection

A reliance on detection means no matter how complex a security solution may be, it can still only protect against what it has seen before. As a result, these solutions fall short when protecting critical financial data against the following common file upload risks:

1. Malicious content

Uploading user-generated files to a financial organization's network offers an easy way for cybercriminals to distribute malware. Vulnerabilities in server-side handling of files can then be exploited by the malware – compromising critical and sensitive information at a potentially catastrophic cost.

Alternatively, malicious content can be used to attack an organization's users. If the file contains malicious content that has passed through detection-based solutions, and a user accesses the file, a cybercriminal can take control of their device – disabling access, and even obtaining sensitive information.

2. Server-side attacks from file overwriting

Existing files on an organization's server can be overwritten if a file is uploaded with an identical file name and file extension. If, for example, a critical file is overwritten, the new file uploaded by a cybercriminal can be used to enact a server-side attack.

Resulting in compromised security protocols – allowing cybercriminals to embed additional malicious content that could be used to disrupt or hold financial organizations to ransom.

Secure file uploads

with CDR (Content Disarm and Reconstruction) zero-trust file protection

File upload protection from Glasswall CDR is different. Instead of looking for malicious content, our advanced zero-trust CDR process treats all files as malicious – validating, rebuilding and cleaning each one against their manufacturer's known-good specification. Only safe, clean and fully functioning files enter an organization, allowing users to access them with full confidence.

In addition, Glasswall's CDR file detection feature can be used alongside a list of permitted file extensions to protect financial organizations against the risk of a server-side attack from file overwriting.

Glasswall currently protects customers across the world in finance, insurance, healthcare and manufacturing – helping to keep their sensitive data safe against the risks from file uploads.

Gartner – CDR is the best model

Benefit rating:
High

Gartner believes that "CDR is an important layer in any organization's defence and content protection strategies..." They expect "CDR will ultimately be considered a best practice."

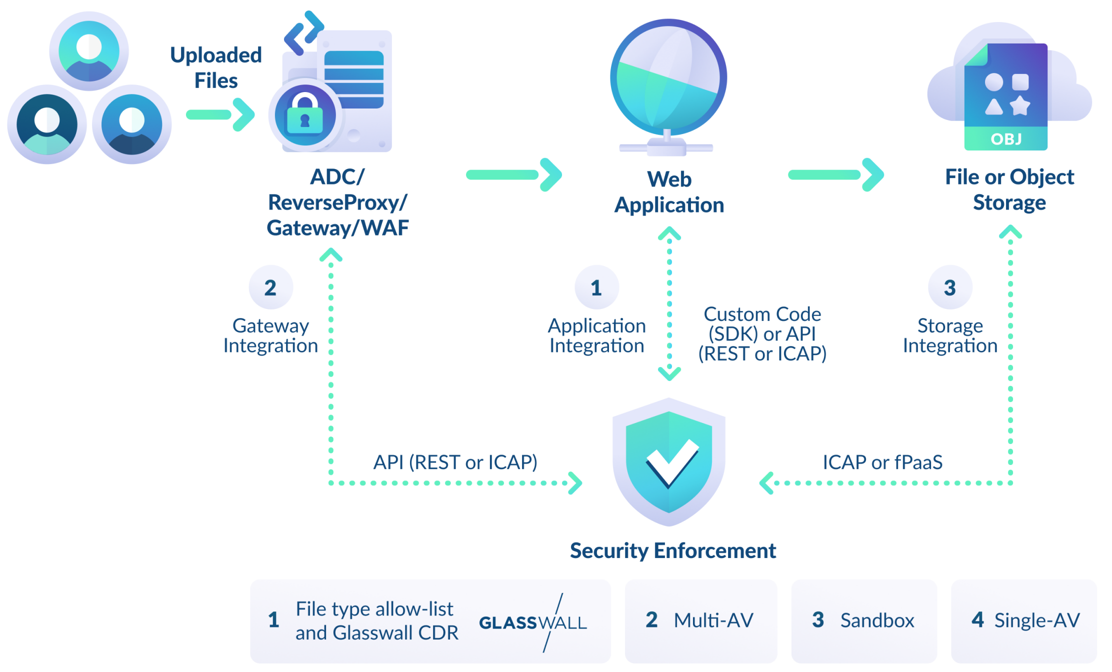
Related to protecting web applications against malicious file uploads, Gartner recommends that CDR technology is considered the most secure technology to do this, followed by multi-AV, sandboxing and finally single AV.

Gartner.

Source: Gartner 'Hype Cycle For Network Security'

Simple, fast and effective integration for file upload protection

Our Embedded Engine and Glasswall CDR Platform can be established at various integration points within a financial organization to protect it against malicious file uploads:



1. **Application Integration** – direct integration into the application/finance portal is our preferred method. This allows for complete control over application flow – improving end user experience by warning users in real time if they upload something they shouldn't.

   Application developers can connect directly to our Glasswall CDR technology via an SDK (Glasswall Embedded Engine) or REST API and ICAP endpoints (Glasswall CDR Platform), enabling them to harness our zero-trust CDR file protection capabilities in line with application workflows.

2. **Gateway Integration** – if a financial organization requires Glasswall file protection across a large number of applications, or if an application is closed source, the integration of the Glasswall CDR Platform, via REST API and ICAP endpoints, can be done at the gateway in front of an organization's application(s).

3. **Storage Integration** – we are able to integrate our zero-trust CDR technology after files pass through a financial portal – at the persistence layer, such as an S3 bucket or within Blob Storage.

About Glasswall

We believe people should be free to open their files without fear.

To click on anything without risk of catastrophe.

To use systems the way they were meant to be used.

That's why we're raising the bar on file security at Glasswall.

We've always been different - we didn't start out as a traditional security product.
In the beginning, Glasswall was one of only two file sanitization filters in the US Intelligence Community's highly classified networks.

And we are approved in the Cross Domain Raising the Bar standard by the NSA too!

Our fresh approach to security can do what other solutions can't. We designed Glasswall CDR to protect businesses against the most advanced file-based threats. Today, we're trusted by commercial and government organizations around the world.

Learn more at glasswall.com

GLASSWALL

glasswall.com
info@glasswall.com