GLASSWALL

Drag and drop file protection for everyone

Introducing Glasswall Clean Room

Glasswall Clean Room

- Harness the power of industry leading Zero-Trust file protection with Glasswall CDR (Content Disarm and Reconstruction)
- Easy and fast deployment that takes minutes, not months
- No training required with an intuitive user-friendly drag and drop browser interface
- Protection for all, with both freemium and paid-for options available
- Removal of all file-based threats – even those anitvirus solutions can't detect

Try Clean Room on your browser

You are at risk from file-based threats, even with your security solution in place

Security solutions that leverage antivirus technologies are a popular choice in the fight against file-based threats. Many organizations have invested in antivirus software, sandboxes and/or firewalls to provide protection against bad actors trying to infiltrate their IT Infrastructure.

These solutions provide good protection against most known threats.

But *good* isn't good enough.

These solutions rely on antivirus databases to identify and learn of threats, leaving organizations unprotected against zero-day threats for an average of 18 days. They also lack the ability to analyze the DNA structure of a file, leaving room for malware, ransomware and other file-based threats to hide from these detection-based solutions.

Glasswall Clean Room: drag and drop Zero-Trust file protection

Glasswall Clean Room is a simple to install and easy to use solution designed to fill the protection gap left by detection-based solutions. It harnesses the industry leading, patented and highly ISG* compliant Glasswall CDR Engine to process files users drag and drop into the browser application.

Clean Room sits on a user's browser making it simple for organizations to deploy, and it is easily scalable to match growing business requirements. In addition, users have complete control over the files they process. If they are unsure a file is trustworthy on a USB device, or one they have simply downloaded from the web, all they have to do is simply drag and drop it into Glasswall Clean Room.

The Glasswall Engine will instantly process the file and return not only the safe, clean file but also produces a report on how Glasswall made your file safe and the original risk of the document.

*ISG – Inspection and Sanitization Guidance standards by the National Security Agency (NSA).

Complete file-based security with Glasswall's Zero-Trust Approach

Glasswall Clean Room assumes a zero-trust approach for every file a user drops into it. Each file is processed as if it were malicious, applying our patented and highly ISG* compliant 4-step CDR process, returning all supported files to their known good manufacturer's specification before delivering it to the end user.

*ISG - Inspection and Sanitization Guidance standards by the National Security Agency (NSA)

1. Inspect

Breaks the file down into its constituent components. Validates the file's structure against its specification.

2. Rebuild

Non-conforming file structures that fail validation are rebuilt in-line with the file's specification.

3. Clean

Removes high-risk file structures that contain active content, based on a configurable policy.

4. Deliver

Semantic checks ensure the file's integrity. The safe and the visually identical file is now ready to use.

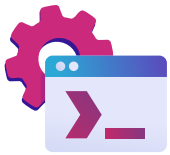
Known-good manufacturer's specifications matter - here's why

Our commitment to returning all files to their manufacturer's known-good specification sets Glasswall apart. Some CDR providers either flatten a file or they use non-proprietary libraries to rebuild the file in question. There are problems with each approach. With file flattening, where a document is converted into an image-based format, the process removes all useability of the original document. And non-proprietary libraries do not always conform to the known-good manufacturer's specifications, so the rebuilt file's structure does not meet published security standards.

What does complete file-based protection guard against?

Acroforms

'Acrobat Forms' look just like any other form, but they may also contain active code such as JavaScript. This active code can be exploited to launch attacks commonly missed by traditional antivirus.



Macros and JavaScript

Forms of active code. These extra file functions can perform actions without a user's permission, starting a chain reaction of malicious events. These are often used by bad actors to mount an attack against the user or receiving system when expressed in a business document.

Dynamic Data Exchange (DDE)

DDEs within Microsoft documents are known to present risk, as the protocol may be used to execute malicious code on the recipient's computer.

Digital Signatures

Whilst signing may not represent a threat, if the ownership and trust of the certificate chain has been compromised, this could trick a user into opening a document that contains something malicious.

Embedded Objects

Embedded objects within files can be used to hide data or provide a way for active code to be triggered. These objects are often harnessed by bad actors to perform actions without a user's permission or knowledge.

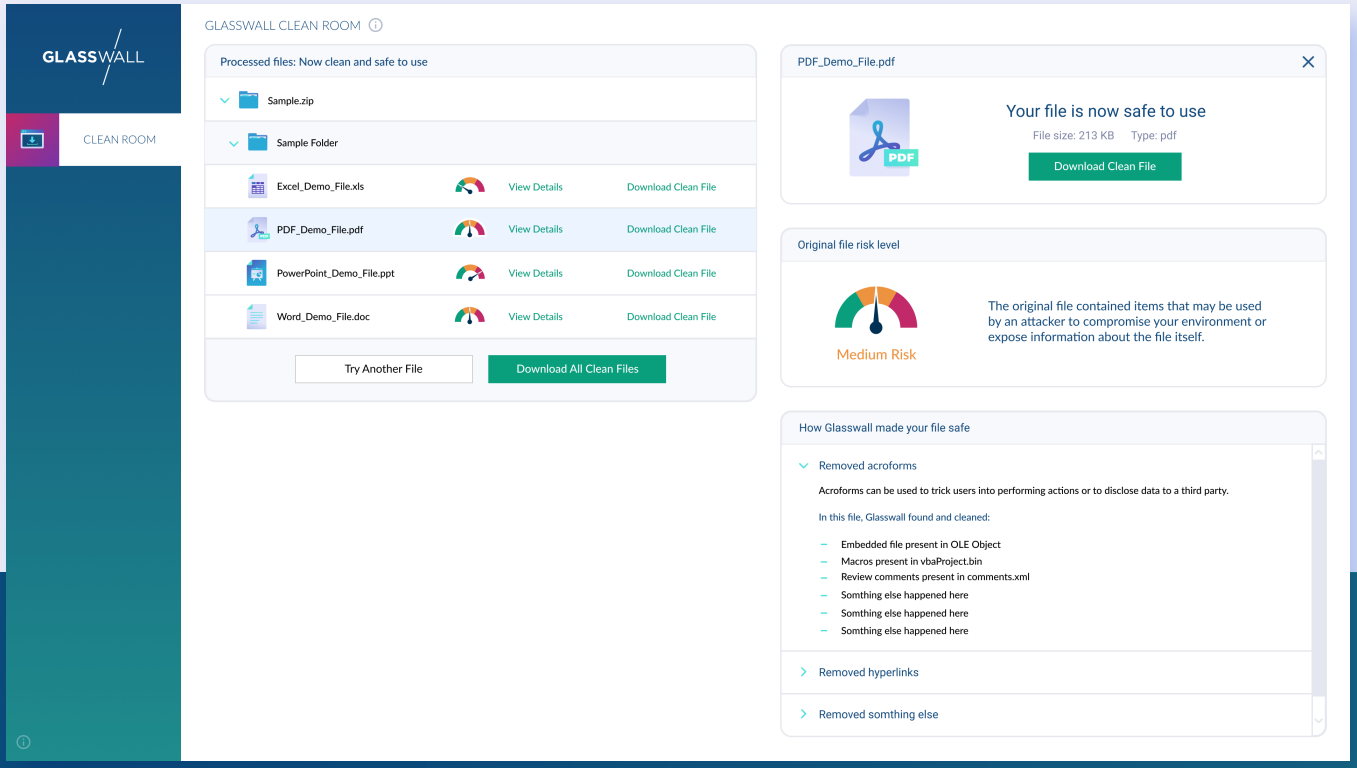
Hyperlinks

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.

Review Comments and 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.

How does Clean Room work?



Clean Room is simple to use. It sits on an individual's browser, and they have complete freedom to drag a file from anywhere on their device into the Glasswall CDR Engine within Clean Room.

Once the file has been processed Clean Room will provide the user with a report on the original documents risk level, and provide them with the new safe, fully functional and visually identical file.

Complete protection against file-based threats really is that simple with Clean Room.

Try Clean Room now

Best-in-class file-based protection from Glasswall

Glasswall has a renowned reputation for Content, Disarm and Reconstruction. Our CDR technology utilizes Kubernetes to provide an infinitely scalable and highly ISG* compliant platform. Our platform is cloud-native, offering easy deployment into your organization, and we offer a range of solutions designed to match different organizational requirements, large or small.

*ISG - Inspection and Sanitization Guidance standards by the National Security Agency (NSA)

How we do it better:

- ✓ Complete file analysis - giving you transparency into file non-conformance with industry specifications
- ✓ Complete file protection - threats removed and files returned to known-good specifications
- ✓ Content management options to shape an organization's security policy based on risk appetite
- ✓ True file type detection going beyond just the file extension or magic number

Try Glasswall CDR in your web browser

Clean Room free trial

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 building 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