GLASSWALL

API-first CDR that secures files in less than a second

Introducing Glasswall REST APIs

Glasswall REST APIs

- Inject industry leading CDR file protection within existing business applications and protection workflows
- Protect and maintain the useability of approximately 70GBs* of data or 38,000* files in a one-hour with each CDR Platform node possessing 8 (virtual) cores
- Utilize dynamic content management policies that can be set for Microsoft Office and PDF files – enabling different protection options for different user audiences
- Support for a managed Kubernetes Service, with Terraform deployment scripts and helm charts, such as AKS, EKS, GKE or OKE for Azure, AWS, Google Cloud and Oracle, or as a standalone machine instance such as an AMI (in AWS)
- Report the true format of a file with our file-detection service, ensuring unwanted file types are not allowed to move into a target environment

Book a demo

Your existing security deployments are leaving you at risk

It is common practice for security teams to deploy detection-based cybersecurity solutions, such as antivirus software and sandboxes, to protect their organization against file-based threats. However, this reliance on detection means no matter how complex a security solution may be, it can still only protect against what it has observed or seen before.

Detection-based solutions fall short

- They fail to protect against zero-day threats, due to quickly outdated antivirus databases that can leave an organization vulnerable for an average of 18 days
- Effective cross application integration is difficult to achieve due to complex architecture
- Detection-based solutions cause disruption due to lengthy file processing and false positives
- They lack the ability to assess and address file structure discrepancies

Glasswall REST APIs: zero-trust file protection at blistering speed

Zero-trust file protection by Glasswall is different. Instead of looking for malicious content, our advanced CDR (Content Disarm and Reconstruction) process treats all files as untrusted, validating, rebuilding and cleaning each one against their manufacturers 'known-good' specification.

The Glasswall REST APIs allow security teams to deliver zero-trust file protection across an organization at blistering speed. REST API endpoints enable security teams to present file analysis and file rebuild requests to the Glasswall CDR Platform – securing files in under a second.

The Glasswall CDR Platforms flexible Kubernetes-based architecture allows standalone machine instances to act together in concert, with a load-balancer configured to allow auto-scaling and self-healing. This is characterized as a disposable Kubernetes cluster configuration.

How Glasswall instantly removes risk

Glasswall CDR uses a patented 4-step process to rebuild files back to their manufacturer's known-good specification.

1. Inspect

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

2. Rebuild

Unknown and invalid file structures are repaired in-line with the file's specification

3. Clean

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

4. Deliver

Semantic checks ensure the file's integrity. The safe and fully functional 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.

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

Try Glasswall CDR

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