GLASSWALL

Glasswall CDR file protection at gigantic scale

Content Disarm and Reconstruction

Glasswall Constellations

- Process large storage containers, and safely transfer files at the gigabyte, terabyte and petabyte scale cross domain at lightning speed
- Ensure only safe, clean and fully functioning files enter and leave networks
- Adopt a recognized best-in-class provider of CDR technology and a designated CDR security filter by the NSA's Raise the Bar initiative for Cross Domain Solutions (CDS)
- Receive detailed file reporting via Constellations REST API
- Seamlessly integrate zero-trust CDR within Azure environments, providing industry leading file protection capabilities for both commercial and government cloud environments at massive scale
- Protect against suspect files with a robust chain of custody process that supports file quarantining and hashing

Book a demo

Your existing security deployments are compromising cross domain file transfers

The migration of large quantities of untrusted data between storage containers and across trust boundaries is a necessity for many organizations. However, ensuring the safety of files at the petabyte scale presents a challenge for security teams.

Detection-based solutions, such as antivirus and sandboxes, can still only protect against what they have seen or observed before. They also take time to process files and can generate false positives/negatives – hampering efficiency when transferring large amounts of data across networks.

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- They fail to protect against zero-day threats, due to quickly outdated antivirus databases that can leave an organization vulnerable for an average of 18 days
- They disrupt data transfers due to lengthy file processing and false positives and negatives
- They lack the ability to assess and address file structure discrepancies
- They are unable to identify the true file format of masquerading files
- They cannot transform complex files types into simple ones prior to cross domain file transfers

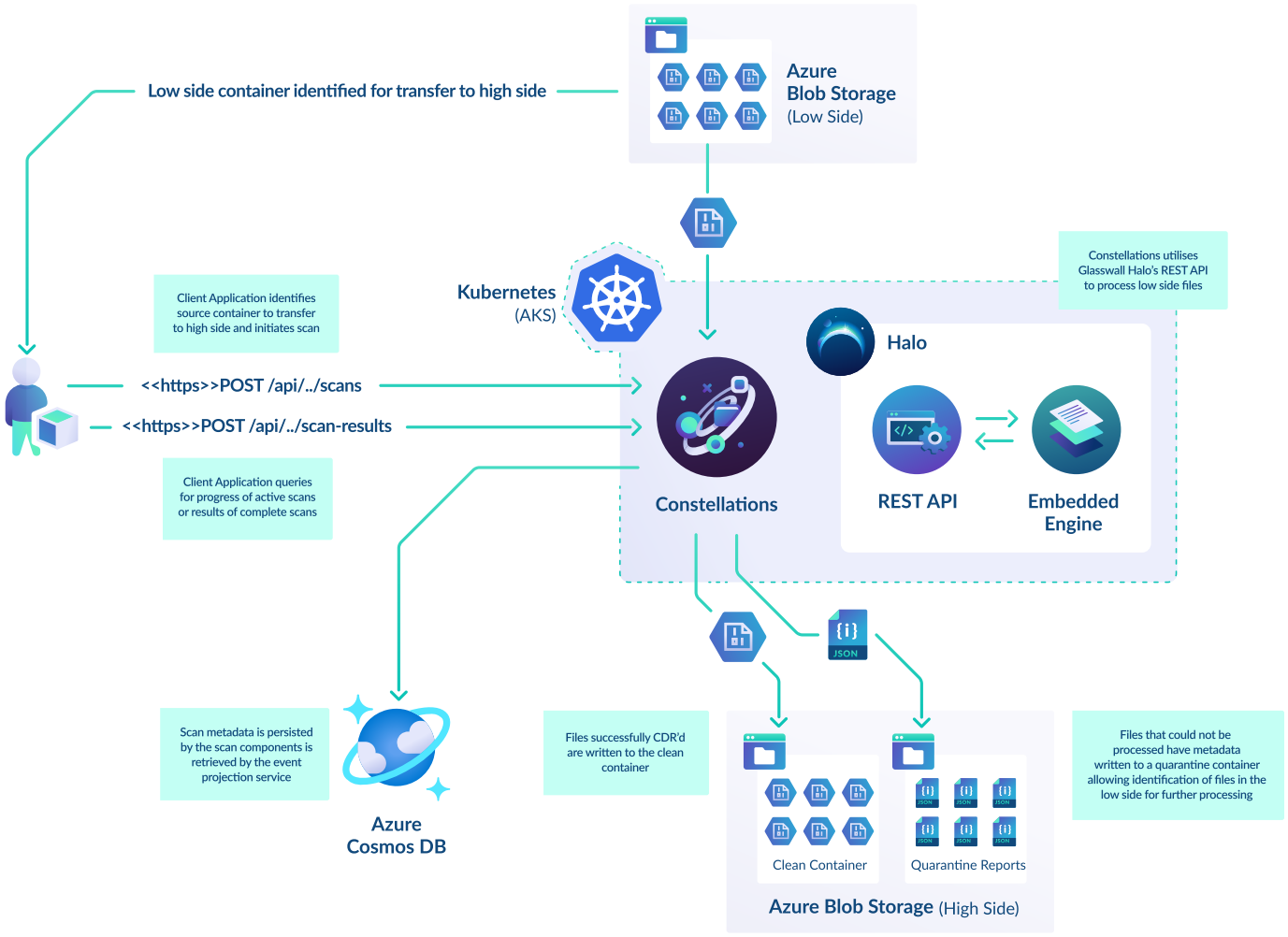
Constellations: a zero-trust file import solution

Constellations utilizes Glasswall Halo to automate the processing and transfer of data across trust boundaries.

It is a zero-trust file protection solution that utilizes our industry leading CDR technology to act as a key component in helping organization's to achieve compliance with the NSA's Raise the Bar standards and other industry guidance.

Instead of looking for malicious content, it's advanced CDR process treats all files as untrusted, validating, rebuilding and cleaning each one against their manufacturers 'known-good' specification.

How does Constellations work?



Glasswall Constellations can be deployed into Microsoft Azure, and facilitates controlled and secure information transfer, making it an ideal choice for organizations that require secure collaboration and data sharing across different security domains.

Book a demo

Technical information

Constellations APIs

Our range of APIs deliver our zero-trust CDR file processing capabilities wherever a file is in motion, or at rest. They ensure our customers files are protected against complex and zero-day file-based threats by our patented four-step CDR process at critical stages within document workflows.

Scan Management API

The Scan Management API enables security teams to start file scans and retrieve the status of active file scans within Glasswall Constellations – our zero-trust file import solution.

View API documentation

Event Projection API

Security teams can utilize the Event Projection API to draw key data from Glasswall Constellations. It provides users with the ability to check the results of file scans that have either completed or that are in process.

View API documentation

NSA Raising the bar on cross domain solutions

The NSA's Raise the Bar (RTB) guidance is an initiative designed to protect vulnerable systems from persistent threats and improve the cybersecurity of all cross domain solutions. It introduced a number of stringent security standards that vendors must adhere to when shipping software into government networks.

Any CDS vendors that desire to sell to the US government must now pass a Lab Based Security Assessment (LBSA) - this is a costly and time consuming process that is designed to ensure only those organizations that match the strict security standards set by RTB are able to ship a CDS into a government environment.

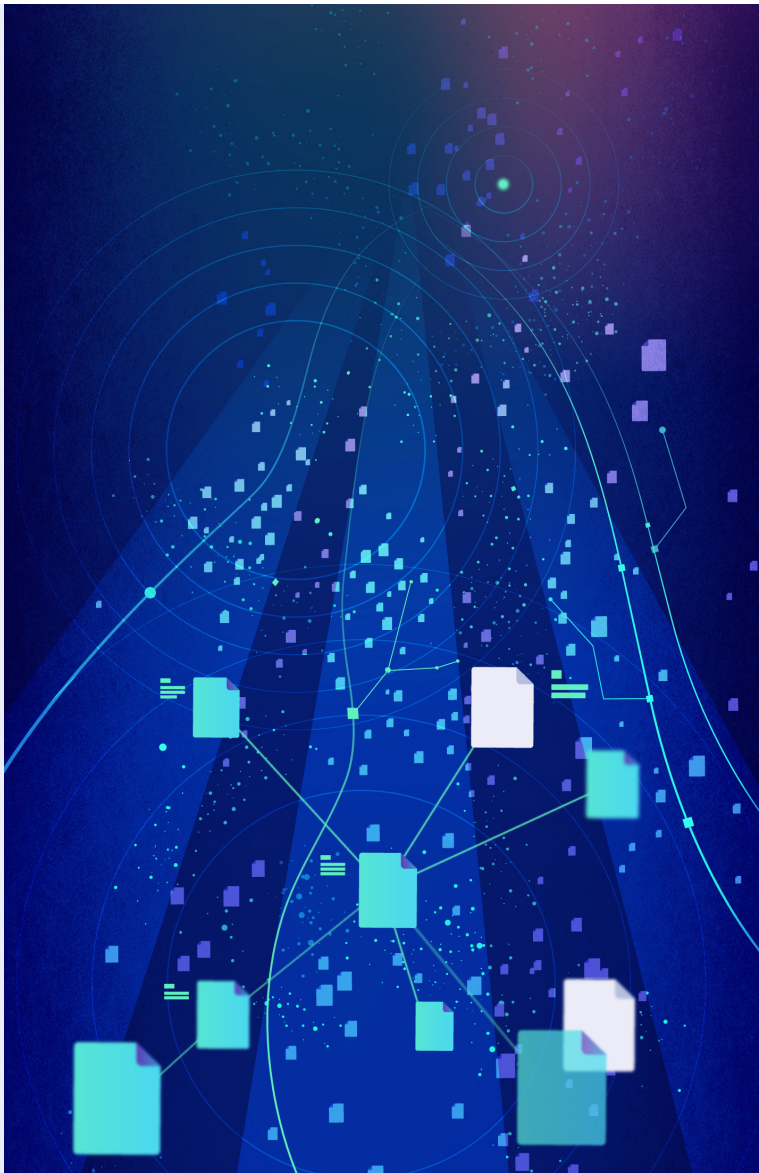
Vendors are expected to meet complex architectural standards, that include the requirement to protect against zero-day and complex file-based threats with multiple zero-trust content filters deployed within a singular CDS.

Glasswall Constellations

Raise the Bar compliant content filter for cross domain solutions

Our Zero-Trust CDR technology has successfully passed LBSA testing is currently deployed as a content filter within Cross Domain Solutions across the US Governments sensitive and highly classified networks.

Book a demo



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

3. 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 Scripts

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 and the names of the file's authors.

Learn more about file-based threats

Best-in-class file-based protection from Glasswall

Glasswall is the market leader for Content Disarm and Reconstruction (CDR). Our CDR technology utilizes Kubernetes architecture to provide an infinitely scalable solution that helps organizations to comply with initiatives such as the NCSC's Pattern for Safely Importing Data, the NSA's Raise the Bar Initiative and the NIST Risk Management framework by the US Department of Commerce.

Our zero-trust CDR solution offers easy deployment into your organization, with a range of solutions designed to match different requirements, large or small.

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

Gigantic throughput at lightning speed

0.33 GBs per second

1.2 TBs per hour

1 PB per month

Three Kubernetes node pools are recommended to achieve this illustration of throughput as part of an auto-scaling setup.

A peak of 1,900 compute cores distributed across the node pools support this gigantic level of throughput.

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-based security

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 now comply with the NCSC's pattern for safely importing data and 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