GLASSWALL

Secure UK government networks & systems

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

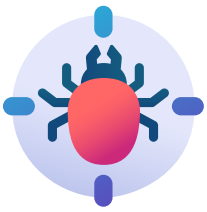
glasswall.com
info@glasswall.com

Secure government networks and systems

with Glasswall zero-trust file protection

The transfer of data across trust boundaries, from open to secure networks, is critical for government agencies. Information delivery must be secure, yet rapid. To achieve this, it is common for departments to deploy Cross Domain Solutions (CDS), which enable the exchange of information between isolated and external networks with a high degree of control.

Legacy Cross Domain Solutions have their weaknesses:



They rely on the detection of malicious content

They are unable to verify complex data types

Active code within documents cannot be removed

The problem with detection

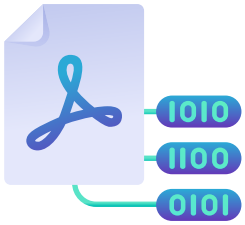
Antivirus and sandbox solutions are often deployed to check data prior to secure transfer. However, these solutions are detection-based and are unable to adequately protect departments against new (zero-day) and existing file-based threats.

This problem is made worse by the air-gapped nature of secure networks, as antivirus solutions require an open channel in order to ingest updates, which may itself represent a security risk.

NCSC pattern for safely importing data

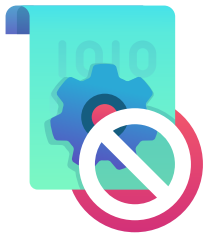
What it is and why it matters

The NCSC pattern for safely importing data are field-developed best practice guidelines, designed to improve the security of cross network data transfers. It provides a strong level of defense against attacks and can be used across a variety of different systems. The aim is to avoid the import of malicious content. The pattern recommends the following:



Transforming complex file formats (documents, etc.) into simple/verifiable ones (SISL/XML)

Syntactic and semantic verification of simple file formats



Prevent the running of active code (such as Macros) on the destination system

Read more about the NCSC pattern here:
https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data

The problem with data wrapping techniques

To adhere to this pattern, departments use data wrapping techniques to make it safer to transfer complex files to a processing location where they are unwrapped behind a gateway/diode. However, once unwrapped, file verification needs to take place and active code still needs to be removed to secure the file before it is transferred to a secure network. With the lack of a better alternative, departments have to accept the risks associated with detection-based solutions.

Supercharge your CDS

with Glasswall zero-trust file protection

Glasswall CDR adds the following functionality to your CDS

- Secure document, image and media file transfer
- Managed binary and CI/CD pipeline transfer
- Transform complex data types to SISL/XML for syntactic verification
- Image conversion to alternative formats such as bitmap
- Data loss prevention via methods such as word search and redaction

Instead of looking for malicious content, Glasswall's zero-trust file protection treats all files as untrusted — validating, rebuilding and cleaning each file to a safe and compliant standard — automatically removing potential threats. This is perfect for air-gapped secure networks, where regular patching and updating is difficult, as there is no dependence on antivirus databases to provide knowledge of a new threat.

Glasswall enables compliance with the NCSC pattern for safely importing data

With Glasswall, only safe, clean and fully verified files cross your trust boundaries, securing your department's critical networks from file-based threats.

There is no longer the need to accept the risk of data wrapping techniques and the shortcomings of traditional AV when importing files to secure networks. Complex file types can be securely transformed into simple/verifiable types, enabling hardware-based syntactic and semantic verification. Glasswall CDR also removes active content from files, so that they are transferred in compliance with the NCSC pattern for safely importing data.

See Appendix A: Integration pattern for Glasswall CDR with diode/flow control for data import

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

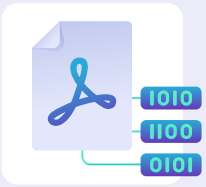
Removes high-risk file structures that contain active content, based on configurable policy

4. Deliver

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

How Glasswall transforms files

Glasswall's CDR Engine can transform complex data formats (documents, images, media, and binary files) into more simple/verifiable ones (SISL/XML) and reconstitute them. This capability exposes a file's internal structure, enabling third parties to carry out hardware/software syntactic and semantic verification.

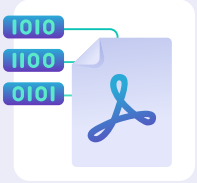


1. Transform

Breaks down the complex data format into its constituent components and converts them into document object models (DOMs) presented as SISL/XML files

2. Verify

The simple format can then be verified and transferred across trust boundaries by hardware devices such as a syntactic verification diode or similar control



3. Reconstitute

The verified simple file format can then be recomposed into the original complex data format

Real world application:

Glasswall secures file imports

HM Government

The challenge

A large UK government agency had terabytes of important data on an isolated network which could have contained malicious content. They required urgent access to this data, but the only option available to secure it was to 'sheep dip' the data – use antivirus and analysis tools to test each file for malware on a separate computer.

Understanding that antivirus detection only offers limited protection and not having the time or resources to analyse every file manually, they required a solution that didn't rely on legacy detection-based methodologies.

The solution

A deployment of Glasswall CDR enabled the cleaning and transfer of files from the untrusted to the secure network.

The outcome

Glasswall was able to move fast, working seamlessly with the government agency. Terabytes of secure data were imported into the new environment within days, and the government agency had complete confidence there was no malicious content present in the data due to our zero-trust file protection capabilities.

Our products

Glasswall Embedded Engine

The core of our product set, the Glasswall Engine aids in the safe transfer of data across networks by providing the following capabilities:

- **Protect:** Rebuilds files to their known-good specification
- **Analysis:** Provides detailed reporting of file content
- **Transform:** Enables third parties to carry out verification of files in simple data formats (SISL/XML)
- **Word search:** Identifies forbidden words and enacts a policy to either redact, report or block files
- **File identification:** Determines the true file type of a file

Glasswall CDR Platform

Built on a flexible and scalable infrastructure, our Glasswall CDR Platform uses Kubernetes-based architecture so you can spin up CDR clusters that provide zero-trust file protection solutions to suit your needs. It is available on-premises, across all clouds or via dockers.

Glasswall Meteor

Glasswall Meteor is a simple to use, highly effective, on-demand CDR application that does not require a connection to the internet to function – making it the ideal solution for isolated environments.

Glasswall Constellations

Addressing the challenge of providing a CDR solution at the terabyte and petabyte scale, requires a highly performant architecture. We have partnered with a large cloud service provider to implement a capability that orchestrates the ingest and cleansing of files, with terabytes of data each day benefiting from CDR technology within top-secret government environments.

Our Integration Partners

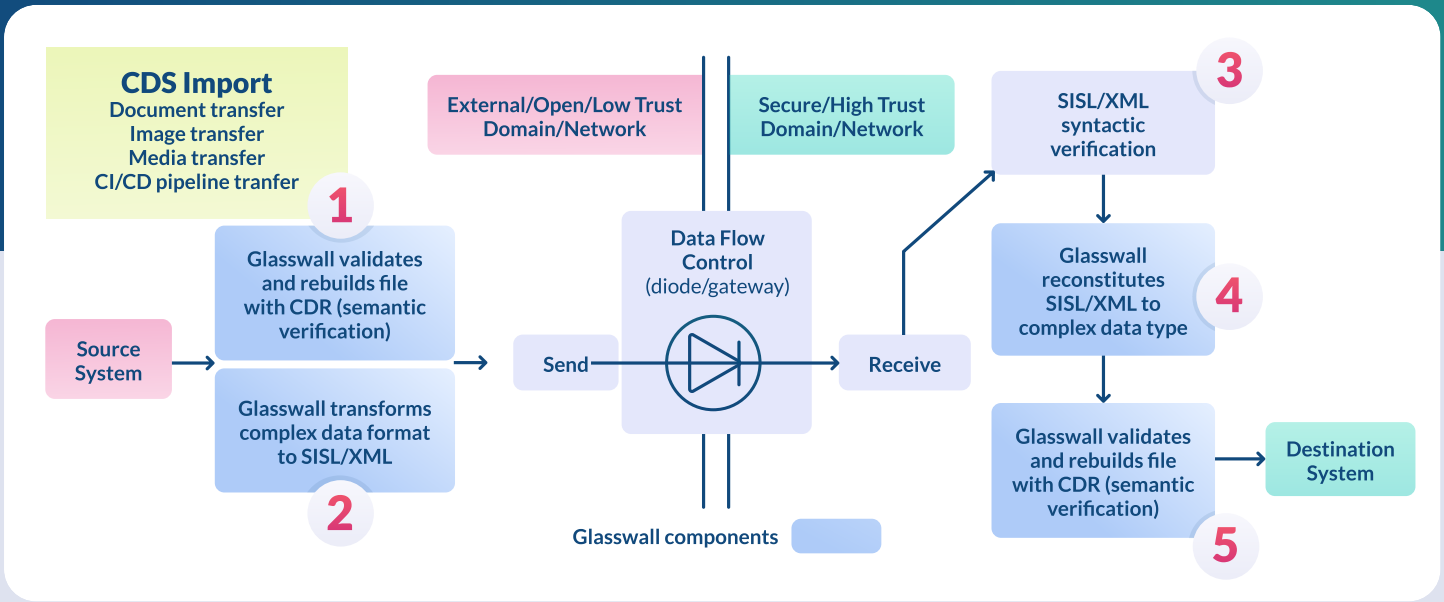
Our partnerships with leading systems integrators enables us to consult and build a solution to protect your specific file-based use case.

CGI PA Bringing Ingenuity to Life BAE SYSTEMS #becrypt 4SECURE HUNNA

Appendix A:

Integration pattern for Glasswall CDR with diode/flow control for data import

This Glasswall-enabled data import process ensures your department complies with the NCSC pattern for safely importing data.



With Glasswall, only safe, clean, and fully verified files cross the trust boundary, securing your department's critical network from file-based threats.

1. Glasswall's Embedded Engine secures the file by performing semantic verification, rebuilding the complex file types to their manufacturer's known-good specification, and removing any active content found.

2. Glasswall Embedded Engine transforms the complex data type (i.e., PDF, DOCX...) into a simple/verifiable one (SISL or XML). The simple data type can then be sent through the gateway.

3. The simple (SISL or XML) data type is, syntactically verified in hardware (i.e., an FPGA) to ensure only correctly formed data types are present.

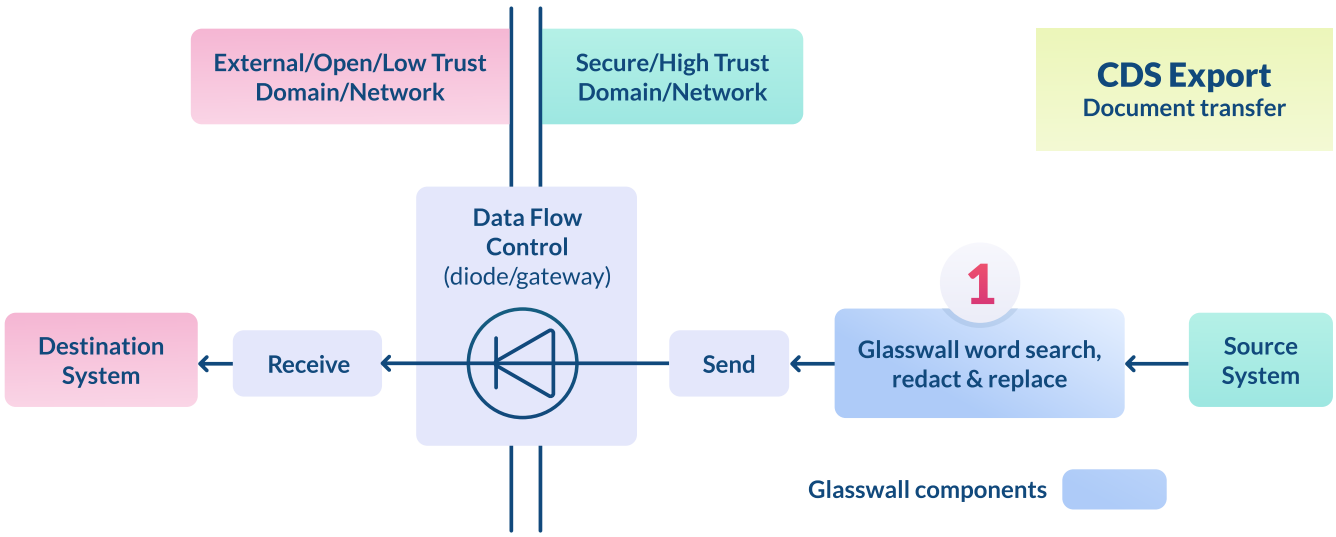
4. Glasswall's Embedded Engine reconstitutes the simple data type back to the original, complex data type.

5. Finally, before delivering the data to the destination system, Glasswall's Embedded Engine secures the file by rebuilding the complex file types to their manufacturer's known-good specification, verifying and removing any active content found.

Appendix B:

Integration pattern for Glasswall CDR with diode/flow control for export

Glasswall's Embedded Engine can be used to mitigate the risk of exporting sensitive information and securely tag documents to create a verifiable audit trail.



1. Word Search and redaction – Can be used to search and redact the text and metadata of a file, or report and block files based on forbidden words. Supports string, character-based matching, and regular expression matching.

GLASSWALL

Talk to us about our industry leading CDR

Book a demo

glasswall.com
info@glasswall.com