GLASSWALL

Trust every file.
Open with confidence.
Share without risk.

d-FIRST™

Technology Brochure

glasswallsolutions.com

About Glasswall

Glasswall is a UK-based file-regeneration and analytics company and a leader in the field of Content Disarm and Reconstruction (CDR).

d-FIRST™

Our patented d-FIRST™ methodology creates safe, clean and visually identical files, mitigating the risk posed by malicious documents.

Rather than trying to detect dangerous content, Glasswall regenerates all files to a safe standard of 'known good', enforcing the format's structural specification and eradicating high-risk active content. Glasswall is a proactive solution. At no point is a signature, an understanding of bad behaviour or detection needed.

Glasswall has clients across business, government, defence and 'Five Eyes' intelligence agencies, and they rely on us to expose and control the risk of sharing files and documents.

GLASSWALL

Trust every file.
Open with confidence.
Share without risk.

Glasswall's Methodology

d-FIRST™

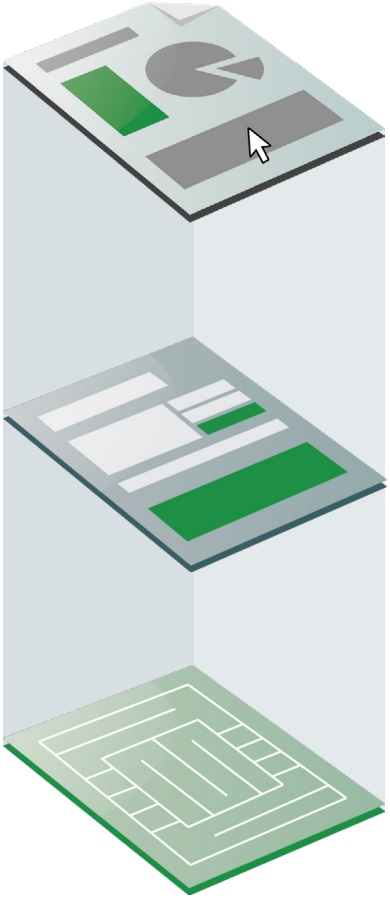
deep-File Inspection

Remediation

Sanitisation Technology

deep-File Inspection

deep-File Inspection takes the attachment and reads it into memory, inspecting the three distinct layers of the file:



The Visual Content layer

The numbers and words on the page. The look and feel of the document.

The Active Content layer

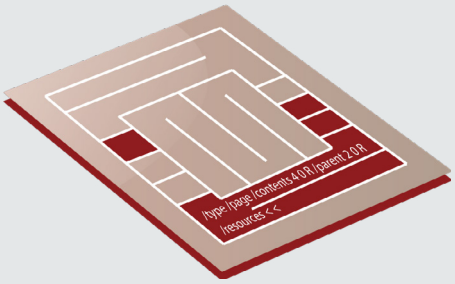
This includes Macros, JavaScript, AcroForms, Hyperlinks, Embedded Files and DDE. They are functional features of files that can perform actions on end user machines. Certain features may be useful to some users, but Active Content is a high risk to all.

The File Structure layer

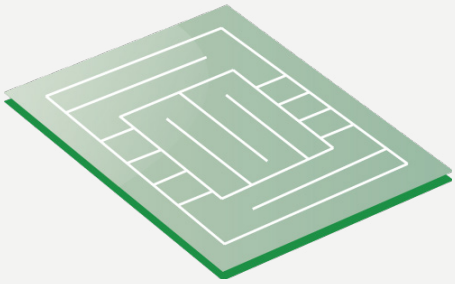
The structures that make up the binary file type container. deep-File Inspection examines structures and how they relate to each other at the binary level, exposing any deviations from the published specification.

Remediation

Remediation ensures a document's structure is compliant with the specification set by the developer of that file type. For example, Adobe has an ISO 32000 specification that details all valid binary structures for PDF. The published specification is what we call, 'known good'.



Non-conforming
File Structure

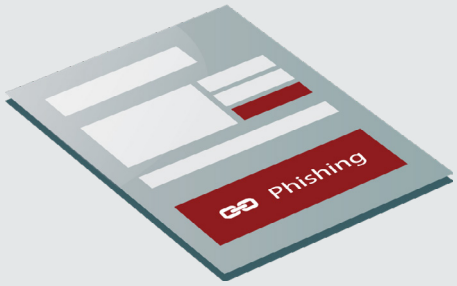


Regenerated
File Structure

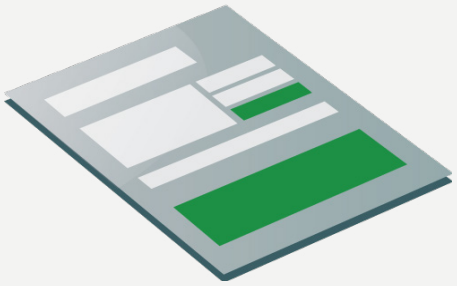
- The remediation process compares the incoming file's structure to the file specification. Any deviations are then marked as non-conforming.
- 93% of the files processed by Glasswall do not conform to the published specification and deviations from standard are often a gateway for sophisticated malware.
- Remediation repairs all deviations, bringing the document back into line with the standard.
- Once all structures have been validated, the file is regenerated. This produces a compliant file in line with the 'known good' specification.
- The result is that any malware hidden or obfuscated in the file structure is either disarmed, destroyed or removed.

Sanitisation

Sanitisation is the removal of Active Content by policy, mitigating the risk of functional features in files. Sanitisation allows users to get the document features they need and strips out all the functions they don't.



Unapproved
Active Content

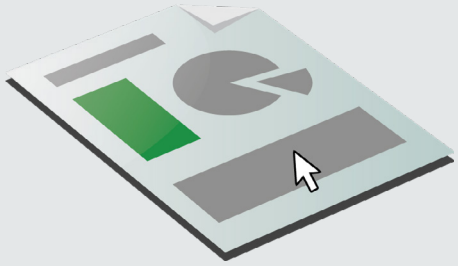


Approved
Active Content

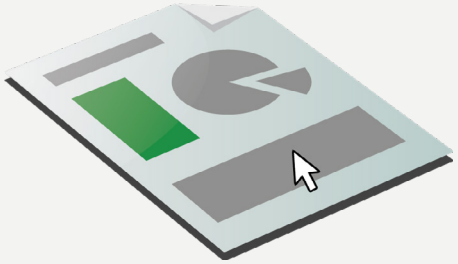
- Sanitisation policy can be set from the group down to the individual user level, offering unparalleled control over your exposure to risk.
- Common policy choices include sanitising out all Dynamic Data Exchange (DDE), Embedded Files, AcroForms and JavaScript for all users, and allowing Macros only for finance teams from select, trusted business partners.
- The depth of visibility provided by Glasswall on file and documents allows organisations to effectively balance risk with business continuity.

Visual Layer

The visual integrity of the document is maintained.



Original
Visual Content



Identical
Visual Content

- Throughout the process, the Visual Content layer is untouched, ensuring that every file regenerated is visually identical to the original.

Put us to the Test

Setting up an evaluation is quick and easy:

Simply BCC email traffic to Glasswall for 30 days.
We process and then black hole the received traffic.

Running BCC email traffic through the service will:

- Expose and capture structural deviations from the manufacturers 'known good' specification in every file.
- Provide visibility and quantify your organisation's exposure to the risk from Active Content in incoming files and documents.
- Report any malware, both known and unknown.
- Offer hands-on experience working with the Rebuild for Email service.

The Deliverable:

On completion of the Proof of Concept, a complete summary report is prepared and presented.

Next Steps:

Schedule a Glasswall Proof of Concept.
Or set-up an onsite workshop to go into the technology in more detail.

UK: +44 (0) 203 814 3890 USA: +1 (866) 823 6652

sales@glasswallsolutions.com us.sales@glasswallsolutions.com

glasswallsolutions.com