GLASSWALL

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

Rebuild for Email

Product Overview

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.

The Threat

66% of advanced malware launches by opening an attachment

(Source: Verizon)

- Files are the lifeblood of every organisation and our reliance on digital documents is growing.
- Bad actors take advantage of this dependence, manipulating complex document specifications and Active Content, opening doors into your network.
- These vulnerabilities ensure that files and documents remain the vehicle of choice for those that seek to steal, damage and destroy your data and reputation.

Every 4.2 seconds a new malware variant is created

(Source: G Data)

- The rapid proliferation of new malware is rendering detection-based techniques increasingly ineffective. These methods of defence cannot protect against threats they don't yet know exist.
- Anti-Virus (AV) requires a Patient Zero with protection deltas of hours, days or even weeks not uncommon.

69% of organisations say threats they face can't be stopped by anti-virus

(Source: Cisco 2018 Cyber Security Report)

- Sandboxes are failing to detect new malware that is increasingly 'sandbox' aware.
- Employees won't protect you. Before they open a file, users often can't tell whether an attachment is dangerous or not. Most click first and ask questions later, if they ask at all.

The Solution

To combat this threat, Gartner and the NCSC recommend techniques such as CDR and Syntactic Verification. Validated and deployed by government agencies in both the UK and US, Glasswall's d-FIRST™ is the leading technology in these fields.

Content Disarm and Reconstruction (CDR)

It breaks down files into their discrete components, strips away anything that doesn't conform to that file type's original specification, ISO standard or company policy, and rebuilds a "clean" version.

This near-real-time process is an effective and efficient approach to removing malware and exploits from files. Although sandboxing and almost all other techniques depend on detection, CDR protects against exploits and weaponised content that have not been seen before.

- Market Guide for Email Security - Gartner Research

Gartner®

Syntactic verification ensures the structure and syntax of the object are correct (e.g., that the content is valid XML or JSON which conforms to a specified schema). Semantic verification ensures that the meaning is valid in the context of the operation or business process being performed. Verification components ensure all potentially active content has been removed.

National Cyber Security Centre
a part of GCHQ

Glasswall's Methodology

d-FIRST™

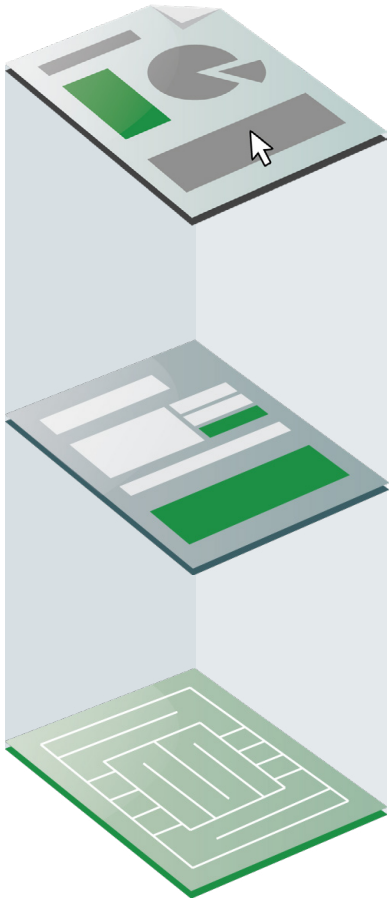
deep-File Inspection

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

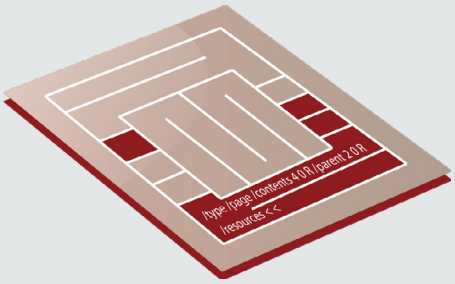
This includes Macros, JavaScript, AcroForms, Hyperlinks, Embedded Files and DDE. They are functional features of files that can perform actions on end user machines. Certain features may be useful to some users, but Active Content is a high risk to all.

The File Structure layer

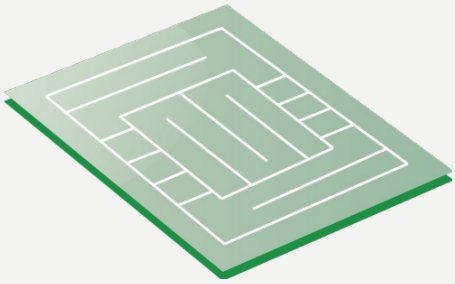
The structures that make up the binary file type container. deep-File Inspection examines structures and how they relate to each other at the binary level, exposing any deviations from the published specification.

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

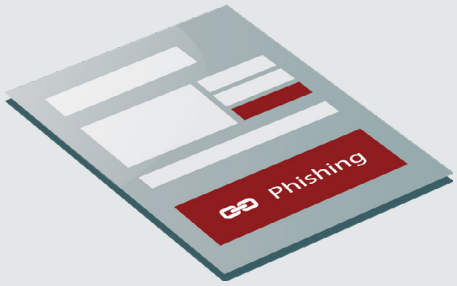


Regenerated
File Structure

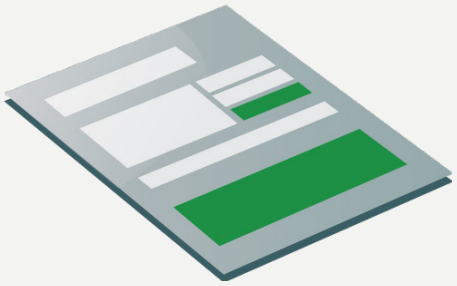
- The remediation process compares the incoming file's structure to the file specification. Any deviations are then marked as non-conforming.
- 93% of the files processed by Glasswall do not conform to the published specification and deviations from standard are often a gateway for sophisticated malware.
- 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

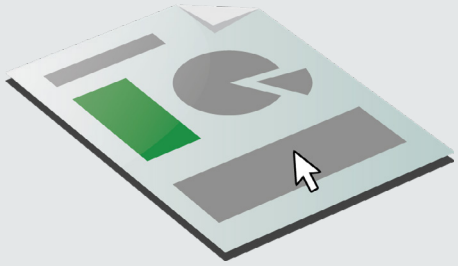


Approved
Active Content

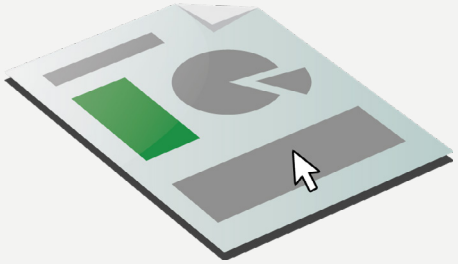
- Sanitisation policy can be set from the group down to the individual user level, offering unparalleled control over your exposure to risk.
- Common policy choices include sanitising out all Dynamic Data Exchange (DDE), Embedded Files, AcroForms and JavaScript for all users, and allowing Macros only 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.

Rebuild for Email FAQs:

What file types do you support?

We support all key business file formats, including Binary Office, XML Office, PDF, PNG, JPEG & GIF files. Unsupported file types can be allowed or disallowed by policy.

How fast do you process files and documents?

Glasswall's processing time is sub-second with most files regenerated in 100-250 milliseconds. This adds negligible latency to the smtp flow.

Who has validated this technology?

Government agencies in the UK and US have put Glasswall through a rigorous testing and validation process. Glasswall's stand-out performance in every test is reflected in the endorsement and deployment of our technology by a number of Five Eyes intelligence agencies.

Where is the service hosted?

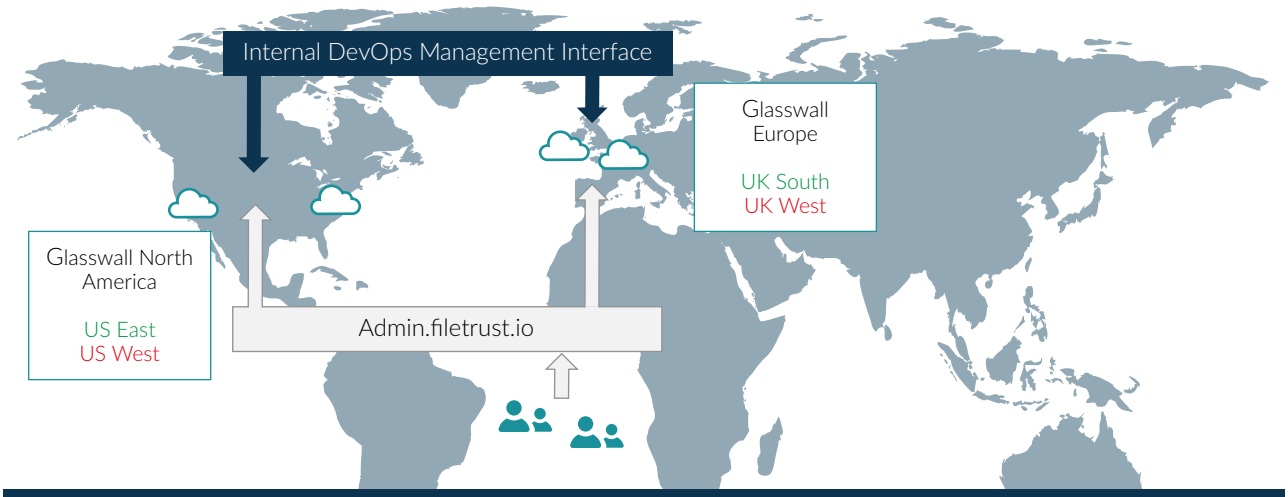
Rebuild for Email is hosted on Microsoft Azure with regional data centres in the UK and US. There is data sovereignty between regions with our client's data remaining in the region where their tenancy resides.

Resilience is a key feature of the platform architecture:

- Auto-scalable micro-services.
- Node scaling.
- Scalable clustering.
- Full data centre hot backup.
- Regional data centre failover

This allows Glasswall to consistently meet our target uptime of 99.99%.

Rebuild for Email Hosted Infrastructure



All data held in regional data centres will not be transmitted to other regions. Internal DevOps scope is global but no customer data is transferred. Admin interface redirects to appropriate local instance where the tenancy resides. Datacentre to datacentre redundancy is restricted by region.

Who controls my data retention?

Our clients have complete control of their data retention on the Glasswall cloud, up to 90 days.

All client data is encrypted and is stored without reference to the attachment or original email.

Only Glasswall Site Reliability Engineers have access to the infrastructure. Access is only enabled for specific maintenance tasks and all actions taken by Glasswall staff are logged.

Which email platforms do you support?

Glasswall supports all of the following platforms:

- O365, Exchange Online
- Microsoft Exchange, On Premise
- G Suite, Gmail
- Any SMTP server

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

Glasswall Partners

Gold Microsoft Partner
Microsoft

FORCEPOINT

BOEING

nteligen

LOCKHEED MARTIN

BAE SYSTEMS

4Secure

Booz | Allen | Hamilton

OWL Cyber Defense

PA

novastone

Awards

BRITISH LEGAL TECHNOLOGY Awards 2019

Winner
New IT Product of the Year

THE GOLDEN BRIDGE AWARDS
SILVER
BEST 2019
BUSINESS WORLD

Silver Winner
Email Security Innovations

SC 2019 awards
finalists
HONORING EXCELLENCE IN INFORMATION SECURITY

Finalist
Best Email Security

BIG INNOVATION 2019

Winner
Best Email Security Solution

ASTORS AMERICAN SECURITY TODAY
2018
PLATINUM AWARD WINNER

Winner
Best IT Email Security Solution

2017 UK IT INDUSTRY AWARDS
computing
WINNER
SECURITY INNOVATION OF THE YEAR

Winner
Security Innovation of the Year

SC MAGAZINE AWARDS 2016 Europe WINNER

Winner
Best Email Security Solution

IET AWARDS The Institution of Engineering and Technology
INNOVATION WINNER 2016

Winner
Innovation

Certifications

CYBER ESSENTIALS PLUS