GLASSWALL

PRIVATE AND CONFIDENTIAL

Company and Technology Overview

glasswallsolutions.com

Contents

Company Overview

Glasswall is a worldwide leader in the field of Content Disarm and Reconstruction (CDR), providing unique protection against file-based cyber threats. Glasswall's CDR Platform technology breaks the security paradigm of detection-based defences, allowing only 'known good' in files and documents.

Glasswall has significant experience delivering its CDR technology to both the private sector and governmental organisations, across a wide variety of use cases. As well as selling its solutions directly, Glasswall has built an ecosystem of technology and channel partnerships, and strategic alliances with a many of the world's leading cybersecurity providers.

Based in the UK with operations in the US, Glasswall's CDR Platform has been tested and validated on numerous occasions in both laboratory and production conditions by industry experts in security and technology, including by organisations working on behalf of US security agencies plus other industry leaders such as Bluecoat Systems, BAE Systems, Detica and Threatsec.

Since inception, Glasswall has successfully protected against all efforts to penetrate the technology even when custom written exploits have been used to test the product. The analytics and policy management output and level of security has always exceeded expectations. To their knowledge, no other CDR technology has undergone such extensive, independent testing.

Glasswall CDR Platform

Reactive v Proactive

Antivirus, sandboxing and other reactive detection technologies offer limited protection against unknown threats and disrupt productivity by blocking 'false positive' files. By proactively regenerating all files to a safe standard of 'known good', Glasswall CDR offers unparalleled protection against all threats, both known and unknown without sacrificing productivity.

Glasswall CDR Methodology

Glasswall's CDR Platform operates through four key processes:

1. **Inspect:** Most files entering organisations do not comply with their file specification - it's 'digital DNA'. Glasswall inspects every incoming file's structure at the byte level and conducts thousands of conformance checks, identifying any deviation from the file's standard structure, as determined by its manufacturer (e.g., 3,500 checks for .pdf, 7,446 for .xlsx and 4,279 .docx). Where there are deviations, our CDR Platform remediates the file, eliminating any possible structural threat.

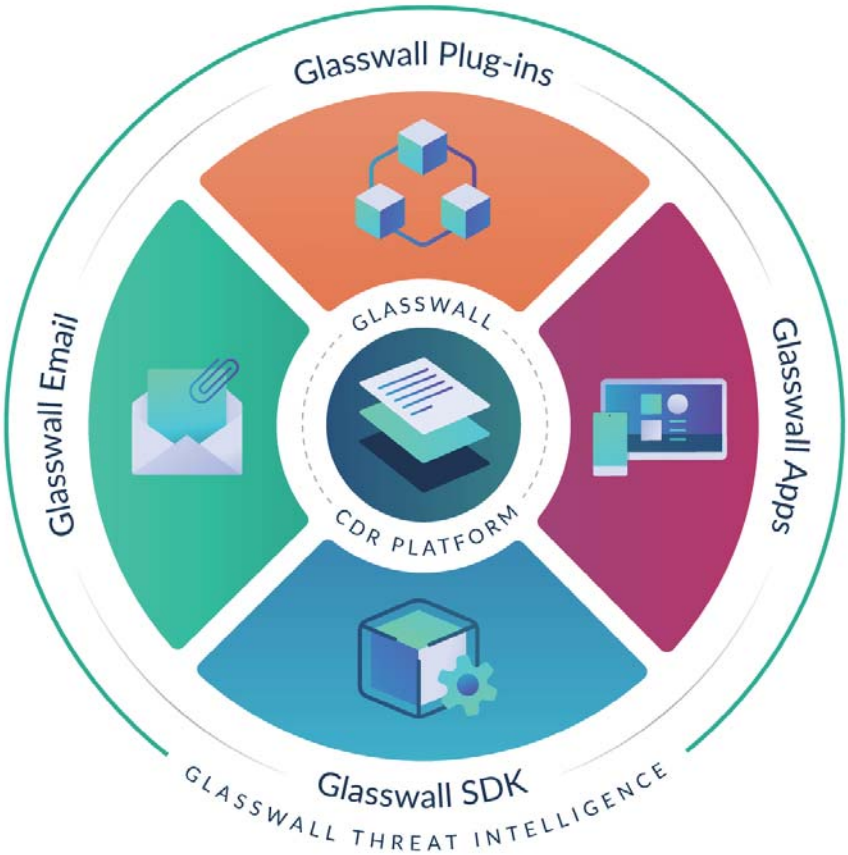
2. **Clean:** Non-structural threats in Active Content (e.g., Macros, JavaScript, embedded files, URLs and metadata) are neutralised by the sanitisation function in the Glasswall CDR Platform. Sanitisation is set and refined through policy management. It allows organisations to take control of every file by allowing the application of granular functional policy management switches designed for particular file types, specific user groups or even individual users.

3. **Rebuild:** After inspection and cleaning, the file is rebuilt to its known good manufacturer's standard, free of risky, unnecessary Active Content, ensuring the file is clean and threat-free.

4. **Deliver:** Upon completion of the process, the user instantly receives a safe, identical file in its original format. The clean file is compliant, standardised and trusted – reducing risk while maintaining operational continuity.

This four-step process is completed in milliseconds, generating a new, structurally compliant and safe file that meets management policy without impacting or changing the content in any way whatsoever.

Glasswall CDR Portfolio



Solutions

Glasswall Email:

Trust only clean and safe email attachments enter and exit your organisation. Flexible and scalable processing of any email volume with full policy control to manage the risk criteria for your organisation.

- Microsoft Office 365
- Microsoft Exchange
- G Suite
- SMTP servers

Glasswall Plug-ins:

Collaborate with safe files with seamless integrations to the Glasswall CDR platform with popular business tools. Provides protection for your web sites and web browser users ensuring your critical business assets - your files - are protected.

- Folder to Folder (Cross Domain)
- Amazon Elastic File System (EFS)
- ICAP

Glasswall Apps:

Ensure files are safe with on-demand processing of files via the web or desktop app. Great for enabling users to run large volumes of files through.

- Web
- Desktop

Glasswall SDK:

Integrate leading CDR technology into your solution or business processes with ease. Trusted by the most security-conscious government, intelligence and commercial enterprises.

- On-premise
- Cloud
- Embedded

- The Glasswall CDR Platform can be integrated into processes in a variety of ways to offer instant file protection. There are two main versions of Glasswall SDK. First, a discrete library that can be embedded into software or a device, which operates without connections to the outside world and is highly performant at processing files in series.
- And second, the Glasswall Cloud SDK which uses a cloud native Kubernetes-based architecture exposing an API to the requesting service–allowing for massively parallel processing scale. The Glasswall Cloud SDK can be deployed within a public, private or hybrid cloud environment and does not require online access to operate.

Key features:

- Cloud native Kubernetes-based architecture provides a Restful API and delivers a highly scalable analysis capability to flex with the demands made by the requesting service.
- Sample API code provided to interact with OpenAPI 3 compliant web service endpoints, including Java, C#, Python, JavaScript, Golang and PHP.
- Support for the most widely used file types, including Word, Excel, Powerpoint, PDF, and media image files.
- Stateless interactions with the Glasswall CDR Platform to ensure that file sanitization requests are returned without delay or requiring complex process handling–all in line with the performance goals of the main application.
- Threat intelligence reporting around file types and volumes; file size; embedded objects and feature counts; and masquerading file counts.

Use Cases:

The Glasswall CDR Platform makes files safe whether in motion or at rest. Use cases include:

- Cross Domain Solutions (CDS)
- Secure email
- Cloud native integrations
- Safe upload / downloads
- Data import / Migration
- Metadata removal
- Safe import of data via portable media

Government Overview

Rated No. 1 by the National Security Agency, Glasswall protects some of the world's most sensitive government and defence networks.

Delivering world class security and ease of integration, we've partnered with the leading providers of Guards and Cross Domain Solutions to ensure that files and documents crossing classification boundaries are safe and ready to use.

Raise the Bar

Raise the Bar is a strategy for improving cross domain solution security and capabilities from a design, development, assessment, implementation, and use perspective. Raise the Bar sets the standard for the security of all cross domain solutions used to protect U.S. Government classified information and all cross domain solutions being sold for export.

Developed by the NSA, the Raise the Bar strategy sets a new strategic direction for the cross domain community, improving the ability to address emerging threats.

Glasswall is one of only two CDR technologies that meet the rigorous standards set out by the Raise the Bar initiative.

Technology Partners:

Forcepoint BOEING BAE SYSTEMS Booz | Allen | Hamilton ECS

Deployments:

NCSC Pattern for Safely Importing Data

The NCSC has identified a set of technical controls which can be used to manage the risks associated with importing data over a network. It is particularly relevant for systems where integrity or confidentiality are paramount, such as those which handle sensitive or personal data, classified information, valuable transactions, or those which operate industrial control systems.

A key requirement of the pattern is syntactic and semantic verification of content. Glasswall is the only CDR technology that performs both syntactic and semantic verification, ensuring that all files processed by Glasswall are structurally compliant with their manufacturers' specification.

Government and Defence Deployments

Partner Deployments

Forcepoint
- Forcepoint Data Guard
- High Speed Guard

Booz Allen Hamilton
- ECDS Cloud Solution

Boeing
- Hardwall CDS

Menlo
- Web and Browser Isolation

Link22 (Sweden)
- Link22 Guard

Lockheed Martin
- LM Cross Domain Solution

PA Consulting
- Oakdoor Gateway
- 10G Diode (Pending)

BAE Systems
- STOP OS integration

ECS Federal
- AWS Diode and Cloud Integration

Hunna (Sweden)
- Hunna USB Sanitiser

Direct Sales

Central Intelligence Agency
- Glasswall Desktop

MoD Defence Cyber School
- Glasswall SDK

Canadian National Defence
- Glasswall SDK

Australia ONI
- Glasswall SDK

Competitive Advantage

As evidenced by laboratory and production testing by some of the world's most security conscious organisations, the Glasswall CDR Platform consistently outperforms all other technologies in its field:

- Glasswall has the best remediation rates in the field of CDR
- The most comprehensive regeneration of files
- The most resilient engine
- World class agility and integration with technical partners.

NSA CDR Test: Glasswall No. 1

The results demonstrate the effectiveness of Glasswall CDR technology against several other vendors

	Total	Glasswall Safe %	Vendor A Safe %	Vendor B Safe %	Vendor C Safe %	Vendor D Safe %	Vendor E Safe %
doc							
	149	100.00	49.66	98.66	51.68	9	100.00
gif							
jpg	1759	99.94	68.62	94.49	0.23	1C	100.00
pdf							
png							
	1	100.00	100.00	100.00	0.00	1C	100.00
ppt							
	10	100.00	90.00	90.00	50.00	ε	100.00
rtf							
xls	3404	99.88	70.92	67.60	16.07	9	99.79
xlsx							
zip							

- This known malware test was carried out by CTC on behalf of the NSA
- The test set covered all variations and traits from the overall NSA malware set
- Glasswall repeats the test at regular intervals to ensure that the technology maintains the same level or greater effectiveness in securing malicious files

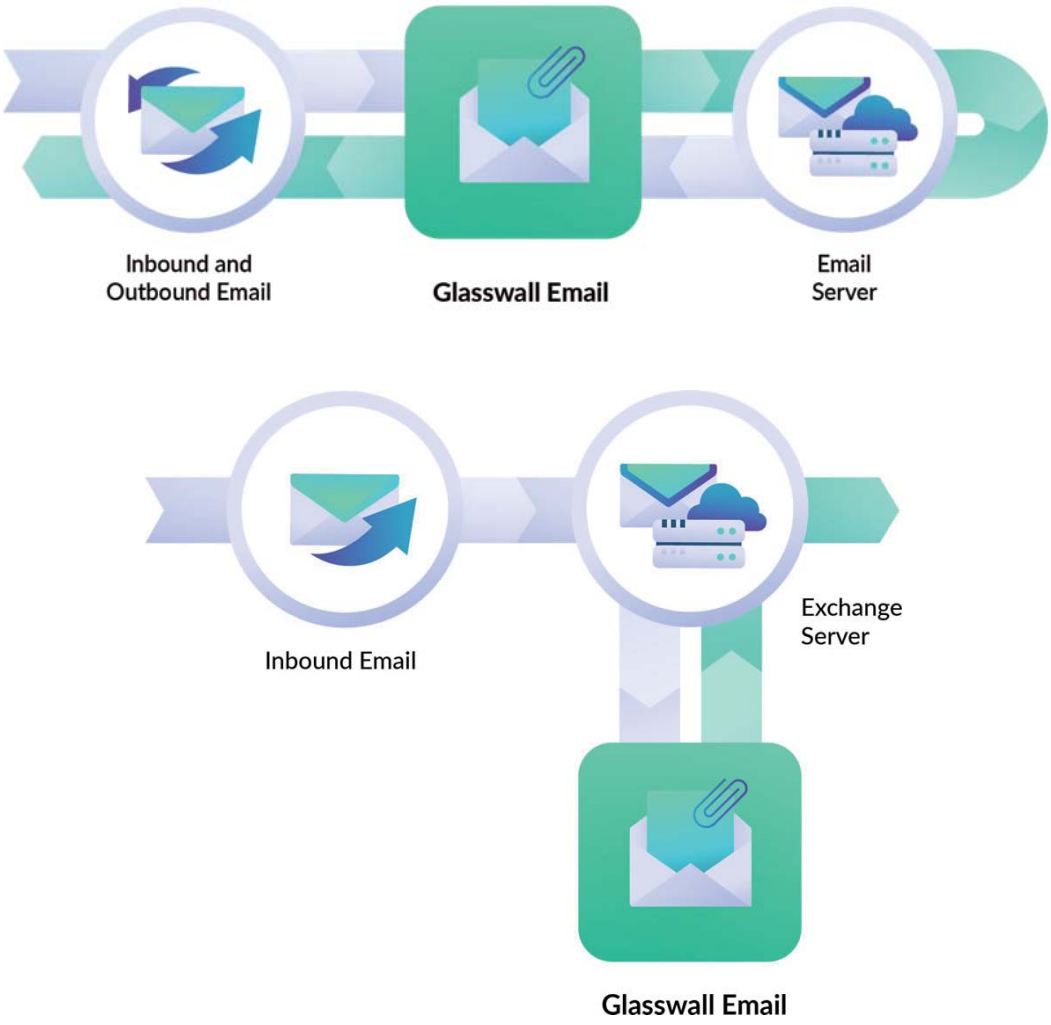
Key Use Cases

Glasswall Email

Glasswall Email sanitises files and documents entering organisations as attachments. While it is a multi-tenant, Azure-hosted service, data can be sited anywhere in the world.

Key features:

- File Type Policy – Allow, inspect or disallow any email attachment based on its MIME type or file type.
- Active Content Policy - Allow, sanitize, or disallow features in PDF, Microsoft Word, Excel, PowerPoint and other supported file types based on the operational needs and risk posture. Policy can be set at the organisational, group of individual level.
- Administrator Console – Manage policy and risk via secure browser.
- File Retention Policy - Retain original copies of attached files for retrospective examination such as e-Discovery, attack analysis or for regulatory/compliance purposes.
- Transaction Log - Find and view reports for all processed emails. Export retained files for further investigation or forward those files to an end user.
- Reporting - Output report data in a CSV format to analyse in any reporting tool.
- Audit - All actions taken by system administrators are audited including all policy changes and files released to end users.
- Optional Weekly Threat Intelligence Reports – Anonymous hashes are sent to Glasswall's Threat Intelligence engine which provides reports on files that were made safe on entry by Glasswall and which were subsequently identified as Zero Day or known malware by the anti-virus industry.



Glasswall ICAP Plug-in

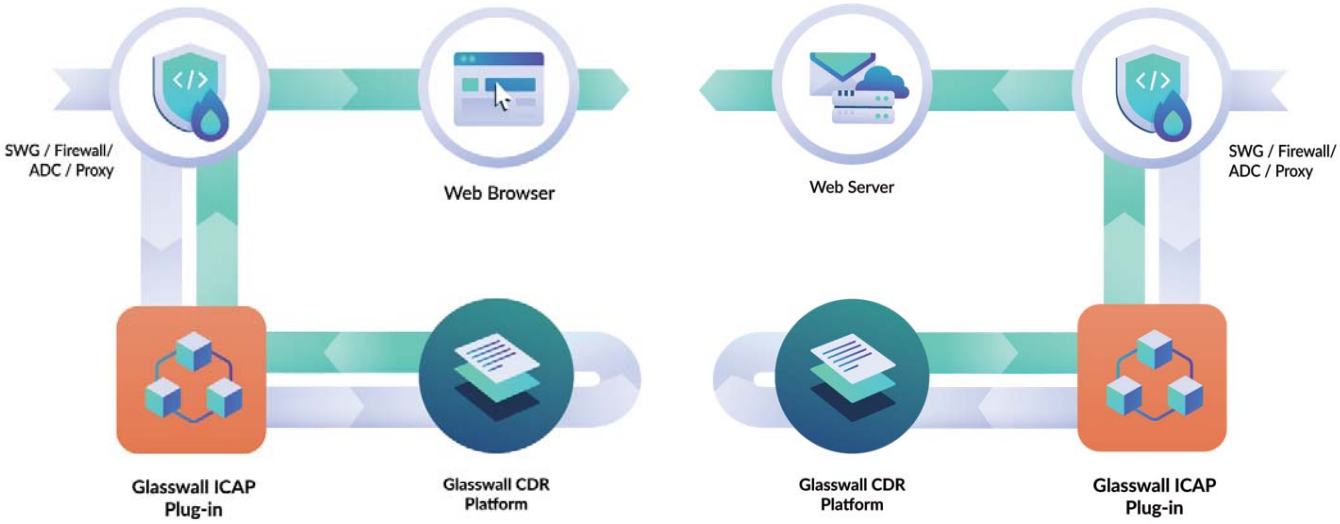
Proxy Servers or Application Delivery Controllers are standard elements within the network to separate trust boundaries. Glasswall CDR can be inserted into the transparent SSL inspection of traffic to disarm and rebuild dangerous files.

Network appliances that support the Internet Content Adaptation Protocol (ICAP) provide an industry standard way to support transparent inspection of traffic by Glasswall CDR. Files are processed by Glasswall CDR Platform with millisecond speed and returned free from threats so they can be safely opened and viewed by the user.

Key features:

- Analysis of files injected from transparent SSL inspection is directed to an open architecture
- Kubernetes deployment to provide burstable speed and scaling as web and user traffic increases

- Ability to disable HTML links in files to protect users from attacks that may appear from legitimate file origins
- Files are rebuilt to a standard format, reducing risk against the most sophisticated attacks
- Secures web traffic, without prescribing how a user achieves their day-to-day business goals



Hunna USB Sanitiser

The Hunna System is portable, air-gapped USB sanitiser. Integrated with the Glasswall SDK, it leverages the industry's leading CDR technology to ensure files and data imported or exported on USB are clean and safe. Built to meet the highest standards of security in the field, the Hunna System delivers military-grade file safety with a simple and intuitive user interface.

Developed and deployed with the Swedish Armed Forces, the Hunna System solves this problem. Integrated with Glasswall's Rebuild SDK, the Hunna System is a portable, air-gapped USB sanitiser that allows users to:

- Import and export of information on USB media, CD/DVD, SD cards without the risk of infecting receiving information systems
- Removes forensic traces of secret information during the import process
- Allows for the safe import and sharing of data in any physical environment

Hunna uses a scan/copy process that moves data from one USB through the system and saves the trusted data on another.

- Files and documents are scanned though up to five AV engines to search for known malware.
- They then undergo complete file regeneration by Glasswall Rebuild, ensuring that all files conform to a standard of 'known good'.

- The safe files are filtered through a whitelist before being copied to a target USB and are signed. The target memory is also signed.

Measurements	The device	Device incl. packaging
Height	104 mm	188 mm
Width	180 mm	502 mm
Depth	328 mm	400 mm
Weight	3,5 kg	7,5 kg

Frequently Asked Questions

Can your solution be used on premise without requiring a live online connection to the vendor and/or its license server?

- Yes. Apart from Glasswall Email which is a cloud-hosted service, all Glasswall solutions can be hosted on premise or on a private cloud.

What are your license models?

- Glasswall offers flexible licence models depending upon the requirements of our customers, including a charge per user per annum, a subscription licence per annum, and capacity-based usage by number of API calls to the Glasswall engine
- Glasswall Email has tiered pricing on a per user basis.
- Access to the Glasswall CDR Platform for all other solutions is on a subscription basis per hub deployment.
- A hub deployment represents the processing of data files in a particular network segment. Separate hub deployments allow for isolation of data processing in an organisation.

Does the license model allow for an unlimited-use license, which includes an unlimited number of files or number of users without “floating licenses” that require online connection?

- Yes. Unlimited use is allowed. Glasswall does not current price on a volume basis for on premise, air-gapped deployments.

What file types can your solution handle (e.g., Microsoft Office files, PDF, JPEG, PNG, MP4, and XML)?

- The table below lists the file formats fully supported by the Glasswall CDR Platform. 'Fully supported' means that the files are subject to inspection at a very low level.

File Extension	Sub Type(s)	Document Type
.pdf		PDF documents
.jpg		JPEG image files
.gif		GIF image files
.png		PNG image files
.emf		EMF image files
.wmf		WMF image files
.tif	.tiff, GeoTIFF	TIFF image files
.bmp		BMP image files

.doc	.dot	Word Binary File Format files
.xls	.xlt	Excel Binary File Format files
.ppt	.pot	PowerPoint Binary File Format files
.docx	.docm, .dotx, .dotm	Office Open XML Document files
.xlsx	.xlsm, .xltx, .xltm	Office Open XML Workbook files
.pptx	.pptm, .ppsx, .ppam, .potm, .ppsm	Office Open XML Presentation files

The table below lists the file formats partially supported by Glasswall CDR Platform. 'Partially supported' means that the files are subject to inspection at a high level.

File Extension	Document Type
.mp3	MPEG-1 Audio Layer III (MPEG-2 Audio Layer III) audio files
.mp4	Compressed audio and video digital data files
.mpg	MPEG-1 and MPEG-2 audio and video compression files
.wav	Waveform Audio File Format (Wave) files

Unsupported file types are controlled by policy, but it is planned that in H1 2022, Glasswall will provide the tools and framework for clients to build support themselves for non-standard file types.

Supported File Sizes:
Glasswall Rebuild provides 64-bit version of a Dynamic-link Libraries (.DLL) for Windows and/or Shared Objects (.so) for Linux operating systems that can analyse and protect files up to the size of 2 GiB (230 bytes) provided that other internal limits (such as recursion depth) are satisfied.

Is it possible to test your solution on premise during a Proof-of-Concept?

- Yes. We welcome any opportunity for our clients and partners to evaluate our products and services.

Did you perform any external security tests of your solution?

- Yes. The Glasswall CDR Platform has been subjected to numerous laboratory and production test, including by the National Security Agency (NSA) and the National Cyber Security Centre (NCSC)
- In every case, the results have met and often exceeded all test criteria.

Is it possible to conduct black box (function) and white box (source code) testing of your solutions?

- Yes. Glasswall would welcome black box testing of any of our solutions. Results of white box testing by Third Parties is available upon request.

Are there any other technologies used to detect malware besides signature-based antivirus scanners?

- While Glasswall integrates seamlessly with other technologies, we do not currently package our products with anti-virus or other signature-based technologies.